Advances in

Communications, Computing, Networks and Security

Volume 8

Editors

Paul S Dowland

Steven M Furnell

Advances in Communications, Computing, Networks and Security Volume 8

Proceedings of the MSc/MRes Programmes from the School of Computing and Mathematics

2009 - 2010

Editors

Dr Paul S Dowland
Prof. Steven M Furnell

School of Computing and Mathematics
Plymouth University

ISBN: 978-1-84102-293-2

Printed in the United Kingdom

Preface

This book is the eighth in a series presenting research papers arising from MSc/MRes research projects undertaken by students of the School of Computing and Mathematics at Plymouth University. These one year masters courses include a significant period of full-time project activity, and students are assessed on the basis of an MSc or MRes thesis, plus an accompanying research paper.

The publications in this volume are based upon research projects that were undertaken during the 2009/10 academic year. A total of 30 papers are presented, covering many aspects of modern networking and communication technology, including security, mobility, coding schemes and quality measurement. The expanded topic coverage compared to earlier volumes in this series reflects the broadening of our range of MSc programmes. Specifically contributing programmes are: Communication Engineering and Signal Processing, Computer and Information Security, Computer Science, Network Systems Engineering, Robotics, and Web Applications Development

The authorship of the papers is credited to the MSc/MRes student in each case (appearing as the first named author), with other authors being the academic supervisors that had significant input into the projects. Indeed, the projects were conducted in collaboration with supervisors from the internationally recognised research groups within the School, and the underlying research projects are typically related to wider research initiatives with which these groups are involved. Readers interested in further details of the related research areas are therefore encouraged to make contact with the academic supervisors, using the contact details provided elsewhere in this publication.

Each of the papers presented here is also supported by a full MSc or MRes thesis, which contains more comprehensive details of the work undertaken and the results obtained. Copies of these documents are also in the public domain, and can generally be obtained upon request via inter-library loan.

We believe that these papers have value to the academic community, and we therefore hope that their publication in this volume will be of interest to you.

Prof. Steven Furnell and Dr Paul Dowland

School of Computing and Mathematics
Plymouth University, May 2011

About the School of Computing and Mathematics

The School of Computing and Mathematics has interests spanning the interface between computing and electronics, through software, networks, and communications. The School contains 61 academic staff and has over 1000 students enrolled on its portfolio of taught courses, over 100 of which are at MSc level. In addition there is a similar number of postgraduate research students enrolled on a variety of research programmes, most of which enjoy sponsorship from external sources.

This School sits alongside four other Schools in the Faculty of Science and Technology, the School of Biomedical and Biological Sciences, the School of Goegraphy, Earth and Environmental Sciences, the School of Marine Science and Engineering and the School of Psychology. There are research and teaching links across all five schools as well as with the rest of the University.

Prof. Steven Furnell
Head of School

Contributing Research Groups

Centre for Robotics and Intelligent Systems

Head: Dr G Bugmann
Email: guido.bugmann@plymouth.ac.uk
Research interests:

1) Cognitive systems
2) Social interaction and concept formation through human-robot interaction
3) Artificial intelligence techniques and human-robot interfaces
4) Cooperative mobile robots
5) Visual perception of natural objects
6) Humanoid robots

http://www.tech.plymouth.ac.uk/socce/ris/

Centre for Security, Communications and Network Research

Head: Professor S M Furnell
E-mail info@cscan.org
Research interests:

1) Information systems security
2) Internet and Web technologies and applications
3) Mobile applications and services
4) Network management

http://www.cscan.org

Contents

SECTION 1 Communications Engineering and Signal Processing

SECTION 2 Computer and Information Security

SECTION 3 Computer Science & Web Applications Development

SECTION 4 Network Systems Engineering

SECTION 5 Robotics

Section 1

Communications Engineering and Signal Processing

Automatic Plankton Detection using SURF

K.P.Krishnan and T.Belpaeme

School of Computing and Mathematics, Plymouth University, Plymouth, UK
e-mail: tony.belpaeme@plymouth.ac.uk

Abstract

The oceans serve as major sources and sinks of bio-active elements. Monitoring plankton population in seas and oceans helps to monitor the health of the planet. So an accurate measurement of their types and the distribution is very important. This plankton monitoring is still done through manual labour, and human identification is slow and often inaccurate. In this paper, we present a technique for automatic detection of plankton using SURF and WEKA. The images used are classified and labelled by the marine experts from Plymouth University. We try to differentiate 12 classes of taxon by training a classifier in WEKA. Even though the experiments are done with low number of images that are low quality we expect that upon its completion, our method will open new ways in automatic detection of plankton.

Keywords

Zooplankton, Automatic Identification, Imaging, Taxonomy, Categorisation, Marine ecology, Machine Vision

1 Introduction

The oceans serve as major sources and sinks of bio-active elements. The oceans contain both living- plankton and the non living –detrital particles. In this paper we concentrate on zooplanktons. These living particles play an important role in the global ecosystem (Matthew et al., 2005) as they are at the bottom of the food chain of most species living in the world’s oceans and seas. One of the pressing problems in marine biology is the automatic recognition of plankton. Monitoring plankton in seas and oceans informs us about the health of our planet. This plankton monitoring is still done using manual labour with highly skilled marine experts identifying and counting plankton in samples collected from different seas.

The process of detection and sampling has started long back; the traditional method done was by taxonomists through microscopic analysis. This has many difficulties of its own. It is very tedious and labour intensive. It will involve sampling, counting and sorting of large numbers of samples. After this the actual identification will take place. These are time consuming procedures and there will be no real time data due to the lag between sample collection and data analysis. The error produced by humans during this process can be large as the process involves huge data samples and long hours of continuous work which can lead to fatigue. Also the number of trained taxonomists is declining (Oliver et al., 2009). Hence the need for automatic recognition is important.

In this paper we explain the new method of plankton identification using SURF (Herbert et al., 2008) and WEKA (Hall et al., 2009). This paper explains identifying and applying the best algorithm available to classify plankton species. Identification will be done using feature matching technique SURF (Speeded Up Robust Features). We test SURF and SIFT (Lowe, 1999) for its performance on plankton identification and found that SURF is better and efficient. Testing of these algorithms will be done using sample images received from the marine department, Plymouth University. The extracted details of each image is fed to a classifier and trained to create a model that can classify unseen images. These classifiers will be based on various decision making algorithms and will be tested using the tool, WEKA. The performance of this method is recorded at the end of this paper. The output of this project will help the implementation of such systems in real world situations and open new methods of unsupervised learning of new species. It was found that this method would work and the suggestions and possible future work are explained in this project. The outcome of this project with limited number of images is not as expected, but this project explores a new way into the automatic detection of plankton.

The paper is organised as follows. Section 2 describes related work, on which our results are bench marked. Section 3 describes the approach of our method and the various schemes used. In section 4, the new method is presented. Finally, section 5 shows the experimental results and section 6 concludes the paper with possible future work.

2 Related Work

Classification of plankton is a very challenging machine vision problem. Some of the challenges facing those attempting to develop automated plankton classification systems are illustrated (Figure 1). According to (Benfield, 2006-07), the challenges vary depending on location, time, and the nature of the survey. There are many problems associated with the automatic recognition of plankton. The medium in which plankton appears contains a variety of nonliving bodies such as marine snow, sediment particles, bubbles etc. which makes the process even more complex. Plankton sizes vary several orders of magnitude. Plankton such as siphonophores and other gelatinous taxa are large. So only a small portion of the total organism can be seen in a single image, which creates recognition problems. Plankton undergoes drastic changes in morphology in their ontogenetic development, in which its shape and size changes with time. Some taxonomic features may not be visible in all images due to lack of resolution or orientation of the species. Planktonic objects imaged are in different orientation in three dimensions relative to the imaging sensor. Thus images of the same individual may have different features depending upon its orientation relative to the camera. Another problem is that images may contain more than one species collocated in space, which makes it more difficult in recognition.

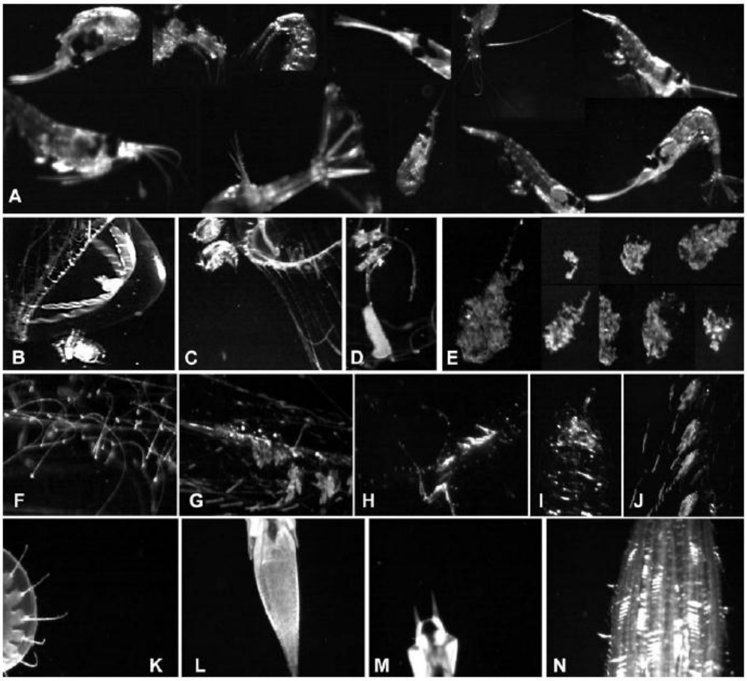


Figure 1: Images of Plankton Source: (Benfield, 2006-07)

The existing method used in the recognition of plankton is low-level feature extraction. These features are in turn fed into a classifier. This method is a bottom-up approach. The steps followed are segmentation, feature extraction and classification. The initial steps are common in most of the methods. The major difference between various methods is in the classification. Classification is done by grouping the individual species based on the low-level features that are extracted. The classification model is based on the quantitative information gathered from features in samples and based on the training set of the previously labelled individual items. In the work of (Matthew et al., 2005) the features are based on the various measurements taken from the images. These features are grouped into five types: simple shape, moments, contour representations, differential and texture features. All these feature extraction methods have their own parameters in expressing the selected features. They are all based on different features of the image. All the features are extracted manually, which is a very difficult task.

Once the feature extraction is over, next task is classification. There are different types of classifiers which are based on different algorithms. In the work of (Matthew et al., 2005) the classification algorithms used are decision tress (DTs), Ridge regression (RRs), k-Nearest Neighbour (KNN), Support Vector Machine (SVMs) and Random Forest. These algorithms implement different classifiers with different desirable properties. All these algorithms have their own property, which help us build the classifier in different methodologies, and out of these each help to get better classification results in a more desirable way.

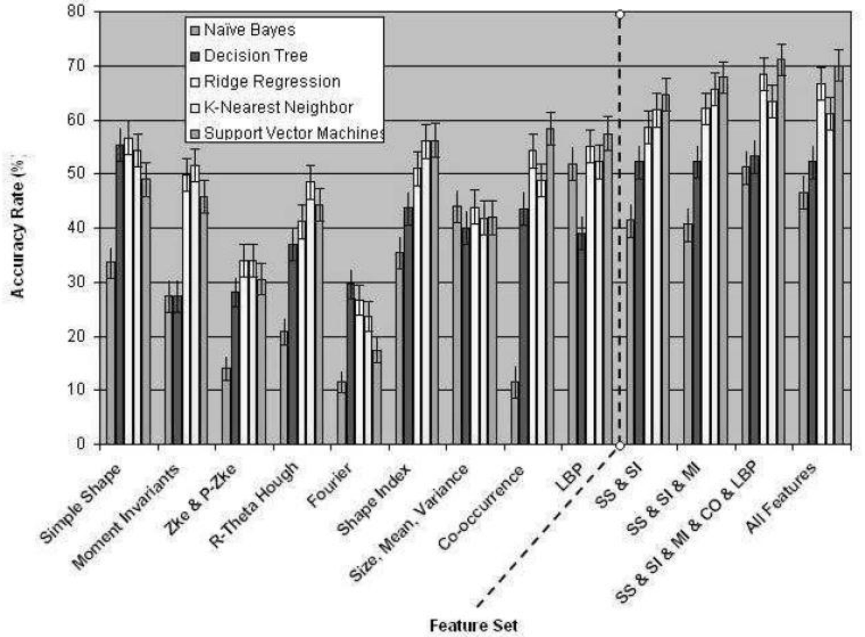


Figure 2: Classification results of various classifier algorithms. Source: (Matthew et al., 2005)

The results as per (Matthew et al., 2005) are based upon the experiments performed using the WEKA toolkit. The data set used consists of 982 images from 13 classes. The results obtained are shown in figure 2. The results out of the experiment show good accuracy in classifying the species. The various coloured bars in the figure are the results of different types of classifiers, the results marked after the dotted line are results obtained when using more than one classifier. It is clear that more than one classifier give better results than using individual algorithms. The low-level feature extraction method gets an overall of 70% accuracy in classification. These results are used to benchmark the results we obtain in this paper. It is the purpose of this project to explore new ways in the automatic detection of plankton using the qualitative information in the image of each species.

3 Approach

The paper explains the method of unsupervised learning and classification of plankton species. There are mainly two steps in this method, the first is extraction of features and the second is training of the classifier. We use SURF for feature extraction, SURF can be divided into three main steps. First selecting interest points in the image such as corners, blobs and T-junctions. Next, representing the neighbourhood of the interest points on a feature descriptor vector and the final step is it has to match the descriptor vectors in two different images.

Once the feature extraction and matching is done the percentage of matching for every image in the database is tabulated and fed into WEKA. WEKA has built in classifiers that help to train classifiers that can identify unseen images. There are different types of classifier algorithms inside WEKA itself. In this paper we use algorithms that were used earlier in (Matthew et al., 2005) work and we add some more algorithms that we believe can give better results.

The images that are used in this experiment are considerably less to train a classifier that can detect plankton as the images of a single species can have various sizes and shapes depending on the angle from which it is taken and the position of the species. In this experiment we had used initially 2 sets of species of less clarity and high noise to test SURF's ability to match images. Later we use 12 classes of groups that are of better quality than the previous. Each set do not contain equal number of images and this has affected the results obtained. There are a total of 4056 images in total used to train the classifier. There was no pre-processing of images done at any stage of this experiment, which if done could have improved the results and this is left to future work.

4 Experimental Setup

In order to collect data to train the classifier we used SURF to run on each image against the whole images in that class to see how well it was matching and a different test was done to see if they differentiate other species by testing each image with the rest of the images from each class. Each class did not contain same number of images. The results were computed taking the percentage of matching interest points from the average of the interest points of the two images that were in consideration. The matching/differentiating is considered based on – matching points divided by average of Image 1 and Image 2 interest points taken in percentage.

This was done for each image in each set and later compared for images in different sets also. Once this was done these values were threshold from values 1 to 50. The threshold value was set for each pair of the image. That is for example, if a value of matching in percentage was 10 then it would be assigned a YES if the threshold was 5 as it is more than the threshold (10>5) and a NO if the value was below the threshold value (x<5). Having done this for every pair of image and a YES/NO table was created for each pair, the average of it was taken in the case of every single taxon to show its overall percentage of matching for thresholds between 1 to 50. That is for example, if a set consists of 15 images and out of it 10 matches then the percentage of match for that particular group with the other is 10 out of 15 and is expressed in percentages. The information produced from all these images were stored in CSV format so as to feed into WEKA. The plot of the information for each category will look like Figure 3.

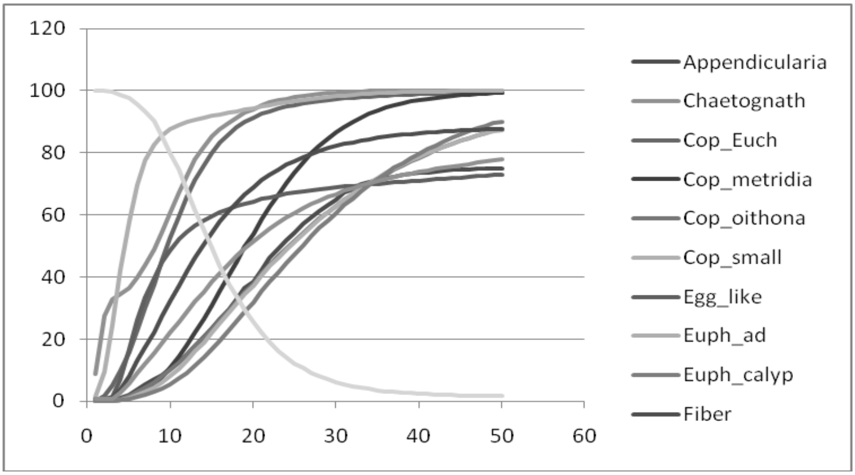


Figure 3: Example of the output for each taxon

The results from SURF have a pattern and to understand this we use WEKA and the classifier in it. The patterns are very small and cannot be easily differentiated by humans and hence we employ WEKA the data mining tool.

WEKA has functions that help to predict performance of a classifier. In this paper we have chosen algorithms that have better classification results. All algorithms considered in this project are selected by trial and error method so as to give better results. We train the classifier based on the 5 classification algorithms namely:

1. LMT (Logistic Model Tree)
2. Random Forest
3. Random Tree
4. SMO (Sequential Minimum Optimisation)
5. Multi Schemes – SMO and K-nearest neighbour

The results obtained were in the form of a confusion matrix. We test the classifier with two sets of images, each set having one image of every group. The data for every unseen species to be fed into the classifier was compiled as in the same way as the data for training was created. Now every image has 14 attributes including the class type and each image was threshold from 1 to 50. These values that are threshold were considered by WEKA as 50 instances for each class. This was fed into the trained classifier using WEKA.

5 Experimental Results

The results were obtained in the form of confusion matrix. For each species the confusion matrix was output. We have compiled all these values and have shown it in the form of a graph in Figure 4 and Figure 5.

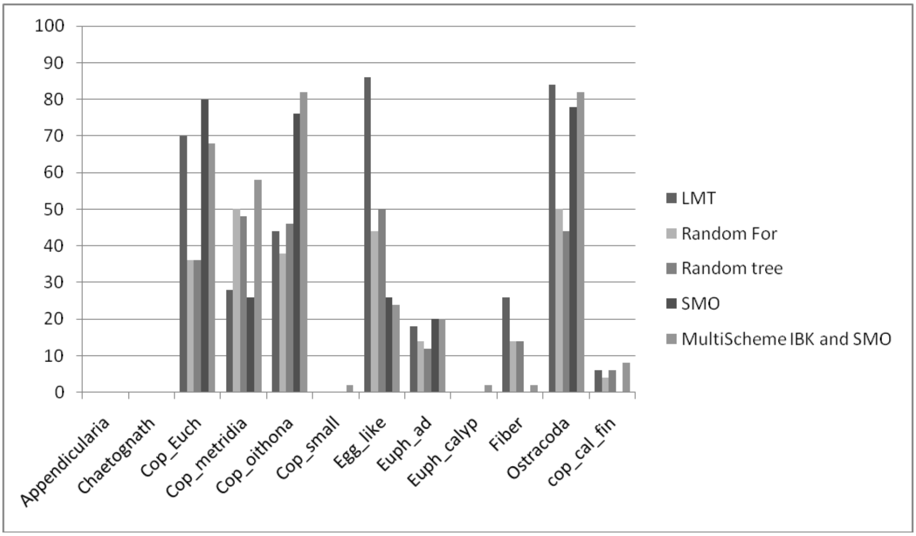


Figure 4: Results for Test Image Set 1

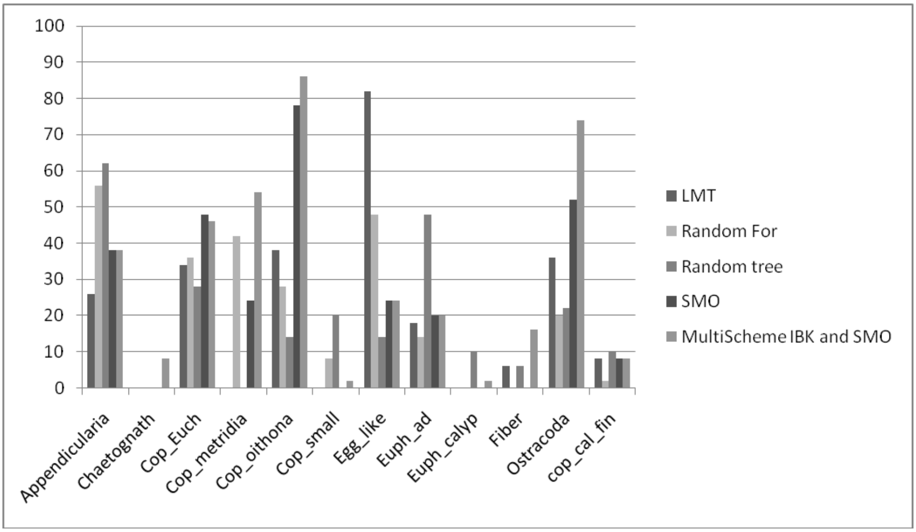


Figure 5: Results for Test Image Set 2

The main noticeable change in the output of the classifier is the difference of performance between set 1 and set 2. The main reason for this is that plankton's do not have a definite shape or size. They are so deformable and can spin when the image is taken, which makes it very difficult to recognize.

Classes Appendicularia, Chaetognath, Cop_small, Euph_ad, Euph_calyp, Fiber and cop_cal_fin are not having satisfactory results. In the case of Appendicularia and Chaetognath, Euph_calyp the results are zero in most of the cases. They are below average and are poor in classification. But when we consider Cop_Euch, Cop_metridia, Cop_oithona, Egg_like and Ostracoda are having 70 to 80 percent classification results. The highest percentage of matching obtained is 86% (Egg_Like) which is very good in the case of classification of plankton.

For the various algorithms used it is clear that each algorithm has its own performance. In the results obtained LMT, SMO and the MultiScheme (SMO+IBk) are having good results when compared to Random Forest and Random Tree algorithms.

6 Conclusion and Future Work

Although the project did not perform as per our bench marked results of (Matthew et al., 2005), this project has explored the possibility of using SURF and data mining tool like WEKA to train and classify – classifiers. The low results obtained for several classes of images is due to the lack of training images for some classes, but is also due to the lack of salient features for some plankton species. Centeral to the project was the use of the free and open WEKA toolkit.

From the results obtained it is clear that if more pre-processing of images such as removing the background noise, debris and other species in the same image, could help to improve classification. This is an area where a large amount of research can be done.

Another main change that could be done to improve this project is to avoiding averaging of values. This removes a lot of information when training the classifier. Instead of averaging the values into a single value, it could be reduced to two or three values by the process of clustering etc. Again the matching of a pair was calculated to input into the classifier, this method trims a lot of information and also makes the process of training the classifier very difficult. The classifier will only find very small differences between the various classes. Use of the process of clustering will help reduce the size of the vector that is fed into the classifier and while losing minimum information that is specific to each class.

From the work done it is clear that better images produce better results. So this work will help to support further funding for research and development team to produce better marine imaging systems.

During the training of the classifier each algorithm gave different results and hence it is worth exploring which algorithms are best to find patterns from plankton image data. Also how and why they perform are things which could lead to a perfectly trained classifier.

This project seems to be a partial success. It has better results when compared to previous works. Another advantage of this project is it has helped to open a wide range of possibilities in automatic detection of plankton using machine vision. And new human approach of classification methods by using WEKA and SURF.

7 References

Benfield, M. C. G., Philippe; Culverhouse, Phil F.; Irigoien, Xabier; Sieracki, Michael E.; Lopez-Urrutia, Angel; Dam, Hans G.; Hu, Qiao; Davis, Cabell S.; Hansen, Allen; Pilskaln, Cynthia H.; Riseman, Edward M.; Schultz, Howard; Utgoff, Paul E.; Gorsky, Gabriel 2006-07. RAPID : research on automated plankton identification Oceanography, 20, 172-187.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P. & Witten, I. 2009. The WEKA data mining software: an update. SIGKDD Explorations, 11, 10-18.

Herbert, B., Andreas, E., Tinne, T. & Luc Van, G. 2008. Speeded-Up Robust Features (SURF). Comput. Vis. Image Underst., 110, 346-359.

Lowe, D. 1999. Object Recognition from Local Scale-Invariant Features. Computer Vision, IEEE International Conference on, 2, 1150-1157 vol.2.

Matthew, B. B., Gary, H., Marwan, A. M., Dimitri, L., Paul, E. U., Allen, R. H., Howard, S., Edward, M. R., Michael, E. S., William, M. B. & Ben, T. 2005. Automatic In Situ Identification of Plankton. Proceedings of the Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05) - Volume 1 - Volume 01. IEEE Computer Society.

Oliver, S., Culverhouse, P. & Belpaeme, T. 2009. Towards Automated Classification of Zooplankton.

Blind Source Separation using Independent Component Analysis

C.K.Kilerci and M.Z.Ahmed

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Blind Source Separation (BSS) is a process of estimating a set of signals by using their mixed representations. In this separation process, the user does not have a prior knowledge of the original signals nor their mixing process. This is also called the Cocktail Party Problem. In this paper, a fixed point algorithm of Independent Component Analysis (ICA) was used to separate linearly mixed stationary and non-stationary mixed audio signals. Also, an attempt was made to solve the permutation problem of linearly mixed non-stationary signals by using the sliding window ICA and Minimum Distance Classifier (MDC).

Keywords

Blind Source Separation, Independent Component Analysis, Sliding Window ICA, Cocktail Party Problem, Permutation

1 Introduction

The problem of separating multivariate data without any prior knowledge of both the original sources and the mixing process has attracted a lot of attention during the past decade. This multivariate data can be taken from many different applications such as human brain activity, financial market prediction, geological activity and audio signals. During this project audio signals were selected for testing purposes because of the availability of useful the data.

The goal of this study is to separate linearly mixed stationary and non-stationary audio signals using the ICA technique. The separation was done using a fixed point algorithm using kurtosis, which was proposed by Hyvarinen & Oja (1997). This technique converges very quickly and gives accurate results for linearly mixed audio signals, but for linearly mixed non-stationary signals separation, a modification was required for the algorithm. This modification for the algorithm which is also known as sliding window ICA was implemented. Therefore the way the chosen algorithm works, a permutation effect arises for each separated window depending on the mixing process and frequency characteristics of input signals. In other words, separated windows are not in the same order as the original versions. For this reason, each window was classified using the frequency characteristics of the input signals and the separated windows were placed in the correct order. These improvements make the fixed point algorithm using the kurtosis technique realisable with linearly mixed non-stationary audio signals.

2 Background

2.1 ICA model

Let’s assume that, s1 and s2 are the audio signals, where two people speak simultaneously. Then, the speech signals are mixed by an unknown mixing matrix **A**. The aim is to estimate the un-mixing matrix which can be found by ICA under the several assumptions. This un-mixing matrix called **W**. Finally, the output signals can be retrieved from the mixed results, which are the exactly same but opposite representations of the input signals. This process can be also expressed mathematically as shown below;

$$x = A.s \tag{1}$$

$$u = W.x \tag{2}$$

Where **x** is the mixtures and **u** is the estimations of the original signals.

2.2 The fixed point algorithm using kurtosis

Kurtosis is a method of measuring non-Gaussianity. This is an important measurement when determining independent components. Using this method kurtosis can be maximised or minimised when calculating independent components. Kurtosis of a random variable *y* can be calculated as shown below (Hyvarinen *et al.*, 2001);

$$kurt(y) = E\{y^4\} - 3(E\{y^2\})^2 \tag{3}$$

From the above formula, the calculated value for *y* can be either positive or negative and this value determines the distribution of the probability density function (pdf). A Gaussian distribution has zero kurtosis while super-Gaussian and sub-Gaussian distributions have positive and negative kurtosis values respectively.

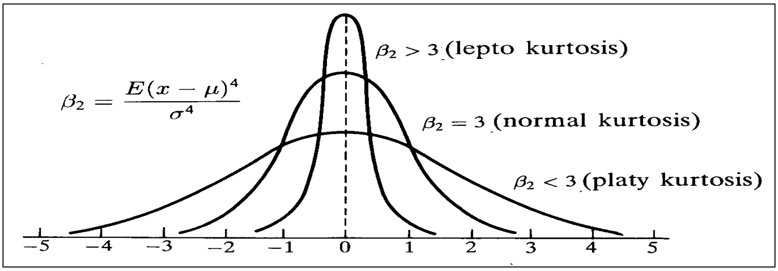
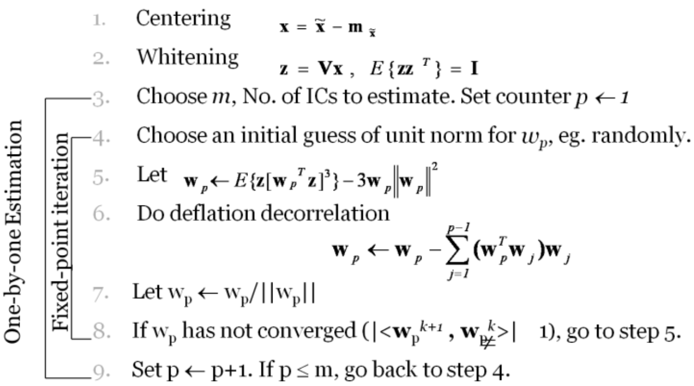


Figure 1: Measures of non-Gaussianity

If a variable has a Gaussian distribution, the kurtosis value cannot be maximised or minimised and for this reason ICA will not work. Another major drawback of the kurtosis can be very sensitive of outliers (Hyvarinen *et al.*, 2001). Hence, observations can be erroneous or irrelevant. To illustrate this drawback, consider the example below;

$$\begin{gathered}
Sample\ size\ = 1000 \\
mean\ = 0 \\
Variance = 1 \\
Contains\ one\ value = 10 \\
kurtosis\ = \frac{10^4}{1000} - 3 = 7
\end{gathered}$$

Although, the kurtosis method is not very robust to measure non-Gaussianity, it is an alternative to gradient based algorithms. The reason for this is that a good learning rate must be chosen to obtain a good convergence for gradient based algorithms and failure of wrongly selected learning rate causes slow convergence and failure of separation (Hyvarinen *et al.*, 2001). Additionally, the kurtosis algorithm is one of the versions used in FastICA, (Hyvärinen *et al.*, 2005) which is the main reason why this method became popular among the other ICA algorithms.


One-by-one Estimation
Fixed-point iteration

```
1. Centering      $\mathbf{x} = \tilde{\mathbf{x}} - \mathbf{m}_{\tilde{\mathbf{x}}}$
2. Whitening      $\mathbf{z} = \mathbf{V}\mathbf{x}, \quad E\{\mathbf{z}\mathbf{z}^T\} = \mathbf{I}$
3. Choose $m$, No. of ICs to estimate. Set counter $p \leftarrow 1$
4. Choose an initial guess of unit norm for $w_p$, eg. randomly.
5. Let $\mathbf{w}_p \leftarrow E\{\mathbf{z}[\mathbf{w}_p^T\mathbf{z}]^3\} - 3\mathbf{w}_p\|\mathbf{w}_p\|^2$
6. Do deflation decorrelation
       $\mathbf{w}_p \leftarrow \mathbf{w}_p - \sum_{j=1}^{p-1}(\mathbf{w}_p^T\mathbf{w}_j)\mathbf{w}_j$
7. Let $w_p \leftarrow w_p/||w_p||$
8. If $w_p$ has not converged ($|<\mathbf{w}_p^{k+1}, \mathbf{w}_{p\neq}^{k}>|$ 1), go to step 5.
9. Set $p \leftarrow p+1$. If $p \leq m$, go back to step 4.
```

Figure 2: A fixed point algorithm using kurtosis (Hyvarinen *et al.*, 2001)

From Figure 2, the essential pre-processing steps of centering and whitening, which is also implemented during this study, can be seen. Without the pre-processing steps, some unsuccessful estimations were observed from the experiments. Also the algorithm estimates the signals on a one by one basis and this is also knowm as deflation. When dealing with two input signals, once the algorithm estimates the first signal then whatever is left from the mixture is the estimation for the second signal and this is true for two signals separation (Hyvarinen *et al.*, 2001). For this reason, estimation of the un-mixing matrix is a very crude version of the original mixing matrix.

2.3 Ambiguities of ICA

In the ICA, there are two important ambiguities (Hyvarinen *et al.*, 2001). Firstly, the energies of the independent components cannot be determined because of the two unknowns (**s** and **A**). This means the amplitudes of estimated signals can be different from the original signals. Secondly, the order of the estimated signals cannot be determined. In other words, estimated signals are permutated versions of input signals.

The ambiguities of ICA can have an effect on the estimated output signals and these problems can be solved once the signals are separated successfully by contrasting their amplitudes and changing the orders of the estimated signals.

During this study, the permutation problem of ICA was observed as a result of the separations in the time domain when the statistical properties of the input data were changed such as the change of mixing process. To observe this phenomenon further, non-stationary signals were applied to the ICA algorithm. This is discussed is section 4.2.

2.4 Gender Identification and Minimum Distance Classifier

ICA is a method for performing blind source separation from linear (instantaneous) mixtures. "*The technique assumes a statistical independence between the sources and allows at most one Gaussian component"* (Mitianoudis & Davies, 2002). Separation can be done both the frequency and the time domain. ICA algorithms give successful results in both domains. Although, separation results of both domains are comparable, the computational complexity of the frequency domain approach is much higher (Mitianoudis & Davies, 2002). In addition, Mitianoudis states that "*one major advantage of working in the time domain is that, at least theoretically, the **permutation problem** does not exist.*" In other words, the separation results of linearly mixed stationary audio signals will not suffer from the permutation problem. However, the frequency domain approach suffers from the permutation problem (Mitianoudis & Davies, 2001). During this study, all the signals were mixed and unmixed in the time domain to avoid the permutation problem for the linearly mixed stationary signals. On the other hand, separation process of the non-stationary signals in time domain can cause similar problems as found in the frequency domain approach. For this reason, the features of the audio signals play an important role in overcoming this problem.

During this research, female and male audio speech signals were analysed as the input data to the ICA program to increase the convergence speed by increasing independence. Gender difference of the input signals provides different frequency range of the voice. This spectral difference can be used for gender discrimination. (Traunmüller & Eriksson, 1994) states that "*Typical values obtained for fundamental frequencies are 120 Hz for men and 210 Hz for women.*" Additionally, there are many different factors which can affect the final gender decision such as age, language, dialect, accent, health and emotional state (Wu and Childers, 1991).

The gender discrimination technique implemented for this research is known as Minimum Distance Classifier (MDC). MDC is a technique of characterising the information by grouping similarities of data features. MDC requires some knowledge about the data, as with the other classification techniques (Dunham, 2003). For this reason, a training set is used to develop the specific parameters required for the classification purposes and in this case, the required parameters about the data would be the Fast Fourier Transformation (FFT) of the different female and male speeches. In this study, 2 or 3 point FFT of the data can give enough information about the data for classification purposes which is verified experimentally. Also, instead of using the full frequency spectrum, reducing the window size and position in respect to where the most of the spectral power density to locate the spectral band that can uniquely identify the speech characteristics.

2.5 Sliding window ICA for linearly mixed non-stationary audio signals

Linearly mixed stationary signals can be separated very efficiently by ICA algorithms and most of the attempts were made to solve BSS in the literature by assuming signals are linearly mixed and stationary. This assumption simplifies the problem because external factors are constant such as reflections and environmental acoustics. During this research, the same assumptions were made for the initial tests. Afterwards, the mixing process of the signals was changed half way through by generating another random or user defined mixing matrix. Hence, the robustness of the ICA algorithm could be investigated further. For this reason, the algorithm was modified by a technique called sliding window ICA. This technique was proposed for image separation by Hyvarinen *et al.* (2001). Guo & Wu (2010) used sliding window technique with infomax to analyse motor imaginary EEG. In this research, the fixed point algorithm using kurtosis algorithm was adapted to sliding window ICA technique to analyse audio signals

3 Simulation Setup

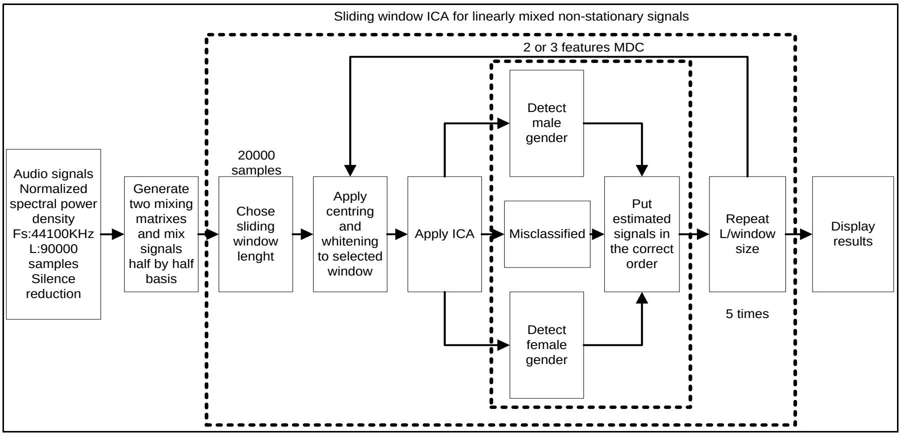

Sliding window ICA for linearly mixed non-stationary signals
2 or 3 features MDC
Audio signals Normalized spectral power density Fs:44100KHz L:90000 samples Silence reduction
Generate two mixing matrixes and mix signals half by half basis
20000 samples
Chose sliding window lenght
Apply centring and whitening to selected window
Apply ICA
Detect male gender
Misclassified
Detect female gender
Put estimated signals in the correct order
Repeat L/window size
5 times
Display results

Figure 3: Logic block diagram of the non-stationary signal separation

The simulation was carried out in MATLAB® and the logic block diagram is given in Figure 3. The program takes data from the size of the window which was defined by the user and treats each window as separate signals. In this way, signals would be separated on a window by window basis. Pre-processing was applied to each individual window. The number of repetition was calculated by dividing the length of the signal by the window size. Once the signals were separated successfully, results were passed to MDC and the genders of the signals identified. Using this identification, separated signals were stored into the created male and female variables. This way the effects of the permutation problem was reduced. However, there is, as expected erroneous data appears in the region of the mixing matrix change. There is nothing that can be done to overcome this failure in this method. Therefore, one window of failure is considered as an acceptable failure rate. Although, one window was accepted as a failure, it can be correctly classified and placed inside the correct gender variable depending on how heavily the signals were mixed. Also, size of the window can be reduced to decrease the probability of failure. Conversely, this may cause a discontinuous transition between the windows and can produce audiable high frequency components.

4 Results and Discussion

4.1 MDC simulations

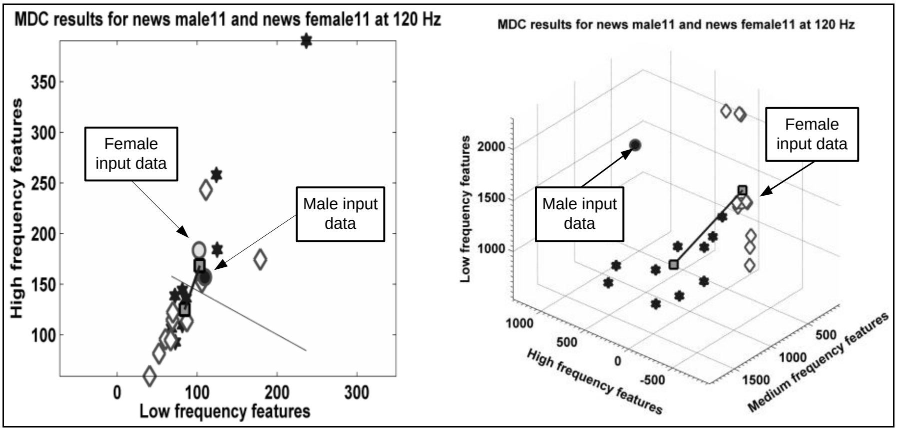


Figure 4: Comparison between two and three features MDC performance

In Figure 4, a two features MDC plot is illustrated on the left hand side. The spectral power density of the data was used at 120 Hz. The training data of the male speech (hexagram) and the female speech (diamond) were not classified perfectly. Centroids (squares) are calculated from the mean values of the training data set and input data (circles) were classified in respect to the distances from the centroids and a decision line (sloped line) was drawn between the two centroids. From the two features MDC plot, it can be clearly seen that the female and male data is misclassified.

On the right hand side plot, a three features MDC is illustrated and this is improvement by carefully selecting of the window's spectral bandwidth to the classification efficiency, where the input data classified correctly.

4.2 Sliding window ICA for linearly mixed non-stationary audio signals simulations

Figure 5, the top two plots represent the original male and female speeches using spectrograms. These audio signals were uploaded to the sliding window ICA program and the statistical properties of the signals were changed. In other words, audio signals appear non-stationary. Hence the permutation problem of ICA was observed. The estimated signals are wrongly ordered as it can be seen from Figure 5. Also, failure is expected at where the mixing process changes, depending on the difference between the mixing matrices. From this point, the three features MDC program used to identify the genders of individual windows so that estimations can be placed to correct gender variable where they are belong.

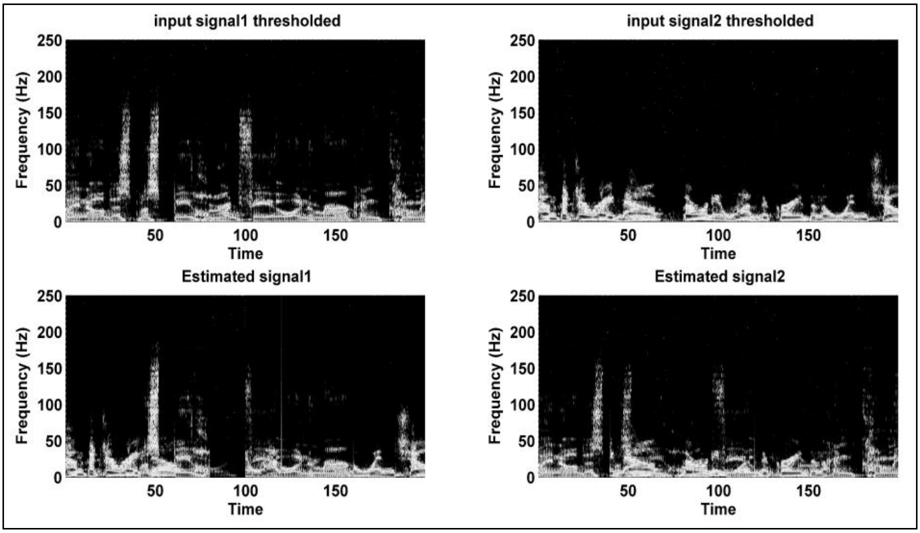


Figure 5: Permutation problem of non-stationary signal separation

Two user defined mixing matrices were generated for the mixing process. Additionally the length of the input data was set to 90000 samples long for the three features MDC. The used window size was 20000 samples long. Hence, input data was separated into five windows. This experiment was repeated for five male and five female audio signals. An audible assessment was done for the evaluation of results and recorded in table 1.

Estimations	M1	F1	M2	F2	M3	F3	M4	F4	M5	F5
Window1	M	F	M	F	M	F	M	F	M	F
Window2	M	F	M	F	M	F	M	F	M	F
Window3	M	F	U	U	M	F	U	U	U	U
Window4	M	F	U	U	M	F	M	F	M	F
Window5	M	F	M	F	M	F	M	F	M	F
M: Male, F: Female, U: Unsuccessful										

Table 1: Three features MDC with sliding window ICA @ 120 Hz

A three feature MDC program gives better classification results for the output signals of the sliding window ICA. Results were verified by listening correctly to the ordered signals. For the classification purposes, the male fundamental frequency spectrum (120 Hz) was used and divided into three equal windows and average of each window taken. Also, as expected some failures were observed at window3. The main reason for this failure is because the ICA cannot estimate two mixing matrices at once. In this case, the random decision was used in window3. To reduce the number of failures, a better classifier can be used such as neural networks.

5 Conclusion

An attempt was made to solve the ICA permutation problem. For linearly mixed non-stationary audio signals, ICA was implemented by dividing data into smaller windows and treating each window as an individual signal. In this research, MDC, the simplest data mining techniques MDC was used to group the male and female speeches by using the frequency characteristics of the data. This technique was implemented by three features from the data. The most spectral power efficient window was used during the classification process. Simulation results have shown that a three feature MDC can successfully classify individual windows. The numbers of failures are reduced and data classified more efficiently. In this way, permutated windows were rearranged respect to gender they are belong to.

6 References

Dunham, M. H. (2003) Data Mining Introductory and Advance Topics. Prentice Hall.

Guo, X. & Wu, X. (2010) 'Motor Imagery EEG Classification Based on Dynamic ICA Mixing Matrix', Bioinformatics and Biomedical Engineering (iCBBE), 2010 4th International Conference on. 18-20 June 2010. pp. 1-4.

Hyvärinen, A., Särelä, J., Hurri, J. & Gävert, H. (2005) FastICA for Matlab 7.x and 6.x. (Version 2.5) [Computer Program]. Available at: http://www.cis.hut.fi/projects/ica/fastica/

Hyvarinen, A., Karhunen, J. & Oja, E. (2001) Independent Component Analysis. New york: Wiley-Interscience.

Hyvarinen, A. & Oja, E. (1997) 'A fast fixed-point algorithm for independent component analysis'. Neural Comput., 9 (7). pp 1483-1492.

Mitianoudis, N. & Davies, M. (2001) 'A fixed point solution for convolved audio source separation'. IEEE workshop on Applications of Signal Processing on Audio and Acoustics. New York: New Paltz.

Mitianoudis, N. & Davies, M. (2002) 'Audio Source Separation: Solutions and Problems'. International Journal of Adaptive Control and Signal Processing, 18 (3). pp 299-314.

Traunmüller, H. & Eriksson, A. (1994) The frequency range of the voice fundamental in the speech of male and female adults. Stockholm, Sweeden: Department of Linguistics, University of Stockholm. Available.

Wu, K. & Childers, D. G. (1991) 'Gender recognition from speech. Part I: Coarse analysis'. The Journal of the Acoustical Society of America, 90 (4). pp 1828-1840.

Watermarking using Side Information

S.Lefort and M.A.Ambroze

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

During the past few years, the development of digital files sharing has been incredible, and led to a certain amount of abuses, the most important one being piracy and illegal copying. Thus, new Methods have been invented to struggle against these abuses and the most well known technique is watermarking. Watermarking allows marking in an indelible way a media so that the message embedded (legal owner/author, right or not to copy…) remains accessible and readable whatever happens to the media itself during its normal use. This thesis suggest a watermarking system using Quantization Index Modulation allowing to embed a watermark in the spatial domain that will resist to the geometric attacks that are commonly used such as cropping, rows/columns deletion and rotation. The system has been tested in different situations and with different attacks to show its strengths, weaknesses and limits.

Keywords

Image, Watermarking, Quantization Index Modulation, Watermark, Side Information, Geometric attacks.

1 Introduction

For a few years, information we trade have changed. We migrated from analogue information to numeric/digital files. The advantages of digital are significant: easier to manipulate, to copy and much faster to transmit. But, this aspect has some drifts, and the best example is piracy. In order to struggle against this blight, a bunch of new techniques have emerged. Thus, watermarking appeared. watermarking is mainly the action of embedding information (a proof of authenticity, a signature, etc...) on a medium (an image, a song or a video).

Among all techniques of Watermarking, “Watermarking using side information” became one of the most popular and powerful technique. Instead of just hiding the signature in the data, the data is analysed and hence the watermark is hidden in it: when the cover image is studied before, it become much easier and efficient to hide the data. For example, when a “don’t copy” watermark have to be inserted on all DVD’s produced by a firm, they can’t know what the content of the DVDs are (Bloom et al, 1999).

Then, half of the noise that can affect the watermark is known, the only noise that remains unknown are the different compression, transmission changes, or attacks that will affect our watermark.

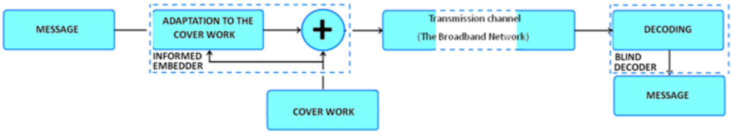


Figure 1: Scheme of an informed embedder / blind detector system

Two main techniques are presented in the literature when speaking of watermarking using side information: Quantization Index Modulation or Spread Spectrum and the use of trellis codes. The main idea behind that is that instead of having one codeword to represent one message, a certain number of codewords will represents the same message, hence the one that fits the best to the Image will be embedded so that he will be hidden much efficiently (Cox et al, 1999).

2 The watermarking scheme proposed

The watermarking system proposed uses the Quantization Index Modulation in the spatial domain to embed a Mark. It also uses a placement detector to choose specific target points in the image to embed our watermarks and a specific anti-rotation algorithm to struggle against rotation attacks.

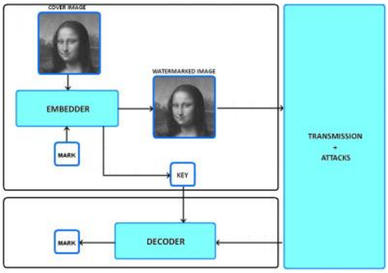


Figure 2: Overview of the watermarking system

2.1 The Embedder

The embedder needs a mark and a Cover Image at the input. The mark is an 8x8 binary matrix and the Original Image is a 512x512 colored Image.

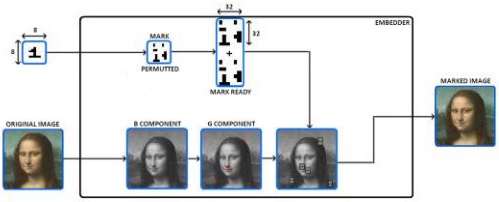


Figure 3: Overview of the embedder

The mark is firstly permuted to make sure that the human eye will not recognize any specific shape (here the ‘1’). This is also made to add a security level to our scheme: in fact, the detector needs to know the permutation algorithm to recover the mark.

The watermark is hence prepared to be embedded. Each watermark is embedded twice around specific key points. The choice of these key points will be explained a little bit later.

The coloured Image is decomposed in its 3 RGB components. The G component will be used to find the target points and the B component will be used to embed the watermarks.

The target points are chose in the G component. It takes the n most important pixel values of the Image, that are far enough from each other to avoid overlapping.

The B component is used to mark the Image because the human eye is less sensitive to the blue variations than Red or Green variations. Each watermark is embedded 2 times in two 32x32 squares around the target points. If 5 target points where chose, 10 watermarks will be embedded.

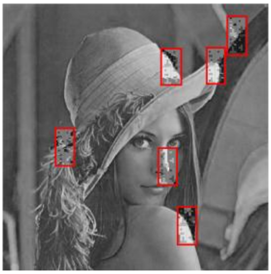


Figure 4: Implantation of the marks

Finally, the marked image is recomposed using the G and R component to give back a coloured Image.

2.2 The decoder

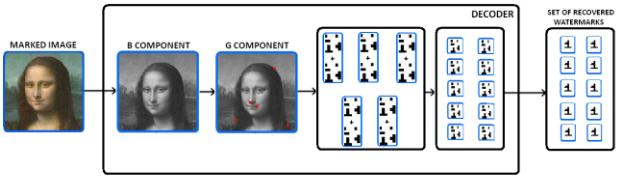


Figure 5: Overview of the Decoder

At the decoder, the marked image is decomposed back into its R G and B components. The target points are searched into the G component like in the embedding process. What is interesting is that even if the target points have moved during the transmission, they still can be recovered.

The Marked area are extracted from the B component using the target points, hence the pairs of watermarks are decoded using QIM decoding and the anti-rotation system. Finally, The operator can decide which watermark was embedded from the set of decoded watermarks he has.

2.3 The anti-rotation system

The anti-rotation system tries to discover the angle of rotation of an attack (if the Image was attacked). It uses the pairs of watermarks to calculate correlation sums, and tries to maximize it by rotating the Image back to its original position.

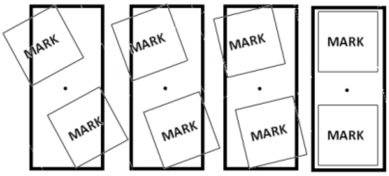


Figure 6: Anti rotation recovery

At the decoder, when the system has the target points, he will try to calculate the correlation sum between the two mark inside the bold rectangle. Then, it will rotate the image a little bit and calculate the sum again. Most of the time, the correlation sum will be the best when the marks will be back to their original positions.

3 Results and Discussion

The system has been tested with different parameters, and the Marked Image has been attacked using different processes to push the system to its limits.

3.1 Experiment 1: Visibility of the Mark against strength of Embedding

The more important is the strength of embedding, the more robust will be the watermark, but the more visible it will be as well. In this experiment, the Cover Work was marked using different strengths of embedding, then the Marked Image was examined to decide whether or not the Mark is visible during normal use or not.

The embedding strength can vary from 1 to 100. This value represents the size of the range of the different split area of the pixel value. For example, if the strength of Embedding is 50, this means that the values will be split like:

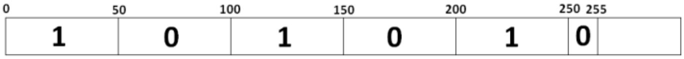


Figure 7: QIM Decomposition of a pixel value

Strength of Embedding	Visibility
5	Totally Invisible : Perfectly Hidden even when watching only the B component
10	Totally Invisible. Can be perceived when looking only at the B component
20	Can be slightly seen when watching carefully
30	Visible
100	Totally visible

Table 1: Marks visibility against embedding strength

After a value of strength of 20, the mark is visible during normal use, so the invisibility aspect of the embedding system is totally lost.

3.2 Experiments 2: Robustness to Cropping attacks

The system have been tested with a few cropping attacks. 5 pairs of watermarks have been embedded with a strength value of 10, which gives 10 watermarks.

The Image has been cropped in 5 different ways:

3.2.1 Image4.jpg + Mark1.

Cropping	Number of Perfect Marks recovered
100 on the left	10
100 on the right	6
100 upper	6
100 bottom	10
50 around	8

Table 2: Marks recovered after cropping using Image4.jpg

3.2.2 Image2.jpg + Mark1

Cropping	Number of Perfect Marks recovered
100 on the left	7
100 on the right	7
100 upper	7
100 bottom	4
50 around	3 + 1 recognizable

Table 3: Marks recovered after cropping using Image2.jpg

3.2.3 Image3.jpg + Mark2

Cropping	Number of Perfect Marks recovered
100 on the left	8
100 on the right	10
100 upper	10
100 bottom	8
50 around	10

Table 4: Marks recovered after cropping using Image3.jpg

The system is relatively efficient against cropping attacks. In fact, the worst result is nearly 4 Marks recovered, which is more than enough to decide which mark have been embedded. If the cropping is not too important, the Mark will always be recognizable at the end of the decoding.

3.3 Experiments 3: Robustness to Rows/Columns deletion attacks

For this experiment, 2 rows and 2 columns were randomly deleted from the Marked Image, and then the marks were decoded. Each time, 5 pairs of watermarks were embedded with a strength value of 10.

Image Used	Number of Perfect Marks recovered out of 10
Image1.jpg	10
Image2.jpg	8 + 2 recognizable
Image3.jpg	10

Table 5: Marks recovered after rows/columns deletion

Again, it can be conclude that the system works perfectly with rows/columns deletion attacks. This can only be a problem if all the target points are on the deleted rows/columns, and this situation has a really small chance to appear.

3.4 Experiment 4 : Robustness to Rotation

Each time, three pairs of marks were embedded with a strength value of 10. Each Image was rotated of different angle and decoded to try to recover the Marks embedded. The number shown is the number of perfect recovered watermarks out of 6.

Image1.jpg + Mark1

ROTATION ANGLE (in degree)	CLOCKWISE	ANTICLOCKWISE
0	6	6
0.2	6	6
0.5	6	6
1	6	6
5	2	6
8	2	6
10	2	6

Table 6: Mark recovered after rotation using Image1.jpg

The anti-rotation system is working almost perfectly. The worst result is when using Image1 with big angles. We can conclude that the system works pretty well.

3.5 Experiment 5: Robustness to Noise

Some different sorts of noises have been added to the Marked Image after embedding, and then the Image has been decoded to recover the watermarks. Each time one pair of marks was embedded with a strength value of 10 and then 20.

The Quantization Index Modulation embedding method allows a pretty good resistance to Salt and Pepper Noise. Each time the watermark is almost perfectly recovered.

A Gaussian noise of 0 mean and a few different variance values have been added to the watermark after embedding. The embedder embeds one pair of watermarks with a strength value of 10.

The system is not robust enough to Gaussian noise. Even after a noise variance of 0.01, the Image is still easily recognizable, and the system can't deal with noise of more than a 0.001 variance value.

4 Conclusion

From all of these results, it can be concluded that the system proposed works pretty well against geometric attacks.

For signal processing attacks, the system is still powerful, but not enough to be used in a practical situation. For the noise tests, the «position recovery» have been switched off and the position of the Mark have been manually given to the decoder. This was done because for example salt and pepper noise add some pixel values in the component that are equal to 255 (Matlab, 2010) and the position recovery system was not able to recover the right target positions. The position detection needs to be adapted to other criteria's than just « the most important pixel values ».

For compression, the system is still pretty powerful until the compression quality is not too low. Unfortunately, even with a compression quality of less than 70%, on a computer screen, the image still appears with a good quality, and the system can't recover an Image with a compression quality smaller than 85%

To continue, the main problem with this system is visibility, in fact, even if the mark is not easy to detect when looking at the RGB whole image, if the attacker knows that a mark is embedded into the Image, it is really easy for him to scan each component and detect that changes appears on the B component, then it is really easy for him to apply some filtering to the B component where the marks are embedded and totally destroy the Message. Using adaptative functions that, for example, calculate the mean and the variance of a certain area of the image will certainly help to hide the mark into the Image.

5 References

Bloom, J.A. (1999), 'Copy protection for DVD video', *Proc. of IEEE,* 4(2), pp. 1267-1276

Costa, M. (1983), 'Writing on dirty paper', *IEEE Information Theory Society,* 29(3), pp. 439-441.

Cox, I.J. (1999), 'Watermarking as communications with side information', *Proceedings of the IEEE*, 87(7), pp. 1127-1141

Cox, I.J. et al. (2008) *Digital watermarking and steganography* (2nd edn.). Burlington:Morgan Kaufmann.

Matlab Help (2010), *Add noise to image* [online], Available from: http://www.mathworks.com/access//helpdesk/help/toolbox/images/imnoise.html [Accessed:28.8.2010]

Tang, C. (2003), 'A Feature-Based Robust Digital Image Watermarking Scheme', *IEEE transactions on signal processing*, 51(4), pp. 950-960

On Trellis Structure of Error Correction Coding

J.Mathew and M.A.Ambroze

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The modern trends in communication field points towards achieving the fastest way of data transmission through communication line, reaching Shannon's Channel Limit. The key to these developments is error correction coding technique which is currently employed in broadband satellite communication and data storage. Constructing Trellis for the codes - a graphical way of code analysis that allows us to avoid repeating the same computations over and again - reduces the decoding complexity, thereby improves transmission efficiency. The paper will investigate the way trellises are constructed for different types of codes, how their complexity can be reduced and how they are used to correct errors on transmission channels. This includes study of trellis pattern for different coders – for both convolutional and block codes and its implementation in a practical communication channel using Monte Carlo Simulation technique. A brief comparison of bit error rate for hard and soft decision decoding techniques for selected coders and for different message lengths is performed with BER Vs SNR plots.

Keywords

Error Correction codes, Trellis representation, Convolutional coding, Hard decision Viterbi decoding, Soft Decision Viterbi Decoding, Monte Carlo Simulation

1 Introduction

In communication system, coding theory dealt with the design and evaluation of efficient signalling schemes for reliable data transmission and storage. It is applied in telephone-line modems, where increasing transmission speeds introduce high levels of noise; compact-disk recorders, in which error is inherent in the production process; and deep-space probes, in which large lag times confound the problems associated with transmission error .(Trachtenberg,2000)

In 1948 Claude Shannon showed that it is possible to transmit information over a noisy channel with arbitrarily small probability of error, at rates up to the capacity of the channel (Shannon, 1948). Error correcting codes are used for reliable transmission of information over noisy channels, which encode input in such a way that errors can be detected and corrected at the receiving site.

The design of error correcting codes that minimize the probability of error on one hand and maximize the information rate on other hand is little complicated. Also it should be capable of reconstructing the most likely transmitted codeword from the error-corrupted sequence observed at the output of a noisy channel.

This paper approach both of these problems by the study of decoding techniques based on graphs. A code which has a low error probability and a reasonably high information rate, and can be decoded efficiently by means of a trellis, is developed. The trellis may be thought of as a constrained finite-state automaton; diagram that allows us to avoid repeating the same computations over and again (something similar to the FFT algorithms); it was originally introduced by Forney in 1967 to explain the Viterbi decoding algorithm.

A Forward Error Correction code is a redundant data added to the message at the sender side and the receiver can use the extra information to discover the location of the error and correct them. Convolutional codes are processed on a bit-by-bit basis, and only cause a processing delay corresponding to a few bit periods. It has memory shift registers. Block codes are processed on a block-by-block basis.

2 Trellis Formation

2.1 Convolutional Encoding

A convolutional code can be defined by kn polynomials and a k*n generator-polynomial matrix. For k=1, a convolutional code can be compactly defined by the generator polynomial matrix,

$G(x) = [g1(x), g_2(x),\ldots\ldots..g_n(x)]$

For a simple code G = [5,7] ; R= ½ ; K=3

$5 = 101 \equiv 1+x^2 \quad = g_1(x)$

$7 = 111 \equiv 1+x+x^2 = g_2(x)$

Let $\{u\} = 0110100\ldots\ldots\ldots\ldots$

$g_1(x)\, u(x) = (1+x^2)\,(x+x^2+x^4) = x+x^2+x^4+x^3+x^4+x^6 = x+x^2+x^3+x^6$

$\{v_1\} = 0111001\ldots$

$g_2(x)\, u(x) = (1+x+x^2)\,(x+x^2+x^4) = x+x^2+x^4+x^2+x^3+x^5+x^3+x^4+x^6$

$= x+2x^2+2x^3+2x^4+x^5+x^6 = x+x^5+x^6$

$\{v_2\} = 0100011\ldots..$

Therefore, $\{v\}$ = 00 11 10 10 00 01 11 ……….

Here the information sequence cannot be identified in the code sequence. Therefore it is non-systematic. Non-systematic codes are preferred when viterbi decoding is used as they offer maximum $d_{\text{free.}}$

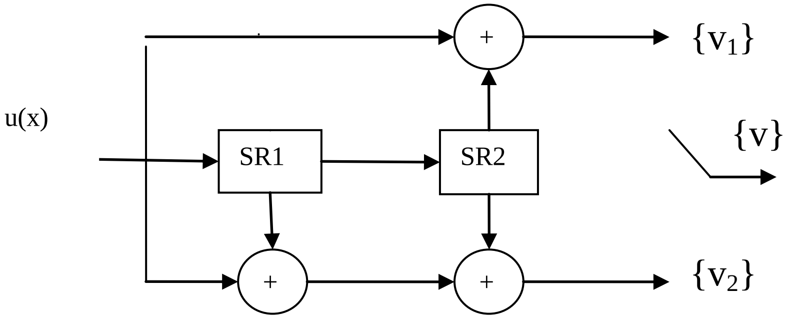


Figure 1: Convolutional Coder G=[5,7]

Original State	Input	Output	Final State
00	0	00	00
	1	11	10
01	0	11	00
	1	00	10
10	0	01	01
	1	10	11
11	0	10	01
	1	01	11

Table .1.FSM for G=[5,7]

Take input sequence as 10101101

V1 = 10000110
V2 = 11010000
V = 11 01 00 01 00 10 10 00

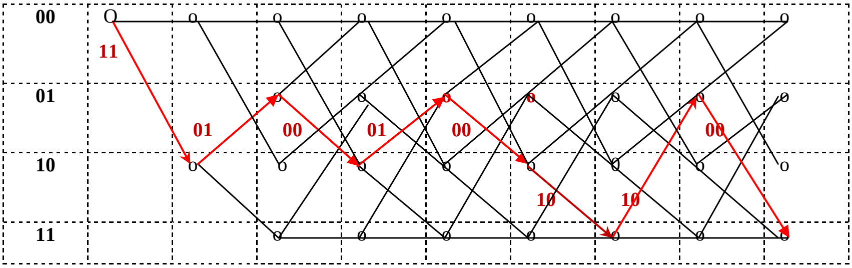


Figure 2: Trellis for convolutional encoder G=[5,7]

3 Decoding

A convolutional encoder is basically a finite-state machine; hence the optimum decoder is a Maximum-Likelihood Sequence Estimator (MLSE). Therefore, optimum decoding of a convolutional code involves a search through the trellis for the most probable sequence. Depending on whether the detector performs hard or soft decision decoding, the corresponding metric in the trellis search may be either a Hamming metric or a Euclidean metric. (Proakis,1995)

The Viterbi algorithm operates frame by frame over a finite number of frames. At any frame the decoder does not know the node the encoder reached, so it labels the possible nodes with metrics- in this case the running Hamming distance between the trellis path and the input sequence. In the next frame the decoder uses these metrics to deduce the most likely path and drop other paths (Wade, 1994).

Hard-decision Viterbi decoding seeks a trellis path which has minimum Hamming distance from a quantized channel output sequence.

Hard Decision Viterbi Decoding For a simple non recursive coder G = [5,7] ; R= ½ ; K=3

Let i = 1 0 1 0 1 1 0 1

V = 11 01 00 01 11 10 10 00

r = 11 **1**1 00 01 11 10 1**1** 00

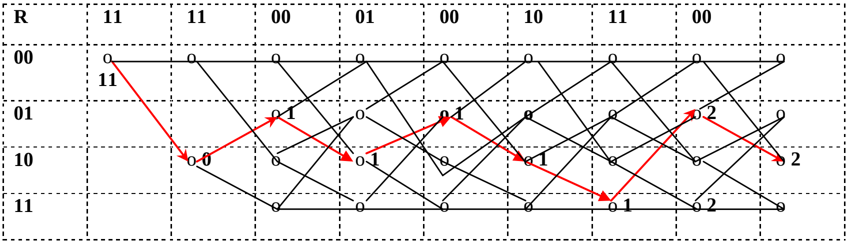


Figure 3: Trellis showing full Viterbi decoding for G=[5,7]

Thus the minimum distance unique path is retrieved and from the trellis we will get the decoded output as: 1 0 1 0 1 1 0 1

Soft Decision Viterbi Decoding For a simple non recursive coder G = [5,7] ; R= ½ ; K=3

For a soft decision input (output of demodulator quantized to more than two levels), maximum likelihood decoding is achieved by minimizing a Euclidean distance. In terms of Viterbi algorithm trellis, this amounts to computing successive branch metrics and accumulating their values in path metrics (Wade, 1994).

$$bm = \Sigma (r - v)^2$$

Let

i = 1 0 1 0

V = 1 1 0 1 0 0 0 1

r = 0.9, 1.1, -0.2, 1.3, 0.2,- 0.3, -0.1,0.9

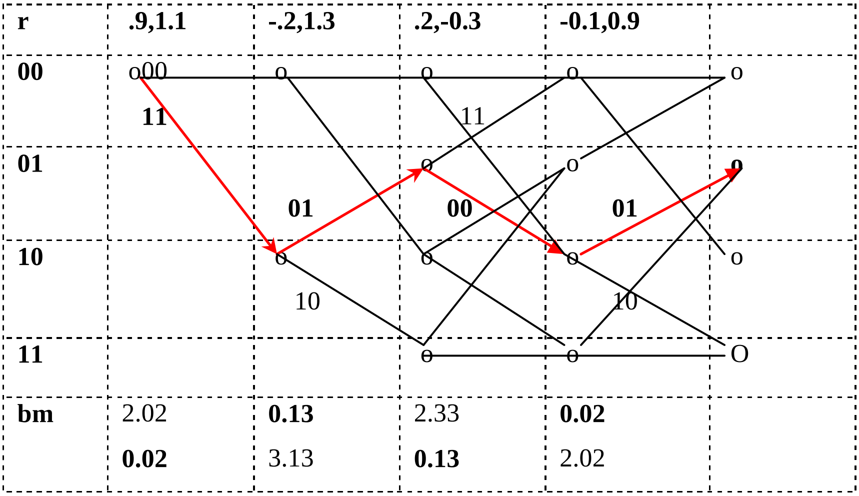


Figure 4: Trellis showing Soft Viterbi decoding for G=[5,7]

On finding the branch metrics, follow the lowest value path, discarding high difference values at each node. This will be the unique trellis path and the output values are getting decoded to original input.

3.1 Trellis representations of binary linear block codes

Trellis-based (Viterbi algorithm) decoding is one of the most efficient methods known for maximum-likelihood (ML) decoding of general binary linear block codes; Certain binary linear block codes could be represented as terminated convolutional codes, and therefore has trellis representations (Forney, 2005). Any (n, n- 1, 2) single-parity-check (SPC) code has a two-state trellis representation like that shown,

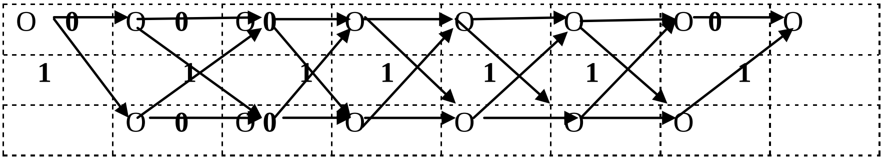


Figure 5: Trellis for Simple Block code

A generator matrix for a linear code is a binary matrix whose rows are the code words belonging to some basis for the code. A generator matrix is in Trellis Oriented Form (TOF) when for each row $g \mathcal{E} \{g_1,g_2,....g_{k-1}\}$. The leading 1 (first non-zero component of a row) appears in a column before the leading 1 of any row below it. No two rows have their trailing 1(last non-zero component of the row) in the same column (University of Crete, 2009).

4 Methodology & Results

In digital communication, the matched filtering technique has been used widely to maximise the output signal by maximising the output SNR (signal to noise ratio). Here the performance of the matched filter for the Base band Binary Transmission in the presence of Gaussian noise is briefly studied and its BER (Bit Error Rate) is estimated using MATLAB simulation (Monte Carlo Simulation) for 3 different coders designed using trellis structure. The BER of the filter for different operating points is generated and plotted against the theoretical value of the BER and is compared. A comparison of the performance of coders for hard and soft decision coding techniques is discussed for different message length.

The theoretical and simulated BER gives a clear picture of the performance of system. After doing Monte Carlo simulation, from the plots it is found that the theoretical line coincides with a majority of the practically simulated points. Thus the matched filter designed is a good one and it approximates very closely to the practical results and gives high performance. The Trellis coding and Viterbi decoding are the underlying features that enables the error free transmission.

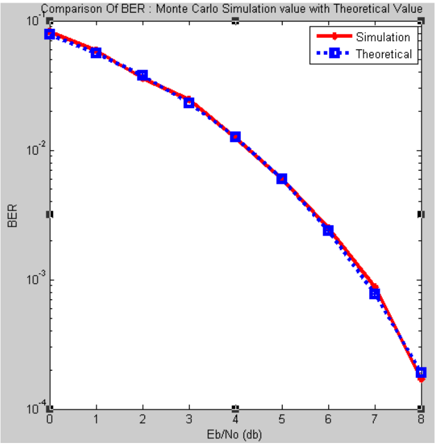


Figure 6: Monte Carlo Simulation Result comparing theoretical & Practical BER for the designed system

It is observed that for larger message length, the number of error bits is comparatively not very high, trellis found greater advantage in reducing error rate. For hard decision decoding, the coder with lower constraint length produces comparatively less error bits. For soft decision, coder with higher constraint length gives less number of error bits. In Table 2, the coder G=[133,171] gives very good performance for soft decision decoding.

Coder	Message Length	Number of error bits		BER	
		Hard Decision	Soft Decision	Hard Decision	Soft Decision
G=[5,7]	1000	16	0	0.016	0
	10000	238	30	0.0238	0.0030
	100000	1899	482	0.019	0.0048
G=[13,15]	1000	41	3	0.0411	0.0032
	10000	252	23	0.0252	0.0023
	100000	2275	364	0.0228	0.0036
G=[133,171]	1000	38	0	0.0381	0
	10000	267	5	0.0267	5.0241e-004
	100000	3079	64	0.0308	6.4031e-004

Table 2: Comparing BER for 3 Coders

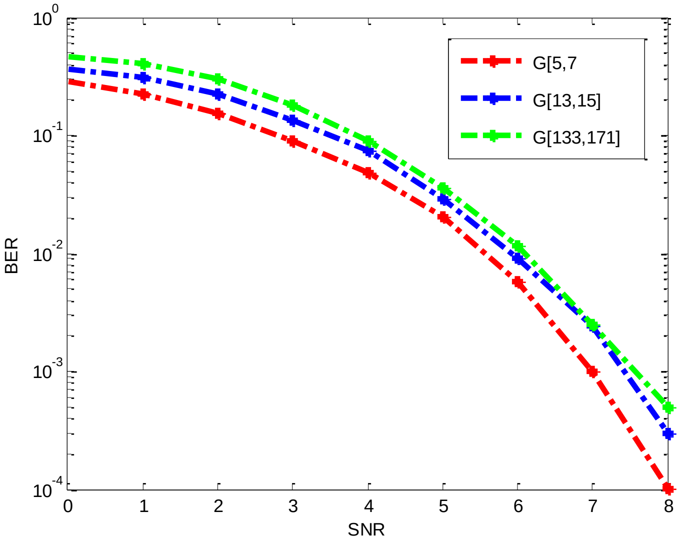


Figure 7: BER Vs SNR for Soft Decision Decoding

In Fig.7, for soft decision decoding, when the SNR value increases, BER drops. Lower constraint length coder give good performance for low SNR, but higher constraint length coder becomes better for higher SNR values.

For hard decision decoding also, it is observed from graph (Fig.4.8.) that the BER value decreases with SNR, for all the coders. When comparing the BER for 3 coders, G=[5,7] < G=[133,171] < G=[13,15] .Note the performance of G[13,15].

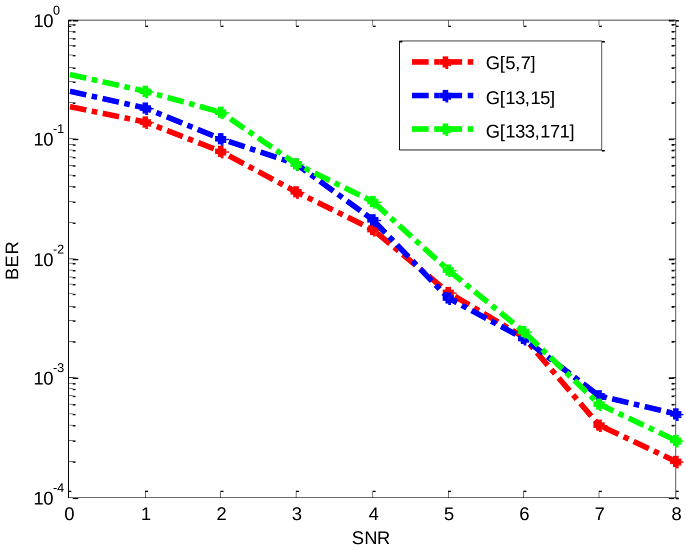


Figure 8: BER Vs SNR for Hard Decision Decoding

5 Conclusion

The demand of high transmission efficiency of communication systems is increasing every day. With the development of new technology data handling and storage become a big issue where coding plays a prominent role. The popularity of error correction codes led researchers to move deep into the existing coding theory and develop new methods to improve the performance. Trellises become an underlying theory to reduce the encoding and decoding complexity because of its great advantage of reduced computational processes. Error detection and path control become more vivid when it comes to a graphical analysis. The low bit error rate gives the choice of coders to be used, selected for a suitable length of data through a noisy environment.

The paper gives more importance to the trellis construction of different convolutional coders and the viterbi decoding steps. The performance of various coders is analyzed for different message lengths and for both hard and soft decision decoding. BER Vs SNR graphical comparison of three different coders gives the performance of the system at different noise levels. The future works includes a detailed study of trellis oriented generator matrix for different types of block codes, particularly for turbo codes, which is widely used in satellite and deep space communication. Minimal state trellises and state –space trellises are emerging techniques in this field.

6 Reference

Forney (2005),*'Trellis representation of binary linear block codes*', [online] MITopen courseware http://ocw.mit.edu/NR/rdonlyres/Electrical...and.../6.../chap10.pdf *[accessed:07-08-09]*

Proakis J.G,(1995), “Digital Communications”, McGraw- hill International Editions

Shannon, C.E. (1948), "A Mathematical Theory of Communication", Bell System Technical Journal, 27, pp. 379–423 & 623–656, July & October, 1948

Trachtenberg,A (2000), “*Error Correcting Codes on Graphs:Lexicodes,Trellises and Factor Graphs”* [online] http://ipsit.bu.edu/phdthesis_html/node41.html [date accesses : 07-06-09]

Togneri R, DeSilva C.J.S (2002), “Fundamentals of information Theory & Coding Design”, Chapman & hall/CRC

University of Crete Telecommunications Division (2009),[online] *http://www.telecom.tuc.gr/Greek/coding_theory/Docs/4_Trellises_For_Linear_Block_Codes.pdf*[accessed on : 02-09-09]

Viterbi, A.J,(1979), “Principles of Digital Communication And Coding” ,Mc-GrawHill, Newyork

Wade G (1994), “Signal Coding & Processing “,Cambridge University Press

Performance of Turbo Codes on the Satellite Communications Channel

S.Osisanya and M.Tomlinson

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Turbo codes introduced in 1993 by Berrou, Glavieux and Thitimajshima have attracted significant interests due to their ability to achieve performances close to Shannon's theoretical limits. This has motivated their use in a wide range of applications cutting cross deep space satellite communications, third and fourth generation family of wireless communications and magnetic recordings amongst several others.

This paper investigates the performance of Turbo codes. Theoretical backgrounds on convolutional codes which are the primary building blocks from which turbo codes are built are presented. Turbo codes are subsequently described in terms of their encoder and decoder architectures and the performances of the [5 7] and [15 13] recursive systematic turbo codes over an Additive White Gaussian Noise (AWGN) channel are simulated. Results are compared and analysed.

Keywords

Turbo codes, convolutional codes, MAP decoding

1 Introduction

The communications channel over which information is transmitted typically corrupts data before its arrival at the receiver. Depending on the characteristics of the channel, multi-path interference, multiple access interference and Gaussian noise interference are some of the factors responsible for the introduction of errors to data transmitted over it. Channel error correction schemes address problems associated with such perturbations. They introduce controlled redundancy which is exploited during decoding in the form of parity bits to the original data sequence.

Shannon in 1948 provided a significant proposition on the limits over which information can be transmitted reliably over noisy communication channels. Precisely, he noted that information transmitted over a noisy channel can be recovered with no or arbitrarily small errors provided the appropriate coding technique was used and data rates do not exceed the channel capacity (Shannon, 1948). In addition, he suggested that the codes be random and of sufficient length. Researchers thus began the search for the "perfect" code. One of the most powerful coding schemes before the invention of turbo codes was the serially concatenated convolutional and Reed-Solomon codes (Abu-Rgheff, 2007). The codes provided large coding gains but suffered a poor convergence towards Shannon's theoretical limit. Some researchers involved in the search for codes that combined both desirable qualities include Gallagher (1962), Tanner (1981), Hagenauer and Hoeher (1989). The introduction of turbo codes by Berrou and his team provided results closest to theoretical limits.

Turbo codes are used in wide arrange of applications. They are particularly useful in deep space applications where data is subject to long propagation delays and suffer extreme degradation before arriving at the receiver. These two factors are suited to the characteristics of turbo codes. Several other satellite applications such as broadcast and telephony, wireless applications such as the third generation wireless services (UMTS, CDMA 2000) and the fourth generation wireless services marketed as Long term Evolution(LTE) employ turbo codes (Gracie and Hamon, 2007).

This paper is divided into four sections. Section 1 introduces the subject of error correction, section 2 introduces convolutional codes and subsequently discusses turbo codes, their architectures and performances. In sections 3 and 4 respectively, results are presented and conclusions drawn.

2 Turbo codes and their performance

2.1 Convolutional codes

Convolutional codes are the primary building blocks from which turbo codes are built. They produce output data sequences which are dependant on the current input and one or more previous input data sequences. To this end, they require that memory devices be implemented in them through sequential circuits. Convolutional codes are broadly classified as systematic or non-systematic. Systematic codes provide the exact input data bits and the parity bits at their outputs while non-systematic provide only the latter. The codes are further classified as recursive and non-recursive with recursive encoders implementing a form of feedback at their inputs while the non-recursive encoders do not. Recursive systematic encoders (RSC) offer significant advantages that make them attractive in implementing turbo codes. Convolutional codes are described in terms of their rate R which is a ratio of the number of input bits k to output bits n and are said to be of order m, the number of memory devices. They are represented in terms of these parameters as $(\mathrm{n}, \mathrm{k}, \mathrm{m})$ codes and are also described in terms of their generator polynomials, G. For a rate $1/2$ recursive encoder with generator polynomials $\mathrm{g}_1(\mathrm{D})$ and $\mathrm{g}_2(\mathrm{D})$ respectively;

$$\mathbf{G}_{\mathrm{R}} = \begin{bmatrix} 1 & \frac{\mathrm{g}_2(\mathrm{D})}{\mathrm{g}_1(\mathrm{D})} \end{bmatrix} \qquad [1.1]$$

Thus, for an input sequence $\mathbf{U}(\mathrm{D})$ and output sequence $\mathbf{V}(\mathrm{D})$ the relationship below holds.

$$\mathbf{V}(\mathrm{D}) = \mathbf{U}(\mathrm{D}).\mathbf{G}(\mathrm{D}) \qquad [1.2]$$

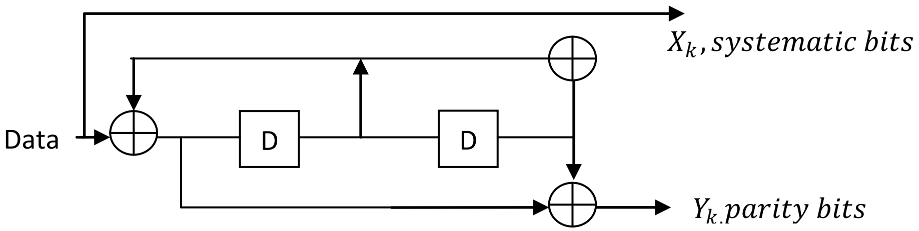


Figure 1: A rate $R = 1/2$, $G(D) = [1 \;\; 1+D^2/1+D+D^2]$ or [5 7] RSC encoder

Since the encoder has two memory devices, its registers can be represented by states of the order 2^2 at most. In binary terms, these are '00', '01', '10' and '11'. Figure 1.0 shows the state transitions for the encoder based on the received input bit- '0' or '1'.

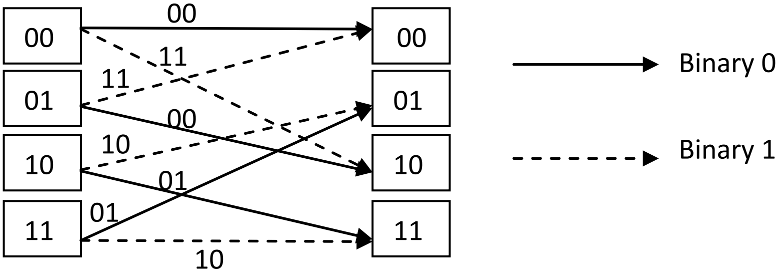


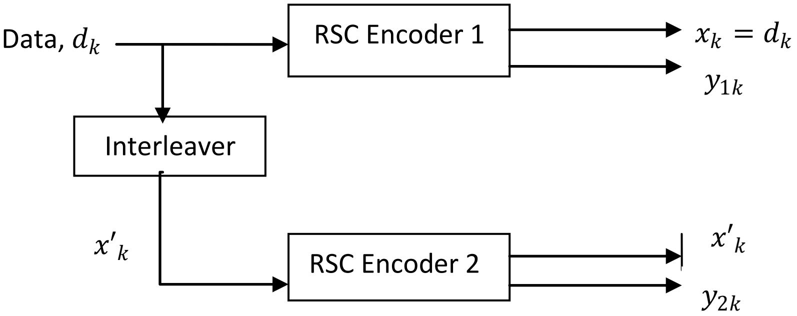
Figure 2: Trellis representation of state changes for the [5 7] encoder

From the trellis, it is seen that if a sequence '1 0 0 … ….' is encoded, the result is "110101………" (Assuming encoders start in the state '00').

2.2 Turbo coding

2.2.1 Turbo encoders

Figure 3 illustrates a basic turbo encoder. The information bit sequence d_k is fed into the first encoder (RSC 1) which provides x_k systematic bits and y_{1k} the parity bits at its output. The data sequence is simultaneously interleaved producing x'_k before being encoded by RSC 2. The output consists of its interleaved input $x'_k$and corresponding parity bits y_{2k}. The interleaved output of the second encoder is easily recovered by an interleaver located at the receiving side and so is not transmitted. The encoded sequence should be appropriately terminated to return the trellis to its starting state.



x_k- systematic data=d_k, information bits; y_{1k}-parity bits from encoder1
x'_k-interleaved information bits ; y_{2k}-parity bits from encoder 2

Figure 3: Turbo encoder

2.2.2 Interleaver

The interleaver produces a pseudo-random permutation of the input sequence which it feeds into the input of the second RSC encoder. An interleaver is also placed at the receiving side to recover the input sequence into the second encoder during decoding.

The device has a major influence on the overall weight (distance) spectrum of turbo codes generated and thus its BER performance especially when combined with the properties of the RSC encoder (Lin and Costello, 2004). They reduce the probability that data sequences which produce low weight codewords in the first encoder repeat same in the second. This reduces the number (multiplicity) of such codewords (i.e., with minimal Hamming distance) and thus the overall probability of errors. This phenomenon is described as spectral thinning and is further discussed in section 2.2.4.

2.2.3 Turbo decoding

Before fully describing the decoding process, an abridged version of the modified MAP algorithm used in turbo decoding is provided. The reader is referred to (Ryan,1997) for further details.

Let u_k=encoder input bit at time instant k ; y = noisy received codeword ; $S^{+,-}$ = set of ordered pairs (s',s) corresponding to transitions from state s' to s at time $k-1$ and k respectively, $+,-$ correspond to $u_k = +1, -1$ respectively; N= length of information block and subscripts s, p represent signal and parity bits respectively.

The algorithm minimizes the probability of bit errors by making passes in both the forward and backward directions of the trellis. The log likelihood ratio is defined as:

$$L(u_k) \triangleq \log(P(u_k = +1|y)/P(u_k = -1|y)) \qquad [1.3]$$

and the decision, $\hat{u}_k = \mathrm{sgn}[L(u_k)]$ [1.4]

Incorporating the trellis,

$$L(u_k) \triangleq \frac{\log(\sum_{S^+} P(s_{k-1}=s', s_k=s, y)/P(y))}{\log(\sum_{S^-} P(s_{k-1}=s', s_k=s, y)/P(y))} \quad [1.5]$$

where

$$P(s', s, y) = \alpha_{k-1}(s').\gamma_k(s', s).\,\beta_k(s) \quad [1.6]$$

$$\alpha_k(s) = \sum_{s' \in S} \alpha_{k-1}(s').\,\gamma_k(s', s) \quad [1.7]$$

$$\beta_k(s') = \sum_{s' \in S} \beta_k(s).\,\gamma_k(s', s) \quad [1.8]$$

$$\gamma_k(s', s) \triangleq P(s_k = s, y_k | s_{k-1} = s') \quad [1.9]$$

The modified MAP algorithm becomes:

$$L(u_k) = \log\left(\frac{\sum_{S^+} \alpha_{k-1}(s').\gamma_k(s', s).\beta_k(s)}{\sum_{S^-} \alpha_{k-1}(s').\gamma_k(s', s).\beta_k(s)}\right)$$

[2.0]

Further modifications are required for the exchange of extrinsic information. Re-writing [1.2] yields:

$$L(u_k) = \log\left(\frac{P(y|u_k=+1)}{P(y|u_k=-1)}\right) + \log\left(\frac{P(u_k=+1)}{P(u_k=-1)}\right)$$

[2.1]

The second term is the extrinsic or a priori probability, L_{ext}. The state transition probability, $\gamma_k(s', s)$ becomes:

$$\gamma_k(s', s) = P(s|s').\,P(y_k|s', s)$$

$$= P(u_k)P(y_k|s', s) \quad [2.2]$$

where

$$P(u_k)\ \alpha\ \exp[u_k L_{ext}(u_k)/2] \quad [2.3]$$

$$P(y_k|u_k)\ \alpha\ \exp\left[\left(y_k^s u_k + y_k^p x_k^p\right)/\sigma^2\right] \quad [2.4]$$

and the definitions below hold: $\sigma^2 = N_o/2rE_b$, the channel information $L_c \triangleq 4E_b R/N_o$ and $\gamma_k^{ext}(s', s) \triangleq \exp\ [\frac{1}{2} L_c y_k^p x_k^p]$. [1.9] becomes:

$$\gamma_k(s', s) = \exp[u_k L_{ext}(u_k)/2].\,\exp\left[\left(y_k^s u_k + y_k^p x_k^p\right)/\sigma^2\right] \quad [2.5]$$

Substituting [2.2] in [1.7] yields:

$$L(u_k) = L_c y_k^s + L_{a\,priori}(u_k) + \log\left(\frac{\sum_{S^+} \alpha_{k-1}(s').\gamma_k^{ext}(s',s).\beta_k(s)}{\sum_{S^-} \alpha_{k-1}(s').\gamma_k^{ext}(s',s).\beta_k(s)}\right)$$

$$L(u_k) = L_c y_k^s + L_{a\,priori}(u_k) + L_{ext}(u_k) \qquad [2.6]$$

The extrinsic information used in iterative decoding can thus be estimated from equation [2.6].

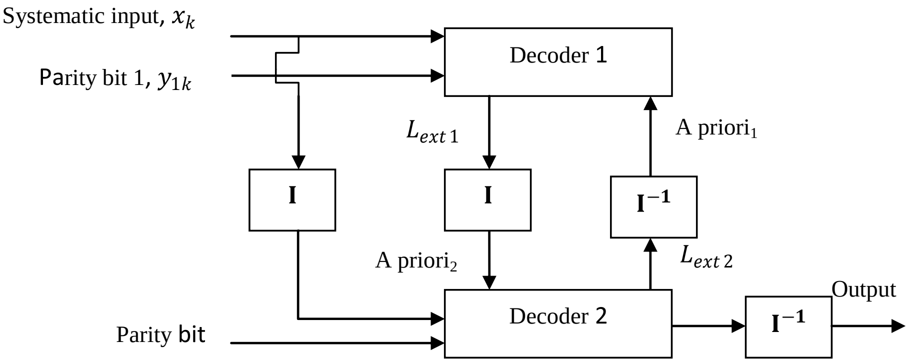


Figure 4: Schematic diagram of a turbo decoder

Turbo decoders are composed of two serially concatenated soft-in soft-out decoders. In the course of iterative decoding, each decoder exchanges reliability information with the other decoder after estimating the received data sequence using the MAP algorithm. The exchanged information is described as extrinsic because it is not part of the received data. Rather, it is produced locally at the decoders and is numerically equal to the subtraction of the “effect” the information bits and extrinsic information received from the other decoder from the estimated log-likelihood ratio of the working decoder. It is thus an independent estimate of the information bit sequence received at the decoder. By exchanging extrinsic values, successive estimates of the information bit sequence are better informed and the independently estimated extrinsic values from both decoders converge. A final estimate of the information bits can be taken. The decoding process is described in outline below:

1. The received values are scaled according to the channel parameters
2. The received systemic bits are passed to the first decoder while an interleaved version is passed to the second. Corresponding parity bits are also passed to the decoders .
3. The a priori probabilities are initialized to 0.5 (equal expectations)
4. Decoder 1 produces its extrinsic and a posteriori probabilities based on the a priori information
5. The interleaved extrinsic probabilities are passed to the second decoder as a priori information which produces its extrinsic and a posteriori probabilities based on the a priori information

6. The extrinsic information (de-interleaved) is passed to the first decoder as a priori information.
7. Repeat step (4) for a defined number of iterations
8. The a posteriori values from the second decoder (de-interleaved) are threshold detected producing a final estimate of the decoded information sequence

2.2.4 Performance of turbo codes

Two factors are responsible for the exceptional performance of turbo codes: the convergence of the iterative decoding process, which as been described above and the structure of the codes. The combination of RSC encoders and pseudo-random interleavers achieves a random codeword weight structure similar to the binomial distribution. This process is called spectral thinning and is advantageous as it reduces the multiplicity of codewords with low weights thereby reducing the probability of error (Lin and Costello, 2004).

An important measure of the error correction probability of any code is its minimum Hamming distance. Turbo codes are characterized by low Hamming distances (Perez et al, 1996) which limits their ability to achieve very low BERs. Rather, they exhibit error floors which are approximations of their performance curves to the free distance asymptotes which are essentially flat curves.

3 Results and discussions

The BER and FER performances of turbo encoders (overall rate, 1/3) with component rate ½, [5 7] and [15 13] RSC encoders were separately simulated using MATLAB®. The results obtained were further subjected to direct comparison and analysed. For both codes, simulations were based on the following parameters: block size of 200 bits, signal to noise ratios (0-5/dB) and a pseudo-random interleaver of length N=200. The terminating criterion was set at a minimum of 10 error frames/iteration for each SNR. Thus, simulations were effectively terminated when the last iteration of interest has more than 10 frames in error. An Additive White Gaussian Noise (AWGN) Channel was assumed in the simulations. Similar conditions were used in simulating the performance of the [15 13] turbo code. In this case, 15 iterations were considered. The BER performance of both codes are also directly compared and analysed.

The BER performance of the [5 7] turbo codes show an improvement with increasing number of iterations. A small BER,10^{-5}, was achieved at a low value of E_b/N_o , 2.5dB. The error floor phenomenon is also evident at BERs lower than 10^{-5}. The FER performance returned similar results as the performance improved with increasing number of iterations.

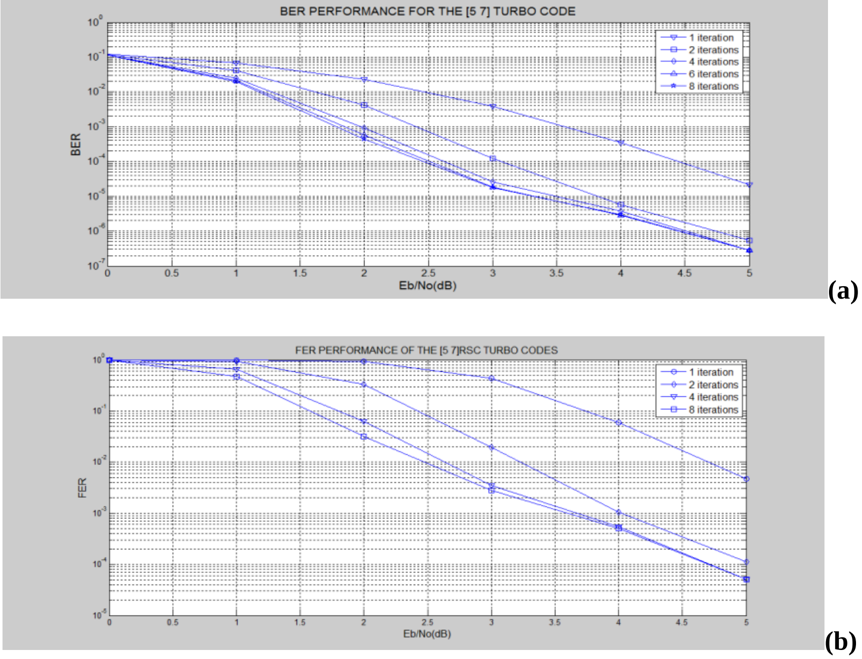


Figure 5a,b: BER and FER performance of the [5 7] turbo code

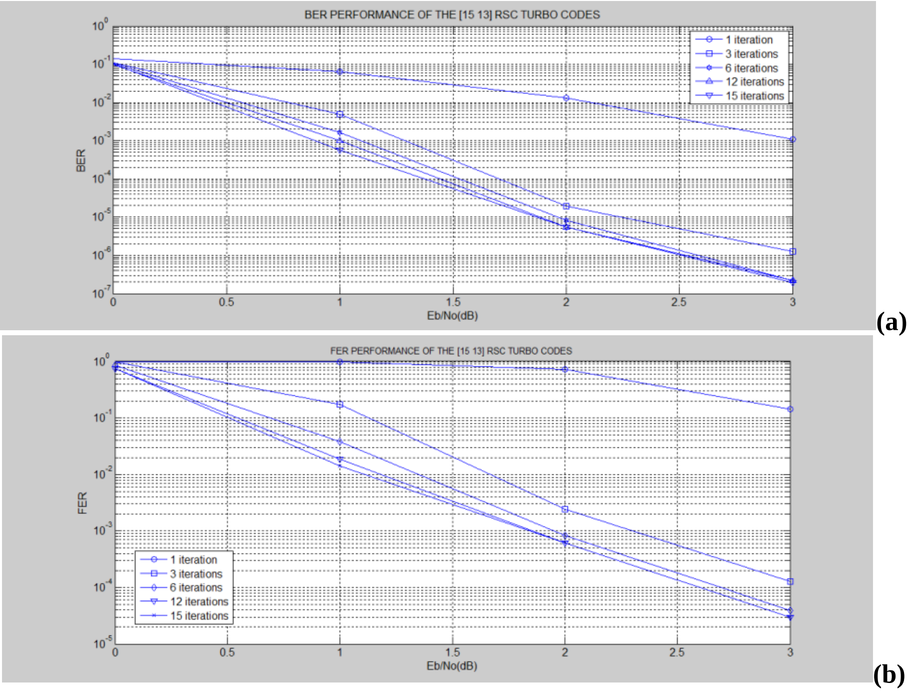


Figure 6a,b: BER and FER performance of the [15 13] turbo codes

The BER and FER performance of the [15 13] codes also improve with successive iterations. Low BERs of 10^{-7} and FER of 10^{-5} are achieved at low E_b/N_o of approximately 3dB. The FER also begins with a probability of 1 at $E_b/N_o = 0$ dB since it is almost certain that at least 1 bit would be in error at low values of E_b/N_o.

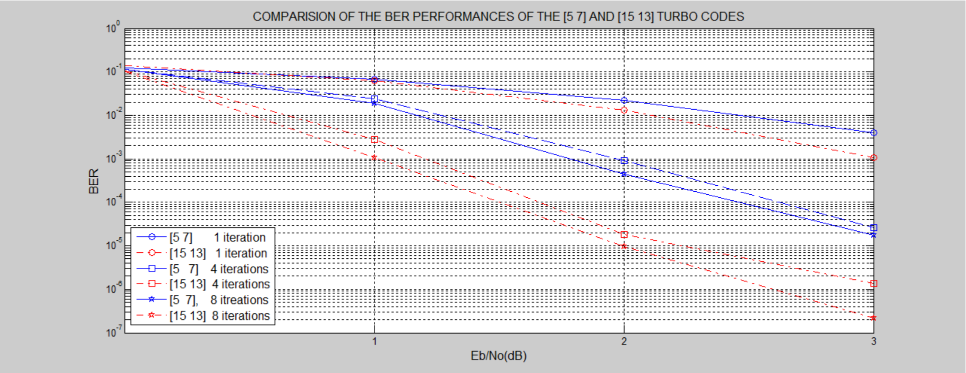


Figure 7: Direct comparison of the [5 7] and [15 13] BER performance of turbo codes

From Figure 7, it is seen that the [15 13] turbo code outperforms the [5 7] turbo code. Both simulations were carried out with similar parameters save for the encoder structure and the difference in performance lies therein. The free distance of the [15 13] encoder is 14 while that of the [5 7] is 10. Since the error correcting ability of turbo codes is directly proportional to the free distance (all other factors kept constant), the superior performance of the [15 13] codes is not difficult to conceive.

4 Conclusion

BER and FER performances for the [5 7] and [15 13] turbo codes were simulated and the improvements accruable form iterative decoding were demonstrated. The error floor phenomenon in turbo codes was illustrated for moderate to high signal to noise ratios. The dependence of the error correcting ability of turbo codes on the effective free distance was also shown by comparing those of the [15 13] and [5 7]. The [15 13] codes with a larger free distance out performed the [5 7] codes.

5 References

Abu-Rgheff M. (2007) Introduction to CDMA Wireless Communications, Elsevier, Oxford

Berrou, C., Glavieux, A. and Thitimajshima, P. (1993) "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," *IEEE International Conference on Communication, ICC, Geneva,* vol.2 pp 1064-1070

Berrou C. (2003) 'The Ten-Year-Old Turbo Codes are Entering into Service', *IEEE Communications Magazine*, pp. 110-116

Gracie, K. and Hamon, M.-H. (2007) "Turbo and Turbo-Like Codes: Principles and Applications in Telecommunications," *Proceedings of the IEEE*, vol.95, no.6, pp.1228-1254

Lin S. and Costello D. J., Jr. (2004) Error Control Coding, Prentice-Hall, New Jersey

Perez, L.C., Seghers, J. and Costello, D.J., Jr. (1996), "A distance spectrum interpretation of turbo codes" *IEEE Transactions on Information Theory*, vol.42, no.6, pp.1698-1709

Ryan, W. (1997) A turbo code tutorial [Online]: www.cs.tut.fi/~tlt5906/TurboRyan.pdf. Accessed (15-12-2009)

Shannon C. E. (1948) ‘A Mathematical Theory of Communication’ *Bell System Technology Journal*, 27, pp. 379-423

On Trellis Structure of Error Correction Coding

S.K.Thomas and M.A.Ambroze

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The major objective of all communication techniques is accomplishing the fastest way of data transmission through a communication channel, i.e. trying to reach the Shannon’s Channel Limit. One of the solutions to these developments is error correction coding technique which is currently employed in broadband satellite communication and data storage. Constructing a Trellis, which is the graphical representation of the code; reduces the decoding complexity, thereby improves transmission efficiency. This project will investigate the way trellises are constructed for different types of codes, mainly linear block codes and how they are used to correct errors on transmission channels.

The project involves in the study of the trellis diagrams for both the convolutional and block codes; and focuses on the encoding and decoding of linear block codes using the trellis diagram. The implementation of the trellis diagram of the Hamming code for both the encoding and decoding process has been done using the MATLAB software. The code has been tested for various codewords and the results are collated in tables.

Keywords

Error Correction codes, Trellis representation, Convolutional coding, Linear Block codes, Hamming code, Hard decision Viterbi decoding, Soft Decision Viterbi Decoding

1 Introduction

A basic block diagram of a communication system is illustrated below. The information source can be either analog source or digital source. The analog source of information needs to be converted to digital bits for efficient transmission and this can be done using a sampler and analog to digital converter. In order to represent the digital information using the smallest number of bits, techniques such as removal of redundancy is used. The conversion of analog data into digital information efficiently is broadly classified as source coding. The channel encoder prepares the data from the source encoder for digital modulation and efficient transmission. The modulator matches the output of the channel encoder to the transmission channel. In the receiver section, the vice versa is performed to the received data to obtain the original data with minimum errors (Michelson and Levesque, 1985).

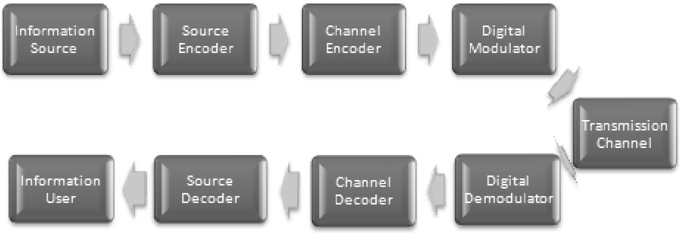


Figure 1: Block Diagram of a Digital Communication System (Michelson and Levesque, 1985)

The concept of error correction coding was introduced to minimise the errors occurring during the transmission of data and to recover the original data with minimum errors. In order to transmit information reliably, the information rate must be less than the channel capacity, and this was stated by Shannon's noisy coding theorem. It states that " It is theoretically possible to transmit information through a noisy channel with arbitrarily small probability of error provided that the information or source rate, R, is less than the channel capacity, that is R<C for reliable transmission"(Wade, 2000).

Error control coding is a practical method of achieving very low bit error rate after transmission over a noisy, band limited channel. An overview of error correction coding can be obtained in the following section.

2 Convolutional Codes

Convolutional coding is a method of channel coding where the check bits are periodically inserted in a continuous data stream.

2.1 Classifications:

Recursive Encoders – In this encoder, the memory bits gets added up and is connected with a feedback root.

Non – Recursive Encoders – In this encoder, the memory bits are added up without any feedback.

Systematic Encoder – A systematic code is one in which the original information bits can be identified.

Non – Systematic Encoder – In these codes, the information bits cannot be identified properly (Sankar, 2009).

Figure below shows a simple convolutional encoder. The information bits are passed into the encoder in small groups of k-bits at a time. The output bits are obtained by performing modulo 2 addition (Exclusive OR operation) on the information bits and also the previous inputs.

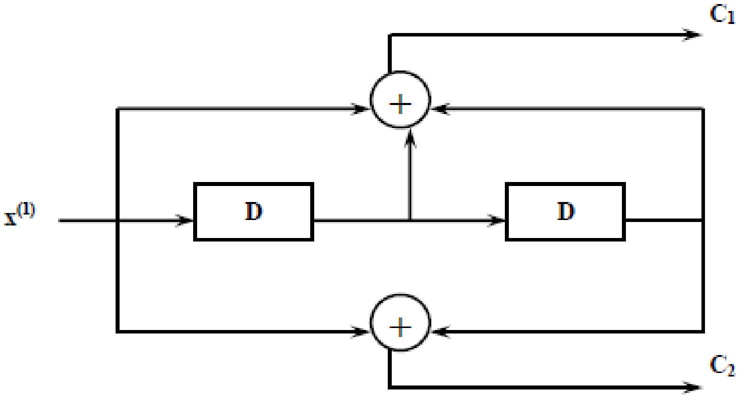


Figure 2: Convolutional Encoder with k=1, n=2 and r=1/2

The code rate R is expressed as R = k/n if the output of the encoder is n bits for every k input bits. In Figure, the value of k and n are 1 and 2 respectively. The constraint length of the code K is defined as the number of output bits affected for each information bit inputted into the encoder. In the above example, the value of K is 3.

All the shift registers are refreshed to a value of 0 before the encoding operation begins. For an input sequence of 01011, the encoded output will be 00 11 10 00 01(IIT, 2010).

3 Block Codes

Block code is the basic type of channel coding in which it adds redundancy to the message so that at the receiver end the decoding is done with minimal errors provided the information rate do not exceed the channel capacity. It contains a set of fixed-length vectors called code words. The main characteristic of block code unlike Huffman coding or Convolutional coding is that it is fixed length code words (Wade, 2000).

The block code has a set of fixed length vectors called code words whose length (n) is the number of elements in the vector. For a code word the elements are selected from an alphabet of q elements. If the alphabet has two elements 0 and 1, then it is a binary code and the elements are called bits. If the elements of a code are selected from an alphabet having q elements and if q>2 then the code is non binary. When q is a power of 2 i.e. q=2b (b is a positive integer), each of the q-ary element has got an equivalent binary representation which consists of b bits. Thus a non binary code having a block length N can be mapped into a binary code having a block length n=bN.

For a binary code of length n there are 2^n possible code words. From these code words we select M= 2^k code words in order to form a code. Thus we can say that a block of k information bits is mapped into a code word of length n which is in turn selected from a set of 2^k code words. The resulting block code is referred as an (n, k) code. The ratio k/n=RC can be defined as the rate of the code. The code rate parameter RC is simply the weight of the code word i.e. the number of non zero elements that it contains. Each code word has got its own weight and for a code the set of all weights constitutes the weight distribution. If all the M code words have equal weight then the code is considered as a fixed weight code or a constant weight code (Proakis, 2000).

For a digital communication we mostly use 0 and 1, the addition and multiplication is as shown below.

0+0= 0	0.0= 0
0+1= 1	0.1= 0
1+0= 1	1.0= 0
1+1= 0	1.1= 1

The multiplication and addition shown above are known as modulo-2 addition or multiplication and we can say that it is almost same as the ordinary arithmetic in which 2 is equal to 0. The symbols used here i.e. 0 and 1 along with the modulo-2 addition and multiplication can be termed as the field (binary field) of two elements. This is usually represented as GF (2) (Lin, 1970).

3.1 Hamming codes

Hamming codes have both binary and non binary properties but we consider only the binary properties. Binary hamming codes comprise a class of codes which follows the property

$$(n, k) = (2m - 1, 2m - 1\text{-}m)$$

Where

m= is any positive integer (i.e. if m=3 then we have (7, 4) code).

The parity check matrix H of the hamming code has a particular property. We have already mentioned in the previous section about the rows and columns of an (n, k) code, i.e. there are n- k rows and n columns for a (n, k) code. So when we consider a binary (n, k) hamming code the n= 2m- 1columns consists of every possible binary vectors with n- k =m elements and except all the zero vectors.

If we want to make a systematic hamming code the parity check matrix H can be arranged in the form below easily

$$H = [-P \vdots I_{n-k}]$$

From this the equivalent generator matrix G can also be obtained.

No two columns of the parity check matrix are linearly dependant or otherwise the two columns will be exactly the same or identical. But we can assume that if m>1, we can find three columns of the parity check matrix which adds to zero. So the minimum distance d_{min} will be equal to 3 for an (n, k) hamming code. A hamming code may also be shortened i.e. it can be made as (n-l, k-l). This is done by removing l rows from the generator matrix or by removing l columns from the parity check matrix.

Hamming distance is the count of the number of places in which each codeword differs from the hard decided received vector. The minimum distance dmin of a code is defined as the minimum Hamming distance between any two codewords of the code.

For any code with the minimum Hamming distance dmin, the number of errors that the code can detect is dmin – 1 and the number of errors it can detect is $\frac{d_{min}-1}{2}$.

For Hamming codes, the minimum Hamming distance dmin = 3 and therefore, it can detect 2 errors and correct 1 error.

In order to correct an error pattern, the receiver calculates the product:

$$S = Hr'$$

where r = c + e is the received vector and e is the error pattern. The value S is called the syndrome of the error and it is 0 if e = 0. If the value of S is a non-zero value, it shows that an error has occurred in the channel and e ≠ 0. In general case, S is a column vector with N – K rows, corresponding to the N – K parity check equations of the code and it can take $2^{N-K} - 1$ non-zero values. If a code can correct t errors, then it has to have enough distinct syndromes to uniquely identify all possible error patterns of up to t errors (Ambroze, 2007).

The Hamming bound or Sphere packing bound for hard decision decoding is defined as:

$$\sum_{i=1}^{t} \binom{N}{i} \leq 2^{N-K} - 1$$

The error correction codes that satisfy this equation with equality are known as perfect codes.

For Hamming codes, dmin = 3, the number of errors it can correct t:

$$t = \frac{d_{min} - 1}{2} = \frac{3 - 1}{2} = 1$$

Let us consider the (7, 4) Hamming code for example where N = 7 and K = 4.

We have,

$$\sum_{i=1}^{t} \binom{N}{i} \leq 2^{N-K} - 1$$

$$\textstyle\sum_{i=1}^{t} \binom{N}{i} = \binom{7}{1} = 7 \text{ and}$$

$$2^{N-K} - 1 = 2^{7-4} - 1 = 7$$

Since both sides of the sphere packing bound equation are equal, it can be seen clearly that the Hamming codes are perfect codes and it can correct 1 error.

3.2 Trellis for Linear Block Codes

Let the non zero code word c= (c1... cn) explains the start of c and is denoted as start (c), the smallest integer for i in the condition ci is non zero. Similarly let the non zero code word c= (c1....cn) explains the end of c and is denoted as end (c), the largest integer for i in the condition ci is non zero. Then the span of c or the support interval of c can be defined as the interval [start (c), end (c)] where the span or the support interval of the zero word 0 is an empty interval as [ ]. The span length of c can be defined by the following equation and it is defined as the cardinality of its span.

L(c) = end (c) – start (c) +1

Where

L (0) =0

The method proposed by Wolf (Wolf, 1978) needs parity check matrix H = (h1 h2... hn). Here hi where i can be assigned values 1, 2 ...n and is the ith column of the parity check matrix which has got n-k elements for GF (2). Trellis is an easy way to represent the 2k code words and it has got n+1 set of nodes and each set has got 2n-k nodes. Now in order for the ease of explanation let us consider i as the sets where i= 0, 1... n. The nodes in any set will also consist of another parameter j where j= 0, 1 ... 2n-k-1 and so we can say that the jth node in the ith set has got an index which is expressed as (j, i). The nodes are connected with branches in a certain manner and also uniquely defined by H, we can say that a trellis is formed. The steps for the procedure are explained below.

- For the set i=0, the branches originate only from the node (0, 0) and there will be two branches. One branch with weight 0 and the other with weight 1. The branch which has got the weight 0 will enter the node (0, 1). And the branch with weight which is equal to 1 will only enter the node (b, 1). ‘b’ is the transpose of the vector h1 is actually the decimal equivalent of the binary number.

- For any other node (j, i) where $i > 0$, which has got incoming branches and also branches are with weight 0 and 1. The destination nodes are determined using the steps shown below.
    - ➢ Calculate x, in which x is the binary equivalent of the decimal number represented by j which is mentioned above.
    - ➢ Now calculate the binary number y= ti+1⊕x. Here ti+1 is a binary number which is shown as the transpose of the vector hi+1.
    - ➢ Now consider z as the decimal equivalent of y.
    - ➢ For the branch with weight 0 the destination node in set i+1 is node (j, i+1)
    - ➢ And for the branch with weight 1 the destination node in se i+1 is node (z, i+1).
- Now repeat the second step again and again for i = 1, 2 ... n-1. By following this procedure a trellis with more paths than the code words will be generated. Now remove all the paths (known as expurgation) which do not end in node (0, n). Thus the remaining will be the 2k unique paths which indicate all the code words in the block code (Buttner et al., 1998).

3.3 Viterbi decoding using trellis

We already know that each branch of a trellis represents a bit in the valid code word. So we can say that the most likely path can be found out by comparing each of the incoming bit or a sample of the received vector (which is called as hard decision and soft decision respectively) with the branch weights. Assume that there are n received symbols for a code word and also they are statistically independent. Therefore the probability of the received sample/bit when compared with the branch weight which is called as a metric can be explained as shown below.

$$Z\ (yi,\ w(x,i),(z,i+1)\ ) = \log\ (p(yi|w(x,\ i),\ (z,\ i+1)))$$

Where, w(x,i),(z,i+1) = weight of the branch from the node (x, i) to (z, i+1) and

yi = ith sample/ bit which is received. When we consider the hard decision implementation the probability of making an error is as shown below.

$$Z\ (yi,\ w(x,i),(z,i+1)\ ) = \begin{bmatrix} \log(1-p) & y_i = w(x,i),(z,i+1) \\ \log(p) & y_i \neq w(x,i),(z,i+1) \end{bmatrix}$$

When input samples/bits are being received corresponding cumulative metrics are being calculated which indicates the most favourable paths. The following rules are been used when Viterbi algorithm is applied to the trellis for decoding.

- Assign zero to the cumulative metric CM00 at node (0, 0).
- For every node in set i+1 which has got atleast one incoming branch we have to calculate one or more metrics. The following computations are to be done depending on the number of branches entering.
    - ➢ M0 = CMji + Z (yi, 0)

  Where CMji is the cumulative metric at node (j, i) and this metric has to be calculated only if a 0-weight branch enters the node.

  - M1 = CMji + Z (yi, 1)
    Where CMji is the cumulative metric at node (j, i) and this metric has to be calculated only if a 1-weight branch enters the node.

- For the node (j, i+1) the cumulative metric at that node is assigned to CMj (i+1) = min (M0, M1). When we take the case of two identical metrics one of them is chosen randomly as the survivor. When only one metric is calculated for a particular node then the cumulative metrics will assume that metrics value. This means in this case CMj (i+1) = M0 or CMj (i+1) = M1. When two branches enter a node in set i+1 one of them will be removed. The one that is most likely to be removed is the branch that has the larger metrics.

- Repeat the above steps for i= 0, 1... n-1 times. When this is done we should get only one path which starts from node (0, 0) and ends in (0, n). Thus the most likely code word can be found out by noting the weights of the branches in the path obtained by following the above steps (Buttner et al., 1998).

4 Result

Let us consider the G matrix: $G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$

For this G matrix, the trellis diagram after encoding is shown below:

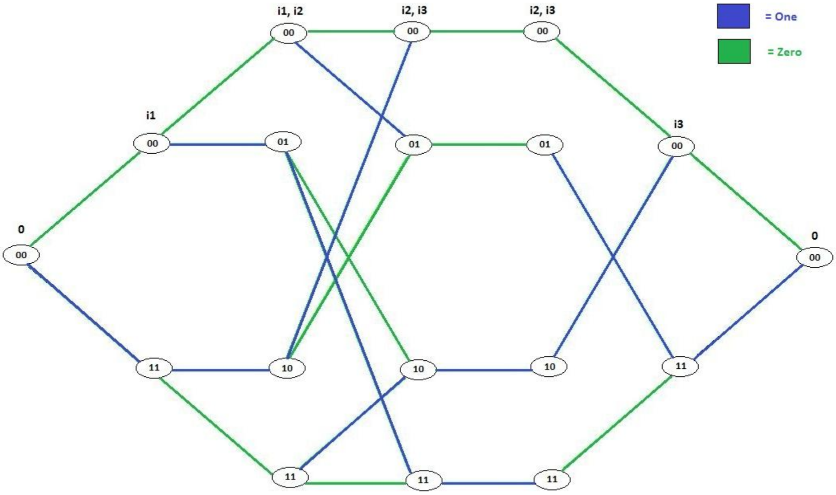


Figure 3: Trellis Diagram

4.1 Hard Decision Decoding

The decoding process for each codeword is done as explained in the previous chapter. The results for hard decision decoding are collated in the tables below.

Received Codeword without errors																		
No.	**Transmitted Codeword**						**Received Codeword**						**Decoded Codeword**					
1	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0
2	0	1	0	1	1	0	0	1	0	1	1	0	0	1	0	1	1	0
3	0	0	1	0	1	1	0	0	1	0	1	1	0	0	1	0	1	1

Table 1: Received codewords without errors for hard decision decoding

Received Codeword with 1 bit error																		
No.	**Transmitted Codeword**						**Received Codeword**						**Decoded Codeword**					
1	1	1	1	0	0	0	1	1	**0**	0	0	0	1	1	1	0	0	0
2	1	1	1	0	0	0	1	**0**	1	0	0	0	1	1	1	0	0	0
3	1	1	1	0	0	0	1	1	1	0	**1**	0	1	1	1	0	0	0
4	1	1	1	0	0	0	**0**	1	1	0	0	0	1	1	1	0	0	0
5	0	1	0	1	1	0	0	**0**	0	1	1	0	0	1	0	1	1	0
6	0	1	0	1	1	0	0	1	0	**0**	1	0	0	1	0	1	1	0
7	0	1	0	1	1	0	0	1	0	1	1	**1**	0	1	0	1	1	0
8	0	1	0	1	1	0	0	1	0	1	**0**	0	0	1	0	1	1	0
9	0	0	1	0	1	1	0	0	1	**1**	1	1	0	0	1	0	1	1
10	0	0	1	0	1	1	0	**1**	1	0	1	1	0	0	1	0	1	1
11	0	0	1	0	1	1	**1**	0	1	0	1	1	0	0	1	0	1	1
12	0	0	1	0	1	1	0	0	**0**	0	1	1	0	0	1	0	1	1

Table 2: Received codewords with 1 error for hard decision decoding

Received Codeword with 2 bit errors																		
No.	**Transmitted Codeword**						**Received Codeword**						**Decoded Codeword**					
1	1	1	1	0	0	0	1	1	**0**	**1**	0	0	1	1	1	0	0	0
2	1	1	1	0	0	0	1	**0**	**0**	0	0	0	0	0	0	0	0	0
3	1	1	1	0	0	0	1	1	1	0	**1**	**1**	1	1	0	0	1	1
4	0	1	0	1	1	0	0	**0**	**1**	1	1	0	1	0	1	1	1	0
5	0	1	0	1	1	0	0	1	0	**0**	**0**	0	0	0	0	0	0	0
6	0	1	0	1	1	0	**1**	1	0	1	1	**1**	1	1	0	0	1	1
7	0	0	1	0	1	1	**1**	0	1	**1**	1	1	1	0	1	1	1	0
8	0	0	1	0	1	1	0	**1**	1	**1**	1	1	0	1	1	1	0	1
9	0	0	1	0	1	1	**1**	0	**0**	0	1	1	1	1	0	0	1	1

Table 3: Received codewords with 2 errors for hard decision decoding

From the above results, it is clear that the decoder implemented in the MATLAB software works perfectly for codewords received without any error and for codewords which have 1 bit error. It cannot correct codewords with errors in two bit locations. As explained, it proves that the Hamming code corrects 1 bit error in the received codeword.

4.2 Soft Decision Decoding

Now, for the same G matrix, let us verify the results using soft decision decoding for the same set of codewords.

Received Codeword without errors																		
No.	**Transmitted Codeword**						**Received Codeword**						**Decoded Codeword**					
1	1	1	1	0	0	0	0.528	0.765	0.664	-0.26	-1.19	-0.76	1	1	1	0	0	0
2	0	1	0	1	1	0	-1.06	1.281	-1.24	0.557	0.55	-0.85	0	1	0	1	1	0
3	0	0	1	0	1	1	-1.06	-1.06	1.449	-0.91	1.063	1.502	0	0	1	0	1	1

Table 4: Received codewords without errors for soft decision decoding

Received Codeword with 1 bit error																		
No.	**Transmitted Codeword**						**Received Codeword**						**Decoded Codeword**					
1	1	1	1	0	0	0	0.746	1.22	**-0.74**	-1.08	-0.93	-1.37	1	1	1	0	0	0
2	1	1	1	0	0	0	1.304	**-0.96**	1.454	-1.62	-1.06	-1.38	1	1	1	0	0	0
3	1	1	1	0	0	0	0.974	0.389	0.861	-1.57	**1.266**	-1.28	1	1	1	0	0	0
4	1	1	1	0	0	0	**-0.46**	0.939	0.324	-1.27	-0.57	-1.34	1	1	1	0	0	0
5	0	1	0	1	1	0	-1.5	**-0.84**	-0.91	1.011	0.578	-0.64	0	1	0	1	1	0
6	0	1	0	1	1	0	-0.89	0.905	-0.99	**-1.08**	0.447	-1.09	0	1	0	1	1	0
7	0	1	0	1	1	0	-1.26	0.69	-1.37	0.831	0.367	**1.305**	0	1	0	1	1	0
8	0	1	0	1	1	0	-0.84	0.994	-1.01	0.748	**-0.68**	-1.04	0	1	0	1	1	0
9	0	0	1	0	1	1	-1.23	-0.57	0.929	**0.814**	0.907	0.732	0	0	1	0	1	1
10	0	0	1	0	1	1	-1.43	**1.144**	0.732	-1.11	1.175	1.329	0	0	1	0	1	1
11	0	0	1	0	1	1	**0.904**	-0.99	1.016	-0.74	1.483	1.148	0	0	1	0	1	1
12	0	0	1	0	1	1	-1.07	-0.8	**-0.94**	-1.33	1.3	1.097	0	0	1	0	1	1

Table 5: Received codewords with 1 error for soft decision decoding

Received Codeword with 2 bit errors																		
No.	**Transmitted Codeword**						**Received Codeword**						**Decoded Codeword**					
1	1	1	1	0	0	0	1.043	1.163	**-0.92**	**0.702**	-1.05	-1.05	1	1	1	0	0	0
2	1	1	1	0	0	0	0.939	**-1.09**	**-0.52**	-1.08	-1.34	-0.49	0	0	0	0	0	0
3	1	1	1	0	0	0	1.39	0.927	0.524	-1.14	**0.951**	**1.087**	1	1	0	0	1	1
4	0	1	0	1	1	0	-1.16	**-1.1**	**1.004**	0.042	0.855	-0.61	0	0	1	0	1	1
5	0	1	0	1	1	0	-1.34	1.295	-0.89	**-1.01**	**-0.94**	-1.49	0	0	0	0	0	0
6	0	1	0	1	1	0	**0.973**	1.507	-0.97	1.013	0.768	**0.99**	1	1	0	0	1	1
7	0	0	1	0	1	1	**1.073**	-0.87	0.882	**0.925**	1.64	0.286	1	0	1	1	1	0
8	0	0	1	0	1	1	-0.29	**1.107**	1.316	**0.474**	0.813	0.912	0	1	1	1	0	1
9	0	0	1	0	1	1	**1.103**	-0.66	**-0.68**	-1.21	1.081	0.701	1	1	0	0	1	1

Table 62: Received codewords with 2 errors for soft decision decoding

5 Conclusion

This project involves in the brief study of error correction coding. Also, a detailed study of convolutional coding and block codes has been covered with more emphasis on linear block codes. A software implementation of the encoding and decoding of the shortened (7, 4) Hamming code has been completed in MATLAB. The code has been tested with various input codeword inputs to the decoder and the results have been summarized in the previous chapter. The software implementation includes both the soft decision decoding and hard decision decoding of the receiver output and the Viterbi decoding algorithm is applied to get the output of the decoder.

6 Reference

Buttner, W. H., Staphorst, L. & Linde, L. P. (1998) Trellis decoding of linear block codes. *In:* Communications and Signal Processing, 1998. COMSIG '98. Proceedings of the 1998 South African Symposium on, 1998. 171-174.

Lin, S. 1970. *An Introduction to Error-Correcting Codes,* New Jersey, Prentice Hall.

Lin, S. & Costello, D. J. 2004. *Error Control Coding, Second Edition*, Prentice-Hall, Inc.

Michelson, A. M. & Levesque, A. H. 1985. *Error control techniques for digital communication*, Wiley – Interscience.

Proakis, J. 2000. *Digital Communications*, McGraw-Hill International.

Wade, G. 2000. *Coding Techniques: An Introduction to Compression and Error Control*, Palgrave Macmillan.

Wolf, J. 1978. Efficient maximum likelihood decoding of linear block codes using a trellis. *Information Theory, IEEE Transactions on,* 24**,** 76-80.

Section 2

Computer and Information Security

Evading Intrusion Detection Systems

I.AlRobia and M.Papadaki

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Snort is a well-known open source Intrusion Detection System that can be used as a second line of defense in a network to detect any incoming attacks from any source (such as Nikto) and alert the network administrator about this attack. This research will test Snort's durability against Nikto's evasion attacks.

Keywords

Evading Intrusion Detection Systems (IDS), Evading Snort, Nikto anti-IDS Evasion Techniques.

1 Introduction

Computer Systems and Networks suffer from complex security threats that arise and grow rapidly along with new computer and network technologies. IT mangers and network administrators are trying to find solutions for new security threats that might arise in the future by any necessary means, such as deploying firewalls, antivirus programs, or any other defending devices. Kerry Cox and Christopher Greg states that in the old days a firewall was most of what an administrator needed to protect a network from attack. (Cox and Greg, 2004) However, it is not enough to focus our trust into firewalls and updated antivirus programs. A second line of defense must be implemented in order to ensure the 'Optimum' level of security. According to James Anderson, Intrusion Detection Systems (IDS) can be that second line of defense. (Anderson, 1980) Where firewalls act like locked doors and windows leading to your computer, intrusion detection systems act more like a burglar alarms to your computer. (Wang, 2003)It will alert you about different intrusions and attacks that have a probability of affecting your system. Additionally, the network administrator must know how to evade an IDS in order to defend it.

The role of an intrusion detection system is to identify and sometimes isolate intrusions against computer systems (Ptacek and Newsham, 1998). It is used as a second line of defence along with the firewall and any other component that can be used to secure the computer system and detect suspicious activities. It can provide detection and notifications for new attacks that have not been discovered by any other security component. Moreover, intrusion detection systems can provide forensic information that might allow administrators to discover the origins of an attack and capture those attackers (Ptacek and Newsham, 1998). However, it is a challenging task to detect these attacks, this is because that attackers tries to develop different evasion techniques in order to bypass the intrusion detection system. Therefore, an administrator has to update his security systems regularly and to be prepared for any suspicious events.

IDS have been one of the key countermeasures against network compromise however this is only if the IDS have been well-configured, they have to know how to select and configure intrusion detection systems for their specific computer system and network environments, and most importantly they have to know how to deal with the intrusion detection system's output and integrate it with the rest of the organization's infrastructure (Bace and Mell, 2001).

In the early generations, it is possible to say that early intrusion detection systems could be just like a tool that have been used to specify extended regular or hexadecimal expressions to match against data payloads of packets called 'ngrep' (Niphadkar, 2008). In other words, detection was heavily relying on the detection of character at the packet payload rather than using more sophisticated detection methods.

The purpose of this project is to investigate how resilient modern Intrusion Detection Systems are to traditional IDS evasion techniques. Apart from detection capability, another issue will be examined which is the performance cost of anti-evasion techniques.

This research will answer the following questions:

- Whether Snort has the capability to detect Nikto evasion techniques with default configurations?
- How well will Snort detect the incoming attacks in when the processing power is being shared by other applications?
- Will Nikto anti-IDS be able to evade Snort by using a Single technique? What about multiple techniques when combined together?
- If the detection was successful, what are the preprocessors used by Snort to detect Nikto evasion techniques?

2 Aims and Objectives of the research

The aims and objectives of this research are to:

- Demonstrate awareness of intrusion detection technologies as well as IDS evasion techniques.

- Design and implement experiments that will investigate the evasion resilience of Snort, an open source IDS tool, under different configurations

- Based on the results of the experiments, propose optimal configurations that help to tackle evasion tools.

3 Research Design

Since this research relays on several components and in order to localize any mistakes and avoid them, this research will divide the research design and setup into five parts and test them individually. These five parts are:

1. Setup and test VMware Workstation.
2. Setup Nikto anti-IDS scanner tool.
3. Setup and test Snort.
4. Test Snort in basic configuration with Nikto anti-IDS scanner tool.
5. Test Snort with configuring the preprocessors (such as frag3 preprocessor) with Nikto anti-IDS scanner tool.

After setting up and testing the mentioned parts the network topology should be like the following figure.

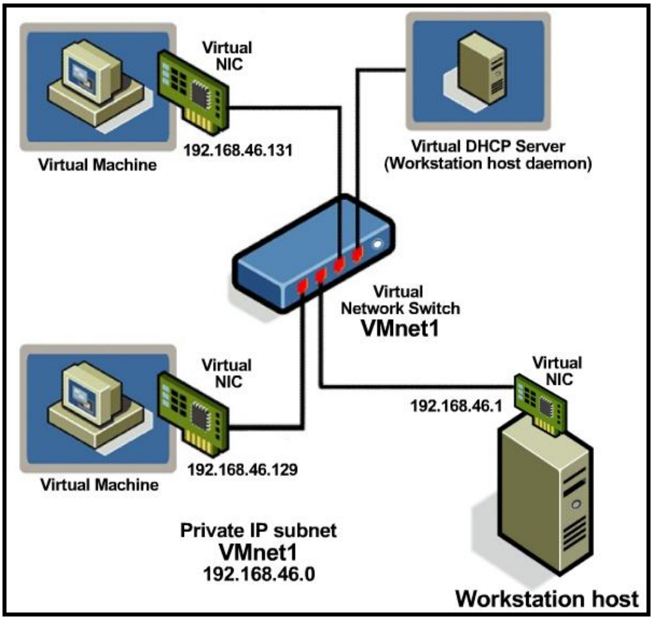


Figure 1: Network topology with packet Monitoring
Source: (Originally from) VMware eLearn course.

4 Results and Analysis

The version of Snort that has been used in this research did detect and analyzed all the attacks that have been sent to it and have an equal amount of alerts (104 alerts) as seen on Figure 2. Most of these detections were by the help of the preprocessors and Snort updated set of rules. When comparing this version of Snort with previous versions, we can find a lot of improvements in Snort detection ability and it processing power.

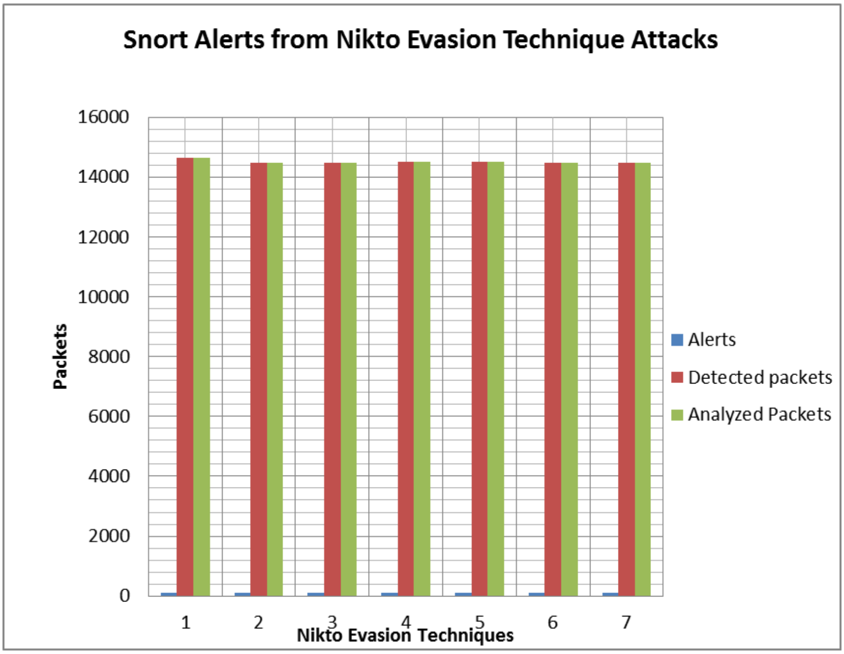


Figure 2: A graph the shows Snort alerts, detected and analyzed packets

This research will compare pervious test results that were conducted in previous researches such as Jarle Ytreberg (2007) research to show how much did Snort improve throughout the years. In Ytreberg's research, all evasion techniques have almost equal amounts of detections with the exception of evasion techniques number four and nine. This exception had occurred because of the method used when the attack had been conducted and transferred through the network. The methods that have been used for techniques number four and nine are *Prepend long random string* and *Session splicing* for evasion techniques four and nine respectively. Evasion technique four send packets that have unordinary long string in the GET request when sent to the virtual machine which will cause Snort to alert more than expected (Ytreberg, 2007). In the other hand, evasion technique nine (which is not supported by Nikto anymore) splits the attack to many small fragments to cause Snort IDS to spend a lot of processing power to reassemble the attack before processing it (Ytreberg, 2007). These evasion techniques did disturb Snort IDS in older versions by either making Snort generate a huge number of unnecessary alerts or by make it to consume a lot of time to reassemble it before processing it which might lead to dropping some legitimate packets. However, these problems did not cause any problem in the current version of Snort that has been used in this research and all evasion techniques did have equal numbers of alerts. The significant improvements in newer versions of Snort were caused by the help of Snort Preprocessors and Snort latest rule set.

When testing Snort in a busy environment, Snort did a great job detecting all evasion techniques generated by Nikto (see Figure 3). All packets that have been sent by Nikto have been analysed without dropping any incoming packets. This is because Snort did get a huge help from Barnyard since it makes Snort to run in full speed by decoupling output overhead from Snort IDS and convert almost any spooled file by adding input and output plugins (sourceForge.net, 2010). Additionally, Snort preprocessors are enabled to help Snort by normalizing any incoming packets in order to make things easier for Snort. In comparison with Yterberg's results (2007) from Figure 3 and 4, we can see that Snort have improved in its detection capability and performance even if tested in a busy environment. Unlike Yterberg's results when testing Snort in a busy environment, current version of Snort did detect and analysed all incoming packets.

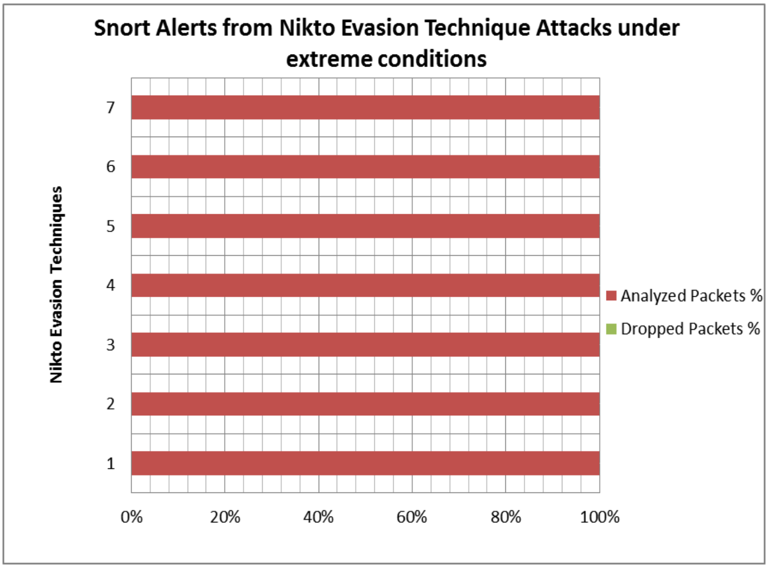


Figure 3: A graph that shows number of analyzed and dropped packets

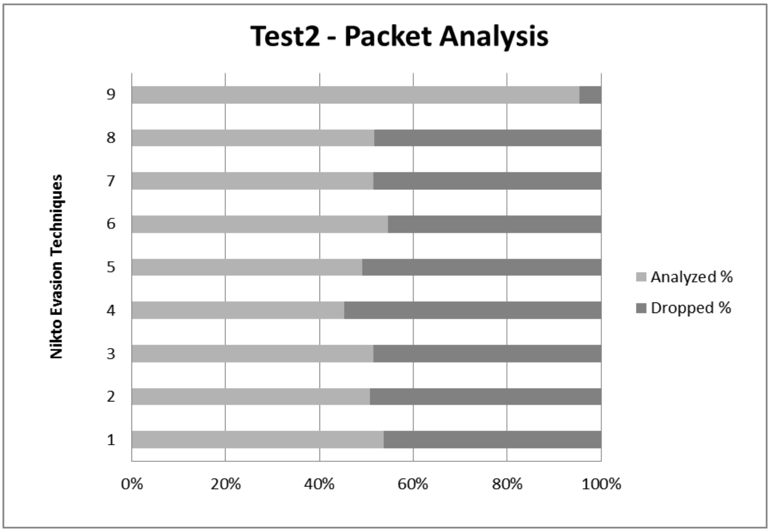


Figure 4: A graph that shows number of analyzed and dropped packets (Yterberg, 2007)

5 Conclusion

Network Intrusion Detection Systems (NIDS) can provide the level of security needed to be able to protect a company’s or organization’s assets. However, it will not be able to stop the attacks directed to the company’s network. It will monitor all packets that are received from a designated network physical or virtual interface and will trigger an alert if it detects any packet that might harm the company’s assets. Afterwards, it is up to the network administrator to decide whether to just ignore this packet or to figure out a way to prevent it from attacking the company’s system.

Intrusion Detection systems (IDS) does have some flaws like any other device such as firewalls and antivirus programs. However, these programs can be very powerful if kept updated regularly. In addition, we can consider the defense in depth countermeasure according to Kerry Cox and Christopher Greg, which deploy multiple overlapping defense measures (such as firewalls, IDS, etc.) in order to get a well secured system. (Cox and Greg, 2004) Nevertheless, updating your systems and countermeasure devices does not give you the reason to rest; every system administrator should know the ins and outs of his system. He should read and try to hack his own system in order to defend himself from possible attacks since the best way to defend is by attacking. Kevin Timm published that BlackHat community develop several methods to evade IDS sensors while IDS vendors, IDS developers, and security researchers tries to develop counter act to bypass these attacks. (Timm, 2002)

Therefore, it is essential for a network administrator to create safe virtual network that is isolated from the physical network and start testing the latest rules that have been provided by Snort. This task is important to see if Snort capable of detecting latest attacking techniques or not and most importantly is to make these test in an isolated network that will not interfere with any external networks to avoid attacking other systems unintendedly. Therefore, it is advisable for network administrators to use one of VMware Workstations in order to create this environment. In addition, VMware Workstation gives the network administrator several options to when it comes to test Snort in different environments. It gives the administrator the option to create several virtual machines in order to mutate a real network. Moreover, the administrator can use the created virtual machine in order to attack Snort IDS with different tools in order to test Snort’s durability. Additionally, VMware gives the network administrator the option to test Snort IDS in different environments by changing the specification of each virtual machine. This option provides a great opportunity for network administrators to test Snort IDS in extreme conditions.

From Nikto anti-IDS scanner tool, the network administrator can test Snort’s detection capability by sending packets from the attacker virtual machine to Snort IDS with different evasion techniques. These evasion techniques can be sent individually or by combining several evasion techniques together. All of these tactics are being implemented to try to confuse or exhaust Snort IDS in order to let it ignore some of the received packet which will lead to a successful penetration.

6 References

Anderson, J. (1980) “Computer Threat Monitoring and Surveillance”, a Technical Report, Fort Washington, Pennsylvania.

Bace, R. and Mell, P (2001), “Intrusion Detection Systems”, NIST Special Publication on Intrusion Detection Systems, [online] Available at:http://www.bandwidthco.com/whitepapers/ nist/NIST%20800-31%20Intrusion%20 Detections%20Systems.pdf

Cox, K. and Greg, C. (2004) “Managing Security with Snort and IDS tools”, O’Reilly Media ISBN: 0-596-00661-6, Pages 1-3.

Niphadkar, S. (2008). “Analysis of Packet Sniffers: TCPdump VS Ngrep VS Snoop”, Available at: http://mason.gmu.edu/~sniphadk/sniffer.pdf

Ptacek, T. and Newsham, T. (1998). “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection ”, Secure Networks Inc., Available at: http://www.insecure.org/stf/secnet_ids/secnet_ids.pdf

Timm, K (2002) “IDS Evasion Techniques and Tactics”, [Online] Available at: http://www.securityfocus.com/infocus/1577

Wang, W. (2003) “Steal This Book 3: What they won’t tell you about the Internet?”, William Pollock Publications.

Ytreberg, J. (2007) “Network Intrusion Detection Systems Evasion Techniques: an Investigation using Snort”, Masters Dissertation, Plymouth University, UK.

Personality Type – A Valid Indicator of Security Champions?

T.Gabriel[1], S.M.Furnell[1] and K-L.Thomson[2]

[1]Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
[2]School of Information and Communication Technology, Nelson Mandela
Metropolitan University, Port Elizabeth, South Africa
e-mail: info@cscan.org

Abstract

Information security training and awareness raising are widely recognised as particularly difficult areas to address. Aspects such as organisational behaviour, the incorporation of educational learning theories and adult education best practise appear to be commonly overlooked in existing security training approaches.

An initial study into security assessment of personnel via psychometric testing appears to provide a cost effective solution. A security assessment questionnaire is designed and constructed the results of which are compared with personality features from psychometric tests using multiple regression. Statistical analyses reveal that a number of personality attributes appear to correspond with an information security inclination. In particular the combination of ‘imagination’ and ‘immoderation’ appear to provide good predictive results.

Keywords

Information security, personality, psychometrics, organisational behaviour, educational theory.

1 Introduction

The difficulties of implementing effective security training are widely recognised as long standing issues; Lacey (2009) providing excellent coverage. It seems appropriate, therefore, to investigate the educational difficulties associated with the area. The focus of this paper is to understand the main problems at a theoretical level and suggest recognised approaches to minimising their effects. The main topics are considered to be organisational and group behaviour, adult education and learning theory, and crucially, the identification of staff that are supportive or averse to security related concepts and procedures.

2 Organisational behaviour

The effects of peer pressure on individuals’ behaviour are a well known and documented phenomenon; the consequences of which go largely unnoticed among day-to-day activities. In the context of security training it can be a significant barrier, providing a largely transparent resistance to change throughout the workforce. In the majority of cases a person joining a group, very quickly and unwittingly adopts its attitudes and practises. The consequences, when a person joins a group that is not security conscious, are clear.

A less well-known (and perhaps less understood) phenomenon is minority influence; as studied by Moscovici, Lage and Naffrenchoux (1969) and Asch (1956). Under particular circumstances a very few, or even a single, individual can slowly influence the majority, effectively reversing the commonly held view of peer pressure (majority effect). One significant difference is the speed of change. Minority influence is a slow, but again, subliminal process. The requirements for this phenomenon are a moderate degree of authority, a consistent yet flexible opinion, repetition, and persistence. When the above are viewed from educational perspectives it can be seen that these are common attributes to many forms of education. Education is commonly a slow constant pressure applied to the majority (students) by the minority (the educator) to impart new and alternative perspectives.

3 Educational Theory

Armitage et al (2007) acknowledge the shortfalls of learning theories but accept that they continue to provide a useful framework on which to build.

Sensory stimulation theory suggests that learning best occurs when each of the senses are stimulated in unison. Reinforcement learning is based upon reward and sanction. Cognitive-Gestalt approaches relate to pattern, relationship and insight based upon prior experience. Facilitation theory sees the educator employed as a learner's assistant – where learner and educator are equals. Action learning is a not too dissimilar approach but the emphasis shifts toward learners sharing their views and experiences amongst themselves with the educator playing a steering and supporting role.

Oxford Brookes University (Dunn, 2002) provides an insightful and succinct view of these and more learning theories.

In addition Tough reveals important personal characteristics which will benefit the trainer; he or she...

"... views personal interaction with the learner as a dialogue, a true encounter in which he or she listens as well as talks. Help will be tailored to the needs, goals, and requests of this unique learner. The helper listens, accepts, understands, responds, helps. These perceptions are in sharp contrast to those of "helpers" who want to control, command, manipulate, persuade, influence and change the learner.

...Such a helper perceives the learner as an object, and expects to do something to that object. He is not primarily interested in that person as a person, and in his needs, wishes, and welfare." (Tough 1979 p91)

By contrast, an afternoon browsing information security sites including NIST, Microsoft, SANS, ICO and ISACA reveals no mention of trainer selection. The Get Safe Online (2010) website mentions the need to "train the trainer" but the idea is not expanded upon. The ENISA (2010) “Train the trainers - SMEs security” page contains links to materials that can be used in trainer training, but these offer only a walk through of the training material provided. Google searches for “training the trainer” and “trainer training” in relation to information security also produced nothing of relevance. A common theme however is the approach taken by, and available from, the National Institute of Standards and Technology (NIST) website...

“Roles and responsibilities of agency personnel who should design, develop, implement, and maintain the awareness and training material, and who should ensure that the appropriate users attend or view the applicable material;...” (Wilson and Hash, 2003)

The language used gives the impression that trainees will have material pressed upon them, that they will be summoned to sessions, and will have little if any say in the content presented. Such an approach appears to be in direct contradiction to learning theories and to Knowles’ (2005) views on adult education.

In addition, no consideration is given to the role, skills, character and influence of the educator. Is this one of the missing pieces in the security puzzle? Have security specialists and business managers focussed so strongly upon content (if security training has been considered at all) that the psychological and educational theories have been overlooked? If this is the case, perhaps a softer but persistent approach is required; one that advocates educational theory and the exploitation of minority effect? This concept seems to fly in the face of current views however, the consensus being (from those who care sufficiently) to get tough on security issues.

4 Mentoring

If a move toward gentler but persistent training is indeed appropriate, coaching or mentoring appears to provide the right approach. Organisational behaviour becomes less of an issue when colleagues carry out the training. The effort is sustained and relevant to the role, the mentor is readily available to offer advice and assistance, and is better placed to monitor behaviour. In effect the trainer is well known, on hand, helpful and supportive, and advice is relevant – aspects recognised by Knowles (2005) as beneficial to adult learning. In addition the unwittingly erected barriers of classroom environments are removed – learners often bring with them the (often negative) personal experiences of similar previous activities, discomfort, a potential for underachievement, embarrassment, lack of relevance and more. There are a number of downsides to mentoring however, namely the high set up costs and effort of mentor training and selection.

5 Mentor selection

The quote below is, in the authors’ view, as important in a mentoring environment as in a classroom situation. The presentation skills mentioned are perhaps less relevant – the contact being less formal – but selecting an individual with the interpersonal skills to fulfil the role is still a priority.

"If you're going to do your training in the classroom, you've got to be prepared to find good presenters – whether that's someone already in your organization, or hiring someone from outside.

At the risk of generalizing, your information security and/or IT staff are seldom the right people to be handling this. Not only are they rarely comfortable in presenting to audiences, they tend to allow themselves to be drawn into too much technical detail…" (Security Awareness Training, 2010)

But equally, an interest and affinity with security concepts is necessary. The social skills required can be largely deduced from daily behaviour and interaction with others, but security interests are less likely to be recognisable. In addition latent interest might exist, but through lack of experience or exposure to materials, remain unrecognised even by an individual themselves. What is needed is a means of identifying individuals with security interests; be they latent or not. These persons might then be offered the opportunity to become mentors and trained to carry out the responsibility.

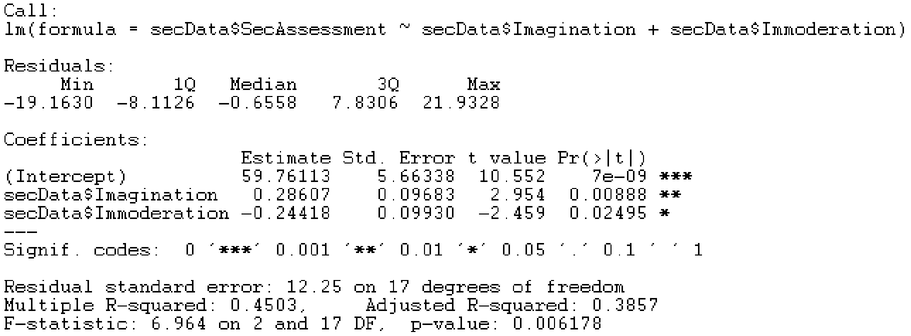
On the other hand, security assessments, standards and processes for personnel selection, or any other purpose, appear to be conspicuous by their absence, and would not in any case determine the *qualities* of those who lack security knowledge or experience. This is a potentially critical point in promoting sufficient numbers to the role of security champion within an organisation, department or team. The numbers of security aware individuals (coupled with the required interpersonal skills) are perceived to be low - a quick and at least moderately accurate selection process of those with latent talent is needed.

6 Personnel selection using psychometrics

Until this point little if anything new has been discussed other than bringing together theories and elements from fields typically removed from the subject of security training. Here however, a novel selection process is proposed and an initial study conducted.

A group of 20, white, European employees and managers, who work within the technology sector were appraised by colleagues and awarded security ratings. The security assessments consist of 17 questions and are based upon 5 categories: passive compliance, active compliance, external pressures, motivation and awareness. Of these, only motivation and active and passive compliance are used within the regression analysis. Awareness and external pressure are considered much less attributable to an individual's personality and are excluded on this basis. In parallel the group undertook personality tests from the International Personality Item Pool; a freely available test instrument similar to the copyright protected NEO-PIR. Available via a research website, the test's short form was used, consisting of 120 questions and taking each individual around 15 minutes to complete. Results consist of percentage scores for thirty personality attributes. The entire group were retested at approximately monthly intervals, the results of which reveal good inter-test consistency. Security assessment results, however, displayed greater inter-assessor variations as might be expected from survey based data. 3 assessors where employed; selected as a result of their (moderate) security knowledge, interest and how well they know the working practises of fellow participants.

When multiple regression analysis is used to compare the security assessments and personality test results obtained, a number of personality factors with moderate correlations are revealed; primarily imagination and immoderation, as shown in Figure 1.



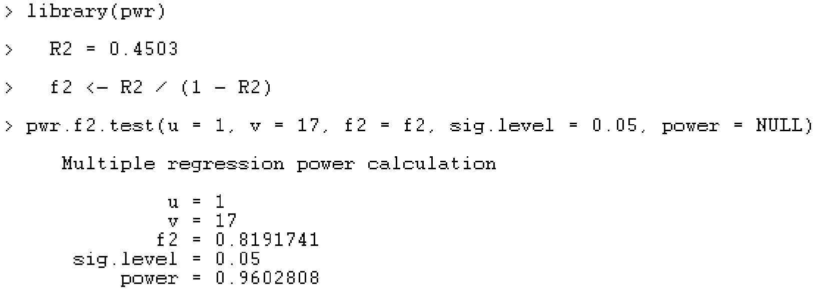
```
Call:
lm(formula = secData$SecAssessment ~ secData$Imagination + secData$Immoderation)

Residuals:
     Min       1Q   Median       3Q      Max 
-19.1630  -8.1126  -0.6558   7.8306  21.9328 

Coefficients:
                     Estimate Std. Error t value Pr(>|t|)    
(Intercept)          59.76113    5.66338  10.552    7e-09 ***
secData$Imagination   0.28607    0.09683   2.954  0.00888 ** 
secData$Immoderation -0.24418    0.09930  -2.459  0.02495 *  
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1 

Residual standard error: 12.25 on 17 degrees of freedom
Multiple R-squared: 0.4503,     Adjusted R-squared: 0.3857 
F-statistic: 6.964 on 2 and 17 DF,  p-value: 0.006178 
```

Figure 1 - Multiple Regression Results

The key points above are that p is significantly below the commonly recognised value of 0.05 (0.0062) indicating that the probability of the result being incorrect is just 0.62%. The multiple R^2 value is substantial (0.45), equating to a large (according to Cohen (1992)) effect size: 0.82 – see Figure 2 below.

The sample population size of twenty, was initially considered too small to produce results of significance, but power tests reveal that regression using two independent variables alone (personality factors) can identify medium to large effect sizes – as defined by Cohen (1992).

Power test results - Figure 2 - indicate that given v (population size - 1 - the number of independent variables used: 20-1-2 =17) the regression analysis power (96%) exceeds the standard benchmarks of 80 or 90 percent. Further tests reveal that the use of 3 or more independent variables does not meet the 80% criteria, in turn highlighting that alternative solutions based upon 3 or more variables may remain undiscovered.



```
> library(pwr)

>   R2 = 0.4503

>   f2 <- R2 / (1 - R2)

> pwr.f2.test(u = 1, v = 17, f2 = f2, sig.level = 0.05, power = NULL)

     Multiple regression power calculation

              u = 1
              v = 17
             f2 = 0.8191741
      sig.level = 0.05
          power = 0.9602808
```

Figure 2 - Power Calculation Results

Therefore, imagination and immoderation provide the best model so far revealed within this data set. Where regression is conducted in parallel against these two variables, strong results (taking the social data factor into consideration) indicate that a predictive measure is available.

Security Rating = (imagination score * 0.28607) +
(immoderation score * -0.24418) + 59.76

When the boundaries of this equation are explored the model's limitations are revealed; the maximum and minimum scores achievable being 88 and 35 respectively using scores of 1 to 100. However, this may not detract from its potential to subdivide a population into 3 security groups which, based upon a 15 minute test, might still provide a useful function in the absence of other options.

It should be noted that correlation must not be confused with causation, however. An unknown third variable, associated with both imagination and immoderation, might be at work.

A key observation of this study is that distinguishing features appear to lie with combinations of personality facets as opposed to the trait level. Traits being groups of facets measuring related attributes. As far as can be determined little if any career-based analysis has been conducted at this level of detail, and none whatsoever has been found with regard to information security and its various roles.

7 Conclusions

The use of personality tests to identify an individual's security inclination remains unproven in both a theoretical and practical sense. It ignores too the ability of an individual to take up and succeed in the mentoring role. However, a parallel investigation into the personality attributes of successful adult educators may reveal that similar descriptive factors exist.

Results for thirty personality attributes were obtained. The 8 strongest indicators of an inclination for security concepts found thus far are; imagination, emotionality, anxiety altruism, immoderation vulnerability, morality and openness to experience.

Immoderation – a tendency to react in favour of short term gains as opposed to longer term consequences – provides the only negative correlation. The weakest indicators found are gregariousness, self-discipline, neuroticism, trust and dutifulness.

It should again be noted that correlation must not be confused with causation - or lack of it. An unknown third variable, associated with any combination of trait or facet may be at work.

The results obtained thus far indicate that personality test results may possess a predictive value. Where further investigations reveal similar results and establish a relevance to the general population, the approach might be used in wider and, as yet, unforeseen contexts in addition to the proposed trainee categorisation and mentor or security champion selection processes.

Current results show predictive levels that might be used to categorise individuals into one of perhaps three security inclination groups. Initial impressions are that this process may lack precision, but in the absence of other approaches and for the purposes of targeted training it is considered to be of a sufficient level of definition. Where the aim is to identify mentors it is highly likely that an interview process will need to follow, confirming the findings, ensuring that candidates are willing participants and are capable of fulfilling the mentor role.

The combination of accurately identifying suitable individuals, training them in the necessary educational and psychological principles, and empowering them in the workplace with a view to the long term, is in the authors' opinion a more effective way of increasing security awareness and compliance. The cost and effort required, especially by businesses that barely recognise the need, will, however, lead to its rejection in almost all cases at the present time. The proposed approach is not cheap, but in the longer term may well prove cost effective where widespread compliance levels are considered essential.

This in turn raises the issue of just what is required for senior managers to recognise and fulfil security requirements. The answer almost certainly lies in legislation and wider publicity. Where organisations suffer data losses the full consequences of a breach should by widely publicised in a constructive manner. Only when the financial costs and reputational damage are recognised and fully acknowledged by senior managers will the need be addressed.

Primarily, future research suggestions include reviewing and refining the assessment process after conducting greater analytical investigation of assessment results. Regression analysis should then be repeated on larger data sets, to establish the legitimacy of current findings.

8 References

Armitage,A., Bryant,R., Dunnill,R., Flannagan,K., Hayes, D., Hudson, A., Kent, J., Lawes, S., Renwick, M., (2007*). Teaching and Training in Post-Compulsory Education. (3rd ed)*, Maidenhead, Open University Press. ISBN 0-3352-2267-6

Asch,S.E., (1956). *Studies of independence and conformity; A minority of one against a unanimous majority*, Psychological Monographs, Vol. 70(9)

Cohen,J., (1992). *A Power Primer*, Psychological Bulletin, Vol 112(1), July 1992, 155-159. http://137.148.49.106/offices/assessment/Assessment%20Reports%202006/CoS/Psychology%203%20of%203.pdf (Accessed 11/7/2010)

Dunn, L., (2002). *Learning and Teaching Briefing Papers Series - Theories of Learning*, http://www.brookes.ac.uk/services/ocsd/2_learntch/briefing_papers/learning_theories.pdf (Accessed 02/07/2010)

ENISA (2010). http://www.enisa.europa.eu/media/news-items/train-the-trainers-smes-security http://www.enisa.europa.eu/act/ar/deliverables/2010/e-mail-security_train-the-trainer-guide (Accessed 03/07/2010)

Get Safe Online (2010). http://www.getsafeonline.org/nqcontent.cfm?a_id=1108 (Accessed 03/07/2010)

ISACA, (2009). *An Introduction to the Business Model for Information Security*, Rolling Meadows, Illinois.
http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf (Accessed 03/07/2010)

IPIP, (2010). *International Personality Item Pool: A Scientific Collaboratory for the Development of Advanced Measures of Personality Traits and Other Individual Differences*, http://ipip.ori.org/ (Accessed 20/12/2009)

Knowles, M. S., Holton, E. F., & Swanson, R. A., (2005). *The Adult Learner (6th ed.).* Burlington, Massachusetts, Elsevier Butterworth-Heinemann, ISBN 0-7506-7837-2

Lacey, D., (2009). *Managing the Human Factor in Information Security.* Chichester, John Wiley & Sons, ISBN 978-0-470-72199-5

Moscovici, S., Lage, E., & Naffrechoux, M. (1969). *Influence of a consistent minority on the responses of a majority in a color perception task*. Sociometry, 32(4), 365-380

Security Awareness Training, (2010). http://www.security-awareness-training.com/ (Accessed 03/07/2010)

Tough, A., (1979). *The Adults Learning Projects (2nd ed.).* Toronto, Ontario Institute for Studies in Education. ISBN 0-8938-4054-8

Wilson, M., Hash, J., (2003). *Building an Information Technology Security Awareness and Training Program*,
Gaithersburg, Maryland: NIST http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (Accessed 03/07/2010)

Evaluation of Current E-Safety Software

Z.Latif and P.S.Dowland

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Filtering and blocking products are being marketed for the home users as a way of keeping their children safe on the internet. In order to evaluate the effectiveness of such products a framework was designed. The framework was conducted to evaluate the effectiveness of five filtering products in communication channels, search engines and in URLs filtering. During the test it was revealed that filtering companies advertise many features but these features have their limitations and can cause the false sense of security. None of the tested products proved accurate to safeguard the children from online risks and threats

Keywords

Internet filters, blocking software, e-safety products, parental control

1 Introduction

The internet usage by children has been increased for the last few years (Livingstone and Haddon, 2009). According to the Ofcom's report 2008, 99% of children aged 8-17 access the internet (Byron, 2008).Largest proportion of children (81%) access the internet at home and 86% at school (Ofcom, 2007). There is explosive growth of websites and web pages on the internet. For instance, there were more than a billion websites by 2000, and many of them were changing daily (Heins *et al*. 2006).The content on the internet can be inaccurate, unpleasant, offensive, and harmful for minors. For instance, pornographic, gruesome, racist, extremist, militancy, self harm, violence, suicide, bomb making and biased information can mislead the children because they lack the skills to evaluate and judge the reliability of online information. According to the findings of Livingstone and Bober, "four in ten (38%) of pupils aged 9-19 trust most of the information on the internet, half (49%) trust some of it, and only one in ten (10%) are sceptical about much information online" (Livingstone and Bober, 2005).

Parents are worried about the safety of their children whilst on the internet. For this purpose filtering and blocking products are being marketed to safeguard the children from these risks. According to a survey conducted by Euroberometer, half of the parents (49%) were using filtering software, 37% of parents were using monitoring software and 27% of parents were using both i.e. blocking and monitoring software (Euroberometer, 2008). But these products may have some of their limitations and over reliance on them may cause the false sense of security. Five filtering products that are being marketed for home users, as a way to safeguard their children from online risks and threats, were selected to evaluate their effectiveness. In background section there will be

2 Background information

2.1 Online risks to children

Children are engaged in number of online activities that can expose them to certain online risks and threats. They can have three types of roles in an online environment: a recipient, a participant and an actor. These roles can be associated with three types of risks: content, contact and conduct respectively. In content risks, children can be the recipient of harmful and inappropriate content e.g. advertising, spam, sponsorship, violent, hateful, gruesome, racist, biased information, drugs, pornographic and sexual content (Livingstone and Haddon, 2009). However, exposure to such harmful content can either be intentional or unintentional. They can receive such content through pop up advert, search engines, general surfing and communication channels. Contact risks, may involve: giving personal information, being bullied, being harassed, being stalked, being groomed, and meeting with strangers, self-harm and unwelcome persuasion. Children can be engaged in certain online activities which provide the opportunities of communications and contacts e.g. Instant messaging, emails, chat rooms, voice chat, video chat, blogs, social networking sites and sharing information with others. Conduct risks, may involve: bullying or harassing others, creating or uploading pornographic material, providing advice of suicide and self harm, gambling, illegal downloads, hacking and online games (Livingstone and Haddon, 2009). According to a survey (2009), conducted by the National Campaign to Prevent Teen and Unplanned Pregnancy, in United States, “one in five teenagers had sent or posted online nude or semi-nude pictures of themselves and 39% had sent or posted sexually suggestive messages” (Jewkes, 2010).

2.2 E-safety products.

The use of e-safety software can be a good option to safeguard the children whilst on the internet. There is a range of e-safety software available in the market place offered by different companies. These products may come with a variety of features e.g. filtering, monitoring, reporting or any combination of these features. Monitoring software records the online activities of children and maintains logs, which parents can view to know the online behaviour and interactions of their child. For instance, parents can visit the websites that their child has accessed and they can view the online conversations of their child. Filtering software regulates the internet access. They block the access to objectionable content and allow the access to legitimate content (Ormes, 2009).

2.3 Previous studies on e-safety products

In 2000, Hunter (Hunter, 2000) evaluated the four popular commercial filters e.g. CYBERsitter, CyberPatrol, Surf Watch and Net Nanny. This study was conducted in the context of under inclusive blocking and over inclusive blocking. If a filter failed to block the access to a site that contains ‘objectionable material’ it was under inclusive blocking. On the other hand if a filter blocked the access to a site that did not have any ‘objectionable material’ it was over inclusive blocking. He employed the RASCi ratings to decide what is objectionable and what is non objectionable. RSACi classifies content into four categories e.g. Violence, Nudity, Sex and Language. Each category is associated with five levels of severity e.g. 0, 1, 2, 3, 4 and 5 (Ormes, 2009). He considered it ‘objectionable’ if any content of the site received RSACi rating of 2, 3 or 4. On the other hand the sites with RASCi rating 0 or 1 were considered ‘not objectionable’. In test methodologies he selected 200 websites to evaluate the effectiveness of filters. He selected these web pages through search engines, popular search terms and portals. Interestingly, 164 web pages were ‘not objectionable’ and 36 web pages were ‘objectionable’ out of total selected 200 web pages. In evaluation he found that over inclusive blocking error rates of CYBERsitter, CyberPatrol, Surf Watch and Net Nanny were 14.6%, 9.1%, 7.3% and 3% respectively and the corresponding error rates for under inclusive blocking were 30.6%, 44.4%, 55.6% and 83.3% respectively. With all blocking decisions combined of four filters the over inclusive and under inclusive error rates were 21% and 25% respectively.

In 2001, U.S. Department of Justice commissioned the eTesting Labs to evaluate the effectiveness of five web content filtering products (eTesting Labs, 2001).They tested the five filtering products that were freely available for 30 day trial e.g. SmartFilter^{TM}, CyberPatrol, Websense Enterprise, N2H2^{TM}, and FoolProof SafeServer^{TM}. In test methodologies, Department of Justice provided them the specific criteria for defining content that should be blocked, and the filtering options to be applied for filtering products. According to that criteria, access should be blocked to “pictures, images, graphic image files, or other visual depictions that depict, describe or represent an actual or simulated sex act or sexual content, actual or simulated normal or perverted sexual acts or a lewd exhibition of the genitals and which lacks serious literary, artistic, political, or scientific values as to minors”. In other words access to sexual or pornographic nature content should be blocked and such URLs were included in the list whose access should be blocked. They created a second list of URLs whose access should be allowed because their content did not meet the criteria that should be blocked. They randomly selected these URLs by using search engine and search phrase. In order to evaluate the effectiveness of five filters, they selected 197 objectionable URLs, whose access should be blocked, and 99 non objectionable URLs, whose access should not be blocked. They processed the both lists of URLs e.g. objectionable and non objectionable, and calculated the effectiveness of each filter. They calculated the Correct Blocking Ratio (CBR) for objectionable content and Incorrect Blocking Ratio (IBR) for non objectionable content. They computed the CBR as the total number of correctly blocked pages (CBP) divided by the total number of pages tested (TNP). Whereas they computed the IBR as the total number of incorrectly blocked pages (IBP) divided by the total number of pages tested (TNP). Higher value of CBR means the filtering product is more effective at correctly blocking objectionable content. Whereas lower value of IBR means the filtering product is better in allowing the access to non objectionable content. In other words lower value of IBR means less over blocking by filtering product. In their evaluation the computed CBR values of Websense, N2H2, CyberPatrol, Smart Filter, and SafeServer were 0.924, 0.980, 0.827, 0.944, and 0.761 respectively and the corresponding IBR values were 0.00, 0.01, 0.061, 0.071, and

0.091 respectively. It was clear by the results that Websense had the lowest IBR value, so it was doing lowest over blocking as compare to other four filtering products. On the other hand N2H2 had the higher value of CBR, so it was more effective in blocking objectionable content as compare to other four products. Interestingly, eTesting Labs, in addition to evaluate the effectiveness of filters, also looked at the other features of the filtering products e.g. Installation, configuration, content monitoring and blocking, and reporting and alerting.

2.4 Limitations of previous studies.

Hunter evaluated the four filtering products. It seems as if his context of evaluation was to know if these filtering products were First Amendment friendly or not. He selected 200 websites, out of which only 18% were objectionable and 82% were non objectionable. It can be possible that equal number of objectionable and non objectionable sites could give better overview of filter’s performance.

On the other hand eTesting Labs, in their evaluation of five filtering products, selected 296 URLs, out of which 66.5 % were objectionable and 33.4%were non objectionable URL’s. The higher percentage of objectionable sites can give a better overview of filters’ effectiveness in protecting children from such sites. It seems their context of evaluation was to know if filtering products effectively blocked the access to those sites that were ‘objectionable’ according to the criteria specified by Department of Justice. In other words, to know if filtering products were efficiently blocking the access to pornographic nature sites and allowing the access to non objectionable sites. But content risks are not limited to only pornographic material because other harmful content like hate violence, racism, anorexia, self harm, promotional content of tobacco, alcohol and banned drugs also comes under this category. Although these studies provide a good overview of filters’ performance but online risks and dangers are not limited to only content risks. For instance, many other risks and dangers come under the categories contact and conduct that are mentioned in earlier discussion. Because children are involved in number of online activities which makes them vulnerable to content, contact and conduct risks. Therefore there is need to evaluate the e-safety products for all the potential risks and dangers with respect to children’s online activities.

3 Testing Methodologies

A framework was designed to evaluate the e-safety products. The framework was consisting of four phases. First phase was dealing with administration capabilities of e-safety products, second phase was dealing with communication channels, third phase was dealing with search engines and fourth phase was dealing with URLs. Framework was conducted to evaluate each of the selected products. However in this paper only last three phases of the framework will be discussed. The following five filtering products were selected. ParetoLogic PGsurfer is freeware whereas rest of the products were available for free trials. These products were obtained from corresponding vendors’ website.

- Net Nanny version 6.5.1.10
- SafeEyes version 6.0.238

- CyberPatrol version 7.7.2.4
- CyberSentinel version 3.1.6.0
- ParetoLogic PGsurfer version 6.1.0

The configuration of the PC system used for performing experiments:-

- Operating System: Windows Vista^{TM} Home Premium (Service Pack 1)
- Processor type: Intel(R) Core(TM)^{2} Duo CPU T5800 @ 2.00 GHz 2.00 GHz
- Memory (RAM):3.00GB
- System Type: 32-bit Operating System
- Browser: IE version 8

The system was connected to the internet via WiFi connection. Filters were installed one by one per vendors' instructions. Moreover contacts were made with vendors via emails and phone calls for different queries. The filters' were set to their full capacity of protection that were claimed to safeguard the children in their online activities. But it was done very carefully in order to be consistent in selecting categories for each filtering product. In other words efforts were made to enable same protection level for each filtering product.

The second phase of the framework was conducted to evaluate the filters' effectiveness to keep the children safe in communication activities. For this purpose six popular application based messengers were installed to engage in chat activities. Web based communication channels e.g. web based chat rooms, web based chat, Social networking sites and web based email were accessed to join communication activities. Moreover, file sharing applications were also installed to engage in file sharing activities. Filters were then evaluated against each activity for two aspects based on two assumptions.

- Parents who want to monitor the behaviour of their children in these channels.
- Parent who just want to block these channels.

First aspect was to evaluate the filter's effectiveness in recording, reporting and sending alerts for these activities. For this purpose intentionally unsafe behaviour was adopted to evaluate the filters' performance. For instance, in public chat rooms personal (but faked) information was sent, adult chat rooms were joined, personal messaging (PM) requests from strangers were accepted, advertisement hyperlinks in public chat rooms and emails were clicked, and spam emails were opened etc. Second aspect was to evaluate the filter's effectiveness in blocking these channels and applications.

The third phase of the framework was conducted to evaluate the filters' effectiveness to keep the children safe in search engines. For this purpose lists of objectionable and non objectionable keywords and search phrases were compiled.

The fourth phase of the framework was conducted to evaluate the filter's effectiveness in blocking the objectionable URLs and allowing the access to non objectionable URLs. In other words over blocking and under blocking of filters were evaluated. For this purpose 500 URLs were selected i.e. 250 objectionable and 250 non objectionable. URLs were randomly collected through three search engines e.g. Google, Bing, and Yahoo. Moreover some of the URLs were collected from different chat rooms that were being sent by spammers and pornographic advertisers. Different "key words" and "phrases" related to different categories were searched. The objectionable URLs were not limited to only pornographic content. Other objectionable content categories were also included e.g. hateful, racist, illegal drugs, adult games, self harm, violent, suicide, bomb making, dating, alcohol and tobacco promotional sites. Each of the site was manually reviewed to decide if it is objectionable or non objectionable. In order to calculate ratio of over blocking and over blocking, two types of calculations were made .In first calculation formula used by e-Testing Labs were utilised and in second calculation accuracy percentage was calculated.

4 Results

4.1 Products's monitoring capabilities for communication channels

Activity	**Net Nanny**	**Cyber Patrol**	**Cyber Sentinel**	**SafeEyes**	**ParetoLogic PGsurfer**
Application Messengers					
Yahoo	Yes	No	No	Yes	No
Windows Live Messenger	Yes	No	No	Yes	No
ICQ	Yes	No	No	Yes	No
Google Talk	Yes	No	No	No	No
Skype	No	No	No	No	No
AIM messenger	Yes	No	No	Yes	No
Web based Chat rooms	No	No	No	No	No
Social Networking Sites					
Facebook	Yes	No	No	No	No
MySpace	Yes	No	No	No	No
Bebo	Yes	No	No	No	No
Twitter	Yes	No	No	No	No
Web based Emails					
Hotmail	No	No	No	No	No
Gmail	No	No	No	No	No
Yahoo	No	No	No	No	No

Table 1: Products' monitoring capabilities for communication channels.

4.2 Product's effectiveness in blocking communication channels.

	Net Nanny	**Cyber Patrol**	**Cyber Sentinel**	**SafeEyes**	**ParetoLogic PGsurfer**
Application messengers					
Yahoo	Yes	No	No	Yes	Yes
Windows Live Messenger	Yes	No	No	Yes	Yes
ICQ	Yes	Yes	No	Yes	Yes
Google Talk	Yes	No	No	No	Yes
Skype	No	No	No	No	Yes
AIM messenger	Yes	No	No	Yes	No
Web based Chat rooms					
camvoice.com	Yes	Yes	Yes	Yes	No
chat-avenue.com	Yes	Yes	Yes	Yes	No
ivideochat.com	Yes	Yes	No	Yes	No
chatforfree.org	Yes	Yes	No	Yes	No
youcams.com	Yes	Yes	No	Yes	No
byfchat.com	Yes	Yes	Yes	Yes	No
shockrooms.com	Yes	Yes	No	Yes	No
iwebcam.com	Yes	Yes	No	Yes	No
Social Networking Sites					
Facebook	Yes	No	No	Yes	Yes
MySpace	Yes	No	No	Yes	Yes
Bebo	Yes	No	No	Yes	Yes
Twitter	Yes	No	No	No	Yes
Web based Emails					
Hotmail	Yes	No	No	Yes	Yes
Gmail	Yes	No	No	Yes	Yes
Yahoo	Yes	No	No	Yes	Yes
P2P file Sharing					
LimeWire	Yes	No	No	No	Yes
Bit torrent	Yes	No	No	Yes	Yes
Proxy Sites	No	No	No	No	No

Table 2: Products's effectiveness in blocking communication channels.

4.3 Products' effectiveness in filtering search engines

Activity	Net Nanny	Cyber Patrol	Cyber Sentinel	SafeEyes	ParetoLogic PGsurfer
Blocking search engines	Yes	No	No	Yes	Yes
Blocking image, video and text search	Yes	No	No	Yes	No
Filtering or refining the search results	Yes	No	No	No	No
Over blocking	Yes	Yes	Yes	Yes	Yes
Under blocking	Yes	Yes	Yes	Yes	Yes

Table 3: Products's effectiveness in filtering search engines.

4.4 Products' effectiveness for blocking Objectionable URLs

Action	Net Nanny	Cyber Patrol	Cyber Sentinel	SafeEyes	ParetoLogic PGsurfer
Correctly Blocked	237	221	196	226	163
Failed to Block	13	29	54	24	87
Total URLs	250	250	250	250	250
Accuracy percentage	94.8%	88.4%	78.4%	90.4%	65.2%
Under blocking percentage	5.2%	11.6%	21.6%	9.6%	34.8%

Table 4: Products' effectiveness for blocking objectionable URLs.

4.5 Filters' effectiveness in allowing access to non objectionable URLs

Action	Net Nanny	Cyber Patrol	Cyber Sentinel	SafeEyes	ParetoLogic PGsurfer
Correctly Accessed	241	235	243	248	237
Incorrectly Blocked	9	15	7	2	13
Total URLs	250	250	250	250	250
Accuracy Percentage	96.4%	94%	97.2%	99.2%	94.8%
Over blocking percentage	3.6%	6%	2.8	0.8%	5.2%

Table 5: Products' effectiveness in allowing access to non objectionable URLs.

4.6 Correct Blocking Ratio and Incorrect Blocking Ratio.

	Net Nanny	Cyber Patrol	Cyber Sentinel	SafeEyes	ParetoLogic PGsurfer
Correct Blocking Ratio(CBR)	0.948	0.884	0.784	0.904	0.652
Incorrect Blocking Ratio (IBR)	0.036	0.06	0.028	0.008	0.052

Table: 6 Correct Blocking Ratio and Incorrect Blocking Ratio.

5 Discussion

5.1 Monitoring capabilities for communication channels

The inconsistencies of filtering products for monitoring chat activities can be seen in the table 1.Net Nanny was able to record the chat activities in social networking sites but it was failed to record the chat activities in web based chat rooms. Although it was able to monitor the chat activities in five tested application messengers but it was failed to monitor the chat activities conducted through Skype. Moreover it was not able to monitor the web based emails. SafeEyes was able to monitor only four out of six tested application messengers and it was failed to monitor the rest of communication channels. CyberPatrol, CyberSentinel and ParetoLogic PGsurfer, were not able to monitor any of the tested communication channels. SafeEyes was able to monitor only four application messengers and it was failed to monitor the web based chat rooms, social networking sites, and web based email.

5.2 Blocking capabilities for communication channels.

Although Net Nanny was most efficient among other filtering products to block the communication channels but it was not able to block the Skype. There was only one product i.e. ParetoLogic PGsurfer, who blocked the Skype but it was not able to block the AIM messenger and web based chat rooms. CyberPatrol blocked all the tested web based chat rooms, but on the other hand it failed to block social networking sites. Moreover it was able to block only one application messenger. Similarly SafeEyes was not able to block one social networking site and two application messengers. CyberSentinel was able to block only three web based chat rooms.

None of the selected filtering products were able to block fresh proxy sites. There were only two products i.e. Net Nanny and ParetoLogic PGsurfer that were able to block tested peer to peer file sharing applications. However SafeEyes successfully blocked Bit torrent but it failed to block LimeWire.

5.3 Products' effectiveness in filtering search engines

Although Net Nanny was efficient for filtering search engines but over blocking and under blocking was seen. CyberPatrol and CyberSentinel were not able to block search engines. Moreover both failed to refine the search results e.g. all objectionable images were viewable. Safe Eyes was able to block search engines, image and video searches. But it was failed to refine the search results. ParetoLogic PGsurfer was able to block search engines but it was not able to refine search results.

5.4 Products effectiveness in filtering URLs

The results clearly illustrate that each product was doing over blocking and under blocking. Interestingly in each product there was more under blocking than over blocking. However, in some products balance of over blocking and under blocking was worst. For instance, in ParetoLogic PGsurfer, the ratio of under blocking was far more than over blocking. Similarly in CyberSentinel and SafeEyes the ratio of under blocking was far more than over blocking. Although in Net Nanny and CyberPatrol there was more under blocking than over blocking, but ratio of under blocking was not far more than under blocking. The higher value of CBR means the filtering product is more effective at correctly blocking objectionable URLs. Whereas lower value of IBR means the filtering product is better in allowing the access to non objectionable content.

According to this criterion Net Nanny had the highest value of CBR. Therefore it can be concluded that it was more effective in blocking objectionable URLs than other tested filtering products. On the other hand SafeEyes had the lowest value of IBR. Therefore it can be concluded that it was more effective in allowing access to non objectionable URLs than other tested products.

Interestingly results are very close to previous studies.For instance eTesting Labs (eTesting Labs, 2001) also evaluated the CyberPatrol, they calculated CBR= 0.827 and IBR=0.061 that is almost close to the results of this evaluation i.e. CBR=0.884 and IBR=0.06. These results are very similar to Hunter. For instance he calculated the over blocking error rate of Net Nanny and CyberPatrol 3% and 9.1 % that are close to results of this evaluation i.e. 3.6 % and 6% respectively.

6 Conclusion

The evaluation of five filtering products gives the overview of their effectiveness to keep the children safe from content, conduct and contact risks. During the test it was revealed that filtering companies advertise many features but these features have their limitations and can cause false sense of security. For instance SafeEyes advertises the features of safe search, and the blocking capability of social networking sites and peer to peer file sharing applications. But during the test it failed to prove these claims. Similarly CyberSentinel claimed to record and block IM conversations but during the test it failed to fulfil theses tasks. Similarly each product failed to monitor the web based chat rooms and web based emails. There was no such product that could block proxy sites. Over blocking and under blocking was found in each product. Each product had its own limitations. None of the products proved accurate to safeguard the children from online risks and threats. However, these products can lessen the contact, conduct and contact risks. These products can be used as a layer of defence. In other words, some of the security is better than none of the security. But over reliance and the false sense of security can lead to potential harms.

Though this project has evaluated filtering products for number of online activities but this is just the overview of the effectiveness of filtering products. Because content on the internet is very diverse and there are billions of websites on the internet. For instance there were more than a billion websites by 2001, and many of them were changing daily (Heins et al. 2006). This point can be well explained by this example, if 250 objectionable websites are tested, and filter failed to block 30 websites. Then what will be the number of failure when there are more than one million objectionable web sites?

The focus of this evaluation was those products that are aimed for home users. Products aimed for schools, organizations, libraries, church, and ISPs may have complex structure, functionalities according to the requirements of their targeted customers. For instance, filtering products that are for networks and being deployed at server level may have different features and capabilities. In the future work those products could be evaluated for wider context. Nowadays smart phones are providing the feature of internet browsing. Children can access the internet via mobile phones or game consoles. Moreover there is rapid growth in internet technologies that are introducing new channels of threats. However there are some other limitations of this evaluation. For instance user content generated sites, personal web pages, and web blogs were not included in the evaluation. Children can upload their personal information, videos, and photographs there. Moreover, new channels introduced by web 2.0 are not limited to the evaluated channels. The future work can be carried out in these dimensions.

7 References

Byron, T. (2008), “Safer Children in a digital World”, the report of the Byron Review. http://publications.dcsf.gov.uk/eOrderingDownload/DCSF-00333-2008.pdf (Accessed 12 September 2009).

eTesting Labs. (2001), “U.S. Department of Justice Web Content Filtering Software Comparison”, Updated Web Content Filtering Software Comparison, U.S.A

Euroberometer Analytical report (2008) “Towards a safer use of the Internet for children in the EU- a parents’ perspective”.http://ec.europa.eu/public_opinion/flash/fl_248_en.pdf (Accessed 30 July 2009).

Heins, M., Cho, C. and Feldman, A. (2006),” Internet Filters, a Public Policy Report: 2nd Ed.” Brennan Centre for Justice NYU School of Law http://www.fepproject.org/policyreports/filters2.pdf (Accessed 10 August 2009).

Hunter, C.D. (2000), “Internet Filter Effectiveness: Testing Over and Underinclusive Blocking Decisions of Four Popular Filters”, ACM New York http://portal.acm.org/citation.cfm?id=332186.332302&type=series (Accessed 13 December 2009).

Jewkes, Y. (2010), 'Much ado about nothing? Representations and realities of online soliciting of children', Journal of Sexual Aggression, 16: 1, 5 — 18. http://dx.doi.org/10.1080/13552600903389452 (Accessed 30 March 2010).

Livingstone, S. and Haddon L. (2009), "EU Kids Online: Final Report."LSE, London. http://www.lse.ac.uk/collections/EUKidsOnline/Reports/EUKidsOnlineFinalReport.pdf (Accessed 10 August 2009).

Livingstone, S. and Bober M., (2005), "UK Children Go Online, Final report of key project findings. http://www.lse.ac.uk/collections/children-go-online/UKCGO_Final_report.pdf (Accessed 15 December 2009).

Ofcom, Office of Communications. (2007), Annex 5: "The Evidence Base-The views of Children, Young People and Parents", Ofcoms's Submission to the Byron Review. http://www.ofcom.org.uk/research/telecoms/reports/byron/annex5.pdf (Accessed 11 November 2009).

Ormes, S. (2009),"An Introduction to Filtering", an issue paper from the Networked Services Policy Taskgroup, UKOLN on behalf of EARL. http://www.ukoln.ac.uk/public/earl/issuepapers/filtering.html (Accessed 3 May 2009).

Social Engineering: Phishing for a Solution

U.Odaro and B.G.Sanders

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Following the remarkable success experienced by social engineers at targeting America Online (AOL) services, they realised the potential for targeting other organisations (Ramzan, 2007). Phishing-based social engineering attacks exploit human vulnerabilities as opposed to software vulnerabilities. As a result, these attacks pose a threat to unsuspecting end users. This research measured users' awareness of phishing attacks. A combination of legitimate and illegitimate emails and websites scenarios were presented to 153 participants through an online survey. The results showed on an overall level that the participants classified 43% of the legitimate emails correctly and 67% of the illegitimate emails correctly. Furthermore, the participants classified 73% of the legitimate websites correctly and 56% of illegitimate websites correctly. The remaining proportion which constituted the misclassified and uncertain responses however revealed a significant lack of awareness on the part of the respondents, indicating a need to improve user awareness in relation to phishing attacks. Additionally, the certificate of a website was included in the study which revealed that only 33% of the respondents had ever checked for the certificate of a website.

Keywords

Phishing, Social engineering, Fraud, Spam, Security

1 Introduction

In the field of information security, social engineering is a term used to describe a non technical kind of intrusion that relies on manipulating people into divulging confidential information and performing unwitting actions (Tipton and Henry, 2006). Social engineering is effective because it is a low risky activity which involves an indirect attack by preying on human vulnerabilities such as fear and consequence, inexperience, desire to be helpful and the desire to be loved, to name a few. These tactics allow the social engineer to avoid raising suspicion (Peltier, 2006). Typical social engineering attacks include phishing, malware, hacking and email scam. Phishing being the most prevalent attack is the focus of this research. Phishing is a form of deception in which the social engineer impersonates a trustworthy institution in an attempt to acquire sensitive information from the potential victim for fraudulent activities (Jagatic, 2007). As a result of the deceptive tactics of social engineering which exploit human vulnerabilities, unsuspecting users tend to be susceptible to phishing attacks.

The aim of this research was to assess the vulnerabilities of end users in relation to phishing-based social engineering attacks. In a similar manner to Karakasiliotis et al

(2007), a survey based research was employed with a major focus on the email aspect of phishing. Alongside the website aspect of phishing, the certificate of a website was also considered. This paper however begins with a background exposition on phishing trends and highlights previous findings in relation to users' susceptibility to phishing attacks.

2 Phishing Trends

While phishing started out with attacking America Online (AOL) users, it is a common facet in today's society. Typical phishing attempts target customers of banks, online payment services and auction sites, to name a few (Ramzan, 2007). Phishing attacks are typically executed through the internet which facilitates mass distribution of emails in a short time frame. In recent times, phishing activities have continued to thrive in spite of the technological measures put in place by organisations, campaign by the target industry sectors and the advent of anti-phishing organisations. According to Anti-Phishing Working Group (2009), the number of unique phishing reports submitted, reached an all-time high of 40,621 in August 2009 which surpassed the previous record high of 38,514 reported in September 2007 by nearly 5.5%. Furthermore, Gartner survey on the cost of phishing attacks in the United States revealed that $3.2 billion was lost as a result of phishing attacks in 2007 (Gartner, 2010). VeriSign (2009) while evaluating the impact phishing could have on an organisation stated that phishing attacks against an organisation could diminish an organisation's online brand and prevent customers from using the legitimate website for fear of falling victim to a phishing attack.

3 Previous research on phishing attacks

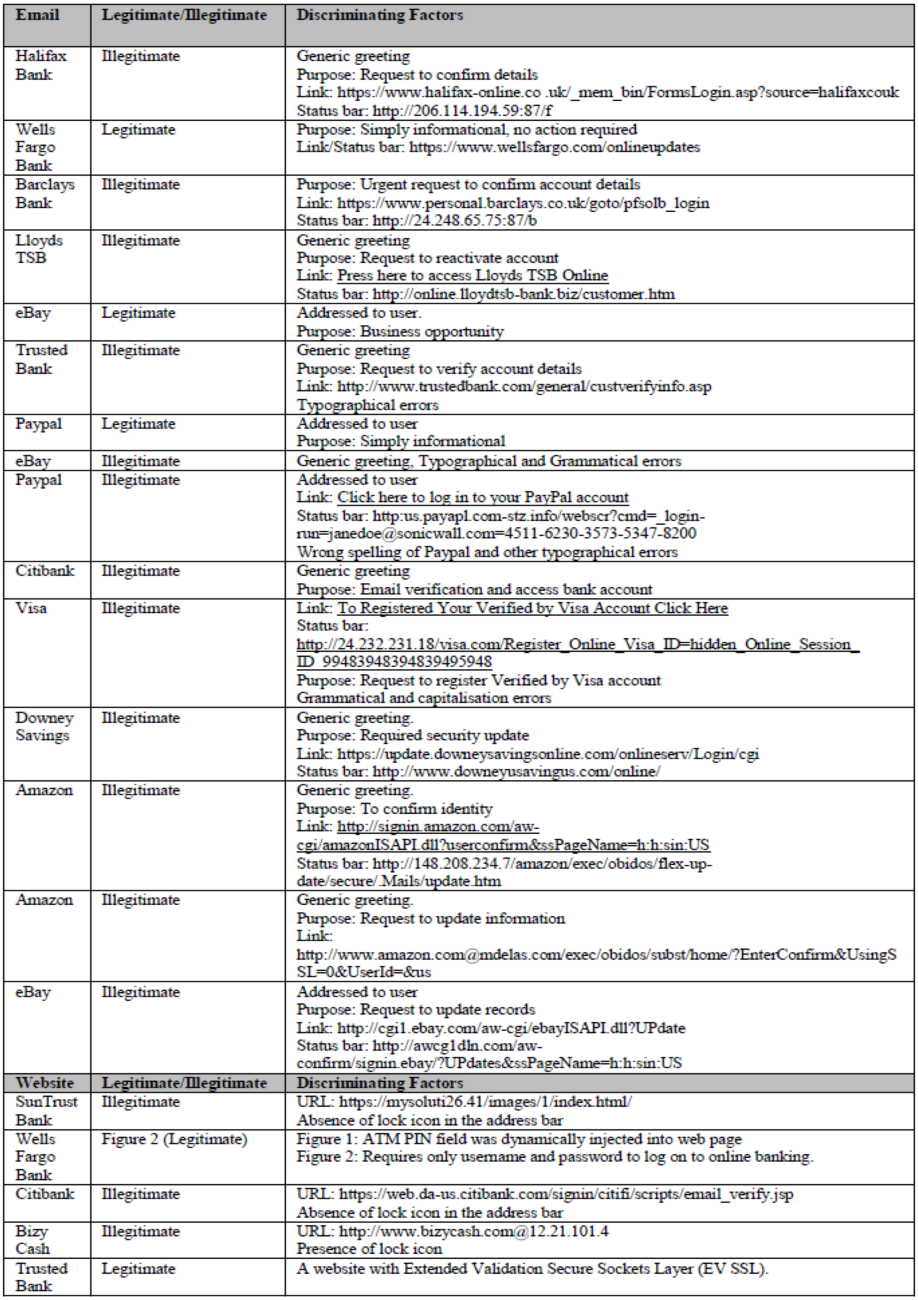
Going by the phishing trends, several researches have been conducted to assess users' vulnerability to phishing attacks. The identified studies in relation to this research are those of Dhamija et al (2006), Karakasiliotis et al (2007) and Herzberg and Jbara (2008) which revealed that users are susceptible to phishing attacks. However, the most similar study to this research was that of Karakasiliotis et al (2007), which presented 20 emails (11 phishing emails and 9 legitimate emails) to 179 participants through an online survey. From the overall level of misclassification of emails, Karakasiliotis et al (2007) concluded that there was a level of confusion among the participants and subsequently highlighted the need for increased security awareness. In view of these findings, there is still a lack of awareness of phishing attacks in spite of awareness raising information from target industry sectors and anti-phishing organisations. Many users may not take the trouble to read the information provided on phishing attacks unless they become victims to phishing attacks (Krebs, 2004). In light of this, it was considered appropriate to measure current level of awareness of phishing attacks.

4 Research methodology

The online survey was facilitated through the LimeSurvey application hosted on the Centre for Security, Communications and Network Research (CSCAN) server at Plymouth University. Considering the shift change in communication preference occasioned by the advent of the internet and the fact that an online survey can be completed in an individual's convenient time, it was envisaged that this method would be appealing to end users and impact on the quantity of research data (Surveybounty, 2009). Furthermore, the quality of research data was improved as respondents are more prone to give more honest answers to sensitive questions than an interview or paper based research by virtue of the affordance of anonymity provided by online surveys (Surveybounty, 2009). The online survey contained 43 questions grouped into four sections including user demographics, usage of computer and online services, general security awareness and scenario study on phishing. The user demographics section gathered demographic details about the respondents including gender, age, country of origin, current country of residence, educational background, area of study and area of experience. Additionally, this section determined the percentage of respondents who had undergone training in computer security. The second section, "usage of computer and online services", established that all the respondents indeed use ebanking and email services. Furthermore, the purpose was to gather details based on the duration the respondents had used ebanking services. The third section, "general security awareness", determined the knowledge and attitude of the respondents in relation to security practices and their ability to recognise security concerns. The final section, "scenario study on phishing", which constituted the major section of the survey was focused on important factors to determining the legitimacy and illegitimacy of emails and websites. Following the study by Karakasiliotis et al (2007) which showed a high level of uncertainty amongst the participants in relation to identifying legitimate and illegitimate emails, it was however considered appropriate to place more emphasis on phishing emails. There was a total of 15 email scenarios and 5 website scenarios which were gathered from different sources on the internet. Table 1 below provides the status and discriminating factors of the emails and websites. In addition to the emails and websites, the scenario study included the certificate of a website, asking the respondents if they have ever checked for the certificate of a website.

5 Results and Discussion

A total of 153 respondents were recruited via email invitation. 56% of the respondents were males while 44% were females. 48% were in the age group 18-29, 40% were 30-39, 9% were 40-49, 2% were 50-59 while 1% was above 60 years. 74% of the respondents were resident in developed countries (United Kingdom, United States of America, Ireland, Denmark and Saudi Arabia) while 26% were resident in developing countries (Nigeria, South Africa, Thailand and Namibia). 69% of the participants held a Postgraduate degree, 28% held a first degree, 1% were undergraduate students while the remaining 2% were educated up to secondary / high school level. The majority of the participants who held a postgraduate degree were students of Plymouth University. 38% of the respondents studied IT/Computing related courses while the educational background of the remaining 62% was unrelated to IT/ Computing. In addition to the educational background of the respondents, 33% of the participants had undergone training in computer security while the remaining 67% had not.



Email	Legitimate/Illegitimate	Discriminating Factors
Halifax Bank	Illegitimate	Generic greeting Purpose: Request to confirm details Link: https://www.halifax-online.co .uk/_mem_bin/FormsLogin.asp?source=halifaxcouk Status bar: http://206.114.194.59:87/f
Wells Fargo Bank	Legitimate	Purpose: Simply informational, no action required Link/Status bar: https://www.wellsfargo.com/onlineupdates
Barclays Bank	Illegitimate	Purpose: Urgent request to confirm account details Link: https://www.personal.barclays.co.uk/goto/pfsolb_login Status bar: http://24.248.65.75:87/b
Lloyds TSB	Illegitimate	Generic greeting Purpose: Request to reactivate account Link: Press here to access Lloyds TSB Online Status bar: http://online.lloydtsb-bank.biz/customer.htm
eBay	Legitimate	Addressed to user. Purpose: Business opportunity
Trusted Bank	Illegitimate	Generic greeting Purpose: Request to verify account details Link: http://www.trustedbank.com/general/custverifyinfo.asp Typographical errors
Paypal	Legitimate	Addressed to user Purpose: Simply informational
eBay	Illegitimate	Generic greeting, Typographical and Grammatical errors
Paypal	Illegitimate	Addressed to user Link: Click here to log in to your PayPal account Status bar: http:us.payapl.com-stz.info/webscr?cmd=_login-run=janedoe@sonicwall.com=4511-6230-3573-5347-8200 Wrong spelling of Paypal and other typographical errors
Citibank	Illegitimate	Generic greeting Purpose: Email verification and access bank account
Visa	Illegitimate	Link: To Registered Your Verified by Visa Account Click Here Status bar: http://24.232.231.18/visa.com/Register_Online_Visa_ID=hidden_Online_Session_ID_99483948394839495948 Purpose: Request to register Verified by Visa account Grammatical and capitalisation errors
Downey Savings	Illegitimate	Generic greeting. Purpose: Required security update Link: https://update.downeysavingsonline.com/onlineserv/Login/cgi Status bar: http://www.downeyusavingus.com/online/
Amazon	Illegitimate	Generic greeting. Purpose: To confirm identity Link: http://signin.amazon.com/aw-cgi/amazonISAPI.dll?userconfirm&ssPageName=h:h:sin:US Status bar: http://148.208.234.7/amazon/exec/obidos/flex-up-date/secure/.Mails/update.htm
Amazon	Illegitimate	Generic greeting. Purpose: Request to update information Link: http://www.amazon.com@mdelas.com/exec/obidos/subst/home/?EnterConfirm&UsingSSL=0&UserId=&us
eBay	Illegitimate	Addressed to user Purpose: Request to update records Link: http://cgi1.ebay.com/aw-cgi/ebayISAPI.dll?UPdate Status bar: http://awcg1dln.com/aw-confirm/signin.ebay/?UPdates&ssPageName=h:h:sin:US
Website	**Legitimate/Illegitimate**	**Discriminating Factors**
SunTrust Bank	Illegitimate	URL: https://mysoluti26.41/images/1/index.html/ Absence of lock icon in the address bar
Wells Fargo Bank	Figure 2 (Legitimate)	Figure 1: ATM PIN field was dynamically injected into web page Figure 2: Requires only username and password to log on to online banking.
Citibank	Illegitimate	URL: https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp Absence of lock icon in the address bar
Bizy Cash	Illegitimate	URL: http://www.bizycash.com@12.21.101.4 Presence of lock icon
Trusted Bank	Legitimate	A website with Extended Validation Secure Sockets Layer (EV SSL).

Table 1: Discriminating factors of emails and websites in the survey

In relation to the email scenarios, an aggregate response showed that the participants classified 43% of the legitimate emails correctly, 28% of the legitimate emails incorrectly while the remaining 29% were "I don't know" responses. Furthermore, the participants classified 67% of the illegitimate emails correctly, 11% of the illegitimate emails incorrectly while the remaining 22% were “I don’t know” responses. Table 2 below illustrates these findings.

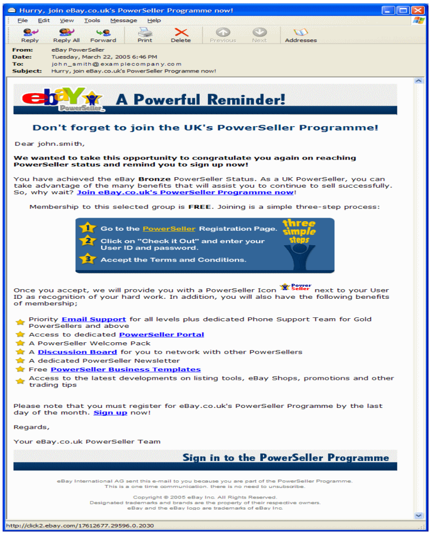
	Correctly classified	Incorrectly classified	I don't Know
Legitimate emails	43%	28%	29%
Illegitimate emails	67%	11%	22%

Table 2: General perception of email scenarios by respondents

Though phishing has continued to thrive in recent years, the findings when compared with Karakasiliotis et al (2007) as illustrated in table 3 below, revealed an improvement particularly in relation to classifying illegitimate emails correctly. This may be an indication that efforts being made in recent times by target industry sectors and anti-phishing organisations with regards to awareness raising strategies have made an impact on end users. Further comparison however showed that the proportion of “I don’t know” responses seemed to be in direct correlation with the findings by Karakasiliotis et al (2007) indicating the need for increased security awareness in relation to phishing attacks.

	Correctly classified	Incorrectly classified	I don't Know
Legitimate emails	36%	37%	27%
Illegitimate emails	45%	28%	26%
Overall	42%	32%	26%

Table 3: Accuracy of message classification (Source: Papadaki et al, 2008)



Hurry, join eBay.co.uk's PowerSeller Programme now!

From: eBay PowerSeller
Date: Tuesday, March 22, 2005 6:46 PM
To: john_smith@examplecompany.com
Subject: Hurry, join eBay.co.uk's PowerSeller Programme now!

A Powerful Reminder!

Don't forget to join the UK's PowerSeller Programme!

Dear john.smith,

We wanted to take this opportunity to congratulate you again on reaching PowerSeller status and remind you to sign up now!

You have achieved the eBay **Bronze** PowerSeller Status. As a UK PowerSeller, you can take advantage of the many benefits that will assist you to continue to sell successfully. So, why wait? Join eBay.co.uk's PowerSeller Programme now!

Membership to this selected group is **FREE**. Joining is a simple three-step process:

1 Go to the PowerSeller Registration Page.
2 Click on "Check it Out" and enter your User ID and password.
3 Accept the Terms and Conditions.

Once you accept, we will provide you with a PowerSeller Icon next to your User ID as recognition of your hard work. In addition, you will also have the following benefits of membership;

- Priority Email Support for all levels plus dedicated Phone Support Team for Gold PowerSellers and above
- Access to dedicated PowerSeller Portal
- A PowerSeller Welcome Pack
- A Discussion Board for you to network with other PowerSellers
- A dedicated PowerSeller Newsletter
- Free PowerSeller Business Templates
- Access to the latest developments on listing tools, eBay Shops, promotions and other trading tips

Please note that you must register for eBay.co.uk's PowerSeller Programme by the last day of the month. Sign up now!

Regards,

Your eBay.co.uk PowerSeller Team

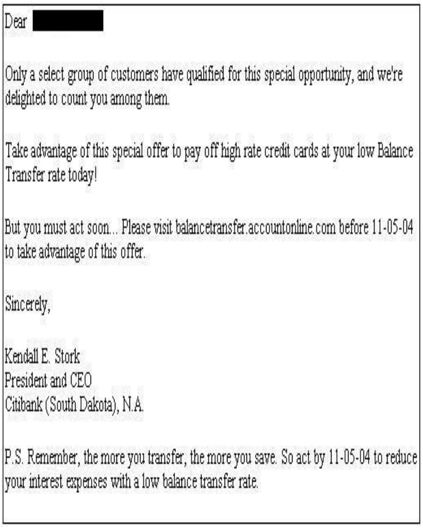
Sign in to the PowerSeller Programme

eBay International AG sent this e-mail to you because you are part of the PowerSeller Programme.
This is a one time communication. there is no need to unsubscribe.

Copyright © 2005 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are trademarks of eBay Inc.

http://click2.ebay.com/17612677.29596.0.2030

Figure 1: Most misclassifed email



Dear [redacted]

Only a select group of customers have qualified for this special opportunity, and we're delighted to count you among them.

Take advantage of this special offer to pay off high rate credit cards at your low Balance Transfer rate today!

But you must act soon... Please visit balancetransfer.accountonline.com before 11-05-04 to take advantage of this offer.

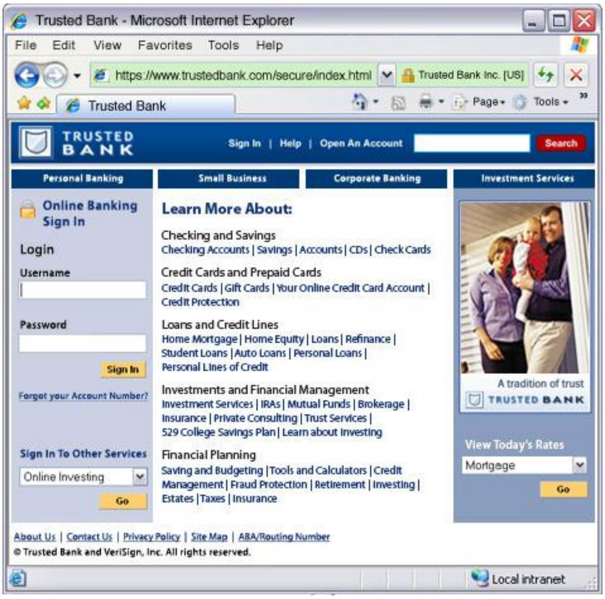
Sincerely,

Kendall E. Stork
President and CEO
Citibank (South Dakota), N.A.

P.S. Remember, the more you transfer, the more you save. So act by 11-05-04 to reduce your interest expenses with a low balance transfer rate.

Figure 2: Most misclassifed email (Source: Papadaki et al, 2008)

Like the findings by Karakasiliotis et al (2007), the respondents seemed to be more prone to classifying legitimate emails incorrectly. As suggested by Karakasiliotis, this may have indeed been due to a heightened level of suspicion with regards to phishing attacks or the respondents may have just been more cautious by reason of the survey exercise. Specifically, the email which was misclassified by the majority of respondents was the legitimate eBay PowerSeller email as shown in figure 1 above, despite the fact that it included a named recipient and did not request for account details. Only 45 (29%) of the respondents were able to correctly identify this email as legitimate. The content of the email showed that there may have been previous correspondence between eBay and the named recipient. However, further analysis of the email revealed that the email exhibited a sense of urgency which included “a powerful reminder” to sign up now for the eBay PowerSeller programme. This may have aroused the suspicion of the majority of respondents who may have been conditioned to associate such emails as scams. This finding is very much in line with that of Karakasiliotis et al (2007) where the majority of respondents also misclassified a legitimate email (figure 2) due to its sense of urgency and despite the fact that it was addressed to a named recipient and did not request for any update on account details. It is important to state that the emails in question from both studies shared a similar characteristic in terms of presenting a business opportunity and special offer to the benefit of the customers. Most business opportunities indeed have a time frame. As a result, email indeed needs to be reclaimed as a viable business tool otherwise organisations may have to be cautious with regards to email dispatched to their customers. In relation to the websites, an aggregate response revealed that the respondents classified 73% of the legitimate websites correctly, 7% of the legitimate websites incorrectly while the remaining 20% were “I don’t know” responses. Additionally, the participants classified 56% of the illegitimate websites correctly, 19% of the illegitimate websites incorrectly while the remaining 25% were “I don’t know” responses. It is important to state that further analysis on the overall rate of correct classification of legitimate websites revealed that the majority of respondents correctly classified the Trusted bank website with Extended Validation Secure Sockets Layer (EV SSL) as shown in figure 3 below. EV SSL provides an easy and reliable way for end users to determine the legitimacy of a website through the display of a green address bar with the name of the organisation and the certificate authority (CA) that issued the SSL certificate (VeriSign, 2009).



Online Banking Sign In

Login

Username

Password

Forgot your Account Number?

Sign In To Other Services

Learn More About:

Checking and Savings
Checking Accounts | Savings | Accounts | CDs | Check Cards

Credit Cards and Prepaid Cards
Credit Cards | Gift Cards | Your Online Credit Card Account | Credit Protection

Loans and Credit Lines
Home Mortgage | Home Equity | Loans | Refinance | Student Loans | Auto Loans | Personal Loans | Personal Lines of Credit

Investments and Financial Management
Investment Services | IRAs | Mutual Funds | Brokerage | Insurance | Private Consulting | Trust Services | 529 College Savings Plan | Learn about Investing

Financial Planning
Saving and Budgeting | Tools and Calculators | Credit Management | Fraud Protection | Retirement | Investing | Estates | Taxes | Insurance

A tradition of trust
TRUSTED BANK

View Today's Rates

About Us | Contact Us | Privacy Policy | Site Map | ABA/Routing Number
© Trusted Bank and VeriSign, Inc. All rights reserved.

Figure 3: Trusted bank website with EV SSL.

68% of the respondents classified the website correctly, 10% classified the website incorrectly while the remaining 22% could not classify the website. This is an indication that a significant proportion of end users are aware of the significance of the green address bar of EV SSL. In relation to the certificate of a website, 50 (33%) respondents indicated that they have attempted to check for the certificate of a website while the remaining 103 (67%) indicated that they have never checked for the certificate of a website. Additionally, only 39 out of the 50 respondents who indicated they had checked for the certificate of a website could indeed identify how to locate it on a website. Furthermore, 48% of the 153 respondents indicated that they know the significance of a certificate while the remaining 52% indicated otherwise. Identifying security indicators such as certificate is not effective against phishing as a large proportion of respondents neither check for the certificate of a website nor know its significance. As a result, phishers can improve their chances at targeting such users equipped with knowledge of only basic indicators (such as https, lock icon and URL) as suggested by Herzberg and Jbara (2008). To this end, usable design framework should take into consideration "what humans do well and what they do not do well" rather than solely relying on traditional cryptographic based security framework as suggested by Dhamija et al (2006). In line with Karakasiliotis et al (2007), the overall findings of this survey revealed that users are susceptible to phishing attacks taking into consideration the significant proportion of misclassification of emails and websites. Further analysis of the survey results according to demographics, revealed that gender did not play a role in the respondents' judgment of the emails and websites. Furthermore, there were no significant differences in relation to the country of residence, educational background; respondents who studied IT related courses versus non-IT related courses, respondents who had undergone training in computer security versus respondents who had not taken any such training and phishing victims versus non-phishing victims. The slightly improved judgment for respondents who studied IT related courses and those who had undergone training in computer security seem to be indicative that such knowledge may just be an added advantage. Individual judgment and perception may have a more significant role in end users' vulnerability to phishing attacks. There was however a progressive level of awareness according to the number of years the respondents had used ebanking services.

6. Conclusion and Future work

This survey based study revealed that users are vulnerable to phishing-based social engineering attacks indicating that there is still a significant lack of awareness in line with previous findings. An understanding of how to identify a phishing attack cannot be underestimated as current anti-phishing mechanisms may not guarantee the user complete protection. As a result increased user awareness is paramount as a countermeasure against phishing. Organisations should equip users on their style of communication and actions they would never require from end users.

In future research, an equal distribution of participants would however improve the findings in relation to users' vulnerability to phishing attacks according to country of residence, educational background and age group. Unlike the study by Dhamija et al (2006) which included an adequate number of website scenarios, this research included only 5 website scenarios as the major focus was on emails. As a result, future experiments with a focus on websites would facilitate a more accurate judgment in relation to users' ability to determine the legitimacy of a website.

7. References

Anti-Phishing Working Group (2009) "Phishing Activity Trends Report: 3rd Quarter 2009" Available at: http://www.antiphishing.org/reports/apwg_report_Q3_2009.pdf (Accessed: 15 January 2010).

Dhamija, R., Tygar, J.D. and Hearst, M. (2006) "Why Phishing Works", Proceedings of the SIGCHI conference on Human Factors in computing systems, Montréal, Québec, Canada. pp. 581-590.

Gartner (2010) "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks", Available at: http://www.gartner.com/it/page.jsp?id=565125 (Accessed: 21 January 2010).

Herzberg, A. and Jbara, A. (2008) "Security and Identification Indicators for Browsers against Spoofing and Phishng Attacks" ACM Transaction on Internet Technology, 8 (4)16, pp.1-36.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menezer, F. (2007) "Social Phishing", Communications of the ACM, 50 (10), pp. 94-100.

Karakasiliotis, A., Furnell, S.M. and Papadaki, M. (2007) "An assessment of end-user vulnerability to phishing attacks", Journal of Information Warfare, 6 (1), pp. 17-28.

Krebs, B. (2004) "Phishing Schemes Scar Victims", Available at: http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18?language=printer (Accessed: 16 June 2010).

Papadaki, M., Furnell, S., Dodge, R.C. (2008) “Social Engineering Exploiting the Weakest Links”, European Network and Information Security Agency (ENISA). Available at: http://www.ifap.ru/library/book349.pdf (Accessed: 21 November 2009).

Peltier, T.R. (2006) 'Social Engineering: Concepts and Solutions', Information Security Journal: A Global Perspective, 15(5), pp.13-21.

Ramzan, Z. (2007) “A Brief History of Phishing: Part 1” Available at: http://www.symantec.com/connect/blogs/brief-history-phishing-part-i (Accessed: 12 January 2010).

Surveybounty (2009) “23 Advantages of Online Surveys”. Available at: http://www.surveybounty.com/articles/surveyadvantages.html (Accessed: 24 November, 2009).

Tipton, H.F. and Henry, K. (2006) “Official (ISC)2 Guide to the CISSP CBK”. Florida: Auerbach Publication.

VeriSign (2009) “Fraud Alert: Phishing – The Latest Tactics and Potential Business Impact” Available at: https://www.verisign.com/static/phishing-tactics.pdf (Accessed: 14 January 2010).

Improving the Usability of Security Features in Tools and Applications

B.Rangarajan and S.M.Furnell

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The purpose of this research is to identify, investigate and improve the usability of security features in tools and application. Users and application developers can benefit by the end of this research after understanding the concepts of usability and how an alternative approach can be useful among the tech-savvy users as well as product developers who can think of making a security much more usable and effective. The main objective of the research is to investigate the issues surrounding the usability of security features in various tools and applications and try to familiarize with the issues. Further, a specific security tool is taken for study and based on which, a usability study is carried out in order to find out the users' attitude level on usability as well as how they understand the security features present in a tool. Also developers too need to focus more on usability and make the users more attracted towards using a product more freely than any constraints. The analysis section of the usability study would be helpful in identifying the common usability issues and participant's attitude level towards handling the security features present in an antivirus application. Based on which, a mock interface implementation would be designed and developed & try to make the security feature more usable. This would benefit end-users and product developers for the future works.

Keywords

Security, usability, user interfaces.

1 Introduction

In our modern technology-focussed world, the need for computer security is ever demanding. There have been numerous developments in the field of Computer and Information Security. As a result, there have been a lot of applications and systems developed and deployed worldwide, such as antivirus, Firewall, Intrusion Prevention/Detection Systems. Although, they provide a good protection level to all kinds of users and consumers, there would be a question arising in the mind whether are these products and their features usable? The answer would be fairly No from an end-user perspective. Developers on the other hand focus upon the technology that they tend to embed into a product and sometimes they forget that the product ought to be useful by a fair means of users. So the need for usable security arises when a security is not understood, learnt, clear enough for any user.

2 Research Aim & Objectives

The main aim of the research is to investigate & identify the issues that surround usability in general. Further to research on the issues surrounding usability of security tools and security features in other tools and applications. Later, a usability study would be conducted in order to get a good research based detailed study on usability issues and users' attitude towards using a security feature in a tool or application like antivirus. To accomplish this, the aims and objectives have been break down into smaller tasks so as to make the thesis a good research based and to provide a good valuable source of information on usability. Some of the main objectives of the research are listed below:

- To investigate the need for security, usability and usable security in an application.
- Further identify the key issues surrounding within the reach of security of usable security in any tool or application.
- Based on this research and a further study that is to be carried out on usability among different users will help to analyze and identify the problem areas where the users find difficult in using the antivirus application.
- This would help to improve or suggest an alternate approach to software developers in the design of usability features present in a tool or application.

3 Usability of security features

Computer and Information Security in this modern world are growing as most demanding needs in various organizations. Home users and other end-users too started seeing security as one of their real-time demand whenever they used their computers. But some of the security features of the products or the products itself are developed for the purpose of security are not usable to users. According to AOL/NCSA 2004 survey titled 'Online Safety Study', nearly 90% of the respondents did not know what action has to be taken when a scan report is shown by their anti-spyware software. Adding to this, a 33% of the users did not understand their firewall's functionality mostly and 20% of them did not understand completely. (AOL/NCSA, 2004) The reason is the products that they were using were not fully usable. So the security that was aimed at was of no use because of any usability to the users.

"*Lack of Usability can cause problems which, at one end of the scale, frustrate or annoy the user and, at the other end of the scale, might be life-threatening*" (Jordan, 1998)

Usability not only frustrates or annoys a user; it also can create great losses to the organization as a product manufacturer in terms of reputational loss, financial loss, loss of loyal customers. (Klien Research, 2010). Thus usability is very much important in a product or application. Usability can be defined by many ways. In computer perspective, usability can be referred to as Human Computer Interaction (HCI).

“Human Computer Interaction, or HCI, is the study, planning, and design of what happens when you and a computer work together. As its name implies, HCI consists of three parts: the user, the computer itself, and the ways they work together”. (Danino, 2001)

Also usability cannot be defined or considered as a single dimension factor. It is a multi-dimension factor where it needed to be characterized and categorized. Usability of a security feature depends on some of the factors like: (Usability, 2010)

- Ease of learning
- Efficiency of use
- Memorability
- Error frequency and severity
- Subjective satisfaction

4 Barriers to Usability

Although, there are a lot of factors regarding usability, there are some barriers that stand as an obstacle in achieving the usability. These barriers are both technical as well as non-technical barriers from an end-users perspective. (Johnston, Eloff, Labuschgane, 2006) They are :

- Lack of Users’ Knowledge
- Complex design interface
- Technical issues:
- Visible and simple details
- Frequent Errors or alerts

To achieve a better usability, first one has to investigate and identify the issues. Later, the cause for the issues followed by studying the issues and figuring out how to overcome it has to be analyzed. Evaluating Usability or identifying the issues surrounding usability is a different approach altogether. One cannot choose a specific method of evaluating. There are various methods like: (Klien Research, 2010)

- Usability Studies
- Contextual assessments
- Competitive analysis
- Heuristic evaluations
- Cognitive walkthroughs
- Focus Groups
- User Surveys

Thus using one of the methods specified above, one can identify and investigate the issues surrounding the usability amongst the end-users. In this research, usability survey is adapted as the evaluation method for to understand the users’ attitude level as well as knowledge level on security features of their antivirus application that they use. Also users were asked about few questions related to prototypical interface depiction of security alerts to read the users' opinions on how it could create an impact on the study for this research.

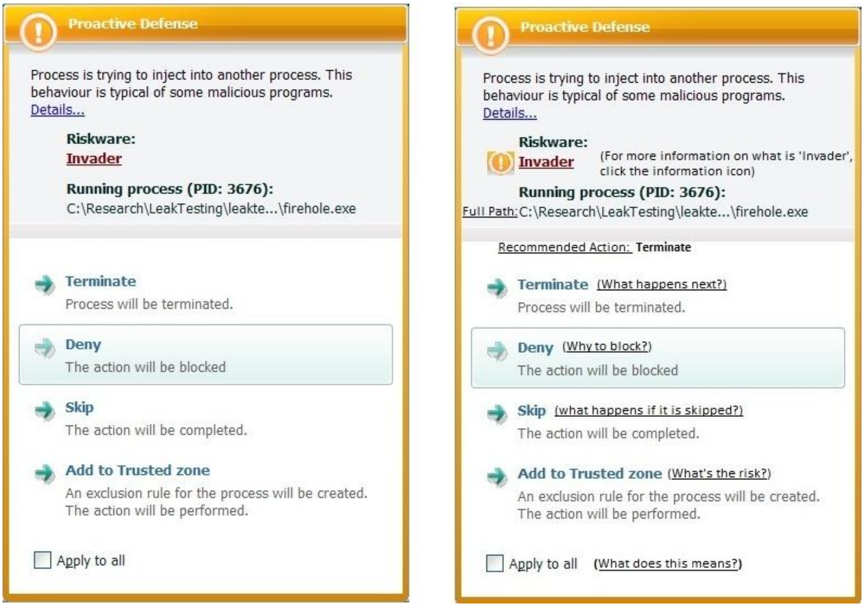
5 Usability Survey

The usability survey was conducted online and obtained responses from 108 participants around the world. It was hosted online within the Center for Security, Communications and Network Research (CSCAN) and it was held online for a period of nearly 10 days and there were a total of 133 responses out of which only 108 were completely filled. So the results of the 108 respondents were considered for the final analysis in this thesis. The majority of the participants who responded were in the age group of 18-25 and next highest participant group were aged 26-35. Participants were asked questions about their opinions on antivirus features that they use, alerts they encounter on a daily basis. Most of the participants felt that their antivirus provides sufficient information on the security alerts but many felt that the information provided by them was too difficult to understand due to insufficient information, too much technical involved, confusing information etc.

When asked about whether their antivirus product provides sufficient information on the security alerts that is encountered, 66 participants answered 'Yes' and 42 respondents felt their antivirus did not provide sufficient information on encountering security alerts. The next set of questions were based on their choices between using an antivirus, understanding the antivirus or is it both easy to use and understand with regards to their personal antivirus application. Out of all participants, 48 participants felt that their antivirus is good enough to ease of use than trying to understand what it is. Some 24 participants felt that it was easier to understand what it does than try using it. And finally 38 respondents felt that their antivirus is both easy to use as well as easy to understand. Asked about whether their antivirus software provides appropriate guidance on which action to be taken in case of a security alert, 67 participants felt they did assist them while 41 others felt that their antivirus products did not provide proper guidance in taking an action on alerts who accounts to 38% of all respondents.

Participants were asked how they usually manage to handle a security alert or any other warning messages from an antivirus. About 37% of the participants said that they would look the internet or the antivirus website for additional information while roughly 30% of them felt they would take default action or seek someone's additional help on this to take a final action. About 7% of the participants said that they would take action upon their experience related to their previous encounters and depending upon the security alert, it would be better to predict their actions. This shows the participant's attitude level. Although there were more participants who felt that they would take default action, it is clear that some users are still not comfortable in taking a decision on their own. Only very few participants he felt that they could use their experience and recall their previous encounters to tackle any security alerts that occurred again. This shows that most of the users were little bit ignorant on responding to a security alert as very few were able to handle by themselves. This could be due to either user's lack of knowledge or it could be due to insufficient information or not convincing warning message from the antivirus that had prompted the users to take upon default action.

Also many of the participants felt that automation of actions from antivirus could be helpful in handling a security alert without the intervention of the participants. About 72% of the participants felt the need for making the antivirus to take actions on their own for few default actions on default threats and reports. There are so many advancements made in the antivirus technology and features in order to make the antivirus product more effective, efficient and more usable. From a users' point of view, they would be relieved if the antivirus takes necessary action upon default alerts like that of update, scan report, virus detecting etc. But in case of a system restart or suspicious file behavior, possibility of automating the actions is quite a tough ask because most users would not like to get their work interrupted and it is not a good idea too if the antivirus takes hold of the system and tries to resolve the issues on its own. This is only for specific related problems but still it is arguable to come to a conclusion.



Proactive Defense

Process is trying to inject into another process. This behaviour is typical of some malicious programs.
Details...

Riskware:
Invader

Running process (PID: 3676):
C:\Research\LeakTesting\leakte...\firehole.exe

Terminate
Process will be terminated.

Deny
The action will be blocked

Skip
The action will be completed.

Add to Trusted zone
An exclusion rule for the process will be created.
The action will be performed.

□ Apply to all

Proactive Defense

Process is trying to inject into another process. This behaviour is typical of some malicious programs.
Details...

Riskware:
Invader (For more information on what is 'Invader', click the information icon)

Running process (PID: 3676):
Full Path: C:\Research\LeakTesting\leakte...\firehole.exe

Recommended Action: Terminate

Terminate (What happens next?)
Process will be terminated.

Deny (Why to block?)
The action will be blocked

Skip (what happens if it is skipped?)
The action will be completed.

Add to Trusted zone (What's the risk?)
An exclusion rule for the process will be created.
The action will be performed.

□ Apply to all (What does this means?)

Figure 1: Kaspersky alert (old & modified)

Some participants who were either intermediate or advanced level felt that too much additional information would also be likely to confuse a user or annoy an end-user. When they were presented with two different figures of same alert and with the second figure being the modified alert, about 82% felt that the additional information contained in the security alert were actually clear and easy to understand. When asked about their explanation to their choices, there were some few interesting things to consider. Some participants felt that the quality or level information contained is likely to help a novice or an intermediate user, but at the same time, the amount of information could eventually become too much for a user to read and he might feel difficult in understanding first of all. Also there were participants who felt that the recommendations from the antivirus on which action should be taken was really helpful not only for a novice user but also to any user who are even comfortable in using an antivirus.

When the participants were presented with a prototype of a security alert taken from that of a newer version of Kaspersky antivirus application and a modified picture as shown in figure 1, of the same alert with additional information on the actions to be taken, help regarding the actions what would happen after taking upon the certain action etc. Out of 108 participants, 89 of them felt that the figure that was modified to have additional information contained sufficient information and helped them in learning and understanding the alert in a better way. Also 79% of the participants felt that the level of detail present in the modified alert was appropriate and very few felt that it was vague and too much confusing. Asked about whether the alert would benefit the user, 67% of the participants said that it s likely to inform the user. But some advanced users felt that too many details were clustered and it was unnecessarily detailed information that even a novice user would be scared of forever. After analyzing the survey, it is found that majority of the users felt that security alerts should be meaningful, clear, provide sufficient advice on what actions to be taken and what would happen if a particular action is taken upon by the user. Also 78% of the participants felt that antivirus should be automated in handling a security alert message without requiring the intervention of the users' choice.

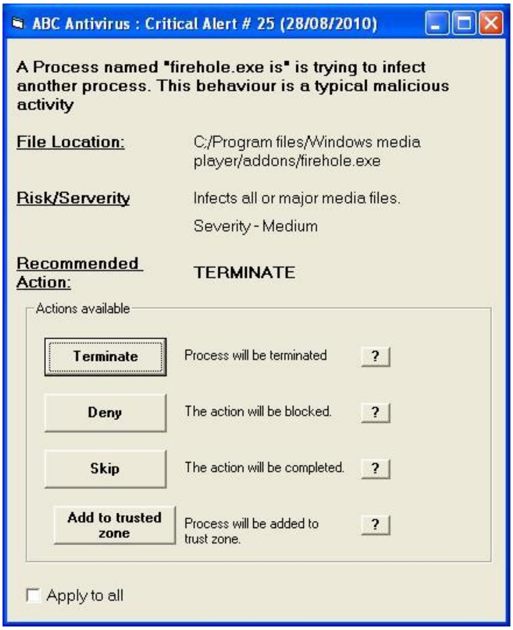
A set of participants felt that the modified alert is really helpful in understanding the information not only easily but also in a clearer way. In addition to the participants' understanding, the figure could have tweaked in a better way. As discussed earlier, the original security alert taken from figure 1 & 2, there are some things that is missing or not added. When looking closer at both those figures, it is evident that it is a security alert from an antivirus application. But looking deeper in terms of overall information, one may have a suspicion that it could be a bogus or fake threat because the title window of the alert did not have the antivirus application's name as the title and instead, it had some different name that could be misleading a user. Also, when looking at figure 2, some users felt that there was information insufficiency. It had some actions to be taken as Terminate, Deny, Skip and Add to trust zone. But it did not contain any further information what each action takes. That part of information is present in the modified security alert and that could possibly help even a novice user knowing that it is from his antivirus software only. An intermediate or advanced level user would identify it easily or comfortably.

Antivirus security alerts do not necessarily have the timestamp on which each alert is generated. For example, if an alert comes up and if timestamp is checked from the reports or events section, it would show the name of the alert and the date occurred. But for this to check, a user should normally navigate through the menus of the application and a novice user would not find it easy to look at it. So it would be a good idea to have a timestamp on the title bar itself along with the alert id or number that could be generated to help the user recall or remember the previous alert occurred and any fake alerts occurred could make the user aware of it and take appropriate actions.

6 Alternate Approach to Usability

Based on the analysis of the survey results, there are some possible alternative approach that could be taken in order to provide a better usable security in an antivirus. With the results and analysis in mind, a mock implementation of a security alert interface was developed. It had the same features like that of the original Kaspersky alert but had some extra information without being clustered. The newly developed interface has a proper title name in the alert window with alert id for the users to identify. It also provides timestamp in the top of the alert window that the user can identify next alert comes up. So on this way, fake antivirus alerts can be detected and users can be aware of it.

Also in the main window, there is additional information on what is the recommended action that could be taken and there are some help buttons for each action's clear information in a simpler language if the user wanted to know what would happen if he had to take that particular action. Also there is a short description on the risk of the file that is suspected to be the detected threat and there is a severity of the file that is infected. This could possibly help a user of intermediate of advanced user and sometimes novice user can also benefit from this by getting to know what the infected file would do.



ABC Antivirus : Critical Alert # 25 (28/08/2010)

A Process named "firehole.exe is" is trying to infect another process. This behaviour is a typical malicious activity

File Location: C:/Program files/Windows media player/addons/firehole.exe

Risk/Serverity Infects all or major media files.

Severity - Medium

Recommended Action: TERMINATE

Actions available

Terminate
Process will be terminated
?
Deny
The action will be blocked.
?
Skip
The action will be completed.
?
Add to trusted zone
Process will be added to trust zone.
?

□ Apply to all

Figure 2: Interface designed as part of a mock implementation

Figure 2 is the newly developed interface as part of a mock implementation. It has all the require information regarding a security alert and possible actions that could be taken by the user.

Some of the distinct features and achievements of usability from this sample interface are:

- It has a good interface design with appropriate name in the title bar of the alert.
- It has a minimal design and almost same amount of information contained as in an original antivirus security alert.
- The design is Informative and learnable for all kinds of users.
- There is no clustering of information and still all the additional information is kept intact to make a user pleased while facing it.
- Error prevention is achieved in this as users after getting to know about the actions taken can prevent from making errors.
- Clarity of language is simple and easy to understand for any kind of user.
- The task identification has been appropriate that no extra unwanted information or task is performed in this mock interface.
- Design has been done in order to facilitate all kinds of users not just a novice or intermediate IT user.

7 Conclusion

The aim of the research was to investigate, identify and improve the usability of the security features present in a tool or application. Usability of an antivirus feature not only lies with the way they are designed and implemented, but also depends on the users' attitude towards it. If only a user can change his approach towards using a product, there can be a massive shift in achieving usability or any other similar feature in a product. But one cannot blame a user for not knowing about the antivirus feature as it is not quite possible for every user to be familiar with a technical product like that of an antivirus. So the organization that develops a product should focus enough on the usable security that could be really usable among all the possible users. If not, at least for the majority of those people that come across that feature or product frequently in their work or profession. Thus going back to the saying, usability is not a single dimension factor. It needs to be characterized, categorized. Thus usability could possibly be achieved better with a good combination of organization's alternative approach and users' way of approaching a product and its feature.

Although the mock implementation looks fairly simple and easy to trade of, there are quite a few limitations on it. The mock interface is only implemented based on the previous opinions from the participants on a similar interface in the survey. So this could be evaluated among a group of participants or as a focus group to know how this implementation can have impact on usability from a users' perspective. Also, the message box that comes after choosing an action is sometimes annoying to the users. So it can be replaced by a tooltip instead just moving the mouse across the action button. Further, in this thesis there was only particular feature analyzed i.e. security alerts used for creating a mock implementation. Future work could be done on some other security features present within an antivirus or any other tool or application.

Automation of antivirus' actions upon a security alert could be done in the future as part of further improvement in this research and could be evaluated.

8 References

AOL/NCSA. (2004). *AOL/NCSA Online Safety Study.* Available: http://www.inspectagadget.com.au/board/docs/safety_study_v04.pdf. Last accessed: 03 Aug 2010

Danino, N. (2001). *Human-Computer Interaction and Your Site.* Available: http://articles.sitepoint.com/article/computer-interaction-site. Last accessed: 28 July 2010.

Jordan, P. (1998). *An Introduction to Usability*. p16.

Johnston J, Eloff J.H.P, Labuschgane L. (2006). Security and human computer interfaces. *Security and human computer interfaces*. 22 (8), p3.

Klien Research. (2010). *Which Evaluation Approach to Use?.*Available: http://www.kleinresearch.com/pdf/klein_which_approach.pdf. Last accessed 13 Aug 2010

Usability. (2010). What Does Usability Measure Available: http://www.usability.gov/basics/index.html. Last accessed: 28 July 2010

Security Culture in the Context of National Culture

J.Thomas and S.M.Furnell

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

On a general level, it becomes clear that different countries have different perceptions with respect security and privacy concerns. For example, while many countries may have legislation in place to cover issues such as computer crime and misuse, or data protection, others may lack concern on such issues. Security may be a primary concern for citizens of countries having a reliable technological infrastructure; on the other hand priority may shift from security to infrastructure development for citizens belonging to developing countries. The above factors highlight the technical influences; in addition a range of societal values may also influence attitudes. As the internet is known to cross all borders and jurisdiction, protecting information and maintaining a sense of security is truly a challenge faced by many countries, especially their government authorities.

Keywords

Security, nationality, culture.

1 Introduction to security culture

Security culture is a new dimension in the area of information security. Up until now the concept of security culture has not been defined. Recent research papers relate security culture to improvement of adherence to the security policies (Security Governance.net, 2010). With the global nature of internet and the number of online transactions being performed on a daily basis, security implementation becomes a challenge. The nature of required security varies from individual to individual and organization to organization. Supporting activities in such a way that information security becomes a natural aspect in all the daily activities of internet users should be the primary objective of promoting a security culture. Security culture helps in building the necessary trust between the different components of the organisation and its reliability on the internet. Information security culture is therefore considered as an integral part of organisational culture (Schlienger, 2003).

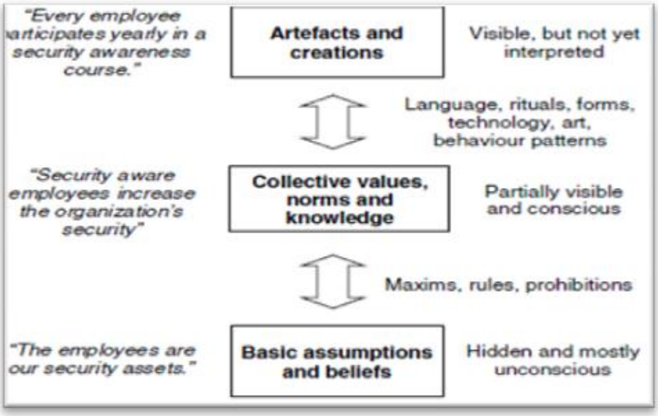

"Every employee participates yearly in a security awareness course."
Artefacts and creations
Visible, but not yet interpreted
Language, rituals, forms, technology, art, behaviour patterns
"Security aware employees increase the organization's security"
Collective values, norms and knowledge
Partially visible and conscious
Maxims, rules, prohibitions
"The employees are our security assets."
Basic assumptions and beliefs
Hidden and mostly unconscious

Figure 1: Three levels of security culture (Source: Schlienger, 2003)

2 The Security culture model

The main substances of an organizational culture are basic assumptions and beliefs. The assumptions are based on the nature of the people, their behavioural traits and the relationships they share. The organizational culture is expressed in terms of collective values, norms and knowledge of the organizations. These norms and values affect the behaviour of the people. Norms and values are expressed in form of artefacts and creations which include handbooks, rituals and anecdotes (Schlienger, 2003). It is noteworthy that ultimately it is the organizational culture which largely contributes to the corporate success. As mentioned earlier organizational culture grows with time and it is shaped by the behaviour of dominant organizational members such as the founders and top-level management. Fig.1 illustrates the three layers of security culture and their interactions.

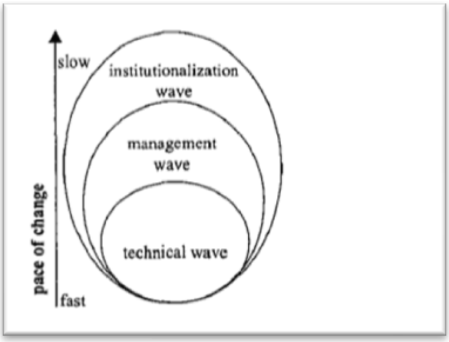


Figure 2: Institutionalization wave, management wave and technical wave (Helokunnas, 2003)

In addition to the above organizational considerations it is important to understand the implications of security culture in a global value net. Resources such as information, knowledge and time are also huge contributors of information security culture. Concepts of value, value creation and value nets are the popularly discussed matters in industrial marketing and management literature (Helokunnas, 2003). Value is measured as a trade-off between benefits and sacrifices. In a typical scenario value is defined in terms of financial benefits, but considering a wider perspective non-monetary assets like intellectual capital, market position and social aspects may be includes as well. In general terms value net could be understood as a network of organizations or actors interconnected with either a direct or indirect exchange relationship (Helokunnas, 2003). Modern day value net and business environments require organizations to connect themselves to telecommunication networks and exchange information. Fig. 2 shows the three waves of information security: the technical wave, management wave and institutionalization wave which are responsible for shaping a healthy security culture.

3 What to analyse in security culture?

In order to understand the implications of security culture on information security, it is important to analyse and understand the factors influencing security culture. Unfortunately there is no standard method or toolset to identify the existence of a security culture or its diversity. Therefore a considerable amount of research is still required in this domain. Due to the complexity and no pre-defined methodology for research, lot of challenges are faced by the experts and researchers. Security culture can be analysed by considering two things

(i) By measuring the collective norms, values and awareness

(ii)Measure the cultural indicators and try to derive the cultures (Schlienger, 2003)

The first aspect seems to be very promising but it has some problems associated with its practical implications. Values are mostly defined by theoretical constructs. Therefore values become increasingly vague and comparisons between individuals on this basis get difficult. Values are difficult to be stated as most of the times they are revealed unconsciously. On the other hand values attributed to negative social sanctions are hidden consciously.

The limitations of the first approach, brings us to the second which deals with analysis of cultural indicators. Qualitative research methods are one good approach to analyse cultural indicators and influences. Security culture encompasses social, cultural and ethical aspects which would be instrumental in understanding and improving related behaviour. In addition, it would be worth noting that security culture does not include basic human norms and beliefs (Schlienger, 2003). However, having this approach of qualitative research could be successful as human behaviour is ultimately driven by cultural, social and ethical aspects. Moreover, human factors influenced by the above three aspects also play an important role in ensuring that policies and procedures are followed appropriately.

4 How to analyse security culture?

For the analysis of the data the above two methods are not effective as they do not propose empirical analysis. So it would be advisable to use a approach which uses empirical outcomes with statistical analysis. So for achieving the above objective, two methods are used

(i) For gathering observable indicators, analysis of documents and other resources were carried out.

(ii) Similarly for measurement of norms, values and beliefs narrative focus group sessions were conducted.

Focus groups are an effective method for gathering information for qualitative research. To analyse security culture a series of five focus groups composed of 3-6 participants were conducted. The sessions composed of participants belonging to different countries with participants belonging to the name nationality in each session. The participants were recruited from the university campus and it was also ensured that there was a balance between students pursuing computer related courses and those pursuing other non-related courses. However there arises a concern with regards to the extent to which the participants actually represent their general national population. The sessions addressed security concerns, measures and other aspects which were to be considered by users while using the internet. These concerns and issues have been illustrated in the following sections. Furthermore the sessions were video recorded for analysis of issues and drawing conclusions.

Achieving good information security awareness in the general population of Internet users is of the fundamental nature if they are to remain secure and electronic business is to flourish. Comparing the home and work environments, it is clear the latter provides more prospects for such awareness programs to take place. However, it is normal human tendency that the practised followed at work need not be followed at home. Some aspects of a nation’s security culture have evolved as a logical response to security threats, and are adopted by the users. Some users learn about practises and policies as part of a natural socialisation process that is not controlled, and that leads to behaviours and attitudes in use that may or may not be approved by the organisation’s managers.

Currently the term "information security culture" is often drawn near models describing organizational culture. However, considering only the organizational culture **is** not sufficient for understanding the influencing factors behind information security culture. Each individual working for an organization or accessing the internet at home is influenced by several ethical, national and organizational cultures. These cultures have an effect on the way the individual infer the meaning and importance of information security. .

In some countries confidentiality of information is often emphasised upon while integrity and availability of information is buried. However, confidentiality, integrity and availability need to strike a balance. Development of information security culture is needed to ensure and balance the confidentiality, integrity and availability of information and knowledge at institutional level and also the home user level.

4.1 Misconceptions

Security culture is vastly affected by the misconceptions that most of the internet users possess. Firstly many users believe that the internet is absolutely secure and that its foundations are not susceptible to attacks. Reality is, 13 of the top-level DNS are vulnerable to flooding, basically targeting the root servers. Secondly government lapses could also be responsible for occurrence of security incidents which may be due to inefficiency, mis-management or ignorance. Users are also under the impression that only large organizations are targeted, but in reality hackers target home users as well. This also means that users have a false sense of security and assume that only intended users can see their systems (which is not the case, the moment a system is connected to the internet, it becomes a potential target). Users also lack awareness with regards to security tools and solely rely on one security mechanism such as firewalls or anti-virus software. As per the survey conducted most of the users were satisfied with the firewall technology, but also felt that it required some improvement. This mis-conception also goes beyond this, where users think their security is someone else’s responsibility.

4.2 Concerns

With the existence of a wide range of vulnerabilities, it is important to understand the potential concerns of internet users. Viruses and malicious code was still a popular concern among most users, in spite of having updated anti-virus software installed. It was even pointed out that most of the malicious codes propagated through emails. Spam was another concern, as users reported to have been receiving mails which had nothing to do with them. However, not many users faced incidents related to hacking, this may be attributed to the fact that those users have given out some user credentials at undesired locations. Having experienced these incidents, users are not sure as to whom to report such incidents. Anti-virus software vendors were a popular choice for reporting malicious activities such as worms, viruses and Trojans. As the law in most countries (especially developing countries) are just evolving, even government officials could not be relied for dealing with such incidents.

4.3 Awareness of security measures

Having mentioned the concerns, users were known to consider some precautionary measures to deal with it. Majority of the users agreed on the reliability of anti-virus software and firewalls to achieve some basic level of protection. Maintaining updates and installing them was also one key point mentioned in each of the survey sessions. Passwords were regarded to be effective in maintaining system level security.

4.3.1 Security measures

A majority of the participants agreed on the reliability of antivirus software’s and firewalls to achieve a basic level of protection. The other issues could be taken care of with some basic user education and promoting awareness. For instance, the way different banks over the world dealt with phishing was known to be different. In developing countries banks were not liable for any financial losses incurred in a phishing incident. While in developed countries banks offered some amount of compensation to the victim. Similarly there was a point raised about the efficiency of judicial systems. Participants also expected government authorities to raise awareness and have effective measures to counteract security incidents.

4.3.2 Security updates

Having all the required security tools installed, updating them was one major point highlighted in each of the sessions. Most of the population considered updating anti-virus software and Operating System related components to be vital. The remaining population considered updating every piece of software and applications being used on a daily basis. The participants believed that most of the security issues and possible vulnerabilities could be addressed by installing updates. There was a considerable amount of awareness with regards to virus updates. This clearly visible when comments about implications of anti-virus software updates was put across. Almost everyone knew what the updates did with respect to updating latest virus definitions.

The next question with regards to updates, was that, how often was it recommended to install an update? The response to this issue was alarmingly positive, in the sense that most of them installed the updated the component as and when the updates where available. Latest application design techniques do not need the systems to be rebooted immediately as and when the update was installed. So most of the population either prefer to use automatic updates or delay to the time of their convenience. However there was some concern regarding the source of the update, and only a handful of the population actually bothered to check the source of the updates. Updates were acceptable, as there seemed to be no usability issues while installing them. The only concern was that, installing updates could introduce some compatibility issues with other applications. In a nut shell, security tools such as anti-virus software, spyware and firewalls where considered to be a primary necessity to have some level of security while connecting to the internet. Updating these components was the next level of security.

4.3.3 Passwords

Most of the above mentioned tools worked with minimum interaction with the user. To protect physical access to a system and information stored in it, passwords were widely accepted as a effective security mechanism. However, there was a need to analyse the participant’s idea of a strong password. Almost all the participants had a similar idea of a strong password, i.e. its composition included multi-case characters, numbers and special characters. The size range of a strong password was perceived to be around 8-16 characters in length. However, it was noticed that forgetting long passwords was a common problem. This induced the undesirable act of writing them down. In spite of having long password, none of the participants recommended using the ‘remember me’ check box below the password input area. Some of them felt that this would mean storing the password on some location on the system and make it available for access. Another issue pointed out was that of changing passwords. Most of the participants never actually changed their passwords. They were concerned that changing passwords too frequently would lead them to forget them. As users are known to have accounts with different systems, it was pointed out that the passwords to each of those systems were different and only accounts that didn't contain sensitive information were known to have same passwords. To conclude, the awareness possessed by users regarding passwords was pretty much similar in nature.

4.3.4 Online transactions

Security is a primary concern while conducting financial transactions over the internet. When asked about the comfort level while conducting online transactions and shopping online, a wide range of answers were obtained from the participants. The population of people belonging to developing countries felt that, though online transactions provided some amount of convenience, they were known to be insecure. While those from the developed countries thought that it was convenient and did not encounter problems while conducting them. Noteworthy was the fact that, though they were aware of the risks associated with such transactions, they only preferred using sites and forums they were well acquainted with. When asked about identifying secure websites, most of them pointed out the padlock symbol next to the URL as a prime necessity to actually perform a transaction on that particular site. A very few users also recommended using site advisors to determine if the site was a legitimate one or dubious. The sample of population who used the internet for shopping and other financial activities, also highlighted the aspect of using it only for transactions incurring a very small monetary value (they preferred shopping for large value items face-to-face).

4.4 Concerns with online transactions:

With the advent of e-banking and online shopping, most of the users were sceptical of conducting online transactions. Making purchases worth a small financial value was considered acceptable by most. Users looked for the security of the website and checked for the padlock while confirming any sort of financial transactions, only a handful of them knew what it meant though. However, there were variations in opinions obtained from people belonging to different countries on the same issue. Individuals belonging to developing countries did not possess the necessary risk taking ability. Convenience was one major advantage of online transaction with security as a trade off for most. The main concern was that of reliability of the infrastructure and the credibility of the websites. However people from developed countries showed more comfort and ease while using online shopping websites. This however reflected that concerns with respect to online transactions varied from country to country.

Social engineering attacks are another category of attacks that cause tremendous damage as well. During the survey sessions the following scenario was put across;

"You receive a e-mail reporting a failed attempt to transfer £950 from your bank account and a request to follow a link to your online banking pages to check for dubious transactions. How would u react?"

Half of the participants of the sessions considered confronting the bank though a telephone call or visiting the bank. They stressed on the fact that they would not click on the link whatsoever. Others pointed out the fact that they would log into their banking website through the actual link. Users were not aware of the fact that banks would not send e-mails pertaining to failure in transactions and direct them to the website and further ask for credentials. The other half mentioned that they would ignore the mail or simply delete it.

Thus it can be concluded that activities involving monetary aspects were considered highly critical and users are aware of the frauds and other scams that take place. This could be attributed to the awareness training programs or other means of educating online banking users.

4.5 Privacy

Privacy was one of the concerns expressed by most participants of the research sessions. A wide range of information was known to be disclosed during initial registrations at various websites and forums. Social networking sites are a very popular platform where users are known to reveal both a lot of unwanted information. When the issue of privacy was addressed, most of the participants instinctively thought about Facebook. All of the participants were known to have a Facebook page. When questioned about the type of information that was required to be protected, a wide range of answers were obtained. In general all the participants thought that personal information and contact details needed to be protected. Date of birth is one such piece of information which was a concern for some while for the others; it was dealt with as a ordinary piece of information disclosed. Contact details such as e-mail address and telephone numbers were the most important piece of information that according to the participants thought needed a high level of protection. A considerable proportion of the population were unaware of the means in which personal and contact information could be misused. Similarly they weren't even aware of the fact that such information could be used for social engineering attacks and other illicit purposes such as black-mailing etc. The condition stays the same for status updates and other preferences that are disclosed over such forums. Interestingly, a few of the participants even felt that medical records had to be protected and maintained confidential. This was mainly because a few of them participants felt that medical history was very personal and incidents of selling medical information had raised some concern. The participants were also aware of incidents related to internet companies selling customer information to other companies.

Social networking sites and other forums are known to disclose a lot of unwanted personal and contact information. Internet users are living under the illusion that privacy is always protected, which is not the case. Considering spam mails yet again, not many people actually know where the mail originated from or when they subscribed for the same. Personal information such as contact information, date of birth and even photographs has been misused over the internet. Yet users disclose such vital information over the internet without understanding the repercussions. Again national background plays a vital role. A particular piece of information considered private in one country may not be regarded the same in another. For instance, date of birth is considered highly confidential in the South-East Asian countries while it is considered just as another piece of information in western countries. Similarly during the survey, it was found that the responsibility protection of such information rested with website owners and government authorities. While it was not pointed that users too have some level of responsibility with regards to the tremendous amount of personal and unwanted information they disclose on social networking sites.

Participants reported to have registered at various forums and other websites through which they would like to receive regular updates and posts. Such websites are known to pay tribute to other organizations which target customers to increase their business. This brings us to the fact that companies may at times sell customer information with other companies to generate revenue. Through the survey topics, it was identified that participants were not aware of any such situation and that they trusted such forums to use their information for only legitimate purposes. The participants were not even aware if there were any laws which ensured protection to their personal information.

4.6 Legal aspects

The legal and judicial systems in different countries play an important role in shaping security culture. As per the survey it was concluded that laws in many countries were still evolving, as defining jurisdiction over the internet was a very complex task. In spite of having issues with information protection and privacy, a handful of the participants were aware of the laws pertaining to the same. Participants belonging to the western developed countries were to some extent aware of the laws protecting data (Data Protection Act). They also mentioned that the act was in most cases conflicting with the Freedom of Information Act. As far as developing countries were concerned the laws were non-existent as security issues were not a priority in those countries.

The legal system has a very important role to play in influencing an individual’s attitude towards security. Legal and regulatory aspects of the internet make the users more confident while using the internet and addressing issues that they may encounter. However, the participants were not exactly aware of the laws governing the internet in their respective countries. Another important factor that governs a particular country’s judicial system is the level of technological advancements achieved by country. As mentioned in the earlier sections, security is one aspect which is dependent primarily on the infrastructure availability within a country. Priorities of a developing country vary significantly from those of a developed country. This brings us to the conclusion that, in developing countries laws and legislation related to technology misuse are just being designed and approved. Countries which have concerns related to privacy have laws implemented to address the same. Data Protection Act is one such instance of law dealing with privacy issues. However Data Protection Act very frequently come into conflict with the Freedom of Information Act. The most challenging aspect of internet law is that, it is difficult to bring justice across the borders, as a particular illicit activity in one country may not be illicit in another.

5 Conclusion

For the purpose of this research, security culture was broken down into themes relating to daily internet usage and awareness with regards to concerns, security measures and legal system. As per the observations made during the survey sessions, every nation has some form of security culture in place. Security culture primarily depends on the technological infrastructure and its usage. For developing countries maintaining availability of the infrastructure is a primary concern, due to which security culture is not so prevalent at the moment. As far as developed nations are concerned, the infrastructure has existed for a while and is improving day by day, securing the infrastructure is the next step, so a more proactive security culture exists as compared to the developing countries. This can also be reflected in the number of users in the developed being comfortable in using the internet to carry out financial transactions and online shopping. However, internet users in developing countries are more concerned and sceptical while using this functionality of the internet. Not having a effective level of security over the has affected the risk taking ability of internet users. A considerable amount of similarity was observed with regards to the security mechanisms adopted, so security perspectives were very similar with this regards. The legal system varies across borders and hence the legislation for laws pertaining the internet are also bound to be different. The significance and sensitivity of the data to be protected also varies when we consider different countries.

Currently the term "information security culture" is often drawn near models describing organizational culture. However, considering only the organizational culture **is** not sufficient for understanding the influencing factors behind information security culture. Each individual working for an organization or accessing the internet at home is influenced by several ethical, national and organizational cultures. These cultures have an effect on the way the individual infer the meaning and importance of information security. .

6 Further Work

The current research work was restricted to the participants from the university campus itself. The research just focused on the various concerns and other factors which would influence the respondent’s attitudes towards security. Qualitative methods of analysis were successful in obtaining subjective answers from the participants; however the future research attempts could have a approach using a combination of both qualitative and quantitative research methodologies. As one aspect of this research focused on the analysis of awareness regarding the security measures, the subsequent research attempts could aim at analysing the usability issues of the same. In the future, a concrete methodology to analyse both qualitative and quantitative data would also be instrumental in given better results to the research.

7 References

Helokunnas, T. (2003). Information Security Culture in a Value Net. *IEEE.* 03 (1), p190-194.

Malcolmson, J. (2009). What is Security Culture? Does it differ in content from Organizational Culture?. *Security Technology*. 43 (1), p361-366.

Schlienger, T. (2003). Analyzing Information Security Culture: Increased trust by an Appropriate Information Security Culture. *IEEE*. 88 (3), p1-5.

Security Governance.net (2010). Security culture Available: http://www.securitygovernance.net/clulture/index.htm. Last accessed 17 July 2010

Section 3

Computer Science
&
Web Applications
Development

The Positive and Negative Implications of Emerging Mobile Technologies

T.Bolitho and B.G.Sanders

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

This paper identifies the positive and negative implications for society of emerging mobile technologies. Results were sourced through the administration of a global research survey, targeting an international audience of a broad demographic with a sample size of 106.

Keywords

Addiction; Capital; Always-On; Balance; Communication; Data; Mobile; Negative; Positive; Productivity; Social; Society; Technologies; Work-Life; Working

1 Introduction and Background Literature

Mobile devices can be loosely defined as portable devices that have in-built computing and/or Internet capability (Morley, 2008). The 1990's saw the dawn of a new age of mobility with a proliferation of mobile computing devices; the age of mobile computing was born (Cook and Das, 2005). A decade of research and development into hardware and software spawned a myriad of mobile technologies that laid the foundations of today's ubiquitous computing age (Weiser, 1991).

The emerging mobile technologies responsible for this age have caused such a shift in society that physical barriers to communication have been largely eliminated. Increased mobility has also made time and location barriers for work almost obsolete. The world is moving towards ubiquitous, seamless data connectivity that enables communication, access and sharing of information from anywhere, at any time, through the combined use of a multitude of mobile technologies (Bing and Lorenz, 2002). These technologies help individuals to fulfil commitments to work, friends and family. As a consequence, social relationships and the relationships between people and work are changing as we now find ourselves immersed in an 'always on' culture (Sorensen, Yoo and IFIP Working Group, 2005).

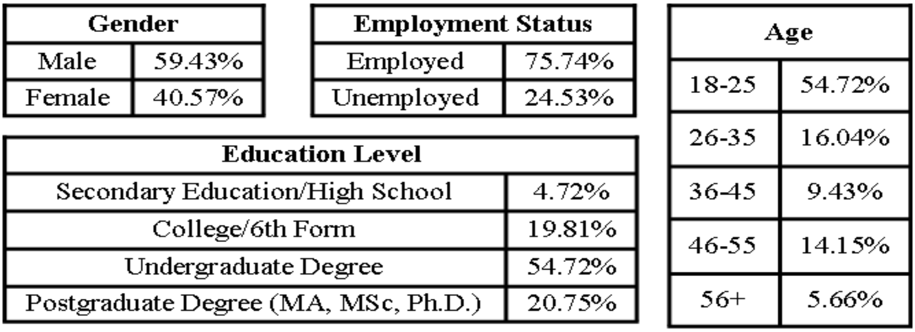
Metcalfe's law states that the value or usefulness of networked systems grows exponentially as the number of users linearly increases (Morville, 2005). In light of the estimated global penetration as of mid 2009 at 60%, totalling 4.1 billion mobile phone subscribers worldwide (Bhatti, 2009), the potential of mobile phones alone to impact on society is inevitably strong. Arminen (2007) highlights issues of increased accountability and social responsibility resulting from mobile technologies. Laursen

(2005) supports this, identifying a developing mobile-etiquette that involves norms for the reciprocation of calls and messages, and to always be available. The ability to multitask irrespective of time and location boundaries can be deemed both a positive and negative consequence of emerging mobile technologies - furthering productivity as well as the pressures to maintain it in both work and social environments.

Mobile communication now “profoundly affects the tempo, structure, and process of daily life around the world” (Katz, 2008: 3). Cairncross (1997) suggested that eradication of distance as a communication cost may be the most significant force that will change society in the first half of this century. Due to the rapidly developing, dynamic nature of mobile technologies, it is an academic subject that justifies continuous reflection and research to identify emerging trends and global sociological impact. Examining the implications for society in light of emerging mobile technologies is the primary aim of this study. Results are derived from a global questionnaire, designed to provide current insight into usage trends and society’s perspective of emerging mobile technologies.

2 Methodology

Primary research was conducted through administration of an online survey with an aim to provide insight into society’s perspective of emerging mobile technologies. 106 full responses were received, representing the sample size of the study. Survey respondent demographics were as follows:



Gender	
Male	59.43%
Female	40.57%

Employment Status	
Employed	75.74%
Unemployed	24.53%

Education Level	
Secondary Education/High School	4.72%
College/6th Form	19.81%
Undergraduate Degree	54.72%
Postgraduate Degree (MA, MSc, Ph.D.)	20.75%

Age	
18-25	54.72%
26-35	16.04%
36-45	9.43%
46-55	14.15%
56+	5.66%

Figure 1: Demographic Makeup of Primary Research Respondents

3 Results

3.1 Social Capital and Communications

Overall, 63% of respondents felt that their social life had improved through the use of mobile technologies. 71% of respondents felt that mobile technologies have increased the amount they communicate with their friends. 23% believed that mobile technologies have increased their number of friends, indicating that the majority of individuals felt that mobile technologies have not positively influenced the size of their friendship base. However, mobile technologies proved to strengthen existing social networks, with 55% in agreement. To further the cohesive influence of mobile technologies, 38% of respondents put forward that, through not embracing mobile technologies, individuals may actually be excluded from social network activity.

Mobile technologies seemingly hold greater strength in influencing society's formation and sustainment of intimate relationships as opposed to general friendships. Mobile technologies enabled 37% of individuals to talk to people they would not otherwise have spoken to. 50% agreed mobile technologies can result in the formation of intimate relationships that otherwise would not have occurred. 60% also believed that mobile technologies increase their inter-family communication and 84% agreed that mobile technologies facilitate parents contacting their children.

SMS was revealed to influence the above findings. 76% of respondents agreed that SMS aids people to develop and sustain existing relationships. 59% of respondents gained increased confidence to communicate with people through use of SMS. 20% of respondents had at some point formed an intimate relationship through SMS. SMS can however result in the misunderstanding of feelings, with 82% in agreement. 62% of individuals also felt that SMS hampered their ability to represent themselves in a positive manner. Despite this, 51% of respondents stated that SMS is now their primary means of communication, surpassing traditional voice calling in popularity.

3.2 3G and 4G

57% of respondents now have 3G capable mobile devices, 47% of which are satisfied with the speeds. Only 10% of those without 3G planned to upgrade soon.

Respondents were questioned on their willingness to upgrade their mobile devices to 4G when it becomes available. 7% of respondents would be willing to pay extra and 54% would be willing to upgrade if no extra costs were incurred.

3.3 Productivity

70% of respondents embrace mobile technologies to fill idle time (waiting for a train/bus etc). 45% of respondents stated they achieved productivity benefits at work through their use of mobile technologies. Overall feelings were however that mobile technologies do not make them more productive at work; only 31% agreed that their overall work productivity had actually increased.

Productivity benefits are seemingly being countered by interruptions in the workplace as a result of mobile technologies themselves; 59% of respondents were in agreement. 53% of respondents stated that mobile technologies actually stimulate unnecessary communication and disruptions in the workplace, lowering productivity. 37% of individuals also believe mobile technologies result in more communication, less time spent reviewing messages and decisions being made hastily as a result.

39% of individuals now spend more time dealing with e-mail and SMS than they spend completing assigned workloads. Emphasis from managers on the importance of effective communication is now imperative to reduce information volumes and the associated problems of 'information overflow'; 72% of survey respondents agreed.

3.4 Work-Life Balance

52% of respondents agreed that mobile technologies facilitate the organisation of their personal lives. A greater majority (74%) also agreed that mobile technologies facilitate the organisation of their professional lives. The ability to receive work communications anywhere and anytime was found to intrude on 36% of respondents' personal lives; explained partially by 45% of individuals that now find it acceptable for colleagues to contact them out of hours on their mobile device.

The negative implications of mobile technologies are furthered by the 37% of individuals that stated that mobile technologies have actually eroded the division between their work and home life, with 46% of individuals now feeling obliged to answer calls from colleagues outside of working hours. 22% of respondents also stated that they had seen no further benefits to their work-life balance as a result of this erosion. 23% of respondents also stated that mobile technologies have resulted in them working more hours, with only 12% actually earning more as a result.

Mobile technologies allow the majority of individuals to spend more time with friends (46% in agreement) and family (44% in agreement). 38% of respondents believed mobile technologies have strengthened their working relationships; however 28% of individuals suffer felt isolated due to mobile working practices. 8% also believed that mobile working has reduced the amount of friends they have at work.

Despite the potential for mobile technologies to facilitate work-life balance, only 27% reported overall work-life balance benefits, with 29% reporting a definite degradation to work-life balance and the rest remaining indifferent.

3.5 'Always On' Culture

Results revealed 84% of individuals' primary mobile communication technologies are always on; 82% keep them by their side at all times. 62% of individuals reply to SMS messages immediately and 46% of individuals respond to emails immediately.

Results identified mobile-etiquette involving norms of reciprocation of calls and messages, and to be always available. 28% of respondents felt that not replying to an email straight away may be interpreted as rudeness. 41% of individuals felt that not replying to an SMS message straight away may be interpreted in the same way. As a result of these evolving norms, 81% now check SMS messages as soon as they receive them; 58% reply straight away. 30% of respondents stated that if they did not reply to an SMS straight away, they were unlikely to reply at all.

3.6 Technology Usage/ Data Addiction

One third of respondents get anxious if emails or mobile devices are left unchecked for a few hours. 54% of individuals now check social network sites such as Facebook and MySpace throughout the day. 45% of working individuals now check work emails and voice messages during lunch hours, after hours and at the weekends. 22% even check work emails and voice messages whilst on holiday. 44% of individuals would now find it very difficult to go without using mobile technologies for a day.

3.7 Personal Security

Mobile technologies now give users more confidence to go out alone; 40% agreed, 33% disagreed and 27% remained indifferent. 48% of individuals are no longer afraid of getting lost due to mobile technologies. 44% of respondents now feel safer to be alone, with 94% stating that mobile technologies are invaluable in emergencies.

3.8 Privacy and Security

Regarding privacy and mobile technologies, 33% of respondents felt that mobile devices imposed on their privacy and personal space. When questioned, 74% of respondents expressed a degree of concern over mobile phone providers keeping records of SMS and calls. Despite these concerns however, only 26% of respondents had ever read the Privacy Statement that came with their mobile contract.

Findings indicated that 34% of respondents now admit to storing personal and sensitive information on their mobile devices. Only 50% of respondents' mobile devices were however protected with a password or PIN.

Only 48% of respondents had ever read the Privacy Statement of any social networking sites they had joined and used through mobile technologies. Reasons for not doing so included their excessive length (56%) or that they had not seen it (20%).

66% of individuals questioned have work colleagues on their social networking page friends list. 36% of individuals questioned have people they have never met face-to-face on their social networking page friends list. 40% of individuals questioned also have people they do not really know on their social networking page friends list.

83% of participants stated they knew how to change their social networking site privacy settings, 75% stated they had done so. However, 27% of individuals expressed concern over certain family members checking social networking pages, 27% of individuals expressed similar worries regarding current employers and 38% also expressed similar worries about future employers checking their social page.

3.9 Health

Mobile phones health implications concerned 42% of respondents. 77% of respondents felt more research is required into mobile phone health risks and 58% of respondents felt that mobile phone health warnings should be more publicised.

4 Discussion and Conclusions

The implications of the findings from the primary research are significant in indicating that mobile technologies positively impact society with regards to increased social capital and quality of social life. Friends and families benefit from the omnipresent connections that now link each individual through their personal mobile devices, strengthening existing relationships and building on new ones. Mobile technologies have been proven to enable individuals the confidence and ability to establish new relationships that would otherwise not have been possible, in some cases resulting in intimate partnerships.

Failing to embrace such technologies has however been found to cause social disadvantage. There is now the potential for individuals to be excluded from social networks and activities as a result of a lack of connectivity to their social network.

Mobile technologies are now overtaking traditional fixed line communication mechanisms, with SMS now being the primary means of society's communication and Wi-Fi now utilised in nearly every home. Whilst use of mobile services such as mobile commerce and mobile banking have yet to be embraced by the majority of society, the increasing usability of emerging mobile technologies including smart phones and PDAs may encourage use. However, as use increases so will the phenomenon of data addiction, a trait apparent in users of such technologies.

Emerging mobile technologies were proven to increase productivity through enabling users to effectively utilise time that was previously spent idle. With regards to working productivity, results highlighted the potential of emerging mobile technologies to increase it through allowing individuals to situate themselves at locations free of distractions and effectively work from anywhere, at any time. However, with only a small proportion of the population stating that their productivity had increased as a result of the use of emerging mobile technologies, productivity benefits are seemingly being countered through increased amounts of interruptions in the workplace as a result of mobile technologies themselves. Issues of 'information overload' were also raised, leading to correspondence being ill-prioritised, causing breakdowns in communications. Organisations need to train employees on correspondence efficiency to help resolve these issues.

Mobile technologies were found to facilitate individuals in the management of both professional and personal lives. These benefits come as a result of the ability to receive work communications anywhere and anytime, as well as the organisational facilities of mobile devices such as mobile calendars and reminders. Mobile technologies were also proven to strengthen working relationships between mobile working individuals, however, not for everyone. Some individuals are now being left feeling isolated through lack of face-to-face communication.

The consequential blending of home and working lives experienced by some individuals outweighed the benefits they received. Mobile technologies were found to be intrusive on personal lives, with some individuals now working longer hours for no remuneration. Obligation to respond to incoming communications is now causing increased intrusion and disruption of home and family lives, leaving almost half of working individuals with no choice but to discuss work outside of working hours. As mobile working increases as a tool to facilitate both the organisational productivity and work-life balance of employees, management practices require review and adaption to ensure that both the needs of the company and employee are met. Both mobile working individuals and organisations must work together to ensure that true productivity and work-life balance benefits are achieved and not simply an increase in working hours, which in turn may reduce an individual's quality of life with no consequential benefit.

Research results revealed that the ‘always on’ culture is prevalent within society. Results identified a developing mobile-etiquette that involves norms of reciprocation of calls and messages, and to always be available, putting pressures on society to be ‘always on’; keeping their mobile devices by their side at all times and checking them throughout the day. Individuals now check work emails and voice messages during lunch hours, after hours, at the weekends and whilst on holiday. Individuals are now expressing feelings of anxiety if they were not to check their email or mobile device every few hours, indicating a strong dependence on mobile devices and data. Such norms are inevitably likely to escalate as social mobile etiquette continues to develop - further fuelling ‘data addiction’ and the ‘always on’ culture.

Social networking applications are spurring a whole new scale of concern over privacy. The use of these applications through mobile devices such as smart phones and PDAs entails a two-fold privacy concern. Social networking organisations need to realise their responsibility in ensuring users remain aware of their rights and how to adjust privacy settings. Both mobile device and social networking organisations also require a radical rethink of the mechanisms used to deliver privacy statements, including summarisation of key privacy issues for those that do not have the time or patience to digest long, complex materials. More emphasis also needs to be made on the implications of privacy statements, as well as their existence and location for those that have simply never seen them. Users of such technologies also need to remain vigilant in who they accept as ‘friends’ to ensure their private lives remain private and do not implicate their professional lives.

The future will bring a convergence of hi-speed Internet and mobile devices; it is then likely that a strict distinction between mobile technologies and fixed point devices will cease to exist. Usage patterns will be increasingly difficult to measure as they become less standardised and the current myriad of devices, potential uses and demographics of users evolve. This global development will continue to stretch demand for speed, usability and feature richness of mobile devices and services.

As put forward by Wise (1997), society has developed the belief that political, moral and social problems are a result of a lack of communication and, if society improves communication, it will also solve some of the various problems that plague modern life. Future development of wireless infrastructures, services and devices will inevitably help to achieve global communication improvements, closing the digital divide, bridging social gaps between developed nations and those still developing with limited infrastructures and human rights. Use of mobile technologies however requires careful management and awareness of the potential threats that they impose to ensure that users’ privacy, security and quality of life is not implicated.

5 Future work

‘Information overload’, ‘data addiction’, work-life balance, security and privacy concerns were the issues identified as most typically implicating society as a result of emerging mobile technologies, potentially threatening future progression of the mobile economy. Future research should seek to further identify the causes and consequences of these phenomena and identify potential mechanisms of resolution. This will help to ensure that mobile technology economy continues to prosper and users continue embrace the true benefits without disadvantaging themselves in terms of privacy, security, work-life balance and overall quality of life.

6 References

Arminen, I. (2007) 'Review Essay Mobile Communication Society?', *Acta Sociologica*, vol. 50, no. 4, pp. 431-437.

Bhatti, B. (2009) *4.1 Billion Mobile Phone Subscribers Worldwide*, [Online], Available: http://telecompk.net/2009/03/03/41-billion-mobile-phone-subscribers-worldwide/ [30 Jan 2010].

Bing, B. and Lorenz, P. (2002) 'Networks: the proceedings of the Joint International Conference on Wireless LANs and Home Networks (ICWLHN 2002) and Networking (ICN 2002) : Atlanta, USA, 26-29 August 2002', Atlanta, 203.

Cairncross, F. (1997) *The death of distance: how the communications revolution will change our lives*, Boston: Harvard Business Press.

Cook, D.J. and Das, S.K. (2005) *Smart environments: technologies, protocols, and applications*, New York: John Wiley and Sons.

ITU (2004a) *Mobile Phone Subscribers Pass 4 Billion Mark*, [Online], Available: http://www.itu.int/ITU-D/ict/newslog/Mobile+Phone+Subscribers+Pass+4+Billion+Mark.aspx [05 Jan 2010].

Katz, J.E. (2008) *Handbook of mobile communication studies*, Cambridge, Mass: MIT Press.

Lan, Y.C. (2005) *Global information society: operating information systems in a dynamic global business environment*, Harrisburg: Idea Group Inc.

Laursen, D. (2005) 'Please Reply! The Replying Norm in Adolescent SMS Communication', in Harper, R., Palen, L. and Taylor, A. *The Inside Text: Social, Cultural and Design Perspectives on SMS*, New York: Springer.

Morley, D. (2008) *Understanding Computers in a Changing Society*, 3rd edition, Massachusetts: Cengage Learning.

Morville, P. (2005) *Ambient Findability*, Farnham: O'Reilly Media Inc.

Osborne, B. (2010) *CTIA survey – 1.5 trillion text messages sent in 2009*, [Online], Available: http://www.geek.com/articles/mobile/ctia-survey-1-5-trillion-text-messages-sent-in-2009-20100324/ [15 Jul 2010].

Royal Pingdom (2010) *Internet 2009 in numbers*, [Online], Available: http://royal.pingdom.com/2010/01/22/Internet-2009-in-numbers/ [15 Jul 2010].

Sorensen, C., Yoo, Y. and IFIP Working Group. (2005) *Designing ubiquitous information environments: sociotechnical issues and challenges*, New York: Springer.

Weiser, M. (1991) 'The Computer for the 21st Century', *Scientific American*, vol. 256, no. 3, pp. 94-104.

Culture of Integration: Literacy Tools for the Masses

A.Darracott and N.L.Clarke

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The purpose of this research is to assess the impact of literacy tools, which for this research are defined as wikis, blogs and discussion forums, on teaching and learning to determine the factors that might be inhibiting a realisation of their potential, and to begin to build a case for a change in research and implementation directions within teaching and learning environments from a focus of one literacy tool to a focus of using all three literacy tools. The survey data suggests that discussion forums are used a lot more in teaching and learning than existing literature suggest; additionally tutors and students use more than one tool for their teaching and learning, and overall students and tutors have a very positive view of their uses in teaching and learning. The data also shows evidence that students and tutors are willing to use the latest technologies such as mobile phones to access literacy tools, but it has to be questioned whether or not using mobile phones and other technologies such as iPads actually contribute to a pedagogic understanding of literacy tools. The results show that there is a lack of tutorial support for both teachers and students: over half of the student population and over three quarters of the tutor population state that they have not received any training on the technical and pedagogical uses and understanding of literacy tools because there is no training available, or that there is training available but they have not been made aware of such training. A culture of integration is possible, where students, tutors, course managers, researchers, institutional managers, and course tutors work together to integrate literacy tools and other technologies such as mobile phones and iPads in a way that complement, not compete with, existing teaching and learning styles within a given teaching and learning environment. More work needs to be completed, however, before a culture of integration is realised: assessing the suitability and effectiveness of existing student and tutor tutorials, integrating tutorial support for tutors within formal teaching and professional development programs, and to monitor the effectiveness of all tutorials to ensure that they are technically and pedagogically appropriate.

Keywords

Wikis, blogs, discussion forums, online learning

1 Introduction

A culture encompasses the beliefs, intentions, opinions, experiences and actions of a diverse set of individuals within a particular boundary, whether it be a religious boundary, a country boundary, or even a business or organisational boundary. In the case of teaching and learning, culture encompasses the tutors' teaching styles and attitudes towards teaching; the students' learning styles and attitudes towards learning, and the methods, tools and technologies used to deliver and enhance teaching and learning. Integration within teaching and learning encourages the inclusion of such styles, attitudes, tools and technologies in such a way that teaching and learning are enhanced. A culture of integration, therefore, is a view of encouraging the students and tutors to integrate technologies in a way that complement, not compete with, the teaching and learning styles and the nature of a given teaching and learning activity, in a manner that enhances the teaching and learning experience.

Literacy tools, which for this research are wikis, blogs and discussion forums, are a set of tools that aid the delivery of teaching and the development of knowledge and learning through the process of literacy itself: reading and writing, along with high order learning objectives: analysis, and critical reflection. Literacy tools provide the means by which learning can take place through collaboration *(Parker and Chao 2007)*, or through reflection and analysis of content *(Parsons 2004; Yang 2009)*. Existing literature, however, has placed focus only on the use of either a blog or a wiki as the main teaching and learning tool, with little or no focus on the use of discussion forums. Even less than this, there has been no attempt, so far as the literature search for this research has shown, to integrate the uses of these tools in order to enhance teaching and learning

This paper begins with reviewing the existing literature to establish a context of what has and has not been achieved followed by a brief explanation of the methodology that has been used. This is followed by a presentation of the most important or substantial findings, followed by a discussion of the findings focussing on comparing all three literacy tools in terms of what is being used and the frequency of their use in teaching and learning, how effective they are viewed by both the students and the teachers for teaching and learning, to determine if whether or not it would be practical to use all three literacy tools simultaneously, and suggest what further work needs to be completed to allow simultaneous use of all three tools in teaching and learning.

2 Literature review

Literature has focussed majorly on the uses and educational benefits of wikis and blogs with very little regard for discussion forums, which have been viewed as a tool to complement the research process rather than teaching and learning *(Wheeler et al 2008)*. To begin development of a culture of integration, there has to be an understanding of the potential uses and educational benefits that all three literacy tools provide to both teaching and learning. The effect that blogs are having on teaching and learning, and the view of their effectiveness as a teaching and learning tool, has been the subject of numerous research *(Yang 2009; Churchill 2009; Chan and Rideway 2006; Song and Chan 2008; Betts and Goldoff 2004; Parsons 2004; McMillion 2005; Craig et al 2008)*. The research suggests that the majority of participants experience no technical complications when using a blog and understanding how it works; however, it is not clear from the research that the students understand the pedagogical processes. Whilst there is some evidence suggesting that students are engaging with the blog in a collaborative manner, there is other evidence to suggest that blogs are best for personalised learning spaces. This does bring up questions regarding students' knowledge and understanding of how blogs work in a collaborative, constructivist learning environment.

Wikis have also been subject to various research regarding their effectiveness as teaching and learning tools (*Deters et al 2010, Parker and Chao, 2007; Tetard et al 2009; Hoorn and Hoorn 2007; Elgort et al 2008; Ritman et al 2005; Wheeler et al 2008 Bower et al 2006*). Just like blogs, there appears to be a lot of evidence to suggest that students have no problem with using the wiki technology. However, there is also a lot of evidence to suggest that students and even tutors are lacking the understanding of the pedagogic nature and benefits of a wiki. Students do not appear to understand how they should work with wikis in a collaborative manner, with little research into how these issues are to be resolved so that students and teachers can learn and teach effectively, respectively, in an online learning environment.

Reasoning behind the lack of pedagogic understanding of literacy tools is pointed towards a lack of student tutorials and the need for such tutorials *(Craig et al 2008; Bower et al 2006; Tetard 2009; Wheeler et al 2008; Ebner and Maurer 2007)*. Some researchers have suggested ways in which tutorials can be used to introduce students to literacy tools for learning *(Lamb 2004; Leung and Kai Wah Chu 2009; Elgort et al 2008; Tetard et al 2009)*. There has, however, been far less questioning and research into the knowledge and understanding of the tutor with regards to the use of literacy tools in teaching. Deters et al (2010) suggest that tutors are more likely to portray a positive influence over the students using a wiki, or any other literacy tool, if the tutors themselves understand the technical and pedagogical aspects of the technology being used.

3 Methodology

An electronic survey was made available to members of the general public for a period of over a month, from early July 2010 to the middle of August 2010. The members of the general public were notified of the survey through video sharing websites, social networking site Facebook, the internal Email system at Plymouth University, and tutor based discussion forums. A total of 92 participants completed the survey, all being current or previous students or teachers having some sort of experience of using wikis, blogs and discussion forums in formal teaching and learning settings or in general, informal settings.

The survey itself was used to collect quantitative data via closed questions, which were a mixture of multiple choice, single answer questions and multiple choice, multiple answer questions. The aim of the survey was to capture the thoughts, opinions, ideas and experiences of participants regarding their use of wikis, blogs and discussion forums as tools for teaching and learning. Also, to determine the level of knowledge the participants had regarding the use and understanding of literacy tools, and to give them the opportunity to evaluate any tutorials or training they might have received regarding the use and understanding of literacy tools.

4 Results

A total of 92 participants took part in the survey, 37 (40%) of which were students and 55 (60%) of which were tutors.

4.1 Uses of literacy tools in teaching and learning

51% of the total student and tutor population use literacy tools as part of their learning and teaching respectively. Both tutors and student population samples were asked to select the tools that they use as part of their teaching and learning:

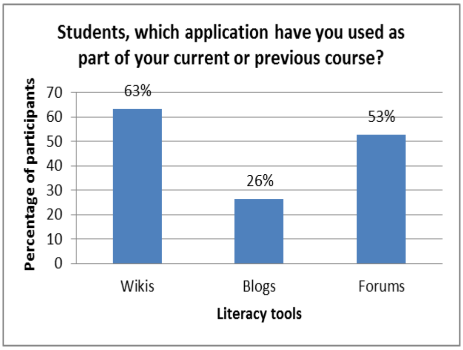


Figure 1: Percentage of literacy tool use by students

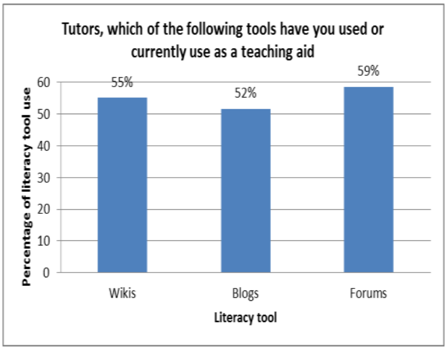


Figure 2: Percentage of literacy tool use by tutors

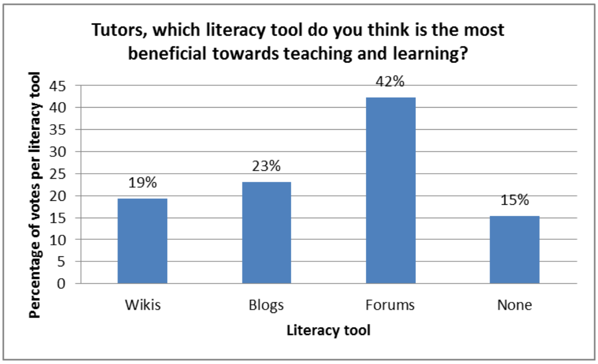


Figure 3: Most popular tool for teaching and learning

The percentages are relative to the subject population; therefore the percentages reflect the student and tutor population only and not the whole population. 48% of the tutor population stated that they use more than one literacy tool for teaching; 37% of the student population used more than one literacy tool for learning. Discussion forums have been voted the most beneficial literacy tool towards aiding the teaching and learning process by the teacher participants.

83% of the students who have used a wiki report a positive view of their use in their learning; 80% of students who used blogs also report a positive view and all of the students who use discussion forums also report a positive view of the use of discussion forums in learning.

Students who used literacy tools also note lack of difficulties in using literacy tools: 92% who used a wiki experienced no problems; 60% of students who used a blog experienced no difficulties, and all of the students who used discussion forums had no difficulties.

All tutors and students were asked if they would consider accessing literacy tools through mobile devices: 61% of students state that they would access the tools through a mobile device; 55% of the tutors have stated that they would also access literacy tools though mobile devices.

4.2 Evaluation of student and tutor tutorials

68% of the student population said that they had not received any training or tutorials regarding how to use literacy tools for their learning. From the 32% who had received training, 83% stated that they found the tutorials to be of good use. The students who stated that they did not have such tutorials, 60% believe that they would not have benefitted from such tutorials. 77% of the tutor population had not taken any form of training, with 73% of them stating that there were no training available, or that training could have been available but they had not been made aware of such training, which would indicate poor personal development skills or inadequate communication skills within the organisation.

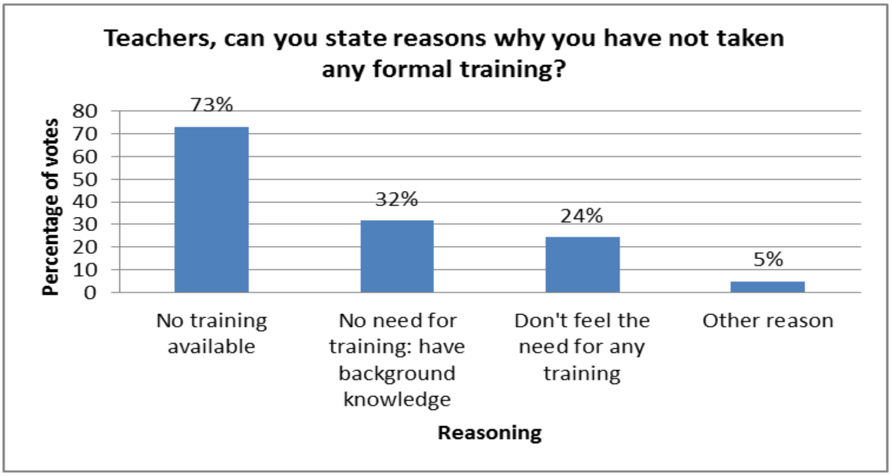


Figure 4: Reasons why tutors have not received any training

The tutorials for tutors do not appear to be a waste of time, because the tutor population who had received training all stated that the tutorials were of benefit to their technical and pedagogic understanding of literacy tools.

5 Data Discussion

Despite a lack of discussion in existing literature regarding the use of discussion forums in teaching and learning, the survey data shows that discussion forums are used far more than what the literature indicates and are viewed by students and tutors as positive learning and teaching tools. This is an unexpected, yet important, finding because it was expected that either wikis or blogs would be the most used due to the amount of existing literature that focuses on one of these within teaching and learning environments. The positive view of discussion forums can be extended to all literacy tools in teaching and learning, a view which is helped by students stating that they have had no technical difficulties in using the literacy tools and backs the results of previous research *(Chan and Ridgeway 2006; Mackey n.d; Elgort et al 2008; Song and Chan 2008; Churchill 2009; Deters et al 2010)*.

The vast majority of the literature evidences literacy tools as a means for providing a collaborative, constructivist learning environment *(Parker and Chao 2007; McMillin 2005; Tetard et al 2009, Hoorn and Hoorn 2007; Elgort et al 2008; Parsons 2004; Yang 2009)*. However, the data from the open ended questions suggest that the contrary is true: students do not view literacy tools as places for collaborative learning; instead viewing them more as personalised learning spaces. This contrary view supports the findings of Elgort et al (2008), Leung and Chu (2009), Ritman et al (2005), Wheeler et al (2008) and Craig et al (2008). Because the survey data along with the relevant referenced literature indicate that students have a positive view of the literacy tools and experience no technical difficulties, it can be suggested that whilst students have a good technical understanding of the use of literacy tools, they are lacking the pedagogical understanding of how to use literacy tools to aid their learning.

There is evidence to suggest that students and tutors are willing to use the latest technology, such as mobile phones, to access literacy tools online. The iPad would have been considered if it had been available in the UK before this research had been initiated. However, whilst mobile phones and iPads might increase the flexibility and efficiency of interfacing with literacy tools, they are not predicted to aid with the pedagogical understanding of how to use literacy tools to aid with the teaching and learning. Increase in efficiency and accessibility can be hypothesised, but not an increase in the pedagogical performance unless that understanding is in place before the technology is introduced and integrated into teaching and learning.

The data indicate students do not understand the pedagogical aspects of literacy tools because there is a lack of tutorials to empower the students with such knowledge. The link between lack of tutorials and lack of pedagogical understanding has been found in previous research (*Chan and Ridgeway 2006; Elgort et al 2008; Ritman et al 2005; Leung and Chu 2009; Wheeler et al 2008; Craig et al 2008; Bower et al 2006; Lamn 2004; Ebner and Maurer 2007)*. The data shows that tutorials for students would not be a waste of resources as the students who had received tutorials stated that they were beneficial, and the importance of student tutorials has been highlighted in previous research *(Elgort et al 2008; Wheeler et al 2008; Bower et al 2006; Lamb 2004; Leung and Chu 2009; Elgort et al 2008; Ebner and Maurer 2007)*

The survey data also shows that there is a serious lack of tutorial support for tutors, which back the findings of Ashcroft and McAlpine (2004), Deters et al (2010), Bruns and Humphreys (2005), Craig et al (2008) and Tetard et al (2009). This would suggest why students have not received any training; if the tutors had not received any training then naturally they are not going to understand the benefits of such training for their own students. It can be argued from the data that, therefore, tutors rely on their general experience and that of the students to guide the use of literacy tools in teaching and learning. However, a general understanding of how literacy tools work does not constitute a substantial pedagogic understanding of the benefits of literacy tools. Participants have suggested that they do not need the training as they have the required background knowledge, and also that they do not think that any literacy tools provide teaching and learning benefits. However, how can this group of tutor participants arrive at this perception without experiencing any form of formal training? How do they know that any learning is taking place when the student data is suggesting otherwise? Without observing the engagement of both student and tutors with regards to their use of literacy tools in the classroom, these questions are difficult to answer with just the survey data.

Altering teacher training courses so that tutors are better educated on the technical and pedagogical aspects of literacy tools would appear to be a positive endeavour, as the tutor participants who had received training indicate that it was of benefit to them. In addition to the survey data, various research literature *(Ashcroft and McAlpine 2004; Deters et al 2010)* calls for a need for tutors to understand all technical and pedagogical aspects of literacy tools; however, there is a lack of research into the current suitability of teacher training and professional development courses. It could, therefore, be suggested that the lack of student understanding of literacy tools can be attributed to the lack of understanding from and suitable training of the tutor.

The educating of the teaching workforce in their ability to understand the technical and pedagogic aspects of literacy tools is very important, because without this knowledge the tutors are not able to select the most appropriate literacy tool or tools for any given learning or teaching activity. They are, therefore, relying mostly on any previous experience that they have had with the particular literacy tool; however, and as has been previously mentioned, a perfect general understanding of literacy tools does not equate to a perfect pedagogic understanding of literacy tools.

There is, however, more work that needs to be carried out in order to establish if whether or not all three literacy tools can be used simultaneously, and to better understand the full benefits literacy tools can provide to teaching and learning, both from an individual and integrated approach. There has to be a detailed analysis of the effectiveness and content of any existing teacher training or professional development program in order to determine the current suitability of relevant training. The existence of any relevant training, according to the survey data, is of benefit to the tutors therefore more work needs to be done to incorporate literacy tool training in formal teacher training and professional development programs. Once the teacher training and professional development programs have been altered to include relevant training on literacy tool use and understanding, these then need to be monitored through longitudinal research to ensure that the tutors are gaining the correct knowledge and understanding. Longitudinal research will also have to take place in the tutor’s classroom to ensure that their own tutorials for their students are just as effective as those on the teacher training and professional development programs.

6 Conclusions

Because of the popularity of all three literacy tools and because, in particular, discussion forums are more popular than was previously suggested, a culture of integration can be developed. In addition, the data has revealed that tutors and students have used more than one literacy tool in a teaching or learning activity; why, therefore, has previous research only focussed on the implementation of one literacy tool when there is evidence that all three have been used? Whilst it is difficult to determine from the student data whether or not all three have been used simultaneously for their learning, there is evidence from the tutor data that more than one literacy tool has been used simultaneously for their teaching. The data supports, therefore, the need for a change in research direction to occur, from focussing on the implementation, uses and benefits of one literacy tool to an approach that considers the use, implementation and benefits of all three literacy tools in simultaneous use in a given teaching or learning activity.

Understanding the individual benefits of each literacy tool will empower the tutors with the knowledge to be able to integrate all literacy tools into any teaching and learning activity. Through gaining the knowledge and understanding of all three literacy tools, tutors would be in a better position to select the best literacy tool that they feel will best serve their teaching and their students' learning needs

Even though more work needs to be done to determine the true impact and nature of literacy tools on teaching and learning, the survey data indicates that it is knowledge and understanding that should drive students and tutors to realising the full learning and teaching potential of literacy tools, not a continuous drive for developing and introducing new technologies into the teaching and learning environment. Teaching and learning needs, in turn, drive the requirement for that knowledge and understanding

Empowering the tutors with the relevant knowledge could take one of two forms, or even both: empowering tutors with the knowledge of all three literacy tools so that they can best select which tool is most beneficial for a teaching and learning activity. Or, empowering the tutors with such knowledge so that they know how to integrate all three literacy tools within any given teaching and learning activity. A culture of integration revolves therefore not just around the use of all three literacy tools, but a knowledge and an awareness of all three literacy tools so that the best tool can be selected for any given teaching or learning activity.Empowerment of the tutors with such knowledge, awareness, understanding and, therefore, the ability to select either one or more than one literacy tool for any given learning or teaching activity comes from obtaining a suitable level of knowledge and education on their teacher teaching courses. This, in turn, would be passed onto their students so that the students can fully understand the literacy tools being used in the way that maximises their own learning potential and facilitate the learning that takes place.

A culture of integration, therefore, goes beyond knowing how to use and understand the technical and pedagogic aspects of literacy tools. This is very important, however, because without this knowledge tutors are not able to select the best literacy tool for their teaching and learning activities and not able to manage and measure the amount and quality of learning, and teaching, that is occurring. It will encourage a culture of integration, but such a culture has to have a much wider view; a much wider context, where technology plays only a part of this culture. It is about tutors changing their attitudes and perceptions regarding how better off they consider themselves as tutors without the use of such tools; it is about tutors thinking outside of their comfort zone and accepting change. It is about students, tutors, institutional management, teaching course designers, teaching course managers, the tutors within those teaching courses and researchers working together to implement and integrate all three literacy tools and other technologies such as mobile phones and iPads into teaching and learning activities in order to find the most effective way that they can facilitate teaching and the management and development of learning and knowledge.

7 References

Ashcroft , B., McAlpine, I (2004): "Student moderators in online discussions", in Atkinson, R., McBeath, C., Jonas-Dwyer, D., Phillips, R (Eds), "Beyond the comfort zone: proceedings of the 21st asciliite conference", 88 – 94, Perth Australia.

Betts, D., Goldoff, S (2004): "Instructional models for using weblogs in elearning: a case study from a virtual and hybrid course", Syllabus 2004 conference, San Francisco California, America, Available at: http://download.101com.com/syllabus/conf/summer2004/PDFs/w01.pdf [Date accessed: 24th January 2010]

Bower, M., Woo, K., Roberts, M., Watters, P. (2006): "Wiki pedagogy, a tale of two wikis", 7th International Conference on Information Technology Based Higher Education and Training, 2006. ITHET '06, p 191 -202

Bruns, A., Humphreys, S (2005): "Wikis in teaching and assessment: the m/cyclopedia project", International Symposium on Wikis, *Proceedings of the 2005 international symposium on Wikis*, 25 – 32

Chan, K., Ridgeway, J (2006): "Student's perception of using blogs as a tool for reflection and communication", *13th international conference of the association for learning technology*, Manchester England. Available at: http://www.dur.ac.uk/resources/smart.centre/Publications/ALT-CEdinburghCHAN.doc [Date accessed: 18th January 2010]

Churchill, D (2009): "Educational applications of Web 2.0: using blogs to support teaching and learning", *British journal of educational technologies*, 40 (1), 179 to 183

Craig, A., Goold, A., Coldwell, J., Mustard, J (2009): "Perceptions of roles and responsibilities in online learning: a case study", *Interdisciplinary journal of elearning and learning objects*, Volume 4, 205 – 219

Deters, F., Cuthrell, K., Stepleton, J (2010): "Why Wikis? Student perceptions of using wikis in online coursework", Journal of online learning and teaching, 6 (1), 122 to 134

Ebner, M., Maurer, H. (2007): "Blogging in higher education", *Proceedings of E Learn*, 767 to 774, Qubec City, Canada

Elgort, I., Smith, A.G., Toland, J (2008): "Is wiki an effective platform for group course work?", Australasian journal of educational technology, 24 (2), 195 to 210

Hoorn, E., Hoorn, D.V., (2007): "Critical assessment of using wikis in legal education", Journal of Information, Law and Technology

Lamb, B (2006): "Wide open spaces: wikis, ready or not", *EDUCASE Review*, 39 (5), 36 – 48

Leung, K., Kai Wah Chu, S., (2009): “Using wikis for collaborative learning: a case study of an undergraduate student’s group project in Hong Kong”, ICKM 2009, Available at: http://ickm2009.pbworks.com/f/Kevin+Leung.pdf [Date accessed: 10th January 2010]

McMillion, B (2005): “Putting the learning back into learning technology”, in O’Neill, G., Moore, S., McMillion, B (Eds), “Emerging Issues in the Practice of University Learning and Teaching”, Dublin, AISHE

Mackey, T.P. (n.d): “The social informatics of blogs and wiki communities: authoring communities of practice”, Available at: http://www.cais-acsi.ca/proceedings/2007/mackey_2007.pdf [Date accessed: 10th January 2010]

Parker, K.R., Chao, J.T (2007): “Wiki as a teaching tool”, *Interdisciplinary Journal of Knowledge and Learning Objects*, Volume 3, 57 – 72

Parsons, C (2004): “Brief thoughts on blogging and education”, Available at http://www.christopher-parsons.com/blog/technology/brief-thoughts-on-blogging-and-education/ [Date accessed: 6th January 2010]

Ritman, R., Augar, N., Zhou, W (2005): “Employing wikis for online collaboration in the e-learning environment: case study”, *Proceedings of the third international conference on information technology and applications*, 2 (2), 142 – 146

Song, H.S.Y., Chan, Y.M (2008): “Educational blogging: a Malaysian university students’ perception and experience”, in *Hello! Where are you in the landscape of educational technology?,* Proceedings of ASCILITE 2008, Melbourne Australia, Available at: www.ascilite.org.au/conferences/melbourne08/procs/song.pdf [Date accessed: 18th January 2010]

Tetard, F; Patokorpi, E; Packalen, K (2009): “Using wiki to support constructivist learning: a case study in University education settings”, Proceedings of the 42nd Hawaii International Conference on systems sciences.

Wheeler, S., Yeomans, P., Wheeler, D (2008): “The good, the bad and the wiki: evaluating student generated content for collaborative learning”, *British Journal of Educational Technology*, 39 (6), 987 – 995

Yang, S.H. (2009): “Using blogs to enhance critical reflection and community of practice”, *Educational technology and society*, 12 (2), 11 to 21

Improving the Usability of Security Features within Tools and Applications

C.Heeren and S.M.Furnell

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

A predominantly observation based study utilising eye gaze tracking and a 'think-aloud' protocol to discover general computer user's perceptions and behaviour towards security. Participants interacted with two security tools, each within a specific task-based scenario while their screen session and eye gaze were logged. Qualitative findings analysed to document each participant's perceptions, leading to usability recommendations for future security tools.

Keywords

Security, Perceptions, Usability, Think-aloud, Gaze Tracking

1 Introduction

With growing risks of increasingly sophisticated attempts to attack vast numbers of systems on-mass, and the evolution of attacks becoming more passive and discreet from the user (Richardson, 2008), typical users who may not have such a comprehensive understanding of computer security specifics need for any security related software to be easy to derive understanding from, manipulate, and function equal to the intension inferred by their interfaces.

The intermediary of the security interface is where perceptions are made of what is occurring in front of them, what they feel they should be made aware of, and how the system is reacting to their interaction. User satisfaction regarding a system may be directly affected by the amount in which a user is able to gain understanding from their interaction. It has been recommended that to align usability and security they must be included as goals throughout the iterative design process, and not an afterthought (Yee, 2004). Lacking the matching of mental models between user perception and what the system actually offers could lead to incorrect assumptions being made as to security processes, therefore producing insecure scenarios (Smith, 2003; Smith, 2008). A security interface may be mentally placing end users outside the active system boundary, facilitating that any negative action is due to user bad practice - ignoring insufficient security design, whereas use-centric design should prevent security compromise solely user (Zurko, 2005).

2 A practical study of usability

A study was conducted with the aim of discovering usability issues which could occur for typical ‘everyday’ non-technical computer users working with security applications within their home environment. Rather than providing a basis to only find the security knowledge an individual has, and their outright performance upon a security related task such as within previous works E.g. (Katsabas et al., 2005; Helala et al., 2008), provision was made to measure more about a user’s outlook and perceptions of what may be occurring with regard to security would be an interesting direction to progress. Issues discovered and perceptions gathered were to be developed into guidelines for methods of security usability improvement. 8 adult participants were evaluated, with their only criteria being that they were regular computer users but not specific technical users. The study took the following design:

Part 1: Completion of a background questionnaire

Part 2: Monitored Security Task Scenarios (Two scenarios, each with six specified tasks, which may be faced within two general and publically available security tools:

Scenario 1: Took place using BitDefender Internet Security 2010 (v13.0.21 during testing), assessed as an affordable yet comprehensive security system which compromises of a deep packet firewall, anti-virus, anti-spyware, and anti-phishing tools (BitDefender, 2010) It appeared understandable for less aware users, having the ability to provide varying levels of interface complexity and control. Participant were faced with having to configure the security system as if it was just installed, with the measures they thought appropriate and to complete the tasks provided as best as possible. Tasks included managing vulnerabilities, firewall manipulation, and selecting an appropriate user interface profile.

Scenario 2: This involved using an encryption package called Advanced Encryption Package Professional v5.3.8 (AEPPro, 2010), which would require the participant to make use of text encryption for the scenario of sending and receiving email needing high privacy. They were to establish a public and private key set, encrypt their message, and email the message to a fictional contact (created by the researcher). Participants then were required to correctly extract a received encrypted message, along with key, and decrypt it so that they may read it. This test was devised due to the previous encryption difficulties found by (Whitten & Tygar, 1999). Although the process appears to be improving in comparison to these earlier findings, AEP Pro was chosen because it was felt it still demonstrated complexity in usability which would provide a good context to observe more participant perceptions than a tool nearer full automation.

Part 3: A usability feedback form to assess their impressions of both of the security tools used, and one perception question for each scenario which was faced, regarding an important part within the scenario.

Part 4: A set of questions regarding their interpretations of the software used.

Throughout: Observations of interesting aspects of each participant's progress, key mistakes or points of confusion, and any discussions or comments they make about the security tasks, and how the software makes them feel.

Finally: The researcher analyses the recorded materials of the participant's test session and scores each session according to the usability metrics listed, prior to further analysis regarding the observations made, and the behavioural data recorded.

HyperCam 2 v2.23.01 (Hyperionics, 2010) was used for screen recording the participant's sessions. For the process of gaze tracking a bespoke headset was created and gaze tracking was detected and logged as the participant's session via Gaze Tracker v1.5.0.211 (Gaze Tracker, 2010). Participant gaze points were utilised in Ogama v3.3 (Ogama, 2010), a usability analysis tool capable of producing visualisations of gaze data upon user sessions.

3 Findings and Recommendations

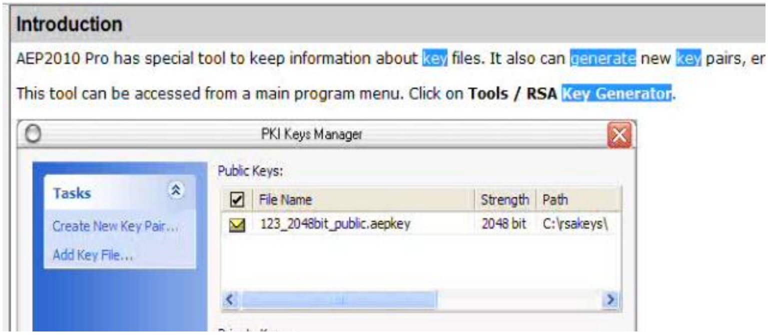
The key findings arising from the study are summarised in the following paragraphs:

1. Help topics which are as specific as the request: A satisfying sight for a confused user could be an exact help topic being found for the issue you searched for, first time. A participant, for example, would check through help, not find an exact matching topic even though other results were returned, and exit to resume the same struggle they were confronted with earlier. Perhaps a level of contempt for poor previous help facilities has made many users reluctant try harder once more? One participant commented on online help and program help as being of "not much help".

2. Helpful information should be in the right places: Looking to generate encryption keys through a help search finds no mention of the menu location under 'Generating key files', whereas it is clearly documented under 'Introduction' (Figure 1), assuming you attempted long enough to find it before giving up. The information may be relevant in both, but at least include it under its own topic, as well. You may think it wise to add each of these discreet help topics, but not if they fail to contain some of the most important information required. One participant was found to take almost half of their encryption task completion time referring to help.

Inadequate and insignificant navigation within BitDefender was also found. Figure 2 displays the gaze tracking for a participant attempting to locate the 'Add Rule' button within Firewall controls. The buttons are insignificant and within the top-right area of the window, where there is a distinct lack of gazing (Figure 2).

3. Inappropriate or inconsistent terminology: Would a typical security user, or even an advanced user for that matter, expect a key '*Comment*' to be mandatory? Within the situation of key generation within AEP Pro it results in actually being the prefix for both file names (as it more subtly states in brackets). Many participants hardly noticed this input box until prompted that the value was missing. To further compound confusion, no explanation of why the comment is needed was ever offered (Not before, in the form of a tooltip, during, as part of an admonition (Yee, 2004), or after as information upon the error message).



Introduction

AEP2010 Pro has special tool to keep information about key files. It also can generate new key pairs, er

This tool can be accessed from a main program menu. Click on **Tools / RSA Key Generator**.

PKI Keys Manager

Tasks

Create New Key Pair...

Add Key File...

Public Keys:

☑	File Name	Strength	Path
✉	123_2048bit_public.aepkey	2048 bit	C:\rsakeys\

Figure 1: An instance where unhelpful help occurs, prolonging the participant's search.

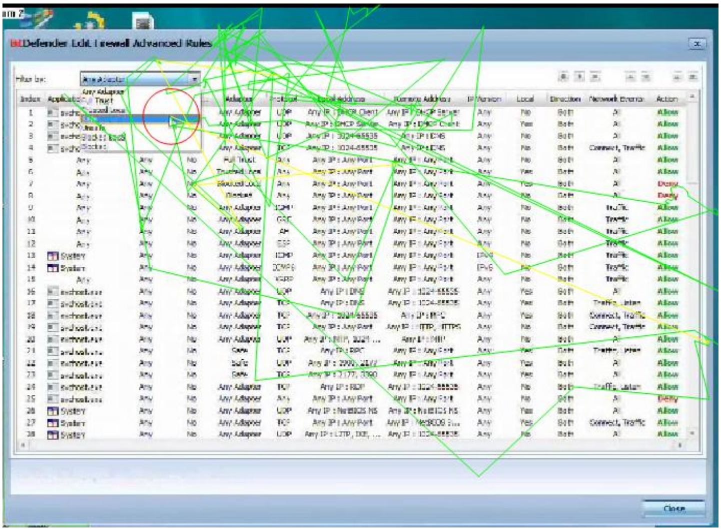


Figure 2: An example of a participant's gaze estimation during a Scenario 1.

One participant even believed that this input box was for the text they wanted to encrypt, and for the combination of password and comment to make keys – An example of the misdirection a system can bestow upon a less technical user.

Another participant thought of the actual task they needed to achieve. They searched help for the relevant topic. This lead them to a screenshot of the menu required, complete with the menu title (Figure 3, left hand) - we are no longer looking for 'generate', but 'create'). This participant appeared to always attempt to match what they saw in help to what they could find upon the interface, as expected you may think. However, within the menus we now have returned numerous re-examinations of more than one help topic simply because this inconsistency is not in keeping with the participant's line of thought. This mismatch appears bring about many of the usability issues mentioned.

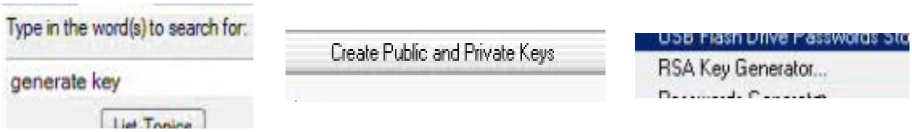

Type in the word(s) to search for:
generate key
List Topics
Create Public and Private Keys
USB Flash Drive Passwords Sto
RSA Key Generator...

Figure 3: Changing terminology through tasks of Scenario 2

4. Avoiding compounding options with terminology: Even if you later are to include more advanced computing or security specific terminology to your windows, keeping this to a minimum or removing it all together from menu or navigation selections can aid. On the opposite outlook, some expert users may want to seek out specifically termed options, but placing them within a submenu or upon a configurable window itself could reduce the aversion less knowledgeable users suffer towards terms they do not understand.

Using technical prefixes and suffixes upon your menu options appear to result in reluctance to try them by unfamiliar and inexperienced users. Participants would repeatedly browse the same menu, choosing options above and below, even stopping to ponder whether terminology-laden options were what they were seeking, and still declined from trying them. 38% of participants displayed signs of being reluctant to click upon ‘RSA Key Generator’ simply because they do not understand what RSA means in this context. More than one participant voiced this feeling during testing. Observations appeared to show that rather than experimenting with where that option would lead, some participants would remain hovering over action, with no guidance provided, as if trying to second guess what the outcome of using that selection could mean – before avoiding it.

5. Failing to match the user’s mind-set: Generating one pair of encryption keys at one time may not be everyone’s way of working, but it is suspected that users wanting to quickly encrypt some text for email want just the one set of keys for this sort of event. AEP Pro’s generation interface continued to display the three options ‘Create, Cancel, Help’ even after key pair creation. Participants were left wondering what was expected from them as little information was provided to signify their task was a success. For many computer users now days, the sight of confirmation being about as descriptive and inconclusive as an *‘OK’* placed with the output list, is an very rare or unseen sight. With a seeming lack of respect for a non-technical user, it echoes command-line confirmation typically dating back three decades previous.

However, the main factor here was their inability for the security’s design to have reflected the thought process of any unfamiliar user at this time. With thoughts such as, having generated their keys, why isn’t the menu closing? - As often expected now days. Even if this wasn’t appropriate, no information guides the participant that they may exit the menu, and the buttoned options remain unchanged - so taking on a misleading interpretation for the participant. Will my keys fail if I leave? Why does it say ‘Create’ when I just created them? Did I actually create them? What about the use of ‘Cancel’; surely users have been trained to think that cancel ends an incomplete task, as their interpretation of it within the real world would concur? Here it becomes the only successful avenue of exit from this window, whether the task was successful or not.

6. Visual depictions of tasks are still well received: Regardless of user background, visual metaphors for the tasks the user wants to achieve appear to help improve understand-ability (insuring that they are used with a mind-set matching the user is a different issue) for a typical user. For example, encryption key management for one participant: No prior knowledge of the keys concept was known, yet through just imagining the task achieved by using either of the depicted states of the envelopes, which key governed which purpose was deduced. For another participant the icon also showed the purpose of the object in question, rather than what is was - a key.

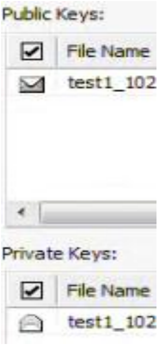


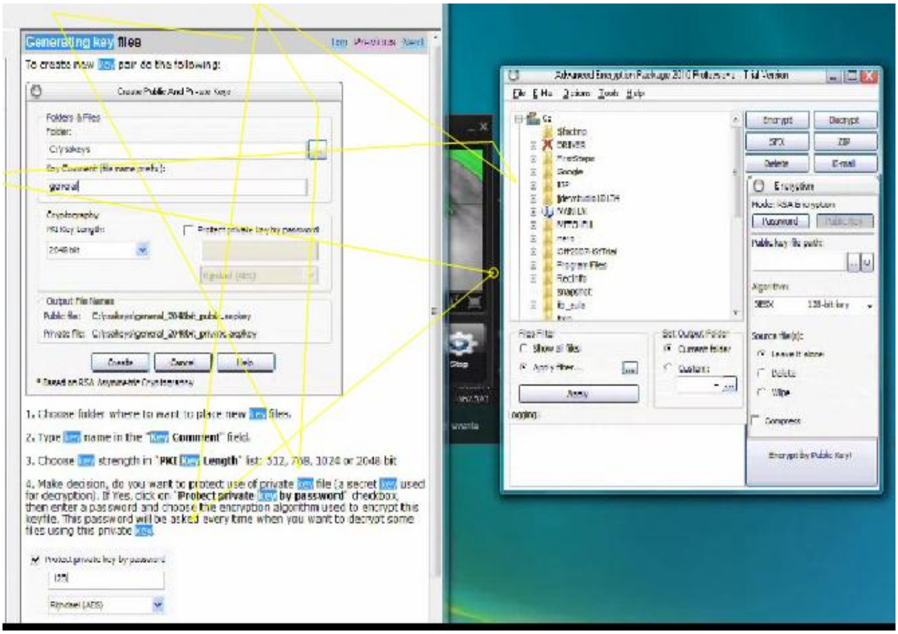
Figure 4: Icons displaying the objective rather than object

7. Safe-staging availability seems necessary: If a 'safe-staging' style of task guidance is not provided, it appears that users may attempt a similar style of working themselves. It was found that 50% of participants exhibited signs of attempting to produce their own form of 'self-safe-staging' when no highly usable guidance appeared to be provided, as an attempt to manage a complicated task in smaller segments. Between each of these users, resorting to the standard in-program help, there was a noticeable effort to survey each pictorial element of relevant help upon half of the screen while attempting to track down which navigation options led to the same factor. It appeared to the researcher that this was similar to the actions which occur during safe-staging and the guidance regularly seen beside tasks to be accomplished.

4 Conclusions and future work

Background questionnaire data suggested that many users are now becoming more aware that threats to their actions are a reality. However, many inexperienced, or rather non-technical users who have little to do with a computing field outside of completing everyday tasks with the aid of a computer can be rather left behind and perhaps reluctant to delve into the correct use of security features which make little sense to them (Chatziapostolou & Furnell, 2007).

The findings showed participant perceptions such as, the belief that *'the type of security profile selected for a tool's interface reflected the level of security protection offered',* and appears to be a regard many general users studied have expressed, with added opinions along the lines of *'more 'expert' users require higher security'* aired by a number, whereas others appear to suggest perceptions along the lines of *'lowest users should have maximum security'*.



Generating key files

To create new key pair do the following:

Create Public And Private Keys

Folders & Files

Folder: C:\rsakeys

Key Comment (file name prefix): general

Cryptography

PKI Key Length: 2048 bit

☐ Protect private key by password

Output File Names

Public file: C:\rsakeys\general_2048bit_public.asckey

Private file: C:\rsakeys\general_2048bit_private.asckey

* Based on RSA Asymmetric Cryptography

1. Choose folder where to want to place new key files.

2. Type key name in the "Key Comment" field.

3. Choose key strength in "PKI Key Length" list: 512, 768, 1024 or 2048 bit

4. Make decision, do you want to protect use of private key file (a secret key used for decryption). If Yes, click on "Protect private key by password" checkbox, then enter a password and choose the encryption algorithm used to encrypt this keyfile. This password will be asked every time when you want to decrypt some files using this private key.

☑ Protect private key by password

Rijndael (AES)

Advanced Encryption Package 2010 Professional - Trial Version

Mode: RSA Encryption

Algorithm: SEEX 128-bit key

Source file(s): ● Leave it alone ○ Delete ○ Wipe

☐ Compress

Figure 5: A participant attempting to 'self-safe-stage' his efforts of scenario 2

This might form an expectations gap between what users expect and what is offered - also how users are guided, yet also looked after. Would it mean that an expert carries out difficult or sensitive tasks, and so requires very high security (and can deal with it?) or would it mean that novice users should be looked after the most (perhaps restricted so greatly, they could result in being annoyed towards the security)? Out of the relatively small sample of participants questioned, these perceptions have already both been noted.

The question may remain as to what would be the ideal security solution, this may be complete and 'perfect' automation, yet even if this were possible, may not guarantee protection about threats even analysts, designers, and users are unaware of. As threats become more subtle towards the user, this may be the only way forward for users with less concern or ability to try and understand more about computer security. A criticism could be that this novice restriction combined with a lack of knowledge on the user's part could lead to a false sense of confidence, in that all the software operations are working optimally (as seen in Bit Defender by green ticks and system reassurance even when major security options are disabled, because the tracking of their status is also disabled), and all choices are the best suited to this user's needs – when this may not be the case.

A user lacking knowledge may feel unaware of how secure their computer <u>is</u> at a 'Novice' level, yet unaware of how <u>to</u> secure their computer at 'Expert' level.

As a suggestion, alongside the learning abilities of security software such as firewalls to establish regular required processes, perhaps the inclusion of an artificial training agent which can assess the level of operational flexibility each user requires and could implement scaling of security control to allow for less distinct changes of profile to be undertaken by users. Participant recommendations, such as the use of a ‘Tree View’ interface deciding this scale of control with interpretation to the security tasks required may provide greater usability for users who feel more reluctant to engage in ‘inefficient’ use of their time, or who lack a greater level of specific understanding.

5 References

AEPPro (2010): Advanced Encryption Package Professional Software; Available at: http://www.aeppro.com/ [Date accessed: 16th June 2010]

BitDefender (2010); BitDefender Total Security Software; Available at: http://www.bitdefender.co.uk/solutions/total-security.html [Date accessed: 15th June 2010]

Chatziapostolou D., Furnell S. M. (2007) “Recording End-Users Security Events: A Step Towards Increasing Usability” Plymouth University, UK. Available at: http://www.cscan.org/default.asp?page=viewabstract&paperid=385 [Date accessed: 10th January 2010]

GazeTracker (2010); ITU Gaze Tracker open source software v1.5.0.211; University of Copenhagen; Available at: http://www.gazegroup.org/downloads/23-gazetracker [Date accessed: 14th June 2010]

Helala M., Furnell S.M., Papadaki M. (2008) “Evaluating the Usability Impacts of Security Interface Adjustments in Word 2007” Plymouth University, UK. Available at: http://www.cscan.org/default.asp?page=viewabstract&paperid=536 [Date accessed: 14th January 2010]

Hyperionics (2010); HyperCam 2 Software v2.23.01 Available at: http://www.hyperionics.com/hc/ [Date accessed: 9th June 2010]

Katsabas D., Furnell S. M., Phippen A.D. (2005) “IT Security: A Human-Computer Interaction Perspective” Plymouth University, UK. Available at: http://www.cscan.org/default.asp?page=viewabstract&paperid=240 [Date accessed: 14th January 2010]

Ogama (2010); O Ogama open source gaze and mouse analyser v3.3; Freie Universitat Berlin (2010); Available at: http://www.ogama.net/ [Date accessed: 17th June 2010]

Richardson, R. (2008); 'CSI Computer Crime and Security Survey 2008'; Computer Security Institute; Available at: http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf [Date accessed: 7th January 2010]

Smith S. W. (2003) “Humans in the Loop: Human-Computer Interaction and Security” IEEE Security & Privacy; May/June 2003; pp 75-79.

Smith S. W. (2008) “Why do Street-Smart People do Stupid Things Online?” IEEE Security & Privacy; May/June 2008; pp 71-74.

Whitten A., Tygar J.D. (1999) “Why Johnny can’t Encrypt: A usability evaluation of PGP 5.0”; Proceedings of the 8th conference of USENIX Security Symposium; Vol. 8 p14; Available at: http://www.gaudior.net/alma/johnny.pdf [Date accessed: 20th Jan 2010]

Yee, K.P. (2004); 'Aligning Security and Usability'; IEE Security and Privacy; Volume 2; Issue 5 (September 2004); pp 48-55.

Zurko M. A. (2005) “User-Centered Security: Stepping Up to the Grand Challenge”; Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005) 1063-9527/05

Section 4

Network Systems Engineering

Application of LDPC Codes on Networks

A.Agrawal and M.A.Ambroze

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The current communication systems face many problems these days during the transmission of data, which are network efficiency and congestion. This relates to quality of service of the data transmitted- i.e. data rate, delay, delay variation and packet loss which are provided to the customer. Congestion causes packets to be lost, due to which retransmission of packets takes place and this in turn can increase congestion in the network. From error correction point of view, retransmissions represent an inefficient type of code called as the repetition code, which is known to have high overhead.

This paper investigated the way to reduce the need for retransmission of the lost packet by using efficient error correction codes, such as Low-density parity check (LDPC) codes. They were invented by Gallager in 1963 and had been forgotten until Mackay rediscovered it. They are able to reconstruct the number of lost packets at the receiver end.

This project discusses the iterative decoding and Gaussian elimination decoding methods for their application to decode the received code word with erasures in the binary erasure channel. The information bits will be encoded which is combination of information bits and the redundant bits called as code word which is subjected to noise when transmitted through the binary erasure channel. The error occurs in the form of erasure of the bits from the code word, which is then decoded with the help of the two decoding methods.

Keywords

Error-correcting codes, LDPC codes, Iterative decoding, Gaussian elimination, Binary erasure channel, communication systems, Code word, Retransmission, Generator matirx, Parity check matrix, Channel capacity, Rate of block code.

1 Introduction

C. E. Shannon originated the error-correcting codes in 1940s, which increased the ability and reliability of digital signals. With the help of these error-correcting codes, users can encode the message and transmit over the channel with decoder at the receiving end to decode the message and detect and correct any error in the message. According to Shannon’s paper “A Mathematical Theory of Communication” the probability of error in a channel depends on the channel capacity (Shannon, 1948). This project deals with the applications of LDPC (Low-density parity heck) codes, which were first introduced by Robert Gallager in 60’s. The LDPC codes needs to be applied on the channel models in order to reduce the error that are created during the data transmission in the channel (Gallager, 1963). The channel that is going to be used in this project is Binary Erasure Channel (BEC), which has the Channel Capacity of 1-p, where p is the erasure probability. Binary erasure channel are not same like Binary symmetric channel in the sense that if the bit arrives it is always correct and the error occurs only when the bit is erased. The encoding and decoding of the message that will be transmitted over the channel in order to provide a simulation to explain the working of the LDPC codes and the approximate error correction mechanism in the binary erasure channel using Gaussian elimination method and iterative decoding method.

2 Error Correction Code

The main problem faced in today’s world is the reliability issues faced while using a digital communication system where we have to expect error at any moment during the connection and should be able to deal with that error. Retransmission of the lost bit is a redundant solution that is time consuming and can also cause congestion in the network. The other approach, called "error detecting and correcting codes" can be used. Error correcting codes are of various types but the one which is used in this project is linear block codes called as Low density parity check (LDPC codes) (Shokrollahi, 2003).

3 Procedure and Methodology

The Process comprises of the encoding of the information bits, transmission of the code word generated through the binary erasure channel and how the information is affected by the noise in the channel. Finally, how the received code words with erasure will be decoded in the decoder with the help of the two decoding process i.e. iterative decoding and the Gaussian elimination process. The encoder will generate the generator matrix with the help of parity-check matrix. After generating the generator matrix, the encoder generates the code word which will be the addition of the information bits and the parity check bits which will be generated with the help of the following formula:

$$\text{Code word } (v) = \text{Information Bits } (u) * \text{Generator Matrix } (G)$$

This received code word is combination of the information bits and the parity check bits. Parity check bits will be helpful in recovering the original information after passing the code word through the noisy channel. This is explained with the help of an example.

Example:

$$\text{Code word } (v) = \text{Information Bits } (u) * \text{Generator Matrix } (G)$$

Where,

$$\text{Generator Matrix } (G) = \begin{pmatrix} 1\,1\,0\,1\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,0\,1\,0 \\ 1\,0\,1\,0\,0\,0\,1 \end{pmatrix}$$

Information Bits (u_1) = 0 1 1 0

$$\text{Code word } (v_1) = [0\ 1\ 1\ 0] * \begin{pmatrix} 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \\ 1\ 0\ 1\ 0\ 0\ 0\ 1 \end{pmatrix}$$

As the matrix multiplication is the between 1 x 4 dimension and 4 x 7 dimension matrix the code word will the of 1 x 7 dimension.

Code word (v_1) = [1 0 0 0 1 1 0]

After the encoding is done on the information bits, then the encoded code word is passed through the communication channel. In Binary erasure channel, if there is any error during the transmission due to noise then an erasure is created in the code word which is denoted by 'e' n the received code word. So the received code words which initially had two input symbols '0' and '1' before transmission will now contain three output symbols '0', '1' and 'e'.

As the channel accepts the input as the encoded code word, the first code word will be

Code word (v_1) = [1 0 0 0 1 1 0]

As the channel will create the erasure at the random position, the erasure will be denoted by 'e'. In this code word the erasure will be at three positions. Hence, the received code word will be,

Received code word (r_1) = [e 0 0 e 1 e 0]

When the erasure is detected in the received code word then it will solve the erasure. It can be done with some specific steps.

1. Firstly it will check for erasure in the received code word (r1) = [e 0 0 e 1 e 0]. It can see that we have erasure in the 1st, 4th and the 6th position.

2. Now it will multiply the parity check matrix and the received code word,

Parity check Matrix (G) * Transpose of received code word (r^T) = 0

Where,

$$\text{Parity check Matrix (H)} = \begin{pmatrix} 1\ 0\ 0\ 1\ 0\ 1\ 1 \\ 0\ 1\ 0\ 1\ 1\ 1\ 0 \\ 0\ 0\ 1\ 0\ 1\ 1\ 1 \end{pmatrix}$$

Received code word (r_1) = [e 0 0 e 1 e 0]

$$\begin{pmatrix} 1\ 0\ 0\ 1\ 0\ 1\ 1 \\ 0\ 1\ 0\ 1\ 1\ 1\ 0 \\ 0\ 0\ 1\ 0\ 1\ 1\ 1 \end{pmatrix} * \begin{bmatrix} e \\ 0 \\ 0 \\ e \\ 1 \\ e \\ 0 \end{bmatrix} = 0$$

$$\begin{pmatrix} e\ 0\ 0\ e\ 0\ e\ 0 \\ 0\ 0\ 0\ e\ 1\ e\ 0 \\ 0\ 0\ 0\ 0\ 1\ e\ 0 \end{pmatrix} = 0$$

3. After obtaining the matrix, it will consider that there are three equations whose value should be zero when it has all the unknown values.

4. It will check which equation has the less erasure; in this case it will be the third row of the matrix.

   [0 0 0 0 1 e 0] = 0

5. In this equation it will do binary addition and find out the total value of the equation, it will substitute the value as 1 with one unknown.

6. As this equation needs another 1 in the position of ‘e’ to satisfy the condition of being equal to zero, it will substitute the value of unknown as 1.

7. Now it will have one solved erasure with only two unknown in the received code word and the equation matrix will be,

Received code word (r_1) = [e 0 0 e 1 1 0]

$$\begin{pmatrix} e\ 0\ 0\ e\ 0\ 1\ 0 \\ 0\ 0\ 0\ e\ 1\ 1\ 0 \\ 0\ 0\ 0\ 0\ 1\ 1\ 0 \end{pmatrix} = 0$$

8. Now it will repeat step no. 4 and check which equation has less erasure, now it will be the second row in the matrix.

$$[0\ 0\ 0\ e\ 1\ 1\ 0] = 0$$

9. In this equation we can do binary addition and find out the total value of the equation, we will get the value as 0 with one unknown.

10. As this equation value is 0, it can say that the value of unknown is also 0, so that it will not affect the equation and its binary addition value.

11. Now it will have two solved erasure with only one unknown in the received code word and the equation matrix will be,

Received code word (r_1) = [e 0 0 0 1 1 0]

$$\begin{pmatrix} e\ 0\ 0\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 0\ 1\ 1\ 0 \\ 0\ 0\ 0\ 0\ 1\ 1\ 0 \end{pmatrix} = 0$$

12. This way it will solve the third erasure as well and it will get the received code word which will be

Received code word (r_1) = [1 0 0 0 1 1 0]

13. It can now compare the actual code word sent by the user with the solved received erasure for our evaluation purpose.

Code word (v_1) = [1 0 0 0 1 1 0] and
Received code word (r_1) = [1 0 0 0 1 1 0]

14. From above two code words, it can say that we have correctly solved all the three erasure.

The Gaussian elimination decoding depends on the usage of the Gaussian elimination method or also called as Gaussian reduction method, to decode the received LDPC code word with erasure. In this method after the decoder has received the code word with the erasure we try to obtain the three equations by the principle,

Parity check Matrix (G) * Transpose of received code word (r^T) = 0.

Then by applying column transformations and row transformations on the received matrix and try to form an identity matrix at the right hand side of the matrix. After doing this step it will have only one unknown in each row. Then it can simply do binary additions for each row and find the value of the erasure in each row. This is the most efficient way of decoding.

1. Firstly it will check for erasure in the received code word (r1) = [e 0 0 e 1 e 0]. It can see that it has erasure in the 1st, 4th and the 6th position.

2. Now it will multiply the parity check matrix and the received code word,

3. Parity check Matrix (G) * Transpose of received code word (rT) = 0

Where,

$$\text{Parity check Matrix (H)} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Received code word (r_1) = [e 0 0 e 1 e 0]

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{bmatrix} e \\ 0 \\ 0 \\ e \\ 1 \\ e \\ 0 \end{bmatrix} * \qquad = 0$$

$$\begin{pmatrix} e & 0 & 0 & e & 0 & e & 0 \\ 0 & 0 & 0 & e & 1 & e & 0 \\ 0 & 0 & 0 & 0 & 1 & e & 0 \end{pmatrix} \qquad = 0$$

4. After obtaining the matrix, it will now apply row transformations on the matrix so that all the erasures are on the right hand side of the matrix.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & e & e & e \\ 0 & 0 & 1 & 0 & 0 & e & e \\ 0 & 0 & 1 & 0 & 0 & 0 & e \end{pmatrix}$$

5. After obtaining the matrix it will now apply row transformations in such a way that it obtains an identity matrix at the right hand side and the erasures are at the diagonal of that identity matrix.

6. First it will subtract R2 from R1 i.e. R1 – R2, after doing this it will achieve one erasure in the first equation.

$$\begin{pmatrix} 0 & 0 & 1 & 0 & e & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & e & e \\ 0 & 0 & 1 & 0 & 0 & 0 & e \end{pmatrix}$$

7. Then it will subtract R3 from R2 i.e. R2 – R3, after doing this it will achieve one erasure in the second equation.

$$\begin{pmatrix} 0 & 0 & 1 & 0 & e & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & e & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & e \end{pmatrix}$$

8. Now the iterative decoding step will be applied once and binary addition will be checked for all the three equations at once and substitute the value of erasure appropriately.

9. For the first erasure the total value of binary addition is 1 so the erasure should be 1. Similarly, the value of second and third erasure will be 0 and 1 respectively.

Received code word (r_1) = [1 0 0 0 1 1 0]

10. It can now compare the actual code word sent by the user with the solved received erasure for our evaluation purpose.

Code word (v1) = [1 0 0 0 1 1 0] and

Received code word (r1) = [1 0 0 0 1 1 0]

11. From above two code words, it can say that we have correctly solved all the three erasure.

4 Results and Discussion

As per Shannon’s seminal 1948 paper, capacity C of a Binary erasure channel is an upper bound on the rate *R* of a code that achieves randomly good error control. To simplify, a reliable code must have $R <= C$. Shannon (1948). So, it the value of R is less than or equal to C then we can solve the erasures in the received code word else it's difficult to solve the received code word. From both the decoding methods explained, we can say that the iterative decoding is a fast method to decode the code word but takes long time as number of iterations is more. On the other hand, the Gaussian elimination method (Liener, 2005) is a slow process but it can be more efficient than the iterative decoding. Even the number of iteration is only once so the time taken for this method will be very less.

5 Conclusion

The main objective of this study is to solve the erasure of the lost packets that were erased during the transmission of the code word in the noisy network. To solve the error of the erased packets a powerful error correcting codes called Low-density parity check (LDPC) codes. It is in the binary erasure channel that the error is introduced in the form of erasing the bits from the actual code word. The study of Binary erasure channel is done to learn about the capacity of the channel and the transmission of the bits. The study of LDPC is done to apply this coding on to the networks to solve the erased bits at the received end. To perform this, a significant level of understanding was achieved and implemented using the knowledge in the C programming language.

Looking at the results, the LDPC code encoding & decoding codes are managed to solve the erasure occurred in the received code word at the receiver end. In the encoding process good results were generated successfully by using the generator matrix. The systematic matrix generation helped in encoding the information sequence simper than encoding with the general matrix. During the transmission of the code word through the binary erasure channel, the channel gets affected by noise to create error in the form of erasure denoted by 'e'.

In decoding process, the erased bits is constructed by applying the equation $H. r^T = 0$. There are two decoding process used to decode the received code word. First one is Iterative decoding, where the received code word is multiplied with the parity check matrix. After the multiplication we receive three equations, which are solved with the help of binary additions and iterations to solve the erasure. This process is fast but it's not accurate and also do not work well with erasure in some position.

The second decoding method is Gaussian elimination method that is more accurate than the iterative decoding. Although the process is slow, it works for more probabilities then the iterative decoding. In Gaussian elimination, the received code word is multiplied with the parity check matrix. After receiving the three equations, the erasures are shifted to the right hand side of the obtained matrix and an identity matrix is formed with erasures at the diagonal position. The erasures are then solved with only one iteration of binary addition.

The program developed cannot take the input through a file, which will be helpful in solving the erasure in the sparse matrix. Also the second method of decoding process, the Gaussian elimination process can be implemented as a C program for both the hamming matrix and the sparse matrix.

6 References

Gallager, R. (1963), “Low-Density Parity-Check Codes”, *MIT Press*, Cambridge, MA.

Liener, B.M.J. (2005) “LDPC Codes – a brief Tutorial”, Available at: http://www.engr.uvic.ca/~masoudg/upload/ldpc-a%20brief%20tutorial.pdf [Accessed Date: 18th august 2010]

Shannon, CE. (1948), “The Mathematical Theory of Communication”, *The Bell System Technical Journal*, 27, pp. 379–423, 623–656.

Shokrollahi, A. (2003), “LDPC codes: An Introduction”, *Digital Foundation, Inc.* Available at: *www.ics.uci.edu/~welling/teaching/ICS279/LPCD.pdf [Accessed Date: 28th January 2010].*

Studying the Security in VoIP Networks

A.Alseqyani, I.Mkwawa and L.Sun

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Voice over IP (VoIP) technology has radically increased due to its advantages such as flexibility and low cost. On the other hand, the security issue in VoIP network has become an important field in order to name and mitigate the several types of attacks including call hijacking, eavesdropping and denial of service (DoS).

This research paper discusses security in VoIP networks by giving a brief background about the VoIP structure and protocols before setting up a testbed in order to conduct different kinds of attack by running some security tools and analyzes the network behavior under these attacks. The results of experiments will be presented and commented in this paper. Finally, a proposed solution to block the flooding attack will be discussed before conclude the main points which found in these experiment.

Keywords

VoIP, network, security, flooding

1 Introduction

Voice-over-Internet Protocol (VoIP) technology is combined of different protocols and devices using the IP network to transfer the voice and video calls instead of the traditional PSTN (Finneran, 2008). It has several advantages such as flexibility, low cost and simplification although of its many problems regarding the security issue. VoIP components including VoIP clients or terminals, gateway to connect different VoIP networks, gatekeeper which is responsible for address translation and access control and the IP network. One of the main protocols in VoIP is Session Initiation Protocol (SIP) which is a signaling protocol covers all session issues such as initiating, modifying and terminating (Handley et al, 1999). This paper will cover the different attacks that could affect VoIP network in addition to the multiple solutions for these attacks and finally, some experiments will be conducted to evaluate the VoIP threats.

2 VoIP Testbed

A VoIP tested as shown in figure 1 is set up to investigate the VoIP security issue. It consists of a VoIP server, two SIP clients and an attacker which explained below.

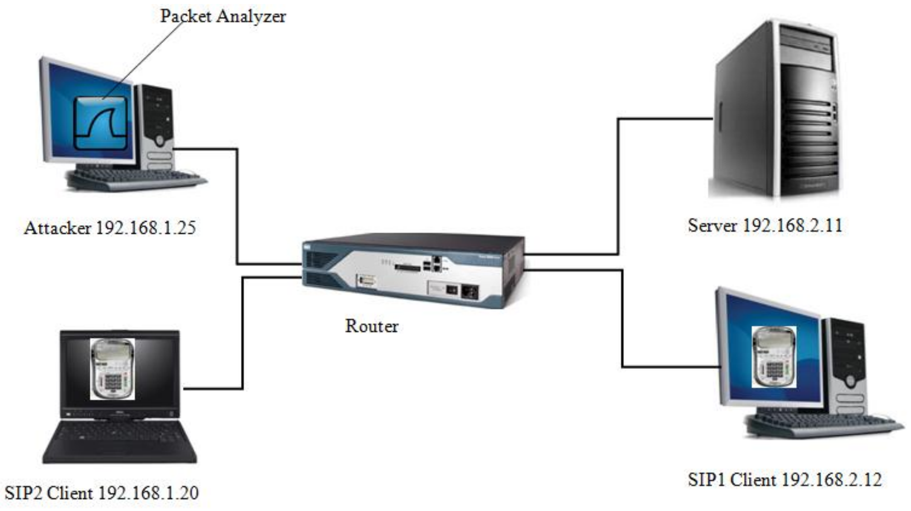


Figure 1: VoIP TestBed

- Asterisk Server: this server connects the different endpoints in the network through performing multiple tasks such as registering the VoIP clients before start calls and forwarding the call from one part to another. In this network, the server has an IP address: 192.186.2.11 and it works on Linux environment. The server hosting the asterisk has properties which are Intel Pentium 4, a CPU of 3 GHZ.
- SIP1: it is one of the two clients in the network. It is a PC with the IP address 192.168.2.12 and has SIP 1 phone works through X-lite program. The x-lite program is free software which allows VoIP clients making the voice and video calls over IP network by using Session Initiation Protocol (SIP) (Xlite, 2010). SIP 1 has the following details: a username as 1000 and password 1234 and it operates on Windows XP with a processor Intel Pentium 4, a CPU of 2.4 GHz and 1 GB memory RAM.
- SIP2: Another client in the network which is a laptop with the IP address 192.168.1.20 has SIP 2 phone works via x-lite program to initiate and receive calls. SIP 2 has specific properties such as a username as 2000 and a password 1234 and it operates on Windows Vista with a processor Intel Core 2 Duo, a CPU of 2.17 GHz and 3 GB memory RAM.
- The attacker: The attacker device is a personal computer and it has an IP address 192.168.1.25 and it will be used to attack the network by installing the tools on it and run these tools. To capture and analyze the traffic in the network, a famous program called Wireshark will be used. This device operates on Linux with a processor Intel Pentium 4, a CPU of 2.2 GHz and 3 GB memory RAM
- The gateway is used to connect the VoIP network clients together or with other clients in different networks. Its IP address is 192.168.2.9.

3 VoIP Security Tools

3.1 Nmap

The Network Mapper (Nmap) is designed to do scanning and security auditing in the small and wide networks (Nmap, 2010). It can come up with different types of information about the network such as available hosts, opened ports, type of operating system, IP addresses and MAC addresses. This tool supports different kinds of scan including TCP SYN Scan, UDP Scans and TCP ACK Scan.

3.2 Cain and Abel

Cain and Abel program is used for password recovery and it has many features including network sniffing for password recovery, recording VoIP conversations, analyzing routing protocols, Brute-Force attacks and using dictionary to crack encrypted passwords (Montoro, 2010). It used in hacking purposes because it has the ability to extract the conversations files and save them in wav files and support **different kinds of codecs such as MS-GSM, G711 uLaw, GSM.**

SIPp

This tool is used to examine SIP proxies, SIP servers and SIP phones. It has many features such as dealing with media traffic, describing calls flow, establishing calls and releasing calls with INVITE messages (SIPp, 2010).

3.3 Wireshark

Wireshark is a tool used by the network managers to capture the traffic and analyze it in order to discover and solve network problems. Between all the packet analyzer programs, Wireshark is the most common open source program used in the network administration (Lamping et al, 2010). Among its many uses, network troubleshooting, security problem testing and debugging protocol implementations.

3.4 Fail2ban

This tool will be installed in the server device to help preventing invite flooding. It has many features such as high configuration, supporting FAM/Gamin, Client/Server architecture and multi threaded (fail2ban, 2010). Fail2ban scans server log files and detects the possible attacking actions after X times of attempts (X can be changed each time) from the same IP address. After detecting the attack, it will ban this IP address for a specific period of time determined in the tool file by the network administrator.

4 Experiments and Results Analysis

4.1 Scanning

This experiment is a very essential step before attacking the network. It helps the attackers to take a general overview about the infrastructure, weak devices and IP addresses as it will be seen below. One of scanning methods is using the efficient tool Nmap. This command below will be used

```
nmap -O -P0 192.168.1.1-254
```

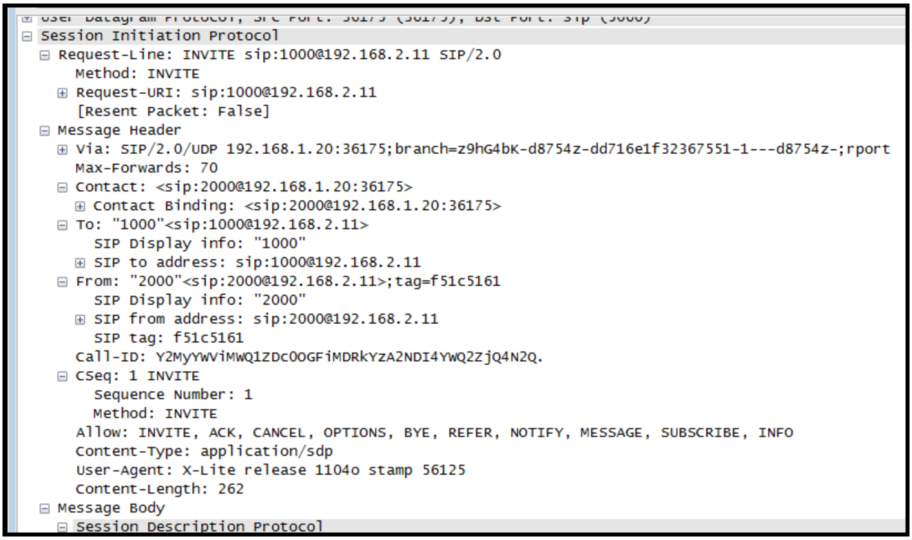
This command will scans all the IP addresses in the network from 1 to 254 and the result will list all network devices with their characteristics. The scan result of 192.168.1.9 is shown in figure 2 and it contains many pieces of information such as the MAC address, open ports (22, 111, and 6000) and the operating system which used.

```
Nmap scan report for 192.168.1.9
Host is up (0.00024s latency).
Not shown: 997 closed ports

PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
6000/tcp open  X11

MAC Address: 00:10:4B:B6:2E:AD (3com)
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop
```

Figure 2: General Characteristics of host 192.168.1.9

4.2 Eavesdropping

Eavesdropping is one of the famous methods that used by attackers to target the network and collect useful information about the VoIP system. A Wireshark tool will be used here to capture traffic and analyze it during connection between two clients. Figure 3, which captured during a call between two endpoints with the IP addresses 192.168.1.20 and 192.168.2.12, shows different types of important data that could be easily obtained. There is much information appears in the figure below including the IP addresses and usernames for the two endpoints in addition to the port number. The type of media that used during the session is also one of the essential information that can be used from the attacker. All of this information is very necessary to be known before different methods of attacks could happen to any target



```
⊞ User Datagram Protocol, Src Port: 36175 (36175), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: INVITE sip:1000@192.168.2.11 SIP/2.0
      Method: INVITE
    ⊞ Request-URI: sip:1000@192.168.2.11
      [Resent Packet: False]
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.1.20:36175;branch=z9hG4bK-d8754z-dd716e1f32367551-1---d8754z-;rport
      Max-Forwards: 70
    ⊟ Contact: <sip:2000@192.168.1.20:36175>
      ⊞ Contact Binding: <sip:2000@192.168.1.20:36175>
    ⊟ To: "1000"<sip:1000@192.168.2.11>
        SIP Display info: "1000"
      ⊞ SIP to address: sip:1000@192.168.2.11
    ⊟ From: "2000"<sip:2000@192.168.2.11>;tag=f51c5161
        SIP Display info: "2000"
      ⊞ SIP from address: sip:2000@192.168.2.11
        SIP tag: f51c5161
      Call-ID: Y2MyYWViMWQ1ZDc0OGFiMDRkYzA2NDI4YWQ2ZjQ4N2Q.
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
      Content-Type: application/sdp
      User-Agent: X-Lite release 1104o stamp 56125
      Content-Length: 262
  ⊟ Message Body
    ⊟ Session Description Protocol
```

Figure 3: Important Information can be obtained from SIP Message using Wireshark

4.3 INVITE Flooding

This experiment covered affect of INVITE flooding Attack on the Asterisk server. SIPp tool has been used to generate INVITE messages. The numbers of INVITE messages started from 0 per second (no flooding) and increased by 5000 each time until 50000 INVITE messages per second. The number of passed calls, failed calls and the delay are calculated each time. This command which used to send INVITE flooding has been run from the attacker device to the server:

Sipp –sn uac –r N –rp M IP address

It will run SIPp with embedded client (uac) scenario at the rate N calls per M seconds.

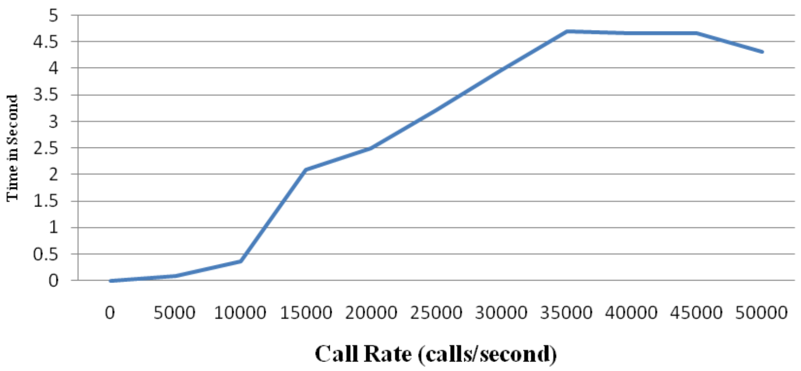


Figure 4 Call Delay during INVITE Flood

The call delay will be calculated in this experiment by using *Wireshark* to capture the traffic during make calls. This delay is referred to the difference in time between initiating the call and receiving this call from the other client.

Figure4 shows that the delay time increases as the number of call rate increases until it is almost being stable from 35,000 to 50,000 calls per second. The normal delay when no flooding attack is generated (at 0 calls per second) was about 2.96 millisecond (0.00296 second). These results appeared because of the effect of the attack on the SIP proxy server which causes it unable to process the call as the number of calls increase. Note that the Asterisk server works with Intel Pentium 4 and its CPU is 3 GHZ and therefore, its performance is expected to be better if powerful server with more features had been used.

Regarding the number of passed calls, 100 calls will be done at each call rate to give more accurate results. As it is shown from figure 5, the Number of calls forwarded by the Server decreases from 100 calls at no flooding (0 calls/sec) until it reaches about 20 passed calls at 50000 calls/sec. The Asterisk server has fixed features which can afford handling certain numbers of clients per specific period of time. After that, the server has to drop some messages to be able to process the other which make the caller sometimes starts to get a timeout message from the phone saying that the number is unavailable now

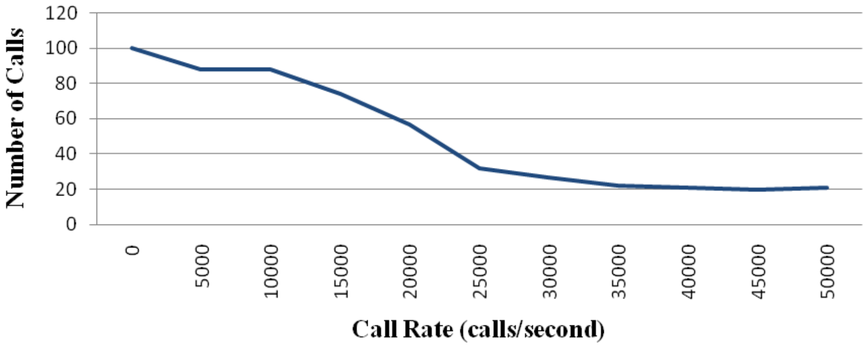


Figure 5: Passed Calls

4.4 INVITE Flooding Mitigation

In this experiment, a tool called Fail2ban has been used to run in the Asterisk server during the flooding attack. This tool requires determining the source and destination IP to block the flooding attack and ban the attacker for specific period of time. SIPp is used to launch the flooding attack from the attacker device through this command

```
Sipp –sn uac –r N –rp M –i IP address1 IP address2
```

Where IP address1 is the attacker IP address (192.168.1.25) and IP address2 is the server IP address (192.168.2.11). Fail2ban parameters have been set to the following: Maximum number of attempts: 5 and Ban period of time: 300 second. By setting these parameters, any IP address trying to attack asterisk server for 5 times is banned for 300 seconds. To do this, Fail2ban checks the log files and determine any suspicious traffic.

Figure 6 shows the difference in delay where it is clearly appeared that the mitigation reduced the delay because the VoIP clients had a period of time to make calls without any flooding attack can affect the service. For example, the delay at 40000 calls per second before using fail2ban was 4.65 second while it dramatically decreased to 0.69 second after applying the solution. The difference in delay can be noticed each time the call rate is increased.

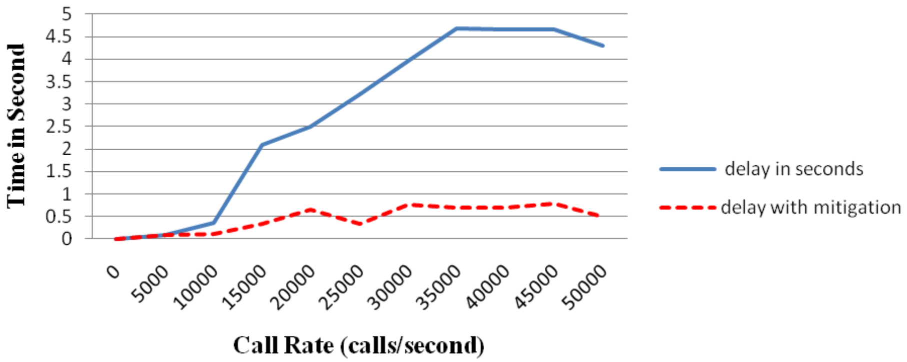


Figure 6: Difference in Delay

Regarding the number of passed calls that succeeded in arriving at the destination, figure 7 shows that about 98% of the calls have been processed by the server which gives an indication about the positive effect of the proposed solution. After applying this solution, the server does not suffer from the flooding attack most of the time because the tool bans the attacker for a specific period of time after detecting the attack which gives VoIP clients the opportunity to successfully make calls. The number of failed calls decreased significantly to the lowest level. For example, at the call rate of 35000 calls per second, no failed calls recorded and all the generated calls were succeeded. The number of passed calls is very high because the possibility of initiating the calls outside the ban period is very low. This happens due that the time which the server takes before banning the attacker is almost lower than 31 second which represents the time out period which ensures the server to forward calls in this period. This number may change at different situation such as increasing the number of clients in the network or decreasing the time period of attacker ban.

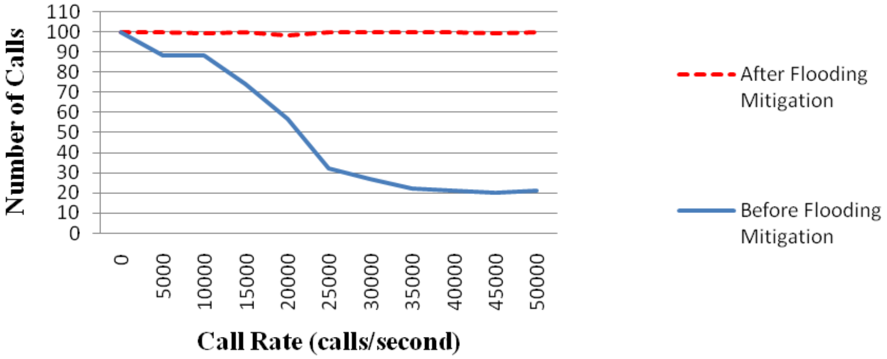


Figure 7: Passed Calls after and before mitigation

5 Conclusion

Security in Voice over IP (VoIP) networks is an important issue that should be taken in account from both users and providers. In order to discuss VoIP security, this paper introduced different types of attacks such as eavesdropping and INVITES flooding.

These experiments also have revealed clearly that VoIP network is vulnerable to different attacks especially DoS flooding attack which has high impact on the VoIP clients and Asterisk server. As we have seen from flooding test, the attack produces more delay when one client contacts the other in a VoIP network because the server could not afford the huge number of INVITE requests and therefore, the number of failed calls increased each time the call rate is increased.

To achieve high level of protection, different countermeasures can be used to detect or reduce the VoIP threats. These solutions include firewall, Network Address Translation (NAT), intrusion detection system (IDS) and encryption technique. However experimental outcomes have shown that the proposed solution using fail2ban tool that used to detect flooding attack can reduce the effect of this attack. These results depend on the ban period time and number of clients in the network.

Further studies are needed to address this topic in the future because none of the proposed solution can present a complete countermeasure for all problems and with time, new threats will be appeared and need to be solved efficiently. But generally the VoIP system will depend in the future on the security part. If the threats in VoIP technology could be solved, the deployment of VoIP will be easier and could replace the traditional phone system.

6 Reference

Fail2ban, 2010, [online] available at: http://www.fail2ban.org/wiki/index.php/Main_Page accessed 25 August 2010

Finneran, M 2008," Voice over WLANs", Page 161-162 Elsevier Inc, America

Handley M, Schulzrinne H, Schooler E, Rosenberg J March 1999, “SIP: Session Initiation Protocol” [online] available at: http://www.ietf.org/rfc/rfc2543.txt accessed 25 August 2010

X-lite, 2010, Counter Path Corporation, [online] available at http://www.counterpath.com/x-lite.html accessed 25 August 2010

Nmap, 2010, Network Mapper, [online] available at : http://nmap.org/ accessed 23 August 2010

Montoro, M 2010, OXID.IT, [online] available at: http://www.oxid.it/cain.html accessed 23 August 2010

SIPP, 2010, [online] available at: http://sipp.sourceforge.net/ accessed 23 August 2010

Investigation, Development and Test of Video over IP Applications for IMS/SIP Clients

R.Bonhomme, L.Sun and I.Mkwawa

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The main purpose of this paper is to investigate and develop Video over IP solutions regarding the current technologies. The objectives are to understand how a mobile device or client can communicate with multimedia servers and others devices and to define the differences with traditional telephony server on the one hand. To investigate and to understand how video calls and real time Quality of Service can be implemented on these clients using these servers on the other hand. A VoIP testbed was set up which includes open IMS core, Asterisk server, Android G1 phone and X-lite VoIP client to facilitate this task. Video calls between G1 phone and X-lite had been enabled using Asterisk server. These calls had been monitored: calculation of delay, jitter and packet loss and a Quality of Experience metric had been implemented to provide information on the call quality.

Keywords

Video over IP, SIP, Quality of Service

1 Introduction

“Users are expecting new multimedia applications that make use of the full capabilities of their devices.” This statement from a research on a mobile multimedia framework (Albaladejo et al, 2008) is a way of introducing this thesis. Today, there are a lot of technologies around us such as 3G, UMTS or IP. Information is everywhere and users are in the middle (Adamek et al, 2002 and Long, 2001). New services appeared these last few years: voice and video call, conferences, video messaging and operators have to improve and modernize their systems and their infrastructures. All these services have a direct cost and users pay it. However open sources solutions can be found such as Open IMS for 3G technology or Asterisk for WI-FI: Internet Protocols allow users to break free from their operators, to communicate between themselves.

2 IMS and Asterisk server

2.1 IMS

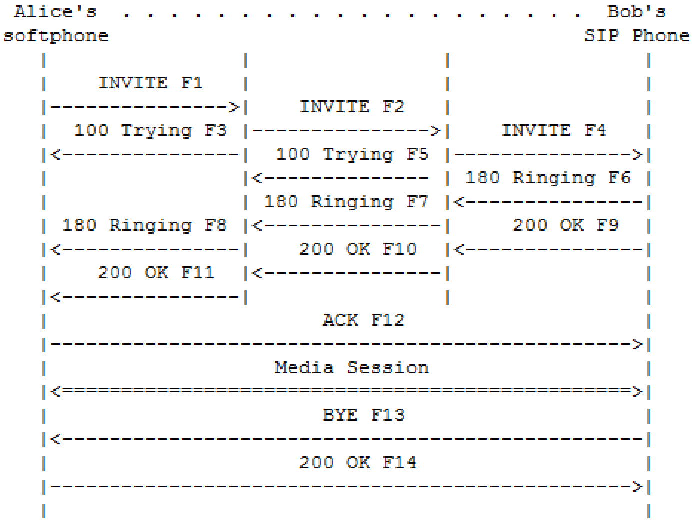
Like defined in 3GPP TS 23.228 (3GPP, 2009b), IP Multimedia Subsystem also called as IMS architecture has the capability to provide multimedia services such as voice, video and data for wireless users. The first contact between user equipment and an IMS network is P-CSCF or Proxy Call Session Control Function. P-CSCF is like a proxy, it forwards information from one point to another: Its mission is to ensure secured communications between end users and the IMS network, to forward requests and responses between end user and others IMS services (I-CSCF for a registration or S-CSCF for a service) and to provide an access to emergency services. Quality of service and SIP messages compression or decompression could be handling at this point (3GPP, 2009b). The second element is the I-CSCF or Interrogation Call Session Control Function. It assigns an S-CSCF during user registration based on information provided by the HSS such as user services or operator preferences (3GPP, 2009b) or it forwards requests for another network. The third element is S-CSCF or Serving Call Session Control Function. It handles all the session services (registration and control) and user services (bill information), accesses HSS to obtain user information. The fourth element is the HSS or Home Subscriber Server. It contains information on the end user such as identification, number, address, access information and location (3GPP, 2009b).The last element is AS or Application Server, it provides services for users on media sessions. As defined in the 3GPP 23.228 (3GPP, 2009a), users can be able to contact others from another network such as PSTIN or GSM.

2.2 Asterisk

Another solution can be found to allow WI-FI devices to communicate between themselves or to different networks: Asterisk. It is an open source project written in C which implements an IP Private Branch Exchange (PBX).This server is a combination of a core and different Application Programming Interface (API) as shown on the figure 4 (Asterisk, 2010). The core is a PBX system: it connects different users together. The four principals are channel, application, codec translator and file format. Channel is used to provide a support for different technologies such as SIP, Inter Asterisk eXchange or Integrated Services Digital Networks. Conferencing, voicemail or paging are added by the application API. Asterisk can also encode or decode different formats with the codec translator API.

3 SIP /SDP protocols

The main purpose of an IMS or Asterisk is to allow users with different clients to communicate together. As soon as a user has connection to a server, though 3G and WI-FI network for IMS or WI-FI network only for Asterisk, he can access services. However it is not “plug and play”, there are several procedures describing exchanges between users and servers for discovery, registration, authentication, calls or servers’ services. Portions of these interactions use SIP and SDP protocols. As defined into different rfc, they are protocols on application layer for “creating, modifying and terminating sessions with one or more participants” and “describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation”. According to rfc 3261 (Rosenberg et al, 2002) SIP protocol has got several features: register and subscribe methods for client declaration and registration, invite method for session creation and bye method for session termination. There are also different responses characterised by a status-code of three digits. These digits are defined from 100 to 699 with six different parts. For example from 100 to 199, it is a provisional state: request has been received and its treatment is in progress. From 200 to 299, it is a success: request has been received and its treatment is ok. From 400, server has problems to understand client requests or from 500, server failed with a valid request. They are important keys in an IP communication, every call starts with a common diagram. As shown on the figure 1, SIP protocol is based on an exchange of requests and responses between servers, proxies and clients



```
   Alice's  . . . . . . . . . . . . . . . . . . . .  Bob's
  softphone                                          SIP Phone
     |                |                |                |
     |    INVITE F1   |                |                |
     |--------------->|    INVITE F2   |                |
     |  100 Trying F3 |--------------->|    INVITE F4   |
     |<---------------|  100 Trying F5 |--------------->|
     |                |<-------------- | 180 Ringing F6 |
     |                | 180 Ringing F7 |<---------------|
     | 180 Ringing F8 |<---------------|     200 OK F9  |
     |<---------------|    200 OK F10  |<---------------|
     |    200 OK F11  |<---------------|                |
     |<---------------|                |                |
     |                       ACK F12                    |
     |------------------------------------------------->|
     |                   Media Session                  |
     |<================================================>|
     |                       BYE F13                    |
     |<-------------------------------------------------|
     |                     200 OK F14                   |
     |------------------------------------------------->|
     |                                                  |
```

Figure 1: SIP session example with two proxies (Rosenberg et al, 2002)

4 Android and Sipdroid

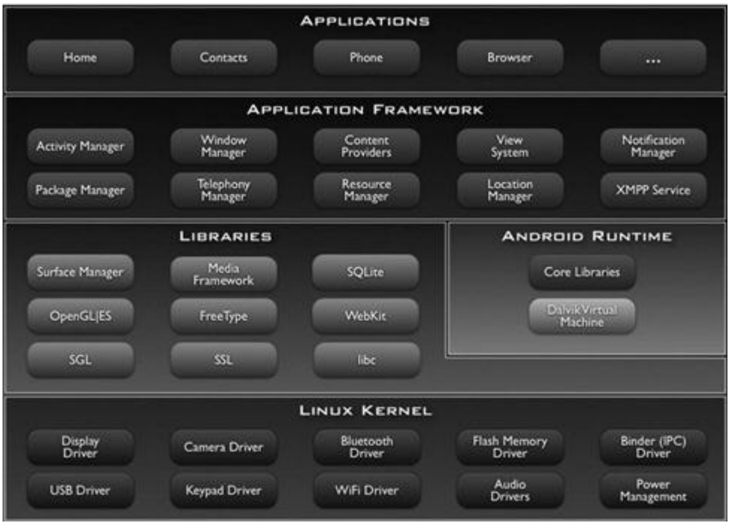


Figure 2: Android architecture (Burnette, 2008)

As shown on figure 2, Android is a mobile operation system based on a Linux kernel and code in java. Different tools are available to allow development and debugging on Android system: Android DDMS and Android development tools (ADT). According to Android developers website (Android developers, 2010a), Android Dalvik Debug Monitor Server (DDMS) provide a debugging tool which can be used on an emulator or a device connected. It can provide data on all applications running. ADT package regroups all Android tools and make them accessible from Eclipse interface or command lines. Sipdroid is a java based SIP client compatible with PBX and IMS architecture. These sources will be used to allow Video communications.

5 Testbed

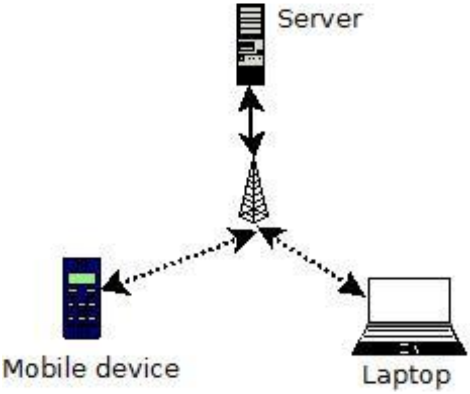


Figure 3: Testbed

As show on Figure 3, the testbed is composed with a mobile device (G1 phone), an Asterisk sever, a wireless connection and a computer with soft phones applications such as Ekiga or X-lite. Monitoring tools have been installed on the G1 phone and the computer to provide traces during the communications. A USB connection between the G1 phone and the laptop is used to transfer applications from Android SKD to the phone and to access tools on the phone.

6 Video applications

The final aim of this project is to investigate and add video calls capabilities to a SIP client (IMS or SIP based). So the first idea was to check if video from G1 phone can be sent to another device or a laptop. In order to do that a one way application is developed: when user has to enter an IP address into an interface and validates his action, a stream will be created between the device and the target. The application has to capture video frames from the camera, to encode them and to send them into the network. According to OpenCORE documentation (PacketVideo, 2009), video can be only encoded in H.263 version 1998 or 2000 known as H.263-1998 and H.263-2000. There are different parameters available such as frame size (QCIF 176 × 144 or CIF 352 × 288), frame rate (15 fps or 30 fps).The real objective of this project is to investigate and develop a video application for an IMS client. The first application was a mean to understand and test how android system reacts to a video stream: use of mediarecorder to create videos packets and creation of rtp packets. The next step is a video call. The Sipdroid project is under a GNU GPL, the sources can be modified but copyrights have to stay and it is not possible to do a commercial version without an authorization of the copyrights holders. On the Sipdroid documentation, it seems that there is not support for Asterisk server for the video calls and users have some problems to register with an Android device (Sipdroid, 2010). In considering the figure 13, we use Asterisk as server for the communication setup. In order to have the device registered to Asterisk server, two files need to be modified: SIP configuration file and Asterisk dial plane file. User profiles have to be added into the first file, they will allow SIP clients to connect and register to the server. To parameters have to be added: Qualify=no (disable round trip time timers) and canreinvite=no (use to resend an INVITE message to the clients before the beginning of the call, so all exchanges go through Asterisk) or the application crashes when there is a call. The last step is to configure the Dial plane to allow the clients to call each other. Different actions can be defined in the plane as such wait, answer, voicemail, dial or hangup. For the testbed, one client call another, so when someone calls extension 100, Asterisk takes the call, dials a SIP id and hangs up when the call is over.

To test the calls, two soft phones were installed on the laptop under Window 7, Xlite and Ekiga. They have to be configured to connect Asterisk server, in each case a SIP account is created with the usernames, passwords defined in the sip.conf file and the IP address of the server. Sipdroid code has to be modified to work properly with an Asterisk server. Android platform is not compatible for the moment with RTP stream, so video calls work in two directions but only one client can see the other camera.

7 Quality of Service and Quality of Experience

With the video application working: packets are sent and are received on the Android device, a monitoring on the quality of the video call can be implemented. It is one of the objectives of this project to provide to users information on their calls and if it is possible to adapt the call quality regarding the network conditions. Two sorts of information will be displayed: packet loss, jitter and delay for an indication of the Quality of Service and a Mean Score of Opinion for the Quality of Experience. As defined in the first part on this thesis, the calculation of the delay, of the jitter and the packet loss are direct measurements opposite to MOS score that is defined by a model. To calculate this score, different models are available such as PEVQ or V-MOS. However in this project, there is only a limited access to the media and only a reference-free algorithm can be used. One algorithm called “regression-based video quality prediction” and defined by Khan et al (2009), uses parameters from the application level to score a MOS for the video and to provide a QoE score that can be used to implement adaptation. Parameters used by this algorithm are frame rate, send bitrate and the packet loss rate. The frame rate and the send bit rate are linked to the softphone encoder. A method is created and it calculates QoS parameters and QoE score. Different variables are defined in static and there are available in all the Sipdroid application: lossvideo, latevideo, data, jitter and Mos. Others variables are used locally for the calculations. When the measure method is called, if the receiving of a RTP packet is possible the parameters are calculated. For the QoS parameters, the first calculated is packet loss rate: the current sequence number is compared to the previous one and if there is a difference: packets are lost. The delay is the time difference between the packet arrival and the previous one. For the jitter, the formula used is defined by Schulzrinne, et al (2003) in the rfc 3550. D is the difference between a packet i and the previous j, R is the time when the packet arrives and S is the RTP timestamp. J is an estimation of the jitter as called interarrival jitter.

$$D(i,j) = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si)$$

$$J = J + \frac{(|D(i-1,i)| - J)}{16}$$

To calculate a QoE score, model defined by Khan et al (2009) is used. In this model, constants characterize different environments: Slight Movement, Gentle Walking and Rapid Movement. As the device is mobile and the user can walk when he uses it, the second category was chosen. So the MOS is equal to:

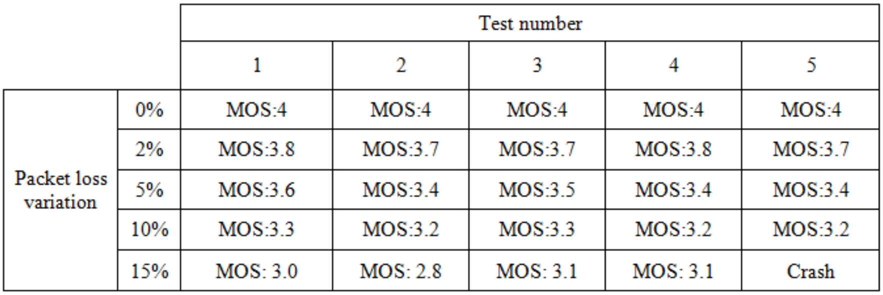
$$MOS = \frac{a_1 + a_2 \times (frame\ rate) + a_3 ln(send\ bite\ rate)}{1 + a_4 \times Packet\ error\ rate + a_5 (Packet\ error\ rate)^2}$$

with a_1=3.4757, a_2=0.0022, a_3=0.0407, a_4=2.4984, a_5=-3.7433

The range of this value is from 0 to 5, from bad to good.

8 Results

At the beginning, packet loss, frame rate and bitrate were calculated by the monitoring class. However Sipdroid seems to crash and/or the camera blocks itself during the tests. To limit these problems, only one parameter varies: packet loss rate and the others are set up. For testing, frame rate is 27 frames per seconds and bitrate is 140Kbytes/seconds. The tc command available under Linux platform is used on the Asterisk machine to add on the network some perturbation such as packet loss or delay. To limit the variation of the packet loss during the call, one minute is used as a reference for all calls.



		Test number				
		1	2	3	4	5
Packet loss variation	0%	MOS:4	MOS:4	MOS:4	MOS:4	MOS:4
	2%	MOS:3.8	MOS:3.7	MOS:3.7	MOS:3.8	MOS:3.7
	5%	MOS:3.6	MOS:3.4	MOS:3.5	MOS:3.4	MOS:3.4
	10%	MOS:3.3	MOS:3.2	MOS:3.3	MOS:3.2	MOS:3.2
	15%	MOS: 3.0	MOS: 2.8	MOS: 3.1	MOS: 3.1	Crash

Figure 4: MOS evolution with packet loss

In the figure 4, there is a summary of the MOS score with the evolution of packet loss during different tests. A visual evolution can be monitored in Figures 5 that was captured from the laptop with different packet loss rate. There is no visual difference between the two captures. When the packet loss is set to 5%, some errors appear in during the calls however overall quality is still good. With 10% and 15%, errors are increasingly presented and Xlite or Sipdroid can crash during the call.

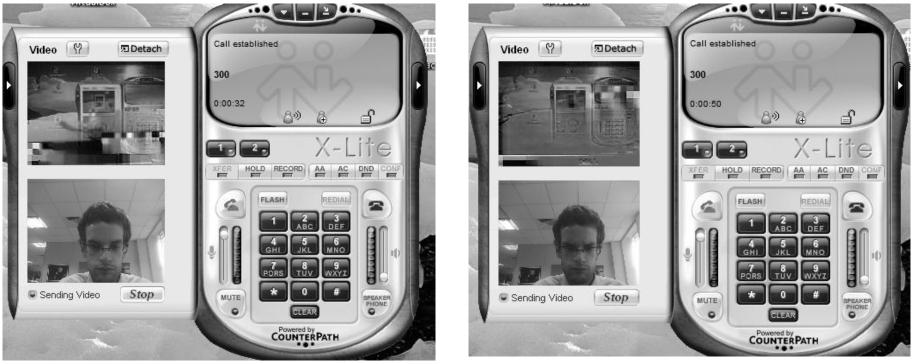


Figure 5 – Video call with 10% and 15% packet loss

With the variation of the QoS parameters during the tests without any modification, the MOS is measured with a delay variation. As with the packet loss test, delay is added on the network interface.

		Test number				
		1	2	3	4	5
Delay variation	0 ms	MOS:4	MOS:4	MOS:4	MOS:4	MOS:4
	10 ms	MOS :4	MOS: 3.9	MOS:4	MOS:4	MOS:3.9
	20 ms	MOS: 3.9	MOS: 3.8	MOS:3.9	MOS:4	MOS:3.9

Figure 6: MOS with delay evolution

According to the formula for the MOS calculation, delay variation should not affect MOS values. However with a packet loss variation during the call, MOS is affected as shown on Figure 6.

9 Conclusions and Future work

This paper has built an Asterisk testbed with a mobile device to implement and test video quality measurements with a no reference algorithm. The next step in this project is to modify the testbed and use these applications with an IMS architecture. As defined at the beginning, IMS server is based on SIP protocol like Asterisk server but using different servers the communications are more complicated. Two scenarios can be made, implementation of Asterisk server as an Application server or implementation of an IMS client.

10 References

3GPP (2009a) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 9). Available at http://www.3gpp.org/ftp//Specs/archive/23_series/23.228/ [Accessed on 1/01]

3GPP (2009b) 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture(Release 9) . Available at http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/ [Accessed on 2/01]

Albaladejo, A. M., Murarasu A. And Magedanz, T (2008) 'Design of a Coherent Mobile Multimedia Framework for Convergent Services'. New York: ACM

Adamek, J.G., Henrikson, E.H., Lassers H.A, Lee, A.Y. and Martin, R.B. (2002) 'Services and Technical Considerations for Wireless IP Multimedia Subsystem' Bell Labs Technical Journal, 7 (2), pp. 91-104. Available at http://www.informatik.uni-trier.de/~ley/db/journals/bell/bell7.html [Accessed on 01/02]

Android developers (2010a). Dev Guide. Available at http://developer.android.com/index.html [Accessed 1/08]

Asterisk (2010) The open source telephony project. Available at http://www.asterisk.org/ [Accessed on 29/03]

Burnette, E. (2008) How Android works: The big picture. Available at http://www.zdnet.com/blog/burnette/how-android-works-the-big-picture/515 [Accessed on 10/06]

Khan, A., Sun, L. and Ifeachor, E (2009) 'Content Classification Based on Objective Video Quality Evaluation for MPEG4 Video Streaming over Wireless Networks', World Congress on Engineering, track on International Conference on Wireless Networks, London,1-3 July. pp889-894.

Long, C. (ed.)(2001) Wireless and Mobile Network Architectures. New York: John Wiley & Sons.

PacketVideo (2009) OpenCORE Multimedia Framework Capabilities. Available at www.opencore.net/files/opencore_framework_capabilities.pdf [Accessed on 03/02]

Schulzrinne, H., Casner, S., Frederick, R. and Jacobson, V (2003) 'RTP: A Transport Protocol for Real-Time Applications', IETF, available online at http://www.ietf.org/rfc/rfc3550.txt [Accessed on 10/06]

Sipdroid (2010) Available online at http://code.google.com/p/sipdroid/ [Accessed on 23/03]

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E. (2002) ' SIP: Session Initiation Protocol', IETF , Available online at http://www.ietf.org/rfc/rfc3261.txt [Accessed on 29/01]

Application of LDPC Codes to Networks

G.V.Joseph and M.A.Ambroze

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Internet is no longer just about emails and websites. It has become the critical medium of communication and entertainment and keeps on growing larger and larger day by day. Internet serves the society with the entire major needs like education, finance and business. The network performance has become a vital ingredient in businesses. Such rapidly growing internet make the network management increasingly important. The more and more emphasis is actually held on speed, connectivity and reliability. The dependence on the network connection by individuals or the enterprises will break down catastrophically if any problem occurs with the internet. The major problems with the internet these days are network efficiency and congestion. Because of such network congestion, the quality of service to the users gets deteriorated. Congestion leads to retransmissions which are considered as high overload. Such increase in transmission results in the packet loss or packet delay causing the applications to retransmit the data and thereby adding more and more traffic which results in further congestion. In order to reduce such retransmissions, the error correction codes are implemented. This research will investigate the ways to reduce the need for retransmission by using more efficient error correction codes. The most efficient form of error correction codes is the Low Density Parity-Check (LDPC) codes. This project involves the implementation of the LDPC codes which will be able to reconstruct a certain number of lost packets at the receiver end without the need to retransmit them again.

Keywords

Error correction codes, LDPC, Encoding, Decoding

1 Introduction

Computer networks are used for various purposes serving the companies and individuals. The digital means of communication has become an essential tool in a technological society. The network congestion is one of the major problems in data networking. The congestion affects the overall efficiency of the network. Because of the reduction in the network efficiency, there are variations in data rate and data delay that might alters the throughput of the network. Throughput is defined as the number of packets sent at a particular time. Reduction in throughput degrades the quality of service. Congestion occurs because of the increase in the number of network and associated devices and also the increase in the transmission rate which causes buffer overflow. This will lead to the loss in the transmitted packets making the application to retransmit the lost packets and adding further increase in congestion. Finally the congestion will get increased more and more and results in a very low level of throughput hence making the communication less useful. The concept of the network coding was first introduced for satellite communication networks (Yeung *et al.* 1999). The first concept was a fundamental one and not thoroughly examined. After continuous investigations, the network coding concept was again fully developed (Ahlswede *et al.* 2000). The secondly introduced concept presented the advantages of the network coding method over the store-and-forward method. Later, the network coding found itself useful in many applications like information theory and coding, networking, wireless communication, etc. The concept of network coding is thoroughly investigated on both single information source and multiple information sources. Due to continuous development, many applications based on network coding have emerged. Thus, the network coding has placed them at a prominent position in the communication technology.

2 Literature Review

Low Density Parity Check (LDPC) codes are the set of linear block codes. Their name comes from the properties of the parity check matrix which contains only few numbers of ones when compared with the number of zeros. They are suitable for implementations that make heavy use of parallelism. The LDPC codes provide the channel-capacity performance on a large collection of data transmission and storage channels while simultaneously admitting implementable decoders. The LDPC codes have underwent rapid progress from the time they have been introduced. Such codes are now been used in many applications. The LDPC codes are applied in satellite-based Digital Video Broadcasting (DVB) and also in optical communication. They are highly adopted in IEEE wireless local area network standard. They are also in the consideration to be employed in third generation mobile telephony.

2.1 Background of LDPC codes

Low Density Parity Check (LDPC) codes were first proposed by Gallager in his PhD thesis in the year 1962. (Gallager, 1962 and 1963). Though the proposal was made, the code was scarcely used for 35 years that followed. The need for high complexity computation and introduction of the Reed-Solomon codes made the LDPC codes non-usable for such long gap. During that period, the concatenated codes were found appropriate for error control coding and hence this was also a reason. Also, the hardware of that time was not suitable to implement an effective decoder for LDPC codes. Hence because of these reasons, the forward error correction was dominated by the convolutional codes and structured block codes. Eventhough they dominated, their performance was well below the limit described by Shannon in his seminal paper (Shannon, 1948). Then the introduction of turbo codes made a revolutionary change in the coding theory which was found to be the best of all the error correction codes. The turbo codes were proposed by Berrou, Glavieux and Thitimajshima in 1993 (Berrou *et al.* 1993).

During the mid 90s, the research on LDPC codes commenced again by MacKay and Luby who introduced a new set of block codes which resembled the same features of the turbo codes (MacKay, 1999). Also, many new generalisations for LDPC codes were given by Richardson and Urbanke (Richardson and Urbanke, 2001). They introduced a set of irregular LDPC codes which outperformed the turbo codes. LDPC codes found to be more effective than the turbo codes. The decoder of the

LDPC codes used to declare if there is any decoding failure whereas decoder in turbo codes has to perform many computations to halt the decoding process. In LDPC codes, the shape of the parity check matrix specifies the creation of any rate and block length LDPC codes. The validity of the codeword is validated even when the error occurs. Moreover, the LDPC codes are not copyright protected and this made them more useful commercially.

LDPC codes are the set of linear block codes with the sparse parity check matrix. As the name suggests, it has very small number of non-zero elements in the parity check matrix. This guarantees both the decoding complexity and the minimum distance that linearly increases with the code length. Except the sparseness in the parity check matrix, there is no other difference between the LDPC codes and other block codes. Even all the other set of block codes can be represented as the LDPC codes by using the sparse parity check matrix. However finding the sparse parity check matrix for the present set of block codes is not so easy and it finds difficulties in practical cases. In LDPC codes, the generator matrix is determined only after constructing a sparse parity-check matrix. Gauss-Jordan elimination (Gaussian reduction) method is used to find the non-sparse generator matrix from the standard parity check matrix. Hence the encoding complexity can become quadratic in the code length. Using appropriate column permutations and back substitution methods, a linear-time encoding is processed. Encoding of LDPC codes and other classical block codes has some similarities. But the difference between them is how they are decoded. Classical block codes are decoded using the maximum likelihood decoding algorithms whereas the LDPC codes are decoded by the iterative algorithms using the graphical representation of the parity check matrix and thereby focussing more on the properties of the parity check matrix.

2.2 Construction of LDPC codes

There are different algorithms present for the construction of the LDPC codes. Those different algorithms are based upon different design approaches aiming different design criterion. It also depends upon the efficient encoding and decoding method. The most obvious method to construct the LDPC codes is through the construction of parity check matrix with a low density and with other suitable characteristics. The original LDPC codes were described by Gallager (Gallager, 1962). He used the regular LDPC codes and defined in H matrix form. In Gallager parity check matrix, the rows are divided into W_c sets with M/ W_c rows in each set. The first set of rows contains W_r consecutive ones ordering from left to right across the columns. All the other set of rows are formed by the column permutation of the first set. The Gallager codes were generalised by Tanner in 1981 (Tanner, 1981). That generalised LDPC codes were used for the study in CDMA (Code Division Multiple Access) communication channel. Gallager codes were extended by MacKay and others (MacKay, 1999).

Another form of constructing LDPC code was given by MacKay and Neal (MacKay and Neal, 2005). They suggested a way in which one column is added with another column positioning from left to right in the parity check matrix. So, the column weight can be chosen for reaching the right bit degree distribution. The location of ones in each column is chosen from the rows that are not full. If there are any unfilled positions, the remaining columns are added. The row degree distribution may vary because of this process. Hence, by staring the process again, the correct row degree distributions are obtained. The only drawback in MacKay codes is that they do not have adequate structure to enable low-complexity encoding.

Richardson and Luby defined the ensembles of the irregular LDPC codes (Richardson *et al.* 2001) (Luby *et al.* 2001). Those codes are parameterised by the degree distribution polynomials. And also they explained how to optimise the polynomials for different communication channels. But the irregular codes do not essentially useful for efficient encoding. However Richardson and Urbanke proposed methods for achieving the linear-time encoding the codes.

Another form of LDPC codes called Repeat Accumulate (RA) codes has been proposed (Divsalar *et al.* 1998). This code has the characteristics of both the turbo codes and the LDPC codes. The RA codes have weight 2 columns in a step prototype for the last m columns of the parity check matrix. This form is of systematic block code and they are efficient and easily encoded. They are capable of operating at capacity limits, but they have low rate. The bits are repeated more than others yielding irregular repeat-accumulate (IRA) codes (Jin *et al.* 2000). The IRA encoder has a low density generator matrix, permuter and accumulator. The IRA codes are capable of operating close to the limits than the RA codes. The difference between them is IRA codes are non-systematic whereas the RA codes are systematic codes.

2.3 Representation of LDPC codes

There are two ways in which the LDPC codes can be represented. The two ways are matrix representation and graphical representation. The matrix representation is similar to the representation of other classical linear block codes.

2.3.1 Matrix Representation

The following is the example of a parity check matrix H represented by the matrix form.

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

This is a parity check matrix with dimensions n × m for a (8, 4) code. In the matrix W_r denotes the number of ones in each row and W_c denotes the number of ones in each columns. W_r denotes the number of ones in each row. W_c denotes the number of ones in each column. For the matrix to be of low density then the following two conditions must be satisfied: $W_c << n$ and $W_r << m$.

2.3.2 Graphical Representation

The second way of representation of LDPC codes is the graphical representation that was introduced by Tanner. They are the graphical depiction of the parity check matrix. This form not only provides the representation but also helps to describe the decoding algorithm. The tanner graph always contains set of nodes. The nodes of the graph are of two different types. They are variable nodes (v-nodes) or Bit nodes and Check nodes (c-nodes)

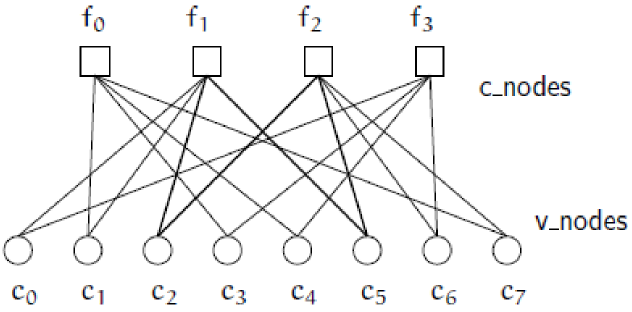


Figure 1: Tanner graph associated with the parity check matrix (Source: www.engr.uvic.ca/~masoudg/upload/ldpc-a%20brief%20tutorial.pdf)

3 Implementation

The following section will clearly explain the methods of encoding and decoding algorithms for the LDPC codes.

3.1 Encoding LDPC codes

The encoding of LDPC codes has two main functions involved. They are (a) construction of parity check matrix that is sparse and (b) generation of codeword with the matrix. Sparsity in the parity check matrix means each symbol node very few connections to the check nodes in the tanner graph. The parity check matrix always contains fewer number of 1's when compared to the number of 0's. In order to reduce the number of 1's in the parity check matrix; there are many algorithms and methods. One such method is gauss elimination that reduces the matrix H by employing elementary row and column operations. Often the generator matrix is not sparse only the parity check matrix is sparse which leads to the complexity in the encoding. The encoding efficiency is quadratic in block length. This is the only contrast with the turbo codes which has linear encode complexity. However it is possible to encode with minimum complexity by performing some process prior to encoding (Richardson and Urbanke, 2001). Some of the methods and algorithms for reducing the number of 1's in the parity check matrix are discussed below.

The LU factorisation was the first encoding method with the linear complexity introduced by Neal (Neal, 1999). This method was used in order to reduce the dense inverse operation that is involved in the encoding process. This method is applicable for both the regular and irregular form of LDPC codes. In the systematic encoding process of the (n, k) LDPC encoder, the parity check matrix H can be divided into two sub groups. Let the two sub groups denoted by A and B. The matrix A is given by [(n-k) × (n-k)] and the matrix B is given by [(n-k) × k]. The codeword can also be split into systematic form that contains two categories of bits. The first k bits are the source message bits and they are denoted by s. The remaining (n, k) bits are the parity check bits and they are denoted by c. Hence the codeword is given by [s, c]. The encoding algorithm should satisfy the following condition, H × codeword ^{T} = 0. The LU factorisation is applicable for any kind of matrix as it finds solutions for all. This method is easy to program and it is very fast. The only disadvantage in this method is that it is difficult to find a good sparse LU decomposition for arbitrary H matrix (Su *et al.* 2005).

The Approximate Linear Triangulation (ALT) algorithm contains the parity check matrix of the LDPC code which is very sparse. But that sparsity is not present in the generator matrix of the LDPC code. The encoding of the LDPC codes is based upon the approximate lower triangular (ALT) form which is given by [L × N] where N - the block length of the code and L - the number of parity check equations. The complexity of encoding is very high because of the absence of sparsity in the generator matrix. Richardson and Urbanke developed an algorithm called RU algorithm that was widely used. The encoding is done with a specified parity check matrix H with a low triangular shape. The complexity in the algorithm is given by $O(n+g^2)$. The only disadvantage with the ALT algorithm is that there is no exact programmable step by step algorithm (Qi and Goertz, 2007)

The Greedy permutation algorithm is used to transform the parity check matrix into an approximate lower triangular form with minimum gap. The gap refers to the number of rows of the parity check matrix that cannot be brought into triangular form by row and column permutation. The complexity of the algorithm is given by $O(n^3)$. This algorithm involves mathematical calculations only and there is no exact programmable step by step algorithm. This method concentrates only with the reduction of the parity check matrix. The method provides the tradeoffs between the gap size and the performance for any given block length.

The Gaussian elimination is the most conventional method of encoding the LDPC codes. This method involves the systematic encoding with the generator matrix derived from the parity check matrix. The Gaussian elimination method is applicable for any type of block code and it does not deploy the sparseness of the LDPC codes. The complexity is $O(n^2)$ where n denotes the length of the codeword. This method is used to determine the generator matrix from the parity check matrix. The generator matrix is determined by performing the row permutations, modulo-2 operation on any two rows and some column permutation. The form of the generator matrix and the parity check matrix are given. Generator matrix is given by $G = [I_k \quad A^T]$. Parity check matrix by $H = [A \quad I_k]$. The parity check matrix is reduced into row echelon form by employing elementary row operations. The codeword after encoding is called the encoder codeword and it is denoted by c. The encoded codeword is obtained by multiplying the generator matrix with the information bits given by c = I × G. Thus the resultant codeword is the output of the encoder and with the help of the codeword, the information bits are received at the decoder.

3.2 Decoding LPDC codes

Many algorithms were developed for the decoding of LDPC codes. These algorithms were discovered independently several times. When Gallager introduced the LDPC codes in 1960s (Gallager, 1962), he also provided a decoding algorithm that is typically near optimal. The decoding algorithms iteratively compute the distribution of variables in graph-based models. Those algorithms were used to serve different purposes and hence they come under different names depending on the context. The commonly employed decoding algorithms are the message passing algorithm, belief propagation algorithm and the sum product algorithm. The term ‘message passing’ relatively represents all the iterative algorithms including the sum product and belief propagation algorithm and their approximations.

In order to explain the decoding algorithms, the simple variant which works on the platform must be explained. They are hard decision decoding and soft decision decoding. Hard decision decoding is easier to implement than the soft decision decoding. However, soft decision decoding offer better performance and decoding results when compared to the hard decision decoding.

When binary codes are used i.e. 0s and 1s, the digital modulator has only binary inputs. If digital demodulator output quantization is used, the decoder has only binary inputs. In this case, the demodulator is said to make hard decisions. Decoding based on hard decision made by the digital demodulator is called “hard decision decoding”. If the output of digital demodulator consists of more than two quantization levels or without any quantization, the digital demodulator is said to make soft decisions. Decoding based on the soft decision made by digital demodulator is called soft-decision decoding. This method does not employ any flipping up of bits as in the hard decoder. The evidence that the checks provide about the bits are accumulated and the probabilities are propagated through the tanner graph. This method of decoding offers a means of bridging the performance gap between the system that uses hard-decision decoding and the system that uses maximum-likelihood decoding. The confidence information can then be used to improve the decoding process in such a way that the probability of decoding error and the decoding delay can be reduced. Hence the performance of the soft decision decoding is far better than the hard decision decoding.

3.3 Iterative Decoding algorithms

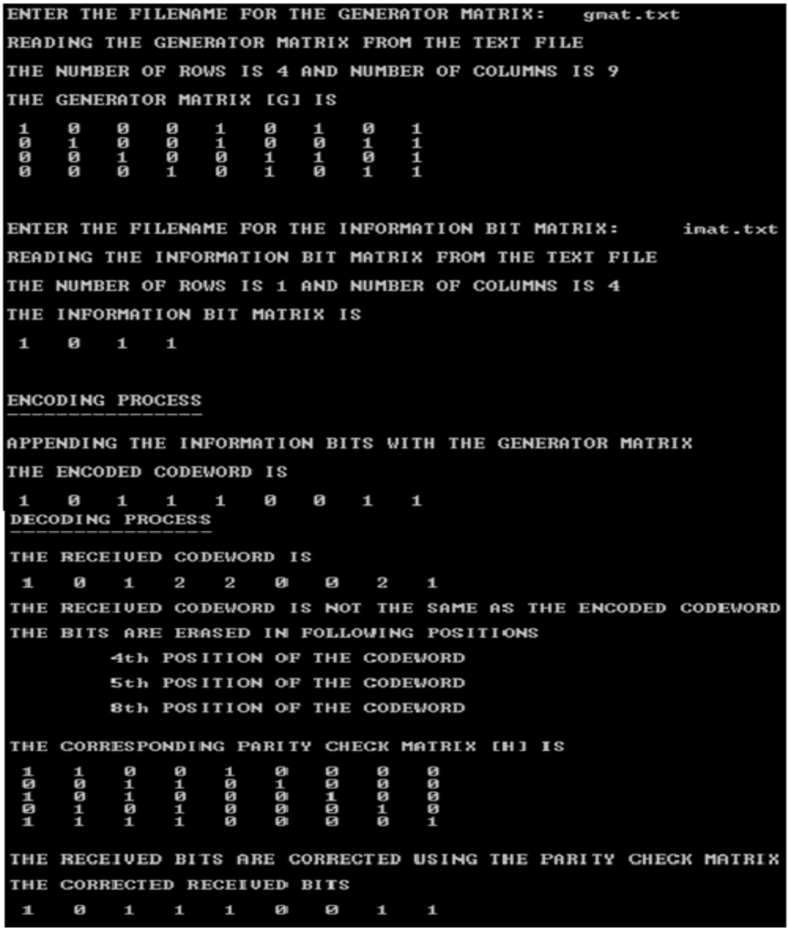
The set of decoding algorithms for decoding LDPC codes are collectively called as the message passing algorithms. Their operation is based upon passing the information along the edges of the tanner graph. These message passing algorithms are called as the iterative decoding algorithms. The messages are passed front and back between the variable nodes and the check nodes iteratively till a result is obtained. Consider the binary erasure channel where the transmitted bits are received correctly or received as erased with the erasure probability ε. In the erasure channel, the received bits are always correct and hence there is no need for the decoder to check the received bits. The main task of the decoder is to determine the value of the unknown bits. The parity-check equations are formed that includes only one erased bit, the correct value for the unknown (erased) bit can be determined by choosing the value which satisfies the even parity. In this decoding method, the check node determines the value of an erased bit if it is the only erased bit in its parity-check equation that is framed already. The messages are passed along the edges of the tanner graph and the process is straightforward. Each bit node transmits the same outgoing message to each of its connected check nodes. The outgoing message is denoted by M. The message is declared as 1 or 0 or x if it is erased. If there is only one error x in the received message, the value of x can be calculated by choosing the suitable parity. The check node returns the message to the bit nodes. This message is labelled as $E_{j,i}$ where the j denotes the j^{th} check node and i denotes the i^{th} variable node. If the bit node of the erased bit receives 1 or 0 then the bit node changes the value to the incoming message. This process is repeated till all the erased bits are identified or the maximum number of iterations are performed.

The bit flipping algorithm is a message passing algorithm that is based upon the hard decision decoding of the LDPC codes. A hard decision is made on all the incoming bits and the result is passed to the decoder. The binary messages are passed onto the edges of the tanner graph. One of the bit nodes sends the message to check node containing the value one or zero. Each check node is connected to other bit nodes. The message received by the check node is forwarded to all the bit nodes that are directly connected to them. The check node determines the parity check equations. It also checks if the modulo-2 sum of the incoming message is zero. If messages received by a bit node are different from its received value; the bit node flips the current value. The process is repeated till all the parity check equations are satisfied.

The sum product algorithm is a type of message passing technique based upon the soft decision decoding. The sum product algorithm is similar to the bit flipping algorithm but the only difference is that in sum product algorithm, the message represents the probability. The bit flipping algorithm decoder accepts the initial hard decision on the received bits as input. But the sum product algorithm accepts the probability on the received bit as input. The incoming bit probabilities are called as the priori probabilities for the received bits. The input bit probabilities are known in advance before running the LDPC decoder. The bit probabilities that are returned by the decoder are called as posterior probabilities. The probabilities are expressed as log-likelihood ratios. The aim of this algorithm is to calculate the maximum a posterior probability (MAP) for each codeword.

4 Results and Discussions

The following section contains the explanation of the results obtained in the project. There are two phases in the project. They are encoding and decoding part. The encoding of LDPC codes involves the generation of the encoded codeword that is used to transmit the information from the sender to the receiver. The codeword is generated by appending the information bits with the generator matrix. Hence the codeword is used at the decoder as well in order to determine the exact information transmitted. The steps involved in the encoding are explained below.



```
ENTER THE FILENAME FOR THE GENERATOR MATRIX:   gmat.txt
READING THE GENERATOR MATRIX FROM THE TEXT FILE
THE NUMBER OF ROWS IS 4 AND NUMBER OF COLUMNS IS 9
THE GENERATOR MATRIX [G] IS
 1   0   0   0   1   0   1   0   1
 0   1   0   0   1   0   0   1   1
 0   0   1   0   0   1   1   0   1
 0   0   0   1   0   1   0   1   1

ENTER THE FILENAME FOR THE INFORMATION BIT MATRIX:     imat.txt
READING THE INFORMATION BIT MATRIX FROM THE TEXT FILE
THE NUMBER OF ROWS IS 1 AND NUMBER OF COLUMNS IS 4
THE INFORMATION BIT MATRIX IS
 1   0   1   1

ENCODING PROCESS
----------------
APPENDING THE INFORMATION BITS WITH THE GENERATOR MATRIX
THE ENCODED CODEWORD IS
 1   0   1   1   1   0   0   1   1
DECODING PROCESS
----------------
THE RECEIVED CODEWORD IS
 1   0   1   2   2   0   0   2   1
THE RECEIVED CODEWORD IS NOT THE SAME AS THE ENCODED CODEWORD
THE BITS ARE ERASED IN FOLLOWING POSITIONS
        4th POSITION OF THE CODEWORD
        5th POSITION OF THE CODEWORD
        8th POSITION OF THE CODEWORD

THE CORRESPONDING PARITY CHECK MATRIX [H] IS
 1   1   0   0   1   0   0   0   0
 0   0   1   1   0   1   0   0   0
 1   0   1   0   0   0   1   0   0
 0   1   0   1   0   0   0   1   0
 1   1   1   1   0   0   0   0   1

THE RECEIVED BITS ARE CORRECTED USING THE PARITY CHECK MATRIX
THE CORRECTED RECEIVED BITS
 1   0   1   1   1   0   0   1   1
```

Figure 2: Output of the LDPC encoder and decoder

The generator matrix is given as the input. The generator matrix is already created by the user and stored in a text file. on. The name of the text file is *gmat.txt* and the matrix stored in the generator matrix is given below. The generator matrix is of the form G = [I_k P] where I_k denotes the identity matrix and P denotes the k × (n - k)

$$G = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{vmatrix}$$

The information bits are stored in the text file and it is also called through a function written in the program code. The name of the text file is *imat.txt* in which the information bits are stored. The contents of the text file are retrieved.

$$I = [\ 1\ \ 0\ \ 1\ \ 1\ ]$$

Using the generator matrix and the information bits, the codeword is generated that is used to transmit over the communication channel.

$$\text{Codeword, } c = I \times G = [\,1 \;\; 0 \;\; 1 \;\; 1\,] \times \left| \begin{matrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{matrix} \right|$$

$$\text{Codeword} = [\,1 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 0 \;\; 0 \;\; 1 \;\; 1\,]$$

Hence this is the encoded codeword generated from the information bits and the generator matrix. This codeword is passed to the receiver through the communication channel.

The decoding phase involves the restoration of the original message that is transmitted. The transmission is done via the binary erasure channel. Binary erasure channel has only two output probabilities. One probability is that the information received is correct and the other probability is that the information bit is erased. There is no chance of getting a bit as incorrect as this is not a characteristic of the binary erasure channel. In this example, such a transmission in the erasure communication channel has caused errors. This can be identified from the received codeword.

From the figure 4.1, it is noted that the received codeword is not the same as that of the encoded codeword before it enter the erasure channel.

Received codeword = [1 0 1 x x 0 0 x 1]
Actual encoded codeword = [1 0 1 1 1 0 0 1 1]

From the comparison of the encoded codeword and the received codeword, it can be inferred that there is error in the 4th, 5th and 8th position of the codeword. The three codeword in the positions 4th, 5th and 8th are erased due to the nature of the transmitting medium.

The erased bits have to be determined and done through the parity check matrix. The parity check matrix can be determined from the generator matrix. For the generator matrix that is used in the encoder phase, the corresponding parity check matrix is given below. Usually the parity check matrix is in the form of $H = [\ P^T \ \ I_r\ ]$. P^T is the transpose of the parity matrix. The parity matrix is found from the generation matrix and the I_r is the identity matrix. Thus the parity check matrix can be easily constructed from the generator matrix and the vice-versa.

$$H = \left| \begin{matrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{matrix} \right|$$

The decoding algorithm used in this project is based upon the simple algebra. The received codeword is determined as correct without any erasure if and only if it satisfies the following condition, c × $H^T = 0$. Hence if the product of the transpose of parity check matrix with the received codeword has no value, then the transmission is said to reliable. If not, there is some error in transmission which is nothing but the erasures.The transpose of the parity check matrix is given below

$$\begin{vmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

Thus the transpose of the parity check matrix is determined.

It is necessary to find out the erasures i.e. calculate and find the bit values in 4th, 5th and 8th positions. The erased values can be found out with the help of the parity check matrix. The parity check matrix is compared with the received codeword which finally gives the erased bits. The method to find is given below.Compare the first row of the parity check matrix with the received codeword.

$$\begin{array}{lccccccccccc} \text{Received codeword} & \longrightarrow & \boxed{1} & \boxed{0} & 1 & x & \boxed{x} & 0 & 0 & x & 1 \\ \text{H matrix} & \longrightarrow & \boxed{1} & \boxed{1} & 0 & 0 & \boxed{1} & 0 & 0 & 0 & 0 \end{array}$$

The bits in the received codeword that corresponds to the positions of the 1's in the H matrix are noted down. The bits are 1, 0 and x. The total of all the values must be 0 which notifies the condition. Hence, for the whole sum to be 0, the value of x should be 1. Finally the value of x is found as 1. The value of 1 must be written in the 5th positions of the codeword. Hence the received codeword is given below.

$$\begin{array}{lccccccccccc} \text{Received codeword} & \longrightarrow & 1 & 0 & 1 & x & \textcircled{1} & 0 & 0 & x & 1 \end{array}$$

Similarly the 4th and 8th positions of the codeword are determined using the next successive rows of the parity check matrix. Finally the 4th and the 8th position are found to be 1 and 1 respectively.

$$\begin{array}{lccccccccccc} \text{Received codeword} & \longrightarrow & 1 & 0 & 1 & \textcircled{1} & \textcircled{1} & 0 & 0 & \textcircled{1} & 1 \end{array}$$

Now all the erased positions are determined using the parity check matrix. In order to determine the calculated erased bits are right, the decoding condition has to be satisfied. c × $H^T = 0$

$$[\,1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\,] \times \left|\begin{matrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{matrix}\right| = 0$$

Hence the product of the corrected received codeword and the transpose of the parity check matrix is 0 and the decoding condition satisfies. Hence the corrected codeword bits are same as that of the encoded codeword. Thus the decoding process is executed.

5 Conclusion and Future Works

During data transmission there are various factors that affect the transmission of the data which in turn affects the performance of the network. This project involves the role of error correction codes in the context of digital communication system. The encoder and decoder are the important blocks of any communication system. The data is encoded before transmission through the channel and it is decoded when it passes out from the channel. Error correction code is implemented in the encoders and decoders in order to maintain the reliability of the transmission. The most efficient one is the LDPC code which is investigated in the project. During encoding, the information bit is encoded with the generator matrix of the LDPC code and finally the encoded codeword is generated. The encoded codeword is transmitted through the binary erasure channel which contains the information bits. Due to the nature of the channel, some bits are erased during the transmission. But the decoder uses the parity check matrix which is closely associated with the generator matrix and compares it with the received codeword. Finally, the correct codeword is determined by the decoder.This project can be implemented in the network layer or transport layer or the application layer of the OSI model. By implementing so, the error correction codes especially LDPC codes reduce the need of retransmitting the lost packets and will be able to reconstruct the certain number of lost packets at the receiver end. From this point of view, the error correction codes (LDPC codes) play a key role in a digital communication system as well as in the data transmission.

Low density-parity-check codes have been studied a lot in the last years and huge progresses have been made in the understanding and ability to design iterative coding systems. The performance in the LDPC codes is better than the turbo codes. The LDPC codes make the possibility to implement the parallelizable decoders. There is a drastic increase in the data transmission technology over the past few years. Many new techniques are provided to shape the data traffic in order to maximise the efficiency of the bandwidth reservation scheme whilst guaranteeing a defined quality of service in terms of data loss and delay. These new techniques come with the challenges of processing more and more bits which requires the powerful code design implementation. More efficient classes of codes that suit the developing data transmission field must be developed and their performance has to be examined. This project involves the LDPC codes which are found to be the most efficient form of error correction codes. The encoding and the decoding algorithm used here are the conventional way of implementation in the communication system. Because of the improvements if communication field, the encoder has to be designed with more linear complexity. Also, the decoding method should use the iterative algorithms and the performance has to be evaluated. The most important consideration in the next generation communication system is to develop the LDPC decoder that enables a close integration between the codes and the hardware architecture designs. The FPGA result shows promise for future ASIC implementation for the use in next generation communication systems. Another consideration is that it is necessary to design new LDPC codes which will not only provide near-capacity performance and also will have efficient structure for low power implementations. If the internet is used for simulation purposes, then it implemented in network/transport level and application level interfaces.

6 References

Ahlswede, R., Cai, N., Li, S.Y.R., and Yeung, R.W. (2000) "*Network information flow*," IEEE Transactions on Information Theory, Vol. IT-46, pp. 1204–1216

Berrou, C., Glavieux, A and Thitimajshima, (1993) P. "*Near Shannon Limit! 3ror-Correcthg Coding and Decoding: Turbo Codes*," in Proc. 1993 IEEE International Conference on Communications, Geneva, Switzerland, pp. 1064-1070

Divsalar, D., Jin, H. And McEliece, R. (1998) Proc. 36th Annual Allerton Conference on Communication, Control and Computing, "*Coding Theorems for Turbo-like codes*", pp.201-210

Gallager, R.G. (1962) "*Low-Density Parity-Check Codes*", IRE Transactions on Information Theory, vol. IT-8, pp. 21-28

Gallager, R.G. (1963) "*Low-Density Parity-Check Codes*", Cambridge, MA: M.I.T. Press

Jin, H., Khandekar, A. and McEliece, R. (2000) "*Irregular repeat-accumulate codes*" Proc. 2nd. International Symposium on Turbo Codes and Related Topics, France, pp. 1-8s

"LDPC codes – a brief tutorial" [Online] Available at:www.engr.uvic.ca/~masoudg/upload/ldpc-a%20brief%20tutorial.pdf (Accessed on 27/12/2009)

Luby, M., Mitzenmacher, M. Shokrollahi, M. and Spielman, D. (2001) "*Improved low-density parity check codes using irregular graphs*", IEEE Transactions on Information Theory, pp. 585-598

MacKay, D.J. (1999) "*Good Error-Correcting Codes Based on Very Sparse Matrices*," IEEE Trans. Znfo. Theory, vol. 45, no. 2, pp. 399-43

MacKay, D. and Neal, R. (2005) "*Good codes based on very sparse matrices*", in Cryptography and Coding, 5th IMA Conference, C.Boyd, Ed., Lecture Notes in Computer Science, Germany, pp. 100-111

Neal, R.M. (1999) "*Sparse matrix methods and probabilistic algorithm*", IMA Program On Codes, Systems, and Graphic Models, 1999

Qi, H. and Goertz, N. (2007) "*Low-Complexity Encoding of LDPC Codes: A New Algorithm and its Performance*", Joint Research Institute for Signal & Image Processing, School of Engineering and Electronics, The University of Edinburgh, UK

Richardson, T.J and Urbanke, R.L. (2001) "*Efficient encoding of low-density parity-check codes*," IEEE Transactions on Information Theory, vol. 47, no. 2, pp. 638456

Richardson, T., Shokrollahi, A. and Urbanke, R. (2001), *"Design of capacity-approaching irregular low-density parity-check codes"*, IEEE Transactions on Information Theory, vol. 47, pp. 619-637

Shannon, C. (1948) "*A Mathematical Theory of Communication*," Bell Syst. Tech. Journal, vol. 27, pp. 623-656

Su, J., Liu, Z., Liu, K., Shen, B. and Min, H. (2005) "An efficient low complexity LDPC encoder based on LU factorization with pivoting", 6th International conference on ASICON, Shanghai, vol. 1, pp. 107-110

Yeung, R.W., Zhang, Z. (1999) "*Distributed source coding for satellite communications*," IEEE Transactions on Information Theory, Vol. IT-45, pp. 1111–1120

Implementing Resource Revocation Utility for Network Operations Centre Management Console

O.S.Kayode and B.V.Ghita

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

In an organization, there exist the possibility of users utilizing prohibited applications or resources. Preventing such activity deemed inappropriate therefore paramount in ensuring effective network administration. This research employed a simulated experimental network topology to develop a utility for terminating the connection of host engaged in activity deemed inimical to network performance. The utility automates network traffic capture; analyses captured traffic to identify prohibited connections (e.g. Peer-to-Peer traffic) and injects TCP reset packets to terminate connections. The research established that instantaneous termination of undesirable connections is effective; even though it could not always achievable due to packet delays, network congestion, false positives and non-identification of some application traffic.

Keywords

Network Operation Center (NOC), Packet Injection, TCP Reset, Automation Scripts, Connection Termination.

1 Introduction

In any enterprise network, it a fallacy to assume that all internal users are well-behaved and aboveboard with regard to their usage of network resources and application. Hence, there exist the possibility that an internal users can either deliberately or inadvertently utilize prohibited application or resources not permitted due to the adverse effect they have on the network. In the same vein, such user may also exceed their allotted network access rights and/or privileges while using authorized network resources.

Adequate network monitoring via a Network Operation Centre (NOC) management console brings such network breaches to the attention of the administrator, who must immediately take necessary action. More often than not, administrators utilize separate network tools to intervene and restore normalcy to the network.

Similarly, the clandestine usage of Peer-to-Peer (P2P) application that is hoarding precious network bandwidth within an enterprise might require a more urgent intervention by the administrator, especially if overtures or attempts to contact the perpetrator fails or is ignored.

These and other such instances highlight the need to incorporate functionalities within NOC management consoles so as to empower administrators with capability to revoke, streamline, limit and enforce network resources utilization in accordance with an organization’s network and security policy.

This research aims to develop and incorporate network intervention functionality into a NOC management console, which enables network administrator to perform resource revocation. The utility terminates P2P communication and revoke resources hoarded by greedy applications/host.

The uniqueness and highlight of the developed utility is that it combines several tasks, which were hitherto undertaken with separate tools. It automates the entire process of capturing network traffic; analyses captured traffic to identify prohibited connections (e.g. Peer-to-Peer traffic) and injects TCP reset packets to terminate connections, all with minimal input from the network administrator. Commercial implication of such characteristics makes it a cost-effective utility.

2 Previous Work

There have been various efforts aimed at expanding the functionalities provided by NOC management consoles in a bid to make them more efficient.

In communication systems, Harry et al. (2001) produced a NOC system capable of testing two-way paging device to determine conformity to specified protocol. In one embodiment, the system comprises a transmitter, a receiver and a protocol engine. The protocol engine sends information to and receives information from a two-way communication device for compliance with multiple communication protocol

An inherent function of NOC is to provide security monitoring of network infrastructures. Behaviour profiling is being adopted for network security monitoring to automatically discover suspicious or malicious tendencies from network traffic. Such profiling also provides plausible interpretation of these behaviours to aid network operators in understanding anomalous events within network traffic (Kuai Xu et al. 2008).

Bali (2005) employed Netmates – an open source packet sniffing software, to fuse a network monitor and an Intrusion Detection System into a single GUI. Integration with Snort backend enabled the native packet sniffing functionality of Netmates to be extended by using smart add-ons and plug-ins to enable it serves as a form Network management systems.

The flexibility provided by web interface was harnessed by Mohyuddin (2006) in producing a NOC management console that provides administrators with a single unified interface for displaying network entities. Such approach enabled remote monitoring through standard web site using HTTP protocol. Though independent, the NOC system has functional dependency on some existing Linux features and some freely available network monitoring tools such as Nmap, Tcpdump and Ethereal.

The combination of two tools - PolyMon Network Monitor and NetMaCon, was used by Agbai (2007) to monitor and generate alerts. The PolyMon monitors network devices and generate alerts when the devices fail. The alerts are stored in a database, which NetMaCon accesses to display the visual and geographical location of network problems. Response to alert was limited to showing the physical location of the faulty device on the network.

Researches on P2P have been varied. While some ISPs, for example Packeteer (2009), are known to rate-limit the bandwidth consumed by P2P traffic by deploying traffic shapers in their network, others go further and ban them completely by injecting forged RST packets. (Schoen, 2007).

Other P2P studies have focused on topological characteristics of P2P networks based on flow level analysis (Sen and Wang, 2002), or investigating properties such as bottleneck bandwidths (Saroiu et al., 2002), the possibility of caching (Leibowitz et al., 2002), or the availability and retrieval of content (Bhagwan et al., 2003; Gkantsidis et al., 2003).

Sen et al. (2004) developed a signature-based payload methodology to identify P2P traffic. The authors focus on TCP signatures that characterize file downloads in five P2P protocols based on the examination of user payload.

3 Research Methodology

This section presents an overview of the methodology employed in conducting the research. In summary, this research methodology consisted of the following major tasks:

1. Setting up the network topology for the conduct of experiments.
2. Identifying undesirable activity on the network, through
   - Capture and analysis of traces.
   - Real-time monitoring of network activity.
3. Identifying host engaged in undesirable activity.
4. Manual termination of offending hosts' network connectivity.
5. Automation of tasks 2-4 above using shell script, and subsequent deployment of the script within a Network Operation Center (NOC) management console.

Details of each tasks summarized above is discussed in following sections.

3.1 Experimental Network Topology

The listing of configuration of each host is shown in Table 1. The computer network ***logical*** topology used for the research is depicted in Figure 1.

	NOC PC	CLIENT PC	SERVER
Operating System	Ubuntu Linux Version:10.4	Windows XP Ubuntu Linux	Windows 2003 Server Microsoft IIS
Other Software	EtherApe		Apache Tomcat
	Wireshark	Wireshark	Wireshark
	Tcpdump/Tshark	Tcpdump/Tshark	Tcpdump/Tshark
	PackeTH	BitTorrent Client	
	Snort	Telnet Client	
	Oracle VirtualBox	Oracle Virtual Box	
	Zenity	OmniPeek	
	OmniPeek		

Table 1: Table of Host Configurations

NOC-PC is a Unix-based machine serving as the NOC management console. It is strategically located at an interconnection point/junction, such that all traffic traversing the network can be easily monitored. Typical network monitoring software running on the NOC-PC included:

- Intrusion detection system software such as Snort – both of which are open-source;
- Protocal Analzers such as Tcpdump/tshark or Wireshark, which is configured to run in promiscuous mode in order to capture all network traffic;
- Real-time network monitoring utility such as EtherApe - running to provide a visual graphical display of network traffic pattern.
- PackeTH – Packet injection software via Graphical User Interface (GUI)

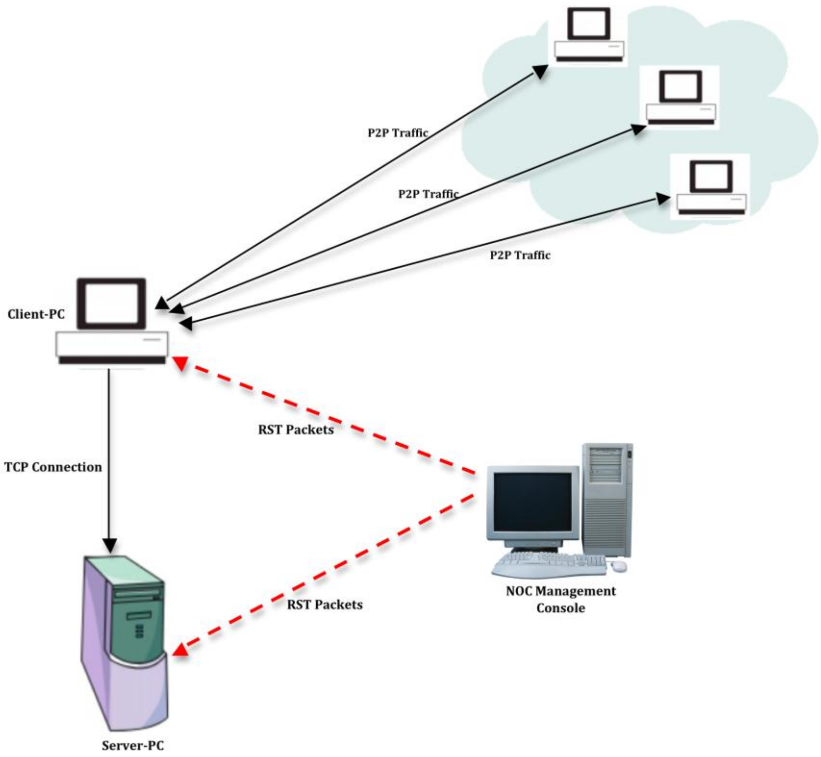


Figure 1: Network topology diagram

After observing network traffic pattern, a baseline of what is considered ‘normal’ was established. Therefore, any deviation from the established baseline is considered an anomalous situation that warrants further investigation.

Client_PC1 is a Unix PC that is used to carry out undesirable network activity. It is located within the same subnet as the NOC_PC and used to initiate:

- Peer-to-Peer (P2P) connection that has adverse effect on network bandwidth utilization.

- Unauthorized connection to the Server-PC via telnet session.

Server_PC is a Windows server machine is assumed to contain classified information. Two server software (Microsoft IIS on WINDOW 2003 Server and Apache Tomcat) were installed on the machine in order to compare any differences in response to CLIENT-PC connection termination.

3.2 Measurement

The traces generated on NOC_PC was filtered to include the source IP address, destination IP address, protocol, source port and destination ports.

Tcpdump/thark was employed for network measurements. It allows collection of TCP/IP packet headers, and (optionally) packet payloads as well.

In order to create a diverse context within which the experiment was carried out and to replicate the type of traffic found in a typical network, some random traffic were generated from these machine to mimic those obtainable in an enterprise environment. Wildpacket's OmniPeek traffic generator was used for this purpose.

Client_PC1 was used to initiate HTTP connection from a browser to a P2P network for downloading and uploading large file contents. In an attempt to study the TCP connection behaviour, a telnet connection was made to port 80 of servers software running on SERVER-PC and an HTTP request issued. While the connection was kept opened, it was possible to observe from tcpdump/thsark how or if the server closes the connection.

3.3 Injecting RST Packets to Abort Internal and External Connection

While there is an established connection from the Client_PC to the Server_PC, reset (RST) packets were *manually* generated on NOC-PC using PackeTH software. These RST packets were targeted towards:

- Client_PC using spoofed source IP address belonging to SERVER-PC.
- SERVER-PC using spoofed source IP address belonging to Client_PC.
- Both Client_PC and SERVER-PC.

While there is an active P2P connection from the Client_PC to an external P2P network and a download and/or upload process is taking place, reset (RST) packets were ***manually*** generated on NOC-PC using PackeTH software. These RST packets were targeted towards:

- Client_PC using spoofed source IP address.

3.4 Automation of Connection Termination Process

The manual termination process entails using separate software tools and some time interval inevitably elapses before each this software is launched, properly configured and executed. Moreover, the output generated by traffic capture software (e.g. tcpdump) needs to be analyzed to obtain pertinent information before it can be fed as input into another software tool (e.g. PackeTH).

In order to automate the connection termination process so that it can be integrated within the NOC management console, a shell script was developed. Figure 2 shows the flow chart of the logic of the script.

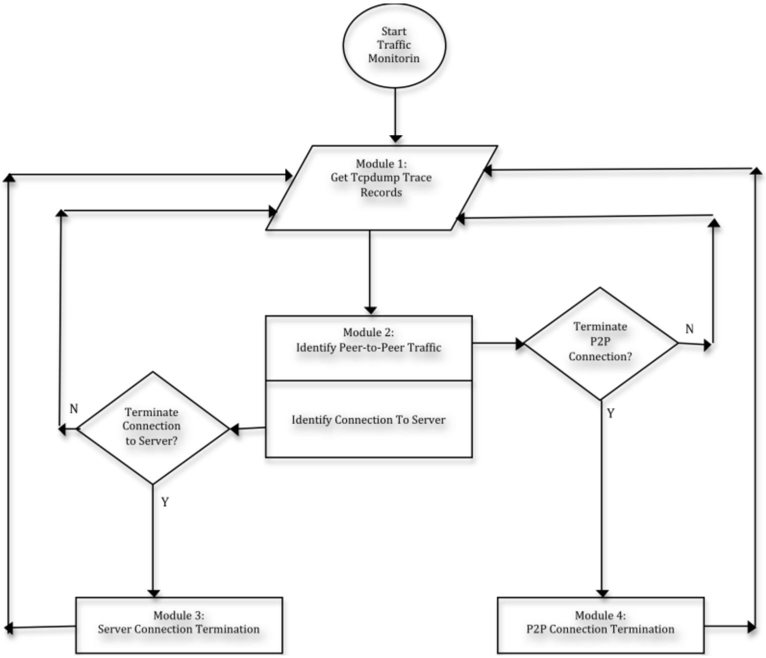


Figure 2: Flowchart for Automation Script

Module One involves the real-time monitoring and capture of network traffic using tshark/tcpdump. Due to memory space constraint Tshark/tcpdump was configured to capture only source and destination IP addresses, source and destination ports. The protocols captured are TCP, UDP, HTTP/HTTPS and DNS.

Module Two processes the captured traffic to identify presence of P2P traffic by comparing the various ports utilized by network protocols against a list of well-known ports normally utilized by P2P traffic. Further analysis of the network traces revealed camouflaged P2P traffic patterns that did not use any of the well-known ports in a bid to avoid detection.

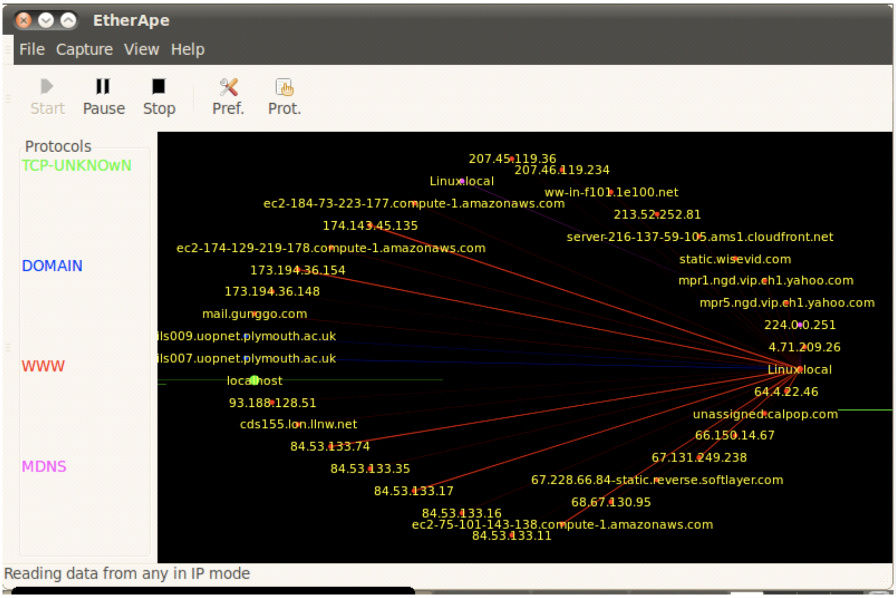
Module Two also identifies any active connection with the SERVER-PC. This is achieved by highlighting connection to Server-PC by searching for the server's IP address as a destination of a traffic flow. The source IP address of such flow is sent then to Module-Four.

The IP address of the host engaged in P2P activity is forwarded to Module-Four for further action. Such connection is then maintained or marked for termination in Module-Four, depending on the network administrator's decision regarding the validity of such session.

Similarly, for any unauthorized connection to SERVER-PC, MODULE-Three performs the actual termination of the connection. The module utilizes an open-source packet injection utility, Packit, to launch the termination process via the command-line.

4 Results and Analysis

The EtherApe software providing real-time monitoring of the test network provided early indication of abnormal traffic flow. As shown in Figure 3, whenever P2P traffic was initiated on the CLIENT-PC, EtherApe displayed corresponding bursts/surge in traffic pattern, thus indicating instances of excessive bandwidth usage.



Reading data from any in IP mode

Figure 3: EtherApe Screen showing Peer-to-Peer Traffic.

The open-source packet injectors used for connection termination in this research suffers from lag conditions**.** This refers to the time interval from when RSTs packets are crafted and injected till the time endpoints receive the RST packet. Two separate lag conditions were observed during the course of the experiments for the research.

One lag condition occurred between the time when the administrator decides that a data packet/flow exhibit criteria warranting connection termination, and the time when *Packit* actually sends out the RST packet.

During this interval, further P2P packets downloads and/or upload had taken place. Consequently, it was observed that the RST packet is "out of sequence" because the sequence number is less than that of the preceding data packet. This condition often caused the target to ignore the RST packets.

Since P2P packets were sent back-to-back, the lag condition is more prevalent when the RST packet injection is in use. In the absence of injection, however, such condition is not expected during normal TCP operation.

The other lag condition was observed when, as at the time the RST packets were injected, further packets were already en-route, or were sent shortly afterwards, since the injector could not stop the traffic originator quickly enough. In these cases, the receiver still receives further data packets from the sender ***after*** it has already received the RST.

This second lag condition was identified by observing data packets with larger sequence number than those found on a previously received RST packet. Under normal circumstance, such condition is rare during normal end-host communication.

While every effort was made to ensure accuracy in identifying connections meant for termination, especially since the experiments were conducted in a controlled environment, it must be stressed that such condition may not be guaranteed in a 'live' production network as obtained within an enterprise.

Consequently, deploying the utility within an enterprise environment is bound to result in some false positive alerts. The possibility exist for network connection of incorrect hosts to be identified as being engaged in undesirable activity, and thus be terminated. Similarly, it is also possible for benign traffic to be wrongly identified as P2P traffic and therefore be inadvertently terminated.

Such cases of false positives are not peculiar to this research. For example, commercially developed firewalls and intrusion detection systems (IDS) have also been found to raise false alerts. The underlining factor responsible for such false alerts is the accuracy of the algorithm or signature employed in indentifying hostile/undesirable activity.

The type of network topology within which the experiment was conducted significantly influenced the result of this research. As depicted in Figure 3.1, all the machines in the topology are in a single collision and broadcast domain, hence, possibility exist for Address Resolution Protocol (ARP) broadcast storm to occur. Consequently, injected reset (RST) packets may be delayed en route to their target due to congestions caused by ARP broadcast storms.

The effect of NAT on the connection termination utility can not be overlooked. In an enterprise environment with multiple branch offices/sites, terminating the connection of remote user engaged in clandestine or inappropriate network activity has to contend with NAT issues. Other likely issues also include traffic tunneling and encryption. Inasmuch as these issues were not factored into the experiments conducted, then, there is possibility that using the utility in such scenario may not be effective or functional.

By targeting injected RST packets at offending host, the result of the conducted experiments showed that it was possible to terminate and/or disrupt established TCP/UDP connections. When compared with isolated tests conducted by issuing the '*KILL'* command on a Unix/Linux system, significant differences were observed.

The '*KILL'* command is executed with the process ID number of target application supplied as argument. The command sends a special, high-priority SIGTERM signal, which instantaneously terminates all main and child processes associated with the target application. All windows associated with the target application are instantaneously shutdown.

On the contrary, RST packets terminate only a session of the application using the targeted TCP flow. For example, the specific Internet browser window used for P2P activity or the window of the telnet client connected to SERVER-PC were the only sessions affected by RST packets. Atimes, these windows sessions simply hang-up and/or stops responding as a resultant effect of injected RST packets. Further checks were necessary to verify that the session/connection was indeed terminated. However, other instances or sessions of the browser or Telnet client remained unaffected.

5 Conclusions and Recommendations

The research established that instantaneous termination of undesirable connections is effective; even though it could not always achievable due to lag conditions, packet delays, network congestion, false positives and non-identification of some application traffic.

It is recognized that the capability being developed can be considered a double-edged sword. The utility can be used to disrupt legitimate user activities on the network if used by unauthorized mischievous persons. Consequently, access right to utilize the program is highly restricted to **ONLY** the network administrator with root privilege.

It is worth investigating the effect a switched network topology will have on the outcome of the experiments. Introducing a Layer-2 network switch into the experimental topology will ensure each host resides in its own collision domain, thereby isolating each hosts from collision within its switch port. In an enterprise setting, such topology will reduce network congestion, and *could possibly* ensure RST packets reach their intended destination faster. Virtual LANs (VLAN) can also be configured on the switch to enhance security and further prevent

The resource revocation utility was not only developed on a Unix/Linux system, but also aimed at NOC management console based on Unix/Linux Operating Systems. The wealth of powerful intrinsic commands offered by Unix/Linux systems informed this decision. Attempts to modify and/or develop similar functionality for a NOC management console hosted on other Operating System platforms can be undertaken as future research.

6 References

Agbai, O. C. (2007) ‘Implementing A Visual Network Management Console’, MSc Thesis, Plymouth University.

Bali, R. (2005) ‘Implementing Network Operation Center Management Console: NetMaCon’, MSc Thesis, Plymouth University.

Bhagwan, R., Savage, S. and Voelker, G. (2003) 'Understanding Availability', International Workshop on Peer-To-Peer Systems, IPTPS, Available at http://iptps03.cs.berkeley.edu/final-papers/availability.pdf [Accessed 5th August 2010]

Gkantsidis, C., Mihail, M. and Saberi, A. (2004) 'Random Walks in Peer-to-Peer Networks', Information Communication Conference, INFOCOMM, Available at http://www.ieee-infocom.org/2004/Papers/03_4.PDF [Accessed 15th July 2010]

Harry V. B., Donna B. (2001) 'Network Operations Center Hardware and Software Design', Patent No.: US 6,259,911 B1

Kuai X., Zhi-Li Z., and Supratik B. (2008), 'Internet Traffic Behavior Profiling for Network Security Monitoring' IEEE/ACM Transactions on Networking, (16)6: 1241-1252

Leibowitz, N., Bergman, A., Ben-Shaul, R. and Shavit A. (2002) 'Are File Swapping Networks Cacheable: Characterizing P2P Traffic', 7th International Workshop on Web Caching and Content Distribution, IWCW, 2002. Available at http://2002.iwcw.org/ [Accessed 15th July 2010]

Mohyuddin, A.(2006) 'Implementing a Network Operation Center Management Console', MSc Thesis, Plymouth University.

Packeteer (2009) http://www.packeteer.com [Accessed 15th July 2010]

Sen, S. and Wang, J. (2002) 'Analyzing Peer-to-Peer Traffic Across Large Networks', Proceedings of ACM SIGCOMM Internet Measurement Workshop, IMW, 2002. Available at http://conferences.sigcomm.org/imc/2002/imw2002-papers/167.ps.gz [Accessed 11th June 2010]

Sen, S., Spatscheck, O. and Wang, D. (2004) 'Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures' World Wide Web (WWW) Conference, Available at http://www.iw3c2.org/WWW2004/docs/1p512.pdf [Accessed 27th August 2010]

Schoen, S. (2007) 'Comcast and BitTorrent', Available at http://www.fcc.gov/eb/Orders/2007/DA-07-4005A1.html [Accessed 15th July 2010

Assessing the Technical Quality of Reporting in the Mass Media

D.M.Paul and A.D.Phippen

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Studies have proven that mass media is the major source of information and has a massive influence over the general public. So there is no doubt that mass media can act as a knowledge source for making the public aware of the widely increased internet threats and about their protection. But the concerns that media are sensationalist and technically inaccurate with the reporting, leading to an ill informed public without the knowledge to protect themselves from online threats led to the research titled "Assessing the Technical Quality of Reporting in Mass Media". The research studies on the role of media in influencing the general public based on the classic adoption and knowledge transfer theories. Then analysis on the selected reports from newspaper as well as TV reports is done to draw conclusions regarding media's appropriateness as a knowledge source.

Keywords

Public perception, mass media, online threat and protection.

1 Introduction

In the technologically driven society the dependency of media has increased into very sensitive issues like the security of a computer or an internet threat. Along with the attacks against organisations or a network we are also facing internet threats that specifically target the end user community. The motives for this may be money, or just typically a mischief and in both cases the end users are the favourite attractions because of their lack of technical knowledge makes them vulnerable to variety of tricks. The information from the internet world is changing every now and so it has to be updated with the new information in just seconds. (Furnell, S. 2005)

So arguments arise based on the technical integrity of mass media on reporting about internet threats. There are concerns that the media are sensationalist and technically inaccurate with their reporting, leading to an ill informed public without appropriate knowledge to protect them from online threat. The research goes into the reality of this problem.

2 Literature Review of Mass Media Effects

The literature review focuses on understanding the media effects in the society and to be specific going to the insight of mass communication and mass media. It also goes through the media transfer theories that explains the factors responsible for the communication of information. The analysis of these theories is also done in reference to various versatile researchers.

In this literature review section a small research on topics like the power of mass media, mass communication and mass audience, mass media and mass audience was also done. Then the theories of media effects were taken into study. The research explains mainly about the various theories as briefly mentioned below.

Powerful effects model: The theories at this time (1928-1932) were characterized as the hypodermic needle theory or the magnet bullet theories by the researchers. They were called so because of the belief that media is like a powerful bullet that penetrates everyone and that too uniformly from which no one could escape from the trap. These theories generally comprise what is called as powerful effects model. (Galician, M. L., 2004)

Minimal effects model: In the 1940's more sophisticated methods of mass media were introduced and this diminished the popularity of the powerful effects model among the researchers in the research community. One important finding of the new research was that the individual differences can make a great difference in the influence of mass media.

Another major finding of the researchers was that the media receivers are less likely to be affected by the information they receive than to have their already existing views reinforced by the media which they select. In other words we accept the views of media that we already have and agree with and disregard the ones which bring conflict with our already held view points. Studies like these became so popular so that there began a generalized research view that mass media have only limited influence or named as limited or minimal effects model.

Agenda setting theory: According to agenda setting theory the mass media is a tool that influences the public opinion by framing an agenda in public discussion. The theory describes how the mass media influence the public opinion but it is not necessarily by supporting one view over the other but it is by highlighting some issues in the public sphere. (Agenda setting theory, 2010)

Third person effect: The third person effect states that a person who is exposed to mass media has a belief that others are having greater influence than themselves.

Users and gratification model: Uses and gratifications model was a more complex audience scheme. The model gets its interest from the media and notes how the audience use and derive fulfilment from the media messages.

Diffusion of innovation: The diffusion of innovation theory investigates about the social processes that takes the first step and then distributes the innovations within a social system. Throughout the diffusion process it is clearly proven that there is no equal amount of influence over different individuals.

Theory of reasoned action: According to this theory an individual's attitude towards some behaviour has got 1) a belief that a certain kind of behaviour will produce certain outcome and 2) a quick assessment on the outcome of the behaviour. If the individual finds some benefits for him from the outcome then he or she may participate in that particular behaviour. It's also added that one's attitude towards behaviour may be his understanding of that particular subject (subjective norm). (Miller, K., 2005)

Sum of effects:

It is clear that the opinion of a general public basically depend upon the opinion of the mass media he relies on. So it is the responsibility of the mass media to provide the public with information that are accurate, precise and up to date.

3 Analytical Method

3.1 Data Collection

The relevant data for the research is collected from the internet. Sites of various newspapers and television channels is searched using the keywords the 'internet security threat' and various reports on internet threats were selected for analysis. It was make sure that the threats selected were the most recent threats from both the newspapers as well as the television news channels. 3 UK news papers, 2 American newspapers and 1 Indian newspaper were selected for analysis. For the television news analysis 3 news channels were selected randomly.

3.2 Data Analysis

Find out the three types of errors listed before:

In the reports itself there are quoted marks for the sources like some security firms, antivirus providers etc. Their actual reports were selected and find out whether they closely associate with those reports selected. Also the reports selected are compared with its sources. Thus various errors mentioned previously are identified and thus evaluate the reports.

Completeness of the reports:

By comparing the news reports and its sources we can find out whether the reports given in the newspaper or the television report is lacking some completeness.

Readability of the reports

The readability of the newspapers is done using the software from the internet. Various readability indices like Automated readability index(ARI), Flesch Kincaid grade level, Flesch reading ease level etc and their formulas were discussed and by using this software we can find out the values of the various indices.

The snapshot of the readability indices calculation software is shown for the report “Hackers stalk Face book to harvest cash secrets” (this is the report from the guardian news paper). The report is selected and then pasted in the space provided by the software and then press the ‘process text’ button to get the results.

Accuracy check list

The following questions are answered and thus find out the accuracy of news paper reports.

- *Does the report clearly defines the topic or does it deviates from what it is actually meant be?*
- *Is the headline accurate and balanced?*
- *Are there any assumptions in the report?*
- *Are the assumptions accurate?*
- *Does the report have proper referencing?*
- *Does the report have the proper justification for the facts raised?*
- *Is the report in the correct format i.e. proper punctuations, symbols etc?*
- *Does the report provide ample choice of quality literature?*
- *Is the report brief (concise)?*
- *Does the report provide you with all the information that is necessary?*

For TV news reports

The research we will go through each factor for the report and find out whether the report is accurate.

Timeliness: Means the news must be new. Something that has happened yesterday is much interesting than something that happened last year.

Proximity: We are mainly concerned of the factors that are related to us. Thus size of the community is also a factor.

Consequence: When more people are affected; the news has greater value.

Complete: Is the report complete. Does the report give all the information that we require.

Technical accuracy: Whether the report has followed the accuracy in all the levels especially the technical side.

Referencing: Is the news supported with proper referencing that too from a reliable source?

4 Result

From the obtained result the graph plotted below shows the percentage of incomplete reports and the average accuracy score. From this it is confirmed that the reports are not complete in giving the reader with the correct technical knowledge they are expecting. Let us answer the questions based on the results obtained.

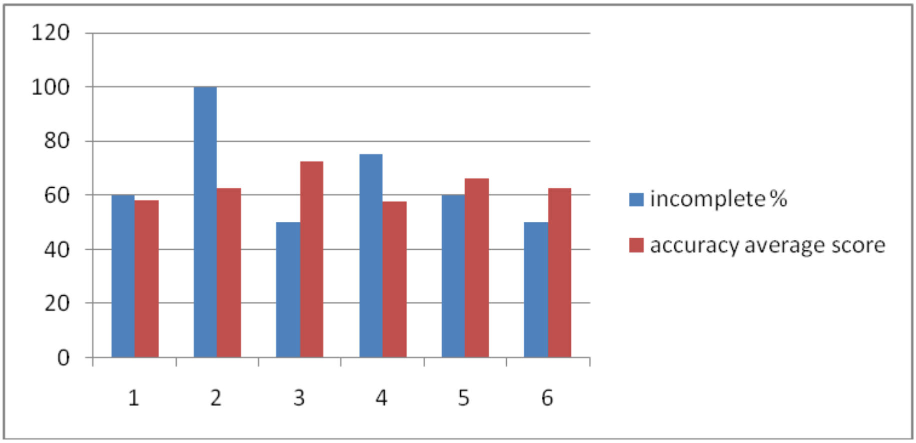


Figure 1: Graph of incomplete % and average accuracy score

From the result obtained we can see a reign of subjective errors which are the major errors in a report. These errors may not be intentional. But they can cause serious misunderstandings inside the country if it is a small newspaper or throughout the world if the whole world reads it. These errors can also affect the accuracy and reliability of the newspapers as well. Reliability of a news paper can be a mixture of accuracy, believability and fairness. And accuracy can be explained as a measure to judge the quality of a newspaper report along with a number of other factors. From the result obtained we can see that the subjective errors are a major issue. Objective error which may lead to some confusion in the statistics or data is relatively less in the result and we can also see a very few minor errors like spelling mistakes, repetition of words etc.

According to Charnley subjective errors occur very commonly and accounts for about 44% of the inaccuracies and the remaining is divided by the minor and the objective errors. The following may be some of the reasons of errors in news paper:

- The reporter failed to independently verify the information.
- The reporter missed some relevant information.
- The editor failed to check the errors or holes in the report.
- The editor failed to check for adequate sources.

The errors will definitely affect the knowledge and understanding of the people. When a reader reads or hear a report (hear a report on internet threats) he is not concerned of the literature or statistics of the report. He may look into the importance of the report from his side and then try to analyse it. His major interest is how he can protect from such a threat if he ever faces that. So he may definitely look for the protective information which is missing in most of the cases according to the research. So the report failed to give what he actually wanted even though he came to know about some facts about that threat. So he is still unaware of protecting himself from the threat after reading the report which means that the report has failed according to him.

The diagram below shows the graph of the readability indices. From this we can found out that the reports are mostly difficult for the readers to read. This may also affect the understanding of the readers. If the report is a standard one they may better understand the matter or else they may neglect reading the matter which is difficult for them to understand.

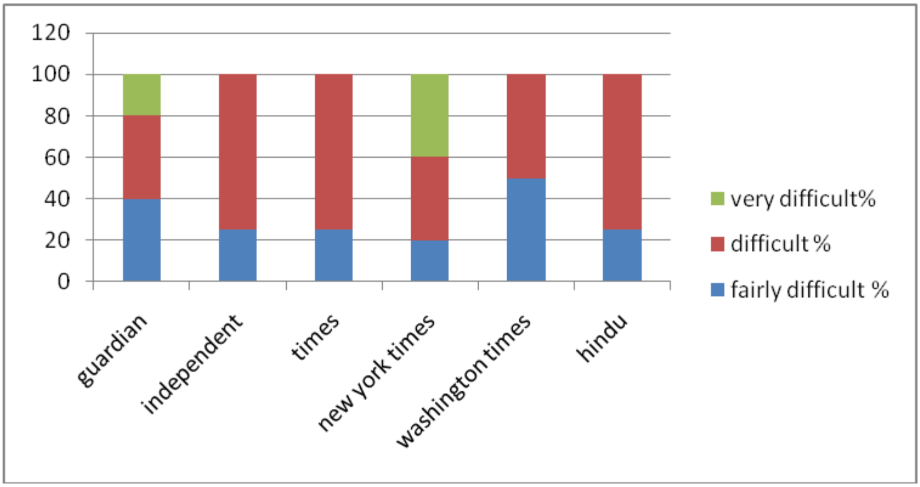


Figure 2: Graph of the readability indices

From the research done it is found out that the media is not too sensationalist. Sensationalism can be defined as being extremely controversial, loud or attention grabbing which is applied for getting some special attention for a matter. From the reports analysed the media even though tried to play with some statistics they did not cross their limitations. Even though some headings like ‘net crime feared more than burglary’ may create some consciousness among the readers but still it can be discarded as it is just headline. From the research it is found out that even though the media failed to give some valuable information to the public they tried not to be too sensationalist according to the research.

5 Conclusion

The researcher came to a conclusion that the media is not too sensationalist. Even though there was errors found in the analysis (mainly subjective errors) the report has got some ‘substance’ that informs the public. There are also many drawbacks in the reports which were used for the research analysis. It was found out that most of them failed to give necessary information to prevent ourselves from the internet threats they were reporting. Instead the report was going after the statistics which is of less use to the general public and also the expert sayings. So the researcher conclude that media is not giving sufficient information to the public to overcome the internet threats they are facing each day.

6 References

Agenda setting theory (2010), Available at: http://www.articleworld.org/index.php/Agenda_setting_theory [Date accessed: 17.7.09]

Furnell, S. (2005) ‘*Network Security* ‘, Science direct, 2005(7), 5-9, Available at: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJG-4GNJV4Y-7&_user=7173283&_coverDate=07%2F31%2F2005&_alid=1067930258&_rdoc=3&_fmt=high&_orig=search&_cdi=6094&_sort=r&_docanchor=&view=c&_ct=15576&_acct=C000013198&_version=1&_urlVersion=0&_userid=7173283&md5=d408cc1eb07c76dba5e658f17acb0976 [Date accessed: 2.7.09]

Galician, M. L., (2004), ‘*Sex, love& romance in the mass media: analysis& criticism of unrealistic*’, USA: Lawrence Erlbaum Associates, Available at: http://books.google.co.uk/books?id=vQWmt44NlW4C&pg=PA84&lpg=PA84&dq=POWERFUL+EFFECTS+MODEL&source=bl&ots=D2gh0mBXgJ&sig=I5MDgKb2PRZsPTZ2IuFvGiV2efE&hl=en&ei=52XtSrPaJIzLjAf_yaylDQ&sa=X&oi=book_result&ct=result&resnum=8&ved=0CCYQ6AEwBw#v=onepage&q=POWERFUL%20EFFECTS%20MODEL&f=false [Date accessed: 10.7.09]

Miller, K. (2005). *Communications theories: perspectives, processes, and contexts*. New York: McGraw-Hill

Statistical Analysis of Snort Alerts

O.B.Remi-Omosowon and B.V.Ghita

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Intrusion detection systems are used to monitor information systems, creating large number of alerts which are difficult to respond to. Many of these alerts do not present threats as they merely report the normal working condition of the system. These information systems are often used for specific tasks that are repetitive or consistent over the period of its use; hence a pattern is expected for these alerts. A single alert may have no significance by itself but can be part of a bigger threat and Analysing these alerts individually can be very tedious and time consuming. Such threats will alter the normal course of the system's statistics. This paper focuses on the processing of high volumes of alerts generated by snort analysing the trend of the hourly alert intensities triggered at the edge of the Plymouth University network. The analysis is conducted on real world data. The goal of this analysis is to identify the true positive alerts that signify actual intrusion attempts. This paper also presents a way to share the statistic property of alerts with researchers without sharing the actual traffic source or alerts that can be mined for information about an enterprise. The research also reveals that the top 6 alerts contribute over 99.6% of the entire alerts. Security administrators and other researchers will benefit from the findings in this research paper.

Keywords

Intrusion detection, alert analysis, snort alarms, trend analysis, network security, STL

1 Introduction

Intrusion detection is the process of monitoring events on a system and analysing these events for the occurrence of a security incident or malicious activities (Bace, 2000). Intrusion detection systems (IDS) do not simply detect intrusions, but instead detect events in traffic that may or may not be intrusions (Endorf et al. 2003). It creates excessive alerts that trigger on detection of malicious activities. The alerts tend to become cumbersome to analyse and respond to, as a number regular system activities also trigger the alerts (Dong et al. 2008). Consequently it is almost impossible for administrators to use intrusion detection systems appropriately.

The alerts triggered by normal system activities are known as false positives and tend to be repetitive in the alert files. IDS systems aim to filter out the anomalies or specific attacks that have been identified in the past by signatures. IDS research has been evolving to improve its performance by reducing the false acceptance rate and reduce its false rejection rate but these systems are still far from perfect at identifying only intrusions in a system. The alerts generated are, in most cases, elementary and difficult to interpret by security administrators; hence, the need for a specialist to decipher the content. IDS systems generate large number of alerts which are consists of several false positives, false negatives, and true positive alerts (Cuppens, 2001; Li and Tian, 2010). This leaves the response to these alerts as a job for the busy security administrator who is unable to interpret the cumbersome alerts.

Individually, these alerts may be insignificant, and are sometimes discarded by the IDS operator. The significance of an alert cannot be measured in most cases, as its significance often depends on its past behaviour and presence. Collectively, these alerts can provide more information about the state of the protected system (Viinikka and Debar, 2004). Thus, alerts accumulated over a period of time are invaluable, and can provide information about the nature of intrusion for the purpose of fingerprinting. The alerts can be aggregated together as they occur sequentially, and examined as an hourly, hence reducing the time required to review the alerts. This creates a time series of the alert intensities, and emphasizes the need to store alerts over a long period of time.

The main objective of this research is to identify the false positives and actual alerts in using a variety of statistical analysis tools ranging from trend analysis to other tools such as the box and whisker plot. This relies on the assumption that the false positives will generate a certain amount of alerts always as the normal activities that trigger it are in most cases repetitive and thus, generates a pattern in the trend. This paper involves trend analysis of the alerts originating from different countries generated by snort at the edge of the Plymouth University network using Seasonal decomposition of Time series by Loess (STL).

Due to privacy concerns, it is also difficult to get real world data for researchers to analyse. The source IP addresses in traffic sources can be anonymised but it will still contain a reasonable amount of information that can be extracted to determine the sites frequently visited but users in the enterprise. Most research is aimed at exploiting the statistical properties contained in the alert sets. Thus, extracting these properties removes the need to share the alert files. This paper suggests a framework for making the statistics available to researchers.

2 Statistical Analysis of Alerts

The statistics of these alerts can provide a basis for identifying the characteristics of the normal system activity. Spathoulas and Katsikas(2010) shows that false alerts can be identified by the frequency with which the alert signatures trigger false positives. Thus, changes in the trend of the alert intensity will also reveal the actual intrusion attempts from the alert sets. There is no single solution to distinguishing the actual intrusion attempts from the normal system activities, but numerous statistical procedures have been used in the past.

Algorithms including REDUCE, which determines the periodicity of the normal system events using Fourier analysis of time series of the alerts, and CLUSTER have been used in some research to correlate the alerts correlation (Julisch, 2003; Viinikka et al. 2006; Dong et al. 2008). The CLUSTER algorithm groups together similar alerts based on the attack patterns. Clifton and Gengo (2000) characterises false alarms using the frequent episodes algorithm by identifying the alarms sequential alarms that occur frequently over a period of time.

Ye et al. (2002) suggests procedures for obtaining efficient results using EWMA control charts. Ye et al. (2003) actualises two of these procedures and tests the performance using EWMA. Viinikka et al.(2004) shows that EWMA does not provide successful results at all times. Stationary autoregressive models (AR) is seen to generate a more detailed result in Viinikka et al. (2006) but with the necessity for removing the trend and periodic components which is tends to introduce artifacts in the series. For this reason, Viinikka et al. (2009) proposes the continuous use of EWMA, instead of the stationary AR model. Debar and Wespi, (2001) propose an algorithm that can be used in aggregation and correlation components of intrusion detection systems. Chantawut(2009) also uses time series approach using autoregressive integrated moving average (ARIMA) method.

The normal system alerts are known to have a periodicity, and hence the time series approach is widely used. Trend analysis of the alerts over a period of time can reveal the behaviour and pattern of false positive alerts over a period of time. The normal state of the system can be observed, and changes to this can be easily spotted. This paper involves the trend analysis using STL to decompose the alert. Unlike AR, STL does not introduce artifacts (Cleveland et al. 1990) and overcomes the shortfall of AR identified by Viinikka et al. (2009).

3 Trend Analysis

A time series is a sequence of successive observations which are ordered in time. It is simply a set of observations (in this case the alert intensity) each one being recorded at a specific time (hourly). Univariate time series analysis, as the name implies involves analysing the collection of observations for a single variable over a period of time, whereas a multivariate Time series involves doing the same for multiple variables. This paper will focus on univariate analysis of the alert intensities observed. A univariate time series, z_t, usually takes the form in equation 1.

$$z_t = f(z_t, z_{t-1}, \ldots, z_1) + a_t$$

Equation 1: Univariate Time series (src: Pena et al. 2001)

Where $f(z_t, z_{t-1}, \ldots, z_1)$ a function of is previous values of the series, and a_t is a sequence of identically distributed variables. It is sometimes written in the form as seen in equation 2.

$$z_t = m_t + s_1 + y_t$$

Equation 2: Univariate Time series (src: Brockwell and Davies, 2001)

where m_t is the trend of the series, s_t is the periodic seasonal component of the series, and y_t is the residual noise component. Time series is usually written as a mathematical model to make it easy to decompose it into its systematic component and noise component. This property of time series makes it suitable for the correlation of alerts.

This paper focuses on the use of STL for decomposing the time series; although STL does not generate a mathematical model. It uses localised models at each data point combining the simplicity of the linear square regression and the flexibility of the non-linear regression (NIST, 2010). This simplicity allows analysis of the properties of the procedure and allows fast computation, even for very long time series and large amounts of trend and seasonal smoothing. This removes the need for determining an appropriate model for each series that is plotted, thus no expertise required in understanding statistical procedures. This makes this a suitable model for implementation by a security administrator.

4 Program Framework

Numerous researches are based on the alert intensity per unit of time, or alert flows based on the IP addresses. Enterprises have to maintain the privacy of its users when sharing information; thus the real world data that is sometimes made available is anonymised to avoid reconstruction of the packets. The payload of the packets is in most cases stripped, and most of the header and trailer information as well. This still leaves the concern of enterprises with concerns of data leakage and data mining. It is often a question of how much information can be distributed that will not present information about the network users.

Most organisations archive the alerts after a long time for legal reasons, or intrusion detection. This practice can provide useful the research community, since the alerts are needed over a long duration. The alert intensities can be computed hourly or daily for individual alert types over different durations before the long-term organisational archiving and backup. IP-to-Country APIs can be used to determine the destination countries to allow for correlation of the alerts based on the source countries. An example is the free Geolocation API available from Maxmind that has an accuracy of 95% for most countries. The frame work will generate index files for the countries and alert types to help researchers identify the alerts and also facilitate a time of day correlation from the respective countries.

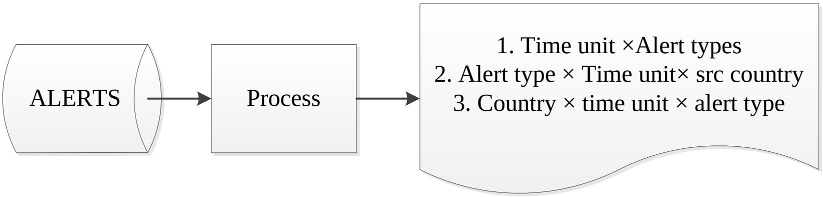

ALERTS
Process
1. Time unit ×Alert types
2. Alert type × Time unit× src country
3. Country × time unit × alert type

Figure 1: Program framework for extracting statistics of alerts

This frame work proposes that 3 types of files, excluding the program with the index of countries and alert types, are needed. The first stores the alert intensity within each time unit (hourly and daily) for different alert types. Next, different files for each alert type present containing the intensities of the alerts during each time unit from all source countries. The third type of file will include files for each source country of the alert containing the alert intensity of different alert types for at every time unit.

5 Experimental Results

Viinikka et al. (2006) concluded that few signatures account for most of the alerts generated by intrusion detection systems. Basic analysis of the alert set shows that 6 of the top alerts contribute up to 99.6% of the entire alerts in the set. Table 1.0 shows the alert distribution for 2 different datasets obtained from the Plymouth University's network.

Dataset 1			**Dataset 2**		
Signature ID	**Intensity**	**Cum %**	**Sig. ID**	**Intensity**	**Cum %**
Slammer (2050, 2003, 2004)	50057355,50057346 50057346	95.2	2	331422	60.3
ICMP (469,466, 483)	4904803, 1830953 322414	99.7	7	115166	81.3
MS-SQL overflow (2329)	116738	99.7	14	47948	90.0
2	63623	99.8	15	39338	97.2
58	50601	99.8	6	7862	98.6
7	43793	99.8	9	6718	99.8
1419	37321	99.9	4	558	99.9
255	30176	99.9	3	258	100.0
472	24685	99.9	2464	8	100.0
All alerts	157747024	100		549288	100.0

Table 1: Signature ID Present in Dataset in order of intensity

Analysis of HTTP Double decoding alerts (SID2) originating from United Kingdom

Snort alerts with ID value of 2 represents HTTP double decoding alerts, invalid FTP commands, Back Orifice client detected, Tear drop attacks, as well as encrypted Telnet sessions. This alert type is present in both datasets and originates from various countries. In 2009, we have United Kingdom, China, United States, Taiwan, and Netherland contributing the following percentages of the entire SID 2 alerts: 75.1, 9.5, 5.4, 0.7 and 0.6 respectively. In 2010, United Kingdom appears as the source of just 60.2% of the alerts while unspecified countries in Europe originate 26%. Italy, United States and Sweden have 11.9%, 1.3% and 0.4 % respectively. There are few alerts from China in 2010 contributing less than 0.01% as compared to the results from 2009. This shows that the trend of the alerts on the internet is changing.

It is also observed that the slammer and ICMP alerts which were massively present in 2009 are no longer present in the dataset captured in 2010. The signature rule-sets used for the experiment were the latest available at the time of the research procedure. It was noticed that just 1 of the 3 slammer alerts was enabled but previous study by Chantawut(2009) showed that the 3 slammer alerts all triggered on the same packets, hence the modifications to the rule set removes two-third of the slammer occurrence if present. We can conclude that snort has been tuned appropriately to trigger the slammer alarms when it detects a more significant occurrence of the worm, or it could also be that the worm is being blocked at a higher layer in the network topology as a result of on-going research to block and remove traces the worm on the internet.

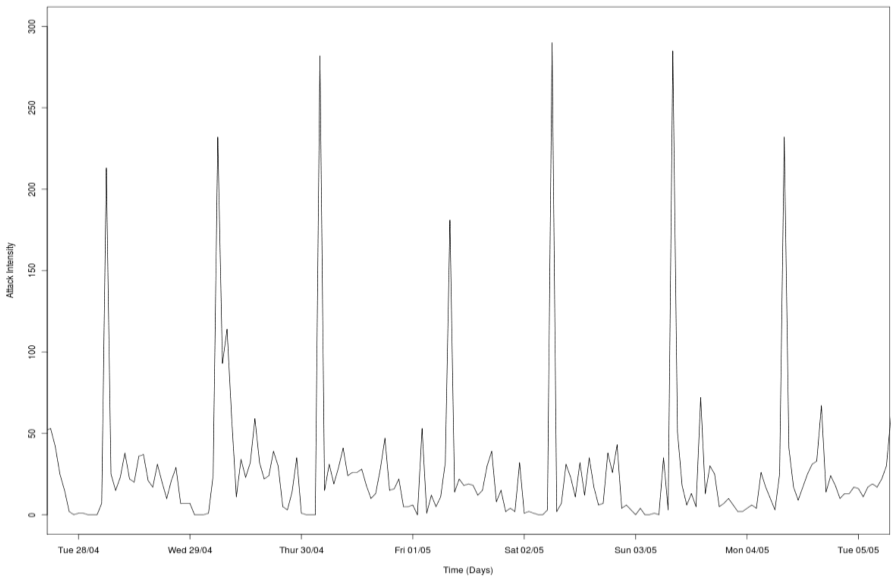


Figure 2: Time series plot of SID2 from United Kingdom from Fri Apr 24 to May 5

The time series plot of the hourly alert intensity reveals a characteristic behaviour for the normal system activities on the network. A pattern can be observed in figure 2 with varying peaks at different times of the day. This depicts the regular system activity for the first week in the dataset. The time of the level shift differs each day, but the pattern continues for the first week. The pattern alternates randomly on different days, with 6 different levels each day at different hours but the intensity remains on the same level. A large increase in the trend can be seen in figure 3.This suggests that the alerts observed on the consistent alert patterns observed are false positives as the alerts are repetitive. The obvious true positive alert here is the event signified by the sharp rise on 20 July 2009 between 3AM and 5AM. The trend of the series also reveals that the intensity varies at each hour of the day.

The box and whisker plot of the daily intensity of the alert in figure 3 also shows that the alerts on the 92 out of 96 days in the alert set have similar values of intensity. It can be observed that the data has a normal distribution as the median lies in the middle of the box

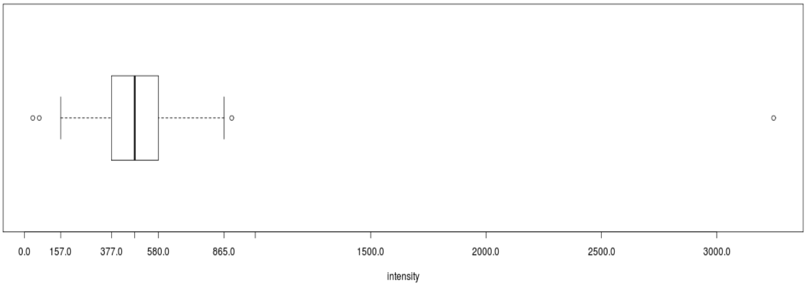


Figure 3: Boxplot of SID2 alerts from United Kingdom

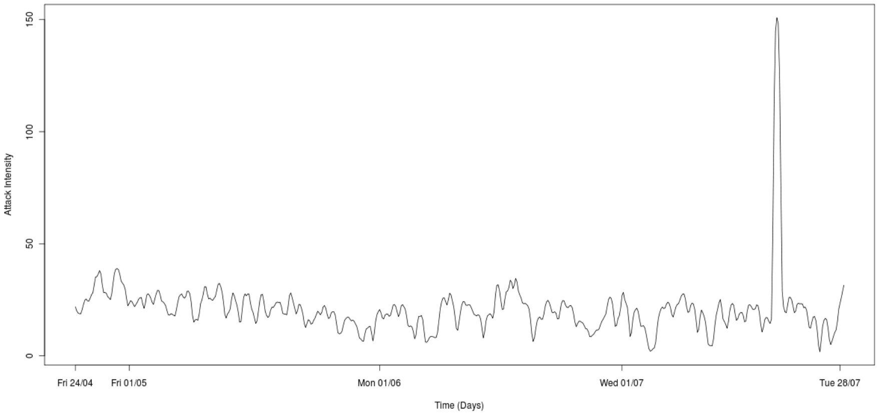


Figure 4: Trend analysis of SID2 from United Kingdom

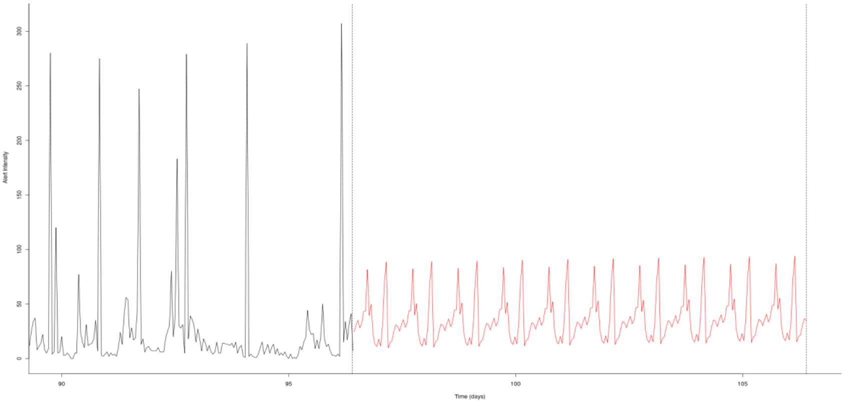


Figure 5: Forecasting 10 additional days of SID2 using the operator module in R

6 Conclusions and Future

This paper presents various statistical analyses of alerts triggered by snort. It shows how false positives can be identified from the trend of the series. This paper shows that the trend can be used to determine levels of false positives in the alert set, periodicity, as well as identify malicious activities. The trend of the series can provide information to support Analysis also showed the lack of ICMP and Slammer alerts in 2010, which may be due to improvements to snort in the last year.

STL is able to decompose the series into the respective components, but it is unable to generate a suitable forecast of the trend. The AR model or ARIMA models should be used for subsequent analysis to allow for significant prediction of the trend.

The program framework can be implemented and combined for use with the major IDS solutions in use in the Industry. This will provide a way for more research to be done and improve the quality of IDS systems faster than the current evolution trend.

7 References

Bace, R. G. (2000), Intrusion detection, Macmillan Publishing Co., Inc.

Chantawut, K., (2009), “Trend Analysis of Snort Alarms”, MSc Thesis, Plymouth University.

Clifton C, Gengo G.(2000), Developing custom intrusion detection filters using data mining, 21st century Military Communications MILCOM 2000, vol. 1; 2000. p. 440–3.

Cleveland, R., Cleveland, W., Mcrae, J. & Terpenning, I. 1990. STL: A Seasonal-Trend Decomposition Procedure Based on Loess, *Journal of Official Statistics*, 6, 3-73,

Cuppens, F. (2001), Managing alerts in a multi-intrusion detection environment, In: Computer Security Applications Conference, 2001, Proceedings 17th Annual, 2001. 22-31

Debar, H. & Wespi, A. (2001), Aggregation and Correlation of Intrusion-Detection Alerts, In: Lee, W., Mé, L. and Wespi, A. (eds.) Recent Advances in Intrusion Detection, Springer Berlin / Heidelberg.

Dong, L., Zhitang, L. & Jie, M. (2008), “Processing Intrusion Detection Alerts in Large-scale Network”, In: Electronic Commerce and Security, 2008 International Symposium on, 3-5 Aug. 2008 2008. 545-548

Endorf, C., Schultz, E., and Mellander, J., (2004), Intrusion Detection & Prevention, McGraw-Hill, USA

Julisch, K. (2003), Clustering intrusion detection alarms to support root cause analysis, ACM Transactions on Information and System Security, 6, 443-471.

Li, W. and Tian, S. (2010), An ontology-based intrusion alerts correlation system, Expert Systems with Applications, 37, 7138-7146.

Spathoulas, G. P. and Katsikas, S. K. (2010), Reducing false positives in intrusion detection systems, Computers and Security, 29, 35-44.

Viinikka, J. and Debar, H. (2004), Monitoring IDS Background Noise Using EWMA Control Charts and Alert Information, In: JONSSON, E., VALDES, A. & ALMGREN, M. (eds.), Recent Advances in Intrusion Detection, Springer Berlin / Heidelberg.

Viinikka, J., Debar, H., Mé, L. and SéGuier, R., (2006), Time series modeling for IDS alert management, Proceedings of the 2006 ACM Symposium on Information, computer and communications security. Taipei, Taiwan: ACM.

Viinikka, J., Debar, H., Mé, L., Lehikoinen, A. and Tarvainen, M, (2009), Processing intrusion detection alert aggregates with time series modeling, Inf. Fusion, 10, 312-324.

Ye, N., Borror, C., and Zhang, Y., (2002), EWMA techniques for computer intrusion detection through anomalous changes in event intensity, Quality and Reliability Engineering International, 18, 443-451.

Ye, N., Vilbert, S. and Qiang, C. (2003), Computer intrusion detection through EWMA for autocorrelated and uncorrelated data, Reliability, IEEE Transactions on, 52, 75-82.

Network Security and User Awareness in IT Organisations

S.Sathiyaseelan and P.Filmore

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

It is obvious that in today's internet world not only the internet users are increasing in number but also the security threats. To protect the network from getting attacked, the security level and the awareness level of the users must be improved to a sufficient level. This research entitled 'Network Security and User Awareness in IT Organisations' aims at analysing the current network security level and level of user awareness in IT organisations. This research is conducted in the form of a survey in which the questions were focussed on the topics namely, security level and security breaches, security trends and methods, security policies, management issues on security.

The questionnaire comprised of 25 questions among which three of the questions were set to be compulsory. Seventy four responses were obtained from seven of the IT organisations. As the questionnaire comprised of less number of compulsory questions, the chance given for the users to skip the questions of concerned in retrospect. From the analysis, recommendations were developed for the users regarding how to handle security issues and how to improve security level in IT organisations.

Keywords

Network security, questionnaire research, security breaches, security trends and methods, security policy, management issues on security.

1 Introduction

The computer users and the usage of the internet are increasing day by day. Computers communicate with each other by the means of a network. The expansion of a network can be restricted within a small building or it may cover a wide area also (Davies and Price, 1984). Not only is the internet usage increasing rapidly but also the crimes on the other hand (Maiwald, 2003). These crimes are happening due to the network vulnerabilities and also due to the user's unawareness in the field of network security (Canavan, 2001). The computer hackers are (Stallings, 2000) creating threats to the computers and vulnerability attacks to the computer network. Lot of laws have been (Devargas, 1993) created by the government to punish the hackers. Implementing these laws alone cannot serve as the best way to reduce the cyber crimes.

Nowadays we are coming across lots of news about the network security attacks by the attackers in newspapers and internet Devargas, 1993). The attackers not only target the private organisations but also target the Department of Defence (DOD) and other government organisations (Devargas, 1993). The attackers either steal or destroy the confidential data of the organisations. They attack the social networking web sites and the most famous commercial web sites such as Yahoo, Amazon, eBay, etc. It is not necessary that the attacker must be external attackers. There are many internal attackers such as employees or former employees of an organisation who attempt to steal the organisation's salary information or important data (Maiwald, 2003). All organisations are monitoring (Canavan, 2001) their own network to prevent unauthorised intrusion and other types of attacks. Every organisation spends a lot of money on network security. Improving awareness of network security among computer users plays a main role to reduce the cyber crimes.

2 Need for Network Security

With a rapid increase in the number of corporate networks, there has been an increase in the bandwidth over the internet. Internet has been put to use for communication purpose, remote connection to the corporate network and also for commercial transaction in recent days (Devargas, 1993). As there has been an increase in the uses of the internet, the number of threats being posed by the hackers are also increasing day-by-day. Due to these threats like spam, phishing, etc., the customer distrusts the corporate companies and organisations for online transaction. As a result, the companies face some amount of loss (Bhatnagar, 2002). There are network security tools and network security policies (CISCO Systems, 1992) to protect the network or computer systems. The network security prevents the unauthorized users to access the network, thereby securing the company's network and otherwise making the organisation as a reliable organisation.

3 Network Security Threats

Any disorder that affects the normal activity of an individual system or the entire network, like affecting the integrity, functionality of the system intentionally or naturally can be defined as threats (Canavan, 2001). Threats that causing damage or loss are classified into following three types (Devargas, 1993), they are active or passive threats, logical or physical threats and deliberate or accidental threats.

4 Methodology

The main purpose of this research is to collect the information based on the questionnaire, understanding the information and processing those obtained information to write recommendations for the IT organisations. This research consists of different types of questions and quantitative methodology.

4.1 Development of questionnaire

4.1.1 Analysis of previous research

Previous research is analysed under the heading ‘Network security and user awareness’. The reports of previous research that undertaken is collected and analysed.

4.1.2 Analysis of previous data collection method and create own research methods

The previous data collection method for the previous researches is analysed. Then our own questionnaire is created for the quantitative research method depending on the research. Then that obtained research method is implemented to collect data.

4.1.3 Trial Implementation of Questionnaires

A trial questionnaire is implemented and it is tested by using the Survey monkey website with suggestion of my project supervisor. Then the URL link of the survey is sent to Plymouth University students by email with permission of my project supervisor. After testing the questionnaire, the reports are collected from the students and analysed. The mistakes are corrected which have been done in the trial questionnaire with the help of observed reports. Specific changes are included in the questionnaire.

4.1.4 Implementation of Questionnaire

The questionnaire is implemented for computer users in IT organisations. The expected minimum respondents are 70 and maximum respondents are 100 for this research. Then the reports from the computer users are collected and analysed.

4.1.5 Analysis of collected data from the reports

The data is collected from the computer users in the IT organizations are documented properly. After collecting the data, the results obtained are analysed and recommendations are then developed. After this process a conclusion of each part of the research is made and a final report is created.

5 Analysis Summary

From this research analysis of the questionnaire it has been observed that 52.4% of the respondents in the IT organisation have some awareness of the technologies and methods being used in their IT organisation. 5.92% of the respondents have commented about the antivirus and firewall used in their IT organisation. It proves that they have some knowledge about network security in their IT organisation. The other 48.6% of respondents do not possess sufficient knowledge regarding the network security methods used in their IT organisation. So it is clear that the computer users need more training regarding the network security and the organisations are responsible for making the computer users aware by providing proper copies of policies and proper security training.

6 Recommendations:

The recommendations are based on the analysis of the results obtained from the questionnaire and the background research. The recommendations are divided into five parts, based on the questionnaire. The five parts are security level and breaches in organisation, security trends and methods in organisation, security policies in organisation, management issues on security in an organisation and issues improving organisation's security level.

6.1 Security level and security breaches

From this research it could be observed that most of the organisations do not show much interest in network security. The security level of the organisations is in an average level (43.20%). **Recommendation:** *The organisation should be aware of network security. The respondents also should cooperate with the organisation to improve their network security from security breaches.*

The results obtained from the research show that 35.10% of the organisations have suffered from Malware and from other types of malicious threats. These types of threats are occurring due to vulnerability in the network and unawareness of respondent on network security in their organisation. This research paper analysed that 28.35% of the organisation have the highest security risk on internet downloads. **Recommendation:** *This is the responsibility of the organisation to improve their security level by implementing proper security mechanisms and tools. The respondents should improve their awareness on network security to prevent themselves and their organisation from these types of malicious threats.*

6.2 Security trends and methods in organisation

This analysis observed that 66.20% of the organisations have secure backup disk for important data and 32.45% of the organisation are not having that secure backup disk. **Recommendation:** *Every organisation must have secure backup disk for important data.* Nowadays most of the employees are using portable devices for communicating with the organisation's network. Some of the employees are working from their home and access the organisation's network. **Recommendation:** *Wi Fi protected access and end point security should be implemented for secure access of organisation's network.*

The research observed that only 48.60% of the organisations are currently using automated patch management and vulnerability scanner. Recommendation: The respondents and the security administrator in the organisation should be aware of implementing the automated patch management and vulnerability scanner in their systems to in order to prevent the attacks from occurring.

It was found out from the research that 30.72% of the organisations are using both antivirus and firewall. 36.42% of the organisations are using Kaspersky antivirus and Norman personal firewall. 18.45% of the organisations are not using either the spam control or the anti spyware. **Recommendation:** *Organisations should implement all types of security mechanisms such as antivirus, firewall, spam control, antispyware, etc., in order to improve their network security level. The respondents and security administrators should be given training and made aware of implementing the security tools in their organisation.*

This research observed that 44.55% of the respondents are interested in using the password authentication technology mainly because of the reason that it is cost effective. 39.15% of the users have felt more comfortable in using the biometric technology because of its enhanced performance. **Recommendation:** *It is suggested that the organisations should implement password authentication and biometric technologies to prevent the IT organisation from security breaches such as identity theft, data loss, etc. The employee must be made aware of the technologies that have been used in their organisation.*

6.3 Security policies in organisation

This research observed that 74.25% of the organisations have network security policy, password policy and some of the organisations are also have a security team. 24.30% of the organisations do not have them. **Recommendation:** *It is very essential that all of the IT organisations must have the policies and also a security team to update those security policies regularly. These policies must be updated frequently based on the security breaches that the organisation is expected to face, so that the organisation could be saved before the attacks have occurred.*

This research observed that 75.60% of the organisations have provided the security policies implemented in their organisation to the respondents. But 21.60% of the organisations have not provided the network security policies implemented to respondents. There is no purpose in creating network policies without them being implemented. From this conducted research it could be observed that only 58.10% of the organisations provide security training to the respondents in their organisations. **Recommendation:** *It is suggested that security training must be provided by the organisations to all of the respondents in their organisations. The respondents should also follow the security policies and security training given in their organisation to protect their systems and network from malicious attacks.*

6.4 Management issues on security in organisation

This research observed that 51.30% of the organisations are spending 11-30% of organisation’s IT budget for security. 64.80% of the respondents accept that this budget is enough to cover their security requirements of the organisation and 32.40% of them do suggest that it is not sufficient enough for their organisation. 63.45% of the respondents assure that it is possible for them to convince their organisation’s management to invest more amounts in security solutions. **Recommendation:** *The respondents have the best opportunity to convince the organisation’s management to make more investment on security requirements. So it is suggested that the* *respondents must use the opportunity to convince the organisation's management about the implementation of the security equipments.*

6.5 Issues to improve organisation's security level

It could be observed from the research that 48.60% of the respondents accept that better awareness on security among employees help to improve the level of security in the organisation. **Recommendation:** *The major issue that helps to improve organisation's security level is the level of awareness of the computer users regarding the security issues. So IT organisation management and employees should cooperate to improve the security awareness level among computer users.*

7 Future Work

As all of the questions were not made compulsory, many of the users used their chance to skip the questions, which could be stated as a very important limitation of the research. In order to avoid this issue and extend the research, future researchers may conduct the same research with all of the questions made compulsory, which will improve the level of analysis.

In this research, the responses have been collected from the employees of the IT organisations. But their role in the IT organisation was not determined. Future researchers may add some extra questions in the research covering the aspects such as the role of the employee in the IT organisation, number of employees in the organisation and the security training methods implemented in the organisation. This will deepen the analysis of the further.

This research was conducted using quantitative methodology, future researchers may conduct the same research using qualitative methodology, which will provide more details for analysis and as a result further better recommendations could be provided.

8 Conclusion

There is a rapid increase in network and also new networking technologies every day. There are lot of challenges that the networks in IT organisations and in other enterprises should face. The new security technologies are also arising everyday to encounter these challenges. In any IT organisation, security is a major issue to protect their network and data. The computer users are considered to be the backbone of an IT organisation. This research is has tried to analyse the awareness level of the computer users in an IT organisation regarding the network security and its tools.

This research analyses in deep the issues such as the security solutions and mechanisms implemented in the IT organisations to protect their own network, security threats to the organisation, security policies and organisation's IT budget to security. These issues are related to the security awareness level of in the IT organisations. The results obtained from this research show that the computer users in IT organisations are having some level of awareness on network security and security methods implemented in the IT organisations. But they do not have a very good level of awareness on the network security and security solutions implemented in their organisation. It seems that IT organisations are not concentrating more on improving the awareness level of the computer users in their organisations. When the users are not given appropriate training they may remain unaware and as a result, they may open the door for the hackers to enter into the secured network of the organisation.

This research has recommended that the IT organisations should improve the awareness level of network security among computer users in their organisation by implementing the network security policy in their organisation and also by providing proper security training to the computer users. The organisation should accept and provide the requested network security requirements of the computer users in the IT organisation. The computer users should follow the security policies and security training given by their IT organisation. The computer users should also have a sufficient level of awareness on network security methods used in the organisation.

9 References

Bhatnagar, K. (2002) Cisco security, Ohio: Premier, ISBN: 1931841845.

Canavan, J.E. (2001) Fundamentals of Network Security, Artech House, London.

Cisco Systems Website, (1992) ‘What Is Network Security?’ http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html, (Accessed 24 June 2010)

Devargas, M. (1993) Network security, Oxford: NCC Blackwell, ISBN: 1855542013.

Maiwald, E. (2003) Network security: a beginner’s guide, California: McGraw Hill, ISBN: 0072229578.

Stallings, W. (2000) Network security essentials: application and standards, New Jersey: Prentice- Hall, ISBN: 0130160938.

Digital Watermarking for Copyright Protection

M.A.Ambroze and V.R.K.Venkateswarlu

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Digital watermarking is a technique which permits the users to integrate or embed the data into electronic contents like image, audio or video. This research project aims to protect the copyright of ownership, and unauthorized copying of digital data by presenting secure algorithm. In this project, the digital watermark using least significant bit (LSB) technique is implemented and discussed. The original colour image which has to be watermarked is formed of thousands of pixels. Every pixel of the colour image is represented with the binary system and is structured to create a digital plane. The least significant bits of all pixels will show randomness and it will not affect the vision effect or the data of the original file even after changing last bit of each pixel. So we can replace the least digit with the watermarking information. This process is implemented in this project by using Matlab coding on an image file and the result shows that LSB technique is to be simple, cost effective and reliable watermarking technique.

Keywords

Steganography, Least significant bit, spatial domain, cost effectiveness

1 Introduction

One of the driving forces behind the increased use of copyright marking is the growth of the Internet which has allowed images, audio, video, etc to become available in digital form. Though this provides an additional way to distribute material to consumers it has also made it far easier to make copies of copyrighted material to be made and distributed. In the past, pirating images, for example, used to require some form of physical exchange. Using the Internet, a copy stored on a computer can be shared easily with anybody regardless of distance often via a peer-to-peer network which doesn't require the material to be stored on a server and therefore makes it harder for the copyright owner to locate and prosecute offending parties

Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. The simple steganography techniques have been in practice for hundreds of years, increase in usage of digital files has demanded for new techniques to hide information's, to protect intellectual properties.

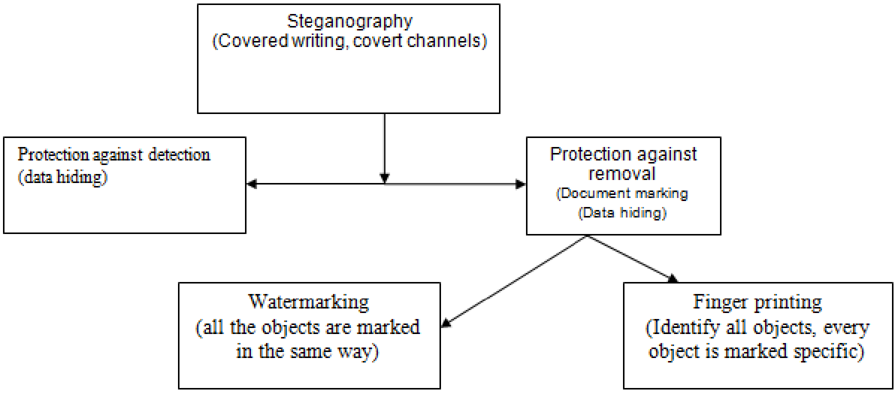

Steganography
(Covered writing, covert channels)
Protection against detection
(data hiding)
Protection against removal
(Document marking
(Data hiding)
Watermarking
(all the objects are marked in the same way)
Finger printing
(Identify all objects, every object is marked specific)

Figure 1: Analysis of Steganographic Techniques (Popa, 1999)

The figure shows a clear classification of steganography, Steganography is classified into protection against detection, which is nothing by hiding the data. This technique helps in hiding the data and prevents the access of the data by unauthorized uses. Protection against removal is a copyright marking in which copyright information are inserted to the copy right protected data. Protection against removal is further classified into watermarking and finger printing. Steganography and encryption are the techniques used for data protection. When encryption techniques are used for data protection, everyone can see both sender and receiver are transferring the secret data. But by using steganography no one can identify secret data are transferred between parties, so steganography is preferred over encryption techniques for more confidential data. Paper watermarking came to into existence in the end of 13th century in Italy. This technique is considered to be the foundation for digital watermarking paper, watermarking are commercialized by using in bank notes and stamps. A digital watermarking technique was originated in 1990s**.** Tanaka et al in 1990 and by Tirkel et al in 1993 where the two publications focused on digital watermarking images in the year 1990 and 1993.van schyndel et al in the year1994 introduced techniques of using m-sequence in the watermarking techniques to change the least significant bit of images. From then lots of research have be carried on this technique, and then research more advanced and proved its potential benefits over other techniques. At present digital watermarking plays a vital role in copy right protection.

In general the watermarking system involves two stages. The first one is embedding to indicate copyright; the second one is watermark detection to identify the owner (Swanson et al., 1998). There are two type of domain for watermarking that can be accomplished are spatial domain and transform domain. The research undergoes on spatial domain using the LSB technique for simplicity and effective watermark.

2 Spatial domain technique

Spatial method analyses the information from the spatial that can be viewed from the point of information. The spatial domain watermarking method the scattered information should be embedded in such a way that the data cannot be detected easily. The various method using pixel and features of spatial methods are (i) by changing the values of the pixel or by adjusting the lower level bits of pixels so that the image should not lose any quality [001] e.g. the image is watermarked in such a way by selecting randomly 8x8 blocks of pixels of the image, (ii) by the use of pseudo noise generates the maximum sequence and added to the original image in LSB of a pixel. The other features using pixel is adding a positive number to the one of the sub group where the image is grouped into two sub groups (pitas). In spatial domain the images are taken in blocks and then inserting the bits in the main blocks where it as good brightness or quality value of the blocked image [caronni]. The other feature for the block method is dividing the image in block with the same size as well as watermark then by adding the watermark in the sub-blocks [delp]. The advantages of this technique is robustness to cropping and translation of the data .but it as a disadvantages to some attacks like noise and compression. Some of the spatial methods are LSB, patch work.

3 Least Significant Bit

LSB hiding is the simplest method and it's effective too. This method is based on substitution of least significant bits of pixel of one cover image to the other secret image from the watermark noise. Here hiding the data by deciding the fixed number of LSB of an image pixel and this is combined to the other image pixels forms a new image. Easy embedding and the extraction are done by using correlation. The advantages of LSB is its pay load but low robustness, this the main disadvantage because of the changes in the LSB that breaks the coded watermark easily.

4 Proposed Model

The method implemented in this project is least significant bit watermark, using an image will be done in spatial domain. Usually there are two process carried out in digital water marking are watermark embedding and watermark extraction. Here I am using bmp file as a cover image and also the secret image. The secret image can be text or image so I chosen the image for the embedding into the original image

5 Watermark Insertion

Embedding process of this project is directly enforcing proper logic in least significant substitution of watermarking, the image is vectorized that means converted array to matrix form. Then each bytes of the image pixel is taken and replaced the last bit (least significant bit) to the secret information of the each bit. The secret information used here is image so accessing each pixel (byte) in a similar way of converting into matrix, then converting into a binary of 0 and 1 and replacing with the east significant bit. The figure1 show the proposed model for watermark insertion.

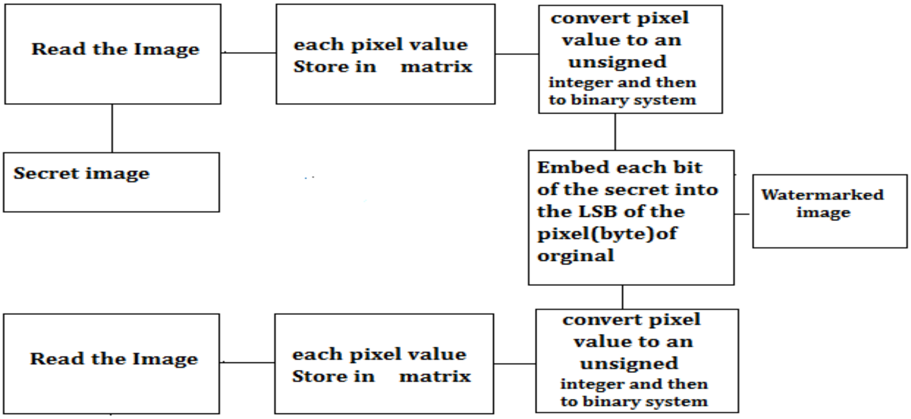

Read the Image
each pixel value Store in matrix
convert pixel value to an unsigned integer and then to binary system
Secret image
Embed each bit of the secret into the LSB of the pixel(byte)of orginal
Watermarked image
Read the Image
each pixel value Store in matrix
convert pixel value to an unsigned integer and then to binary system

Figure 2: Proposed Model for Watermark Insertion

6 Watermark Extraction

After successful completion of the watermark there is a need for extraction to the ownership protection. The extraction process is similar but, here we have to use the reverse process. Finding the difference of original image and secret image and removing the bits using the logic. The output of the watermarked image will be in the form of bytes so after that least significant bits are extracted. These extracted bits are then formulated into a group the watermark information can be obtained. The figure 2 shows the proposed model for the watermark extraction.

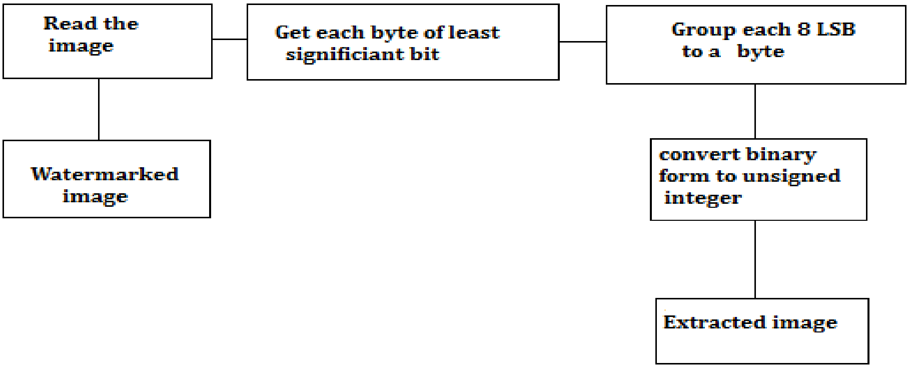
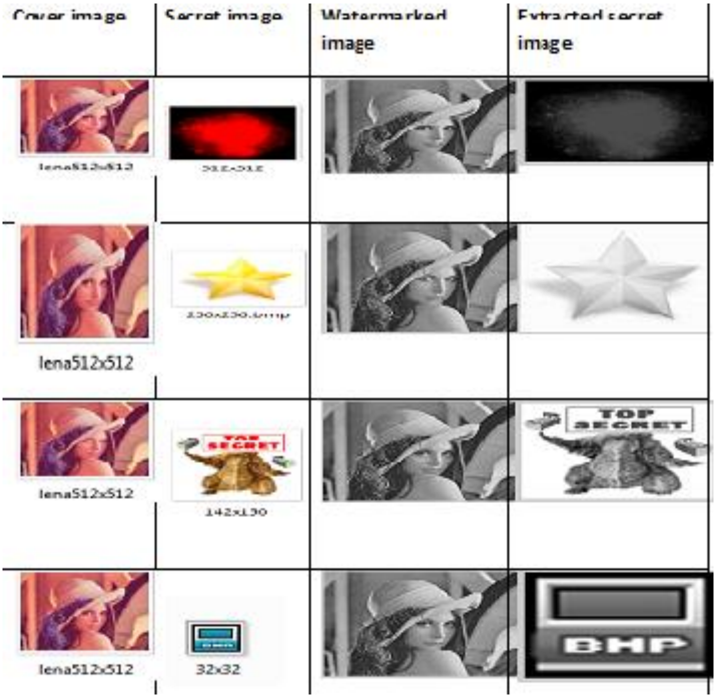

Read the image
Get each byte of least significiant bit
Group each 8 LSB to a byte
Watermarked image
convert binary form to unsigned integer
Extracted image

Figure 3: Proposed Model for the Watermark Extraction

7 Result and Discussions

This section will highlight on the results obtained after the LSB watermarking that was practically implemented. The obtained results are been compared with the theoretical results that was ideally to be achieved and also emphasize on the different attacks possible and an explanation to those of the attacks over them. The bmp file is used for cover image as well as secret image. The size of the original image that has taken here for explanation is 24 bit 512*512 color version of Lena bmp image. The secret image is 24 bit 389 x 308 24 bit bmp image, for the normal LSB watermarking. The secret image is changed for cropping used 256 *256 for better results and for rotation using 32 * 32 color image. The input to be embedded in the original image is resized into 16 x 16, the image can be resized in any size like 34 x 34 or 64x 64 etc and then it is converted into a gray scale image. the different secret images used for to check the effective of the quality and is show below in table 1.



Cover image	Secret image	Watermarked image	Extracted secret image
lena512x512	512x512		
lena512x512	256x256.bmp		
lena512x512	142x130		
lena512x512	32x32		

TOP SECRET
BHP

Table 1: Different

As far as the results obtained, this section concentrates in analyzing the results obtained after the normal LSB scheme is worked out on the specified cover and secret images when compared with the ideal LSB watermarking. By comparing the images with different block size, we can conclude that the changes in the block size did not make any distinguishable changes in the effectiveness of the watermarked image. From this analysis, it is made sure that the imperceptibility is achieved using block size variations

An attack over the normal LSB substitution transform watermarking is discussed. Geometrical attacks like rotation and cropping are applied. Apart from Rotation and cropping attacks there are also many other attacks associated with geometrical attacks. But only rotation and cropping can be easily implemented to check the robustness for the retrieval of the watermark. The results of cropping and rotation attack on LSB watermarking are shown below.

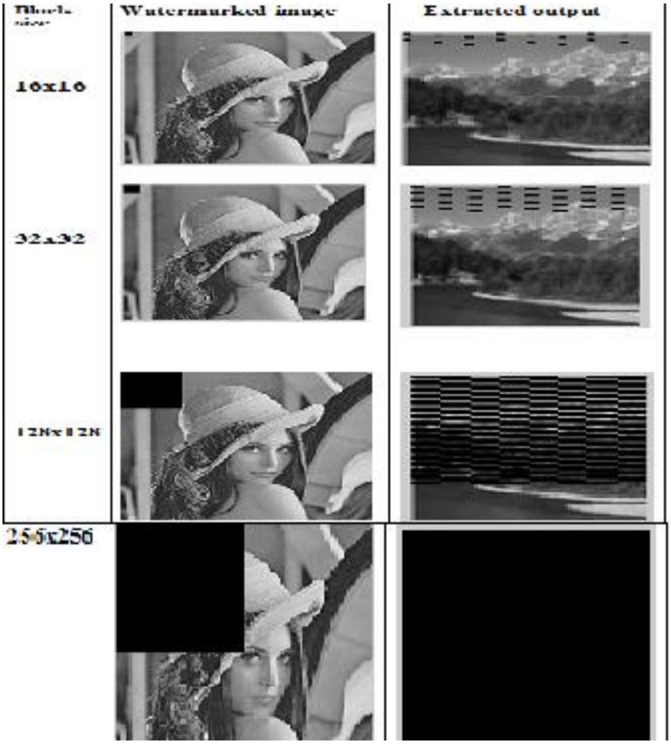
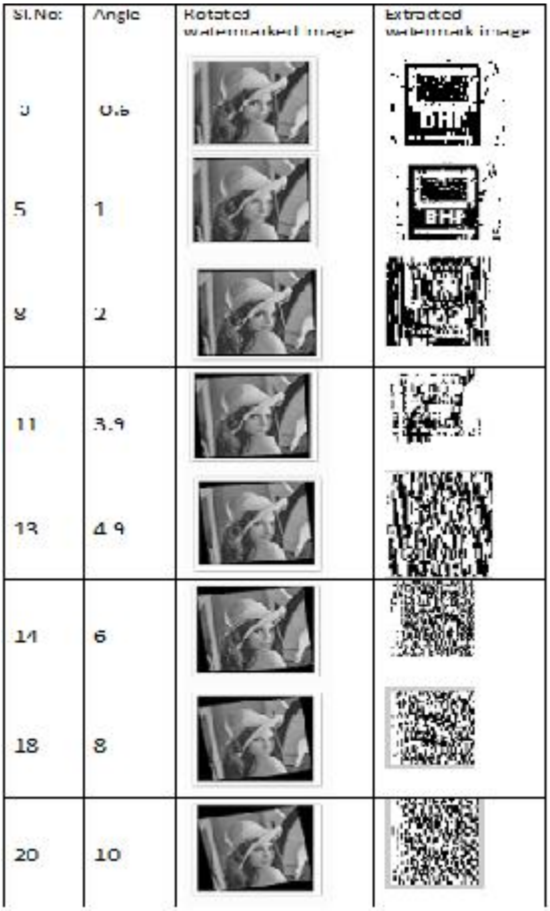

Block size
Watermarked image
Extracted output
16x16
32x32
128x128
256x256

Table 2: Cover Image and Secret image modification on Cropping

The LSB watermarking that practically was implemented is potentially a stable watermarking model without the attacks. The results reveal that LSB watermarking cannot hold any modifications on the cover as it affects the credibility of the cover, and finally the marking algorithm gets affected. Hence it is not possible to imply any forms of attacks on them as they defeat the entire marking system.

From the analysis made on the cropping attack it can be concluded that the secret image will get degraded when it is tampered. Higher the block size decrease more the quality of the secret image on the watermarked image. Furthermore the analysis is made using the rotation attack and it is concluded that the robustness involved is more limited as the angle value increases to rotate the image from the ideal position



Sl.No:	Angle	Rotated watermarked image	Extracted watermark image
3	0.5		
5	1		
8	2		
11	3.9		
13	4.9		
14	6		
18	8		
20	10		

Table 2: Cover Image and Secret image modification on Rotation

The result reveals that that there is a compression going on while embedding is happening. This is done just because the reason all kinds of cover and secret can be brought into a considerable size, no matter how large or small the image is. Just because of this, the secret seems to be really small. This is the reason, for the small size of the recovered secret. This problem can be corrected by resizing the image. However, the adoption of such an attack can reasonably damage the recovery of the secret. The research actually tried to adopt such an attack, just because there was no considerable outcome that was not highlighted in this dissertation. This again proves that the LSB marking scheme is really weak towards attacks.

8 Conclusion

From the above research work, the implementation disclose practically similar to the theoretical assumption which were analyzed in the literature. This scheme is again a successful watermarking in the perspective of the factor cost was concerned. In future, this research work is further improved by improving the security and the robustness. This can be done by ideally imparting the concept of spread spectrum and side information principles. Moreover, the expansion in this project work can also be done by using different cover images as samples instead of using the samples in grayscale and color images.

9 References

Caronni G. “Assuring Ownership Rights for Digital Images,” pro Of Reliable IT Systems, VIS, Viewing Publishing Co., 1995

Delp E.J, Wolfgang.R.B “A watermark for still Image,” In Inter. Conf. On Image Processing, 1996

Pitas, “A method for Signature Casting on Digital Image,” Proc. Of ICIP, Vol. 3, pp.2 15-2 18, 1996.

Popa.R . An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering

Swanson, M., Zhu, B., & Tewfik, A. (1998, September). Transparent robust image watermarking. *International Conference on Image Processing Proceedings,* ICIP 96, pp. 211-214.

Wolfgang.R and Delp.E.J., “A watermark for digital images,” *Proceedings of the 1996 International Conference on Image Processing*, Lausanne, Switzerland, Sept. 16-19, 1996, vol. 3, pp. 219-222.

Wireless Short Range Information System

Y.Vijayakumar and M.Tomlinson

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

In this paper, we discuss the simplest way that a user or a client (a computer) can request and stream or download movies or movie trailers from an internet active computer server (a web server). It is said as simple because the internet active computer server is located somewhere within 200-500m range from the client computer, so that client computer does not have to go through different networks and its peers to download or stream a movie across the wireless network. Here the user utilizes network bandwidth, time and sometimes money spent for downloading a movie. This device which request and receive information from internet active computer server located in a short distance is known as Short Range Device (SRD). This project is a client-server model implemented using Microsoft Visual Basic 6.0 on the client side programming and Microsoft IIS (Internet Information Services), ASP classic and MS Access on server side. The final outcome of the project will let the user login (authentication from the web server) and access movies (list of movies from the web server) based on different categories and watch them on windows media player (movies streamed from the web server).

Keywords

Wireless Networks, Video Streaming, Web Server

1 Introduction

At the first place, when the internet came into existence, user expectations were limited and were satisfied with the text and still images on the web pages they see. Due to the continuous change in the web technology, user started expecting more on their web pages. And then they expected their videos to be downloaded fast as well as with a good quality as the same as TV. But unfortunately we still lack from providing high quality video over the internet due to bandwidth constraints and other network related problems such as congestion and connection problems. Video has been most significant media for entertainment for many years now. Videos were initially transmitted in analogue form and then once digital integrated circuits introduced, video transmitted in digital form. Initially video came in the form of downloading over the internet, user able to download the movie over internet. Though there is delay in getting the movie downloaded, the QOS (Quality of Service) is always better. But due to the time constraints, as next possible solution video streaming is introduced over the internet. An appropriate example of video streaming application used over internet is You Tube. There are many other applications which use video streaming technology. (J.Apostolopoulos et al, 2002)

1.1 Aims

The aim of the project is to construct a portable battery operated wireless device (computer) that can request and receive information from an internet active, computer server located anywhere within 200-500m range through wireless network. Computer is used as a short range device in order to request and receive information from the web server, another computer which acts as a movie server located near the Short Range Device (SRD).

2 Overview, Experimental Setup and Results

2.1 Background

There is an increasing demand for video streaming over Wireless networks. The network bandwidth variations and delay variation are the major problems in providing high quality media streaming. Video streaming applications are a demanding and challenging service to be transferred over wireless networks. There is always a compromise between the capacity of the wireless network and the quality of the video streaming application. The basic steps in sending out content through streaming are:

- ✓ Create or obtain content. The content might be a video which is already stored in the web server, or it could be the one captured live using webcam and multicast them.
- ✓ Encode the content into the special streaming format
- ✓ Use a streaming server to send the content to your listeners.

2.2 Video Streaming Principles

Video streaming is a server/client technology that allows multimedia data to be transmitted and consumed. Streaming applications include e-learning, video conferencing, video on demand etc. The main goal of streaming is that the stream should arrive and play out continuously without interruption. However, this is constrained by fluctuations in network conditions. There are two types of streaming services, on-demand or live streaming. (Wu et al, 2001)

2.2.1 Video Streaming over Web Server

In Contrast, the streaming client proceed the audio and video while it is downloading unlike the download and play client, hardly after few seconds wait for buffering, proceed the method of gathering media file before playing. To play the media file continuously even during heavy traffic in network this small backlog of data or buffer is needed. In this delivery type method the user recovers information as quick as the web server network and user will let exclusive of bit rate parameter of the compressed stream. Progressive playback type is maintained merely by definite media files formats like MS Advanced Streaming Format (ASF) which is among the popular type one.

2.2.1.1 Step by step Streaming

Working with streaming video file as easy as browsing the web but to make the process possible lots behind the scenes.

1 Streaming video and audio characteristics is determined in a site using the web browser you use.

2 The file you need is found along with the image when u click on it link or integrated player with mouse is found.

3 This streaming server receives the request of file from the server.

4 The file which is splitted into pieces through the software in streaming server is passed then to the computer using real time protocol.

5 The information as it comes is decrypted and exhibited on your system using the available browser plug-ins, standalone player or flash application.

6 Your computer rejects the information.

7 A player, a server and a stream of data are the three components needed to match with each other.

Creating and distributing a streaming video or audio file requires its own process. Streaming video or audio needed its own procedure to make and spread.

1 By means of film or digital recorder you can store first quality video or audio file.

2 By transferring the information to a computer and if in need convert it using editing software.

3 When you decide to make a streaming video you should reduce the image size and frame rate.

4 The file is compressed and converted to suitable format using the codec available on your computer.

5 In the server the file is transferred.

6 In turn the server streams the file to users computer.

Creating streaming videos at home as become more comfortable to people due to betterment in Personal Computer and software. Buying and sustaining a personal streaming server is not a affordable task but rather make up a service provider to host the videos. Due to the hike of accessibility of streaming video as also made way for few challenges. One of the challenge includes copy right which includes both legal and illegal action. The illegal one is easier to copy TV programs other videos and send them on the web and the legal action is common one taken by copy right owners.

2.2.2 Advantages of Streaming over Web Server

It is the fact that there is only one benefit to stream with a web server quite than streaming media server which is utilizing existing infra structure. Since the web server utilize a common web server approach which will be used in the administration previously, so there is no requirement of new software infrastructure to establish or administer. Effect of this leads to incremental learning and staffing costs to study and handle the more complex nearly in addition more powerful window media server environment. It needs extra hardware of web server to examine the user requirements this results frequently when web server based streaming put exaggerated load on existing web server infrastructure. Selecting a web server streaming throughout a devoted streaming server supported on hardware price alone generally does not affect in savings.

2.2.3 Protocols

I considered using web server in this work which proved to be a good option since it uses HTTP protocol which resides on top of TCP which is known for its reliability and congestion control. Though TCP is not known for real time streaming, it is reliable. Web Server is also a streaming method using HTTP/TCP as its protocol. Moreover a web server can be easily developed using free software which is prebuilt in windows operating system though not preinstalled. Web server used in this work is Microsoft IIS 7.0 and support software such as ASP, ASP.net etc are prebuilt in Windows Vista. Both ASP Classic and ASP.net are programming software but only should be used to implement web server. I considered using ASP classic, the reason for that is discussed later in this phase.

2.3 Research Methodology

2.3.1 Hardware Requirements

1. Client (SDK or Laptop)
2. Web server (Laptop)
3. Wi-Fi router (for internet)

2.3.2 Software Requirements

The various software requirements are:

1. Microsoft Visual Basic 6.0.
2. Microsoft IIS 7.0.
3. Windows Vista.
4. ASP Classic.
5. Microsoft Windows Media Player.

2.3.3 Test Bed Setup

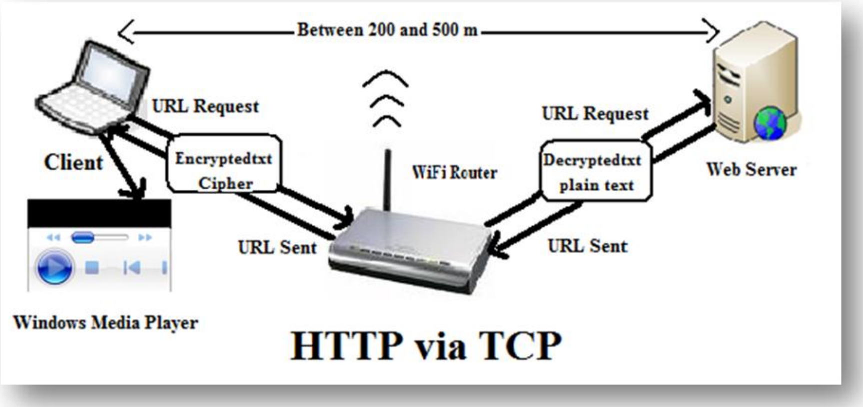


Figure 1: Test Bed Design

From the following diagram, it is clear this project is client-server based project not peer to peer network. There are two computers (one for the client and other for the server), Wi-Fi router shows that this project is based on wireless network. These are the two components that I know initially. The known initial requirements are client, server and Wi-Fi router, the client acts as SDK (Short Range Development Kit) that is connected to server over the wireless internet located between 200 and 500 metres. Further findings and difficulties are discussed later.

The basic ideas behind this project initially are:

1. To make the client request for a movie is sent to server via wireless internet.
2. Wi-Fi router which is interconnecting device which in turn pass the client request to destined server which is very near to client.
3. Server in turn sends the movie requested.
4. Wi-Fi router in turn sends the movie to the client.
5. Protocol for web server is HTTP which is a TCP protocol.
6. Then media player used on the client side is WMP (Windows Media Player).
7. Security method implemented is two-way security, which includes both password authentication and encryption (high level security), the text is encrypted at the client end and decrypted at the server end. So this work provides a high level security for users.

Client use the media player to watch the movie (downloaded or streamed).

2.4 Programming concepts

To create client software we will use Microsoft Visual Basic 6.0 Because of its user-friendly programming and fast libraries which Visual Basic .Net lacks. User must have install Dot Net Framework which to use Visual Basic Dot Net Applications. In Visual Basic 6.0 Advantage is that we just have installed the runtime libraries of Visual Basic 6.0 Which consist of Dll Library Named “MSVBVM60.DLL”. Visual Basic IDE (Integrated development environment) is very simple. Visual Basic Also have Good Debugging capabilities. It Consist Of Huge COM Libraries and Controls to facilitate programmer. It also provides support to RAD (Rapid Application Development).

For Server software we will use ASP Classics because of its quick processing capabilities and user-friendly programming. ASP.net lacks a user-friendly programming environment. Microsoft provides some application to work through ASP (Active Server Pages) Classic such as Microsoft InterDev 6.0. But there is no standard application for ASP Classic. One can even use notepad to program ASP Classic. ASP Classic has an advantage that one can work on any version of IIS where as ASP.NET does not support all the versions of IIS. The table below shows difference clearly.

2.4.1 Client

Client application start With Main() Subroutine Which Shows The “frmLogin” Form. There Are Two Text Boxes with User Name And Password. And Two Button login and cancel. When user enters the username/password and press login, the software submits the username and password to server in encrypted form with Internet Transfer Control. If the user enters a correct user name and password, client software loads movies database from server through Internet Transfer Control.

Client software: It Calls MovieStore Class to process the raw Data received from Server. Then It Download Banner Images for each of the Movies and Saved Each Image in Temp Folder Which is created by the client software for further usage of these banners. Then client software loads up the frmMovies form, which contains other controls will be explained later in these articles. In This form there is a detailed list of movies with detailed tool tip for each movie. From this form user can sort and search movie by his choices user can search movies by multiple genres (action, Adventure, Animation, Biography, Comedy, Crime, Documentary, Drama, Family, Fantasy, Film-Noir, Game-Show, History, Horror, Etc). User can also search movie by title, year, release date, genres, plot, runtime, country, language, company. From The list box user can double click on any movie he wishes to watch. then another window will open up which has a WMP control will connect to .wmv file belongs to that movie.

2.4.1.1 Gobal.bas

1. Sub Main() start with program.
2. Function VerifyAuth() Takes Username and Password as input and return a custom data type VerificationResults which consists of
   - **a.** Outcome.

     Outcomes further defined as enum SubOutComeResult contains two values.

     1. Successful

     Returned when user logged in successfully.

     2. NotSuccessful

     Returned when user didn’t logged successfully.
   - **b.** ErrorType.

     It is further defined as enum subverificationerror contains 5 values.

     1. EmptyValues

        This error returns when username and password is empty.
     2. Unknown values

        Returned when unknown error occurred.
     3. Wrong values

        Returned when user entered wrong username/password.
     4. NoErrorOccurred

        Returned when no error occurred and user successfully logged in.
     5. RejectedExceedTry

        Returned when user exceed his invalid username/password tries.
3. Function XtracMovies() Returns String of Movie data from server.
4. Function DownloadImageTo, this function downloads Image from Server of named passed in its 1st argument and Saves it in path passed in 2nd argument.

2.4.1.2 Encryption.bas

Function **EnDeCrypt** used to encrypt and decrypt strings passed to it. This encryption algorithm is included in both client and server. Here we use RC4 algorithm for the best outcome since it is highly secure over the internet based client server systems.

2.4.2 Server

Server program is needed in order to authenticate user using user login table stored in database and allow the legitimate users to access the movie form to watch movie. Though server programming contains less programming than the client, it plays major part in this project. Server program is linked with Microsoft IIS in order to make it as web server. Server program is programmed using ASP Classic. It is programmed in such a way that when the client enters username and password, he/she gets authenticated by the web server using Auth.asp which handles all the login credentials that the user needed for login which is stored in database table named user logins. This authentication program even take cares when the user enters incorrect login details and necessary steps as same as explained in the client program such as when the login details are empty, unknown and incorrect. Added to this, here it also logs the bad logins to bad logs table in database. Finally it also can restrict particular user for five minutes from accessing the movie form if he/she exceed the maximum number of tries. The maximum number the times the user can try to login is five. If the user tries the sixth time, the account is not accessible for five minutes. XTrac.asp is another program which retrieves list of movies when user login successfully. Final part of the server program is security as in the client program. Secure.inc is the program used for encryption, which encrypts and decrypts the data transferred from client to server and vice versa.

2.4.2.1 Auth.asp

In this, we retrieve the username and password from user login table and incorrect login details from bad logs table and authenticate or reject user Here it has different variables for different purposes. The variables used are:

1. Function **IpConnection** is used to create database object on server for the connection
2. Function **IpRecordSet**, IpRecordSet2 is used to create database object on server for the records.
3. Function **StrDbPath** is used to get the physical path of the file data.mdb which is a database table that contain different tables for user logins, bad logs and for list of movies.
4. Function **TmpUserName** is used in order to store the usernames in user login table.
5. Function **TmpPassword** is used in order to store the password in the user login table.
6. Function **EnDeCrypt** is used for encryption and decryption. Secure.inc (RC4 algorithm) is called here in order to encrypt. [Note: It is mandatory that the password encrypted should match both server and client.]
7. Function **AlreadyFailed** is used to check the number of incorrect logins made by the user and limit the user when the maximum numbers of tries are over.

2.4.2.2 XTrac.asp

This part of the program retrieves the list of movies after the successful login and data sent from client to server and vice versa in the encrypted form using EnDeCrypt function in Secure.inc.

Function **IpConnection**, **IpRecordset, StrDbpath and TmpStr** are used for the same purpose as in Auth.asp.

The string which open the record set of the movies tables is *lpRecordSet.open "SELECT * FROM [Movies]".*

The command which retrieves list of all the movies and movie information such as title, year,release date, language etc is

```
TmpStr = TmpStr &
lpRecordSet("S/n").Value & "&|&" &
lpRecordSet("lpTitle").Value & "&|&" &
lpRecordSet("lpYear").Value & "&|&" &
lpRecordSet("lpReleaseDate").Value & "&|&" &
lpRecordSet("lpGenres").Value & "&|&" &
lpRecordSet("lpPlot").Value & "&|&" &
lpRecordSet("lpRuntime").Value & "&|&" &
lpRecordSet("lpCountry").Value & "&|&" &
lpRecordSet("lpLanguage").Value & "&|&" &
lpRecordSet("lpCompany").Value & "&|&" &
lpRecordSet("lpImageId").Value & vbcrlf .
```

2.4.2.3 Secure.inc

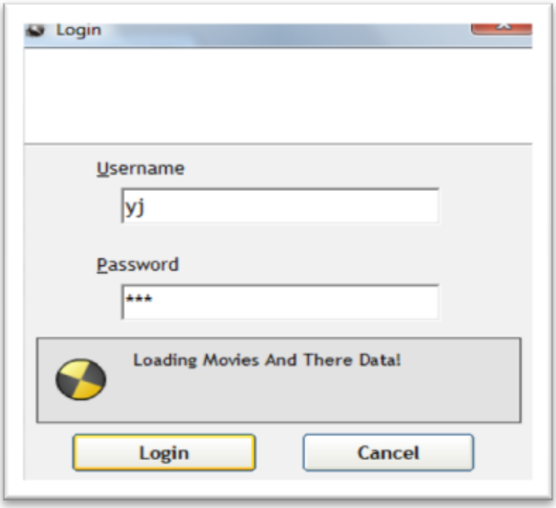
As the file name indicates, it is an ASP program written in notepad, which is used to add more security to this work. In this program, RC4 algorithm is used for Encryption and Decryption purpose. This algorithm is already a defined one, which is the popular one for web security, it is just include in this work to provide security. Function **EnDeCrypt** is used to encrypt and decrypt data between client and server. Same algorithm is used on client side.

2.5 Outputs

In this section, the sample outputs snapshots are taken during the runtime of this project. The outputs of this project are divided in to three. One, when the user login successfully, second one is for incorrect login which is further divided in to two: 1) Incorrect Login 1 2) Incorrect Login 2. The third output is when the movie starts playing.

2.5.1 Successful Login

Here user enters a valid username and password, so user login successfully. The following output snapshot shows that it is loading movies and there data, so in this user login successfully



yj

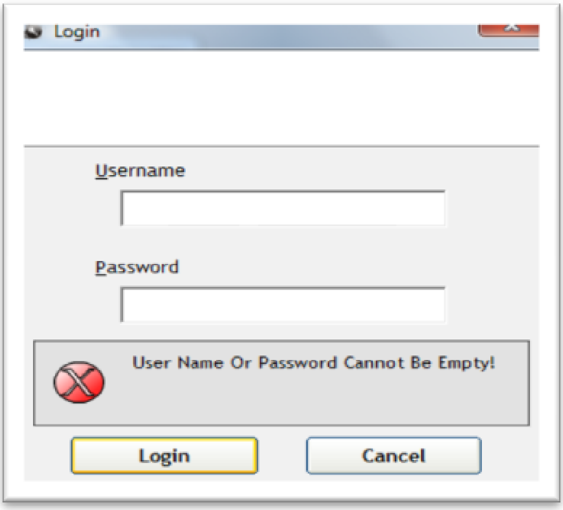
***

Loading Movies And There Data!

Figure 2: Correct Login

2.5.2 Incorrect Login 1(empty values)

If the user does not enter any values, the following output shows the same:

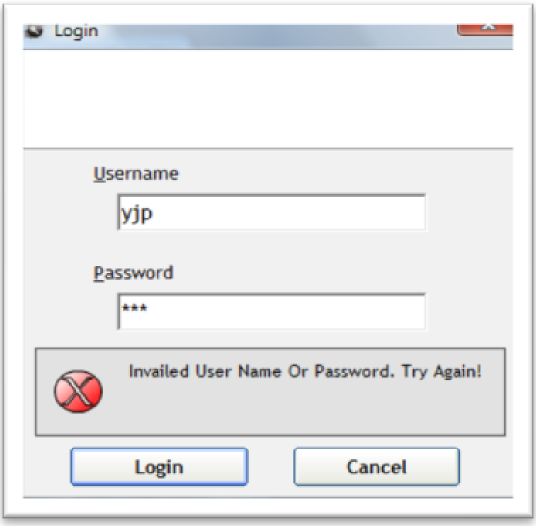


User Name Or Password Cannot Be Empty!

Figure 3: Empty values

2.5.3 Incorrect Login 2(invalid values)

If the user enters an invalid username/password, the following diagram shows the same:



Username

yjp

Password

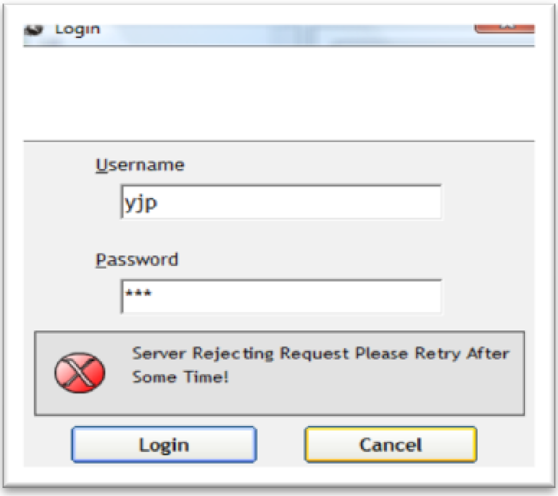
***

Invailed User Name Or Password. Try Again!

Figure 4: Incorrect Values

2.5.4 Login Rejection (exceeded invalid trials)

The snapshot below appears when user enters the incorrect username or password for the sixth time.



Username

yjp

Password

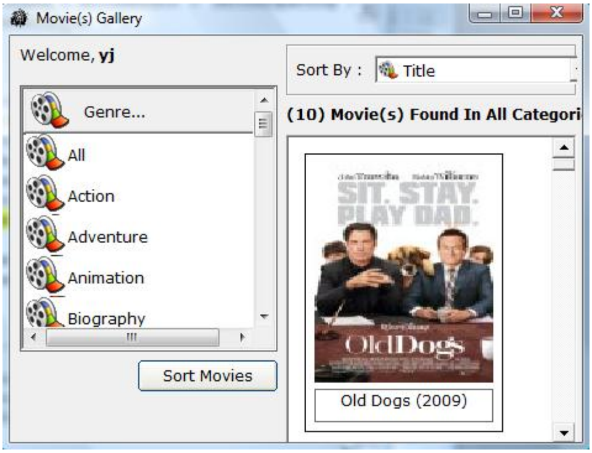
***

Server Rejecting Request Please Retry After Some Time!

Figure 5: User Rejected

2.5.5 Movie list and Categories

The snapshot below appears when user login and when the movie data are loaded:



Welcome, yj

Sort By : Title

(10) Movie(s) Found In All Categori

Figure 6: List and Categories

2.5.6 Playback Snapshot

This snapshot appears when the user clicks on a particular movie, movie playback starts in Windows Media Player:

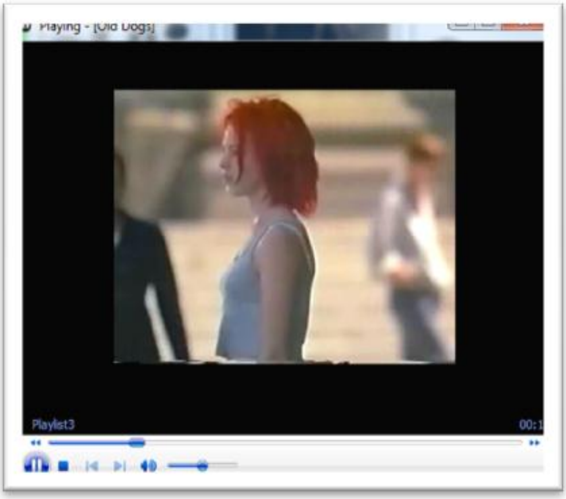


Figure 7: Playing Movie

3 Conclusions

In this paper, the different stages of design and implementation are discussed and evaluated. At the first stage of this work, the basic software and hardware requirements are found; initial tasks were identified and implemented. This includes protocols, different streaming methods, security methods that need to be implemented. Then the appropriate selection is done based on performance and robustness. TCP is the protocol discovered for this work. The second stage of the work is discussed, as the first step the final design is discovered and implemented using appropriate software or application. The different snapshots of designed form are shown. All the necessary coding is done and the necessary outputs are shown with the help of a snapshot. Final output of this work ensures high level security for the users.

I hereby conclude that this project will provide better quality and user experience. Security method implemented here is an added advantage for the users. Since bandwidth is shared in a home network, the network traffic will be less than that of the existing systems. And web server located near to client, makes the video streaming easy without much delay. In overall this project will provide good Quality of Service (QoS).

3.1 Future Works

This project is implemented using HTTP and TCP. Though TCP is more reliable protocol, it suffers from delay and jitter. So there is chance for the users to get slightly annoyed. This work can be improvised using TCP based application such as TFRC (TCP Friendly Rate Control) which supports multimedia, which is a non-TCP application. Though windows media player supports buffering and streaming, it is slightly of low video quality, can be improvised using latest media player which is of high video quality. Further the security method implemented can be improvised by using RC5 or RC6 algorithm.

4 References

Apostolopoulos, J., Tan, W. and Wee, S., (2002),*"Video Streaming: Concepts, Algorithms, and Systems,"*Mobile and Media Systems Laboratory.

Bouthillier, L. (2003), *"Streaming Video vs. Downloading Video,"* Retrieved December 23, 2009 from the World Wide Web: http://www.streamingmedia.com/article.asp?id=8456 &page=1

Holzner, S., (1998), "*Visual Basic 6 Black Book,"* Coriolis Group, ISBN: 1576102831, pg: 485-551, 581-827.

Mehra, P. and Zakhor, A. (2009), "*TCP-based video streaming using receiver-driven bandwidth sharing,"* Retrieved December 22, 2009 from the Worl Wide Web: http://www.mehras.net/pmehra/pubs/pv03.pdf

Petroutsos, E., (1998)*"Mastering in Visual Basic 6,"*SYBEX, ISBN: 0-7821-2272-8, United States of America, pg: 101-128

Schmerbeck, A., *"Streaming Video,"* Multimedia Authoring, Retrieved December 20, 2009 from the World Wide Web: http://www.edb.utexas.edu/multimedia/Streaming%20Video.pdf

Walnum, C., (1998), *"Complete Idiot's Guide to Visual Basic 6,"* Macmillan Computer Publishing, pg: 91-160.

Web Server vs. Streaming Server, Retrieved December 20, 2009 from the World Wide Web: http://www.microsoft.com/windows/windowsmedia/compare/webservvstreamserv.aspx

Section 5

Robotics

Social Learning in Artificial Embodied Agents – An Artificial Life Approach

J.Bailey and D.Marocco

School of Computing and Mathematics, Plymouth University, Plymouth, UK
e-mail: davide.marocco@plymouth.ac.uk

Abstract

In this paper we present an artificial life simulation in which a population of 10 artificial agents has to develop a simple behaviour in discriminating between two foraging areas. We show in this paper that through social facilitation, different models by which social influences are chosen and the varying of levels of influence by changing the amount of robots which can alter the rate of social learning we can produce effective results. We move on to prove how and why we believe this to happen and conclude that research into social learning should not be limited to the method by which information is acquired, but by how much can be learnt at the individual level.

Keywords

Social Learning, Social Enhancement, Learning and Evolution.

1 Introduction

It can easily be said that social learning plays a much greater role in human beings than in any other species. This is because as complex beings we exhibit learning traits like explicit imitation, and it is this reason which has lead most researchers, in recent years, to study social learning and attempt to generate specific algorithms which try to replicate behaviour by directly duplicating it.

Even though this is true, and humans do show much greater potential for social learning, simpler forms of social learning should not be ignored entirely when attempting to create social learning in agents and robots. It can be seen in various species of animals how simpler forms of social learning can be highly effective. For instance, food preferences developed by Norway Rats (Rattus norvegicus) are directly influenced by that of conspecifics by the smelling of said conspecific’s breath (Galef, 1996). Similarly, female guppies (Poecilia reticulata) have preferences for mating with males which they have seen performing the act of mating before (Dugtakin, 1996). The importance of these examples is that transmission of these behaviours is realised without the need of complex cognition, but by simple processes (i.e. the smelling of breath) that can directly influence learning at the individual level.

The development of artificial organisms, or in our case robots or simulated agents, can be a very useful way of exploring these social dynamics. Artificial life techniques can be useful when taking into account varying levels of analysis, including learning at the individual level, selective pressure at the population level, learning between individuals and learning between individuals and the environment. These factors can be difficult to analyse when relying only on research gathered by observation or laboratory experiments.

In this paper, the problem that is to be addressed is an experiment into how we select the model by which robots that have an influence on the rate of social learning in the population. The experiment will be run on an entirely social population, as it was proven that a social population is the most successful at adapting in a situation of varying environmental pressure (Acerbi et al, 2007. Marocco et al, 2007). This experiment will expand on this discovery by changing the number of agents in the simulation that have an influence on the rate of social learning in the population. Secondly, the method by which new producers are selected will be changed from being genetic inheritance in the first simulation to being based on the experience of the individual.

2 Experimental Design

To investigate the exploitation of sociality with respect to the method by which the learning model is chosen, the experimental simulation was designed to be as much the same as the experiments discussed above in the literature review section, so a comparison could be made to similar results from these papers. The environment created within the simulation is a 2000x2000mm area surrounded by walls. The area has a grey floor on which are placed two 600mm diameter circles, one coloured black and one coloured white, as shown in Fig. 1.

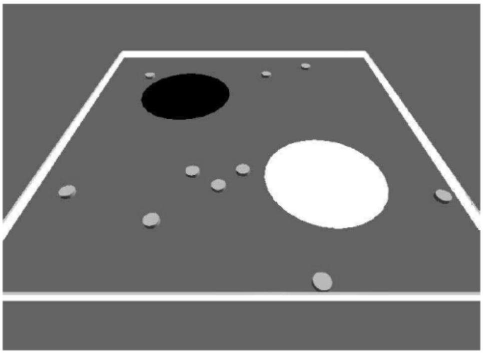
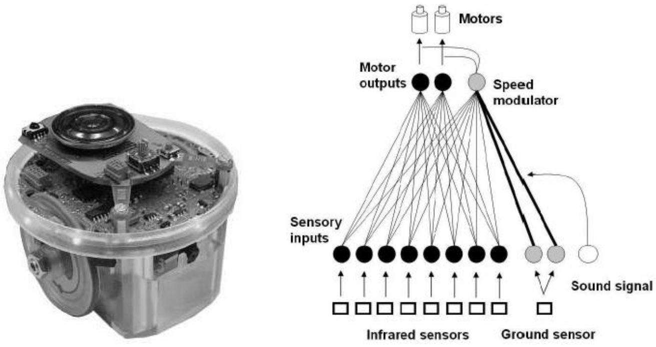


Figure 1: The simulation environment, the dots represent robots (Acerbi et al, 2007)

The population consists of 10 robots, which are simulated e-puck robots. These robots are 37mm in diameter and controlled by an artificial neural network. This neural controller consists of 10 sensory neurons and 3 motor neurons, as shown in Fig. 2(b). Eight sensory neurons encode the states of the 8 infrared sensors positioned evenly around the circumference of the robot that allow the detection of obstacles up to a distance of 40mm, and two neurons measure the activation of the ground which read the colour of the floor beneath the robot. Two of the motor neurons encode the desired speed for the robots to navigate around the area and successfully avoid obstacles, normailsed between values of +MaxSpeed and –MaxSpeed. The third neuron is used to regulate the value of MaxSpeed and allow the robot to slow down and stop within a target area. The 8 sensory neurons from the infrared sensors are connected to all 3 motor neurons and the remaining two sensory neurons that read the ground colour are only connected to the speed regulation neuron. It should be noted that the robots have no realization of the effect of the current area on their life force. They are essentially 'blind' to this and know only the colour of the area in which they reside. This means that the experience of a particular area does not provide any information about the correct behaviour that should be performed in that area. For information on the training of the neural controller please see Acerbi et al (2007).



(a) The e-puck robot.

(b) The neural controller.

Figure 2: An example of an e-puck robot and the neural controller

Each robot in the population has a genetic code that consists of two genes. The first is gene φ, which represents the current learning rate of the individual, or the amount in which social cues have an effect on how the robot modifies its behaviour. The second of which is gene ψ. Gene ψ represents the robots ability to produce sound, and can take values of either 0 or 1, 0 if the robot is not a sound producer and 1 if the robot is. All the robots have a microphone and a speaker to allow them to receive and transmit social cues between one another, while in one of the foraging areas, if the value of the robots gene ψ is 1, then its microphone will constantly emit a sound of fixed intensity. In previous experiments (Marocco et al, 2007; Acerbi et al, 2007; Acerbi et al, 2009), the social robots always produce a sound intensity of 0.1, making the maximum learning rate in a completely social population 1.0. However, in this experiment the robots are all social, and we wish to experiment with the number of robots that have the ability to produce sound. It seems unfair however that in a population which only has one producer that the maximum learning rate only be limited to 0.1, so during the simulations the maximum value of gene φ (1.0) is shared between the number of producers in the population. So in a simulation where there is one producer, that one robot produces a sound of intensity 1.0/1 (1.0), whereas in a simulation where there are 10 producers they all produce 1.0/10 (0.1) intensity.

The robots are initalised with 2000 life energy. If they should learn to adapt and survive well enough, then they will live to be over 2000 time steps old. Should this happen then every time step there is a 0.1% chance or a 1 in a 1000 chance that the robot will die of old age.

In the two different simulations, the main way in which they differ is the method by which the value of the gene ψ is passed within the population. In one simulation the initial amount of sound producers, depending on the number in the parameters, is chosen randomly from amongst the population. From there, whenever a sound producer dies, the gene value is passed directly onto the offspring. In the other, it is designed so that the eldest robots in the population are always the sound producers. We define the eldest robots as the robots that have the greatest lifecycle, i.e. the robots that have been alive for the largest amount of time steps. Again, the robots are initiated with random position and orientation. When a sound producer in this simulation dies, the gene passes onto the oldest robot in population that is not a producer. This way the oldest robots in the population are always robots with a gene ψ value of 1.

3 Results

Figure 3 shows the overall average mortality for the two models of social facilitation.

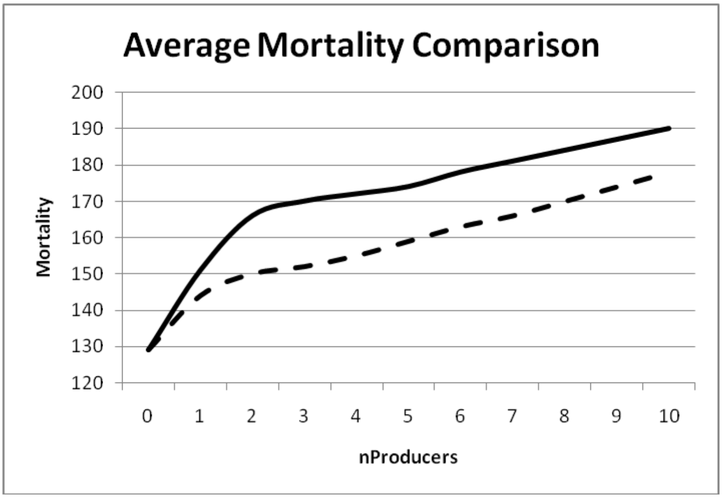


Figure 3 - A graph of the average mortality comparison for all simulations. The solid line represents the simulations where the gene ψ is hereditary, and the dashed line represents the simulations where the eldest robots influence the learning rate.

It was hypothesised before the experiment that when the population has the maximum number of social influencers the performance between the models would be very similar, possibly even identical. This was thought because the simulations are initalised in the same way (randomly placed robots outside the foraging areas and all population members as producers). Then the method by which the new producers are selected becomes essentially the same through both mechanisms, and we have an identical simulation. This should provide a useful control group between the experiments. During the experiment this was proven to be true.

It was also hypothesised also that the performance between social modes would trend towards the model for experience because after a certain point in each simulation all of the eldest robots would be in the positive foraging area. This means that the producers would be constantly in the white area after this point and the other robots would learn to adapt to it quicker. This should mean that the mortality for this model should be overall less than that of the genetic inheritance model.

This trend can be seen in Fig. 3. This graph shows us that with the exception of the condition where the black area has the same pressure as the white area, so 0 energy loss, that this hypothesis is true. This indeed proves that in overall performance, the condition where experience relays the rate of social learning between the populations is definitely more successful at adaption to the environment than the condition where the gene value is hereditary. It should be mentioned that the differences between these two social models are statistically significant, to a rate of $p<0.001$. The only conditions which are not so are the ones which we would expect to be so, when all the robots in the population have social influence and for all values of environmental pressure where this is the case. And in other cases where there is no environmental pressure from the negative foraging area.

The trend of the results for inheritance of gene ψ is very clear and concise. A quick rise in mortality for the control simulations where the energy loss of the black area is equal to either that of the white area or the grey area, and from the point where it is greater than these, where the energy loss is 2 or greater, the quick increase stops and becomes a linear trend as the environmental pressure becomes greater, due to the increase in speed from which robots adapting to the black area die.

The trend of results from the model for experience does have a slight discontinuity though. The line would form a near linear increase from the beginning of the experiment if it was not for a slight rise in mortality between 1 and 3 energy loss. This is due to the counter-adaptive behaviour which we expected from this trend, where the energy loss in the negative foraging area is not great enough to kill the robots before they have a chance to become producers, and therefore the robots have chance to adapt to the black area before finally only adapting to the white area, and linear trend can begin.

This theory of counter-adaptivity can be proven by reviewing the amount of time spent by the producers in the positive and negative foraging areas, compared to situation of higher environmental pressure. These results are shown below in Fig. 4. These results are once again taken from the average of the same 100 trials by which we came to find the other results.

These results are calculated by counting the number of producers that die in both the black and white area, while counting the total amount of time steps producers spend in either area. When this has been counted, the total time steps is divided by the number of producers which died in that area which gives us an average time spent by producers in that area.

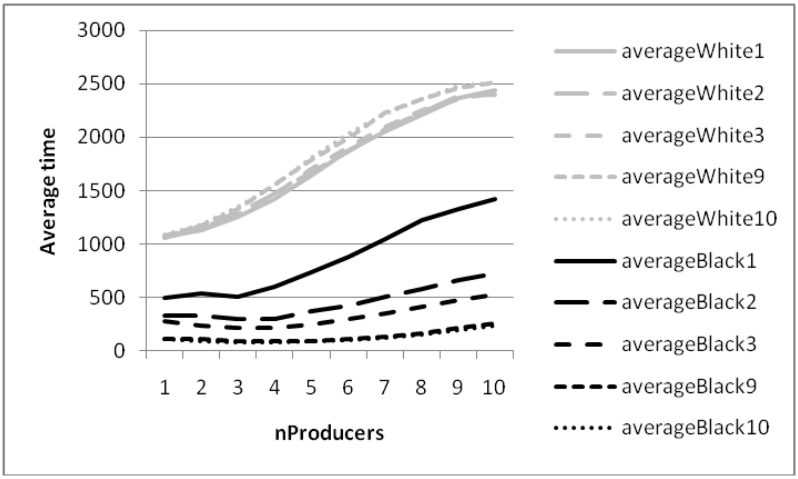


Figure 4: A graph showing the average time spent by producers in both areas for varying selective pressure.

From these results we can see a very clear trend. In the conditions of lower environmental pressure, the average amount of time spent by social influencers in the black area is much higher throughout different amount of influencers than in situations of higher pressure. Acerbi et al (2007) state in their paper that this counter-adaptive behaviour is due to the ‘blindness’ that each robot has to effect that the area in which it currently resides has on its life force. This proves that the rise we see in mortality for these social conditions is due to the counter-adaptive behaviour which we expected.

It is from this that I suggest that organisms which have a higher level of cognition could avoid this. However, as in the case mentioned above (Galef, 1996), Norway Rats could for example learn to eat food that is not good for them, as they could see a conspecific consume the food, but any visible ill effects of consuming this food may not show for hours afterwards, this could be assumed as a lesser value of environmental pressure, whereas seeing a conspecific eat something deadly, rat poison for example, would not copy its fellow because the bad effects would be immeadiate. This could be an example of higher environmental pressure. It would also be assumed that the rats would be more likely to pay attention to what an older member of the population consumes as they have survived the longest and would have a better idea of what is safe to eat. As in our situation where the robots survive better listening to other robots who have lived for the longest.

4 Conclusion

It has been demonstrated in a simple experimental scenario how the model by which influence on the rate of social learning passes from one robot to another in the population, whether it is by genetics or by experience, can effect adaption to the environment and social facilitation within the population. It should be noted that here social learning is not the advanced form of social learning which we see in humans and life forms with higher cognitive abilities, but a simple method by which a number of members of the population have a small, or in some cases large, influence on the speed at which the other members of the population learn.

It is also worth mention that it is not only populations with larger amounts of social influence that adapt and survive best. Due to a counter-adaptive behaviour produced in some conditions, it can be seen that sometimes a population where one robot holds all the social influence in the population can be more successful than one where all robots have a small influence on the rate of social learning in the population. It is believed that some forms of what we refer to as social learning are the outcomes of such social dynamics and artificial life simulations are an important tool by which to test them.

There is of course plenty of further research to be done in this field. For example, it could be said that no one has deeply considered the role of the learning rate and how its strength impacts the adaptively of the learning process, by which we mean, is it always the best solution to learn faster? It said in Kriesel, (2007) that a higher learning rate when training an artificial neural network can lead to a state of over-learning, can this theory also be applied to the learning rate of our populations?

It is also planned to do research into the how the number of foraging areas in the environment can affect the adaption and social facilitation of the robots, we can achieve such results by either increasing the number of foraging areas or altering the number of robots in the population. Even changing the environmental conditions as the simulations runs could make a difference to the behaviour of the agents in the trial.

The hope is that our research leads to a bigger investigation into this field after we have constructed basic theories into these behaviours and that others will step in and help develop the specifics which are considered to need attention, possibly also in relation to human ontogenetic development.

5 References

Acerbi, A. Marocco, D. (2009) Orienting Learning by Exploiting Sociality: An Evolutionary Robotics Simulation. In: *International Joint Conference on Neural Networks, 2009*. Atlanta, GA. pp. 20-27.

Acerbi, A. Marocco, D. Nolfi, S. (2007) Social Facilitation on the Development of Foraging Behaviours in a Population of Autonomous Robots. In: Almeida e Costa, F. Rocha, L. Costa, E. Harvey, I. Coutinho, A. *Advances in Artificial Life. Proceedings of ECAL 2007*, Berlin: Springer, 2007, pp. 625-634.

Coussi-Korbel, S. Fragaszy, D. M. (1995), On the Relation Bewteen Social Dynamics and Social Learning. In: *Animal Behaviour*, 1995, pp. 1441-1453.

Dugtakin, L. A.(1996) Copying and mate choice. In: Heyes, C. M., Galef, B. G. Jr. (eds.): *Social Learning in Animals: The Roots of Culture.* Academic Press, San Diego (1996) pp. 49-64

Galef, B. G.(1996) Social enhancement of food preferences in Norway Rats: A Brief Review. In: Heyes, C. M., Galef, B. G. Jr. (eds.): *Social Learning in Animals: The Roots of Culture.* Academic Press, San Diego (1996) pp. 49-64

Kriesel, D. (2007), *A Brief Introduction to Neural Networks*, available at http://www.dkriesel.com

Laland, K. N. (2004) Social learning strategies. In: *Learning & Behaviour 32* 2004, pp. 4-14.

Marocco, D. Acerbi, A. (2007) Adaptation and Social Facilitation in a Population of Autonomous Robots. In: Berthouze, L. Prince, C. G. Littman, M. Kozima, H. Balkenius, C. Eds, Lund: *Proceedings of the Seventh International Conference on Epigenetic Robotics,* LUCS, 2007.

van der Post, D. J. Hogeweg, P. (2006), Resource Distrbutions and Diet Development by Trail-and-Error Learning. In: *Behavioral Ecology and Sociobiology 61, 2006, pp. 65-80.*

Nolfi, S. Floreano, D.(2002) Synthesis of Autonomous Robots Through Evolution. Trends. In: *Cognitive Sciences, 6(1)*: 31-37.

Schwab, C. Bugnyar, T. Kotrschal, K. (2008), Preferential learning from non-affiliated individuals in jackdaws(Corvus monedula). In: *Behavioural Processes 79* 2008, pp. 148-155.

Face Detection for ButlerBot

J.Durand and G.Bugmann

Centre for Robotics and Intelligent Systems, Plymouth University, Plymouth, UK
e-mail: G.Bugmann@plymouth.ac.uk

Abstract

In the same way that human beings use eyes to analyse the world around, a robot will use stereovision to evolve in its environment. This thesis presents a complete system of stereovision that provides a highly accurate map which identifies the presence of people in a room. The system uses a new method to find points of interest for the stereovision algorithm. Rather than using intensity of images to find points of interest, as is usually the case, this method directly uses faces that are present in the image. The system thus uses a face detection program included in the OpenCV library, famous in the world of vision. Another part of this thesis presents an algorithm for designing paths, tailored specifically for ButlerBot. This algorithm allows the ButlerBot to move in a room populated by individuals, to serve all people beverages.

Keywords

Stereo-vision, Face detection, points of interest, Map, path planning, OpenCV, I²C Serial, correlation.

1 Introduction

Robotics today encompasses a wide range of applications particularly in industry, in the areas of research. The current development of robots is to make robots more autonomous and intelligent, they can, contrary to basic industrial robots, perform numerous tasks simultaneously and think by themselves to interact with their environment.

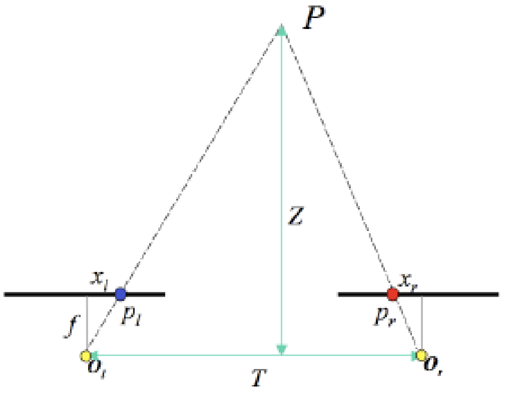
The ButlerBot project, has been led by the School of Computing, Communications and Electronics of Plymouth University in 2006, and is the brainchild of Peter White, which has been interpreted by Guido Bugmann. Butlerbot should be completely autonomous and able to bring drinks for groups of people during receptions. In addition to many sensors, ButlerBot has two webcams that allow a good interaction with the users. Currently, the ButlerBot robot is equipped with a Toradex board. Unfortunately this board is not powerful enough and not fast enough to properly handle the stereovision.

2 Stereovision

The stereovision is defined as a process giving the impression of relief from a couple of images recorded at different points of view. In particular, binocular vision is the interpretation of two distinct views of the scene to resolve the ambiguity of depth. In humans, for example, both eyes are separate a few inches and see, therefore, two very similar but different images from the same scene. It is in this same small separation that gives us the information needed to reconstruct the lost dimension. The more the point is closer to us and more its projections on the two retinas are become remote. The extent of this relative distance allows our brain to estimate the coordinates of the triangulation point in space and appreciate the relief. A computer that receives images taken by two cameras will do the same.

Three important steps are needed to define the position of a point in space, using stereovision. At first the image capture, it is necessary to take a minimum of two views of the same scene from two views side by side by two identical cameras, this requires that the captures are well synchronized. Then the most difficult and time consuming task for a stereo vision system is the identification corresponding pixels between the left image and the right image and it is called correlation. At first it is necessary to identify the points of interest on the images. The most commonly used method detects the pixels that have the greatest intensity. The best method to detect pixel intensity is the Haris detector (Harris and Stephens, 1988). Once points of interest have been detected, it is time to find the correlation between these points. The correlation algorithms most commonly used are SSD(Sum Square Difference) and ZNCC(Zero Mean Normalized Cross Correlation).

Once we know which pixels on the right image correspond to the pixels on the left image, it is easier to find the distance between the pixel and the camera. Knowing the focal distance of the camera, the distance between the optical centres, and a simple calculation of triangulation allows us to find out the depth (Forsyth and Ponce, 2002).



$$\frac{T + x_r - x_l}{Z - f} = \frac{T}{Z}$$

$$Z = f\,\frac{T}{x_l - x_r}$$

$$d = x_l - x_r$$

$$Z = f\frac{T}{d}$$

Figure 1: Triangulation calculates.

3 Maps and path planning

Any robot that wants to move in an environment by following a planned path needs to have a map. Displacements may be multiple - movement of a robot on the floor, or a robotic arm that moves in a three dimensions space. There are different kinds of maps; the most commonly used are the metric maps. The metric maps are grid maps with cells that are either occupied or free. There are also topological maps containing nodes and links between nodes. The nodes can represent locations, contact information, and rooms. The links may contain distances, route descriptions and time travel. Mathematical topological maps are called graphs (theories of graphs).

the goal is to see the different ways that the robot can get to from one point to another. Assuming that the robot has an accurate map of the environment and that it knows all the points in which it must go, there are many algorithms to determine the most optimized way among all these points. The visibility graph is an algorithm that can convert metric maps to graphs. The objects are converted to polygons; angles of polygons become nodes of the graph, and nodes are connected together by a straight line whenever possible.

Voronoi diagrams are another way to divide space. A Voronoi diagram is generated from a set E of points, called sites or nuclei, in the plane. Each E point is inside a convex polygon, which delimits a surface formed from the design points that are closest to this site from other sites. Voronoi diagrams are very useful structures - it is not surprising to see them used to model crystals or large structures in the universe. They can be observed in nature, e.g. on the carapace turtle or neck of a giraffe. Voronoi diagrams are also data structures to solve many problems such as finding nearest neighbours and motion planning.

4 Hardware implementation

As explained in the introduction, one part of the project was to replace the Toradex board with a more powerful system to handle the processing of stereovision.

For reasons of portability of the project, and the combination of the need for high power, it was chosen to use a laptop. The computer will have additional freedom in terms of programming, and the use of library, but the disadvantage is the Windows XP operating system does not allow for real-time programming. We must, therefore, be careful in the orders sent and with some control signals, particularly to the motors.

The Toradex board communicates with the robot via an I2C communication, and via serial communication. The laptop has only USB communication ports, it also had to buy converter modules, one I2C-USB converter and one USB-SERIAL converter.

5 Software implementation

This program should work on a laptop, so it was chosen to develop this program with Microsoft Visual Studio 2008 Professional Edition in C language.

The software has two main parts a main function and a thread. The thread watches the status of sensors, and updates a flag according to their statements. This will allow the main function to act accordingly.

The main function is divided into four different parts. The first part is the initialization for camera, opens communication ports, and 2D map. Then, the second part is that the robot looks around to find a visible person in order to create a map. The third part is to move the robot towards people found on the map. And finally the last part is the function that communicates with the Atmega board, which controls the engines.

6 Results

6.1 Face detection

Finding points of interest is an important part of stereovision and generally the intensity of pixels of the image is used. The innovation in this project is that these points of interest are in fact the centre of each face detected on images.

At first the function finds rectangular regions in the given image that are likely to contain objects that the cascade has been trained for, and returns those regions as a sequence of rectangles. The program used a cascade trained for face detection with Viola Jones algorithm (Viola and Jones, 2001).

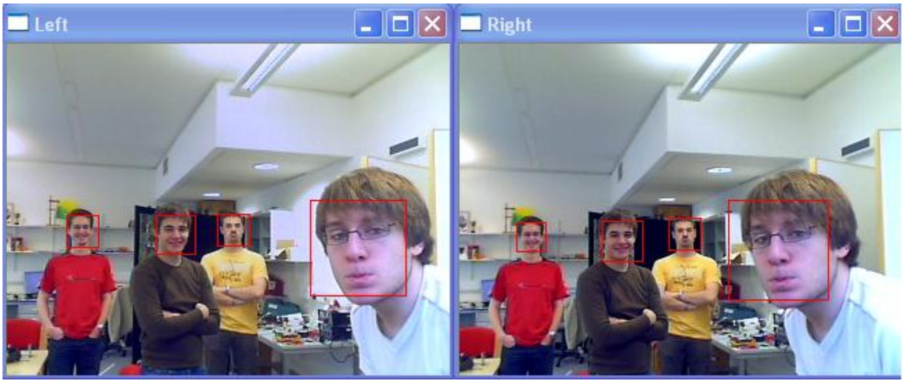


Figure 2: Face detection with Viola Jones algorithm.

6.2 Correlation and cost matrix

The correlation function of the program uses a dynamic cost matrix to save the values. A calculation allows comparing of the faces in the image on the left and right and to compare their height in the image. A high percentage (costY) is attributed to two faces that are on the same horizontal line and a low percentage for faces very sparse.

$$costY = \frac{images\_height - (y1 - y2)}{images\_height}$$

Images_height represents the total height of the image, y1 and y2 represents the ordinates of the point of interest, respectively, for the left and right images.

Similarly, the width and height of faces are compared to each image.

$$\mathrm{costWidth} = \frac{\mathrm{images\_height} - (\mathrm{width1} - \mathrm{width2})}{\mathrm{images\_height}}$$

Then a first filter removes the percentages that are too low.

$$cost = \frac{\mathrm{costY} + \mathrm{costWidth} * 0.5 + \mathrm{costHeight} * 0.5}{2}$$

if (cost<0.95) cost=0 else cost=1

Then finally, the value is stored in the matrix (see Figure 2.3.4).

costMat[][]=cost

It is possible to have two faces of the same size placed on the same horizontal line. To differentiate between these two images aligned, another filter use the horizontal shift between the faces of the left image and right and with a simple comparison, it is possible find which are the corresponding pairs of faces. A final filter check determines whether each column of the matrix contains only one value, if not, the filter puts the entire column to zero.

6.3 Depth by triangulation

In order to detect people in space within a room, one must apply simple trigonometry calculations.

$$Z = \frac{T * focal}{disparity} = \frac{T * f}{disp * pixel\ Size} = \frac{T}{disp} * \frac{f}{pixel\ Size} = \frac{T}{disp} * C$$

C is the constant of intrinsic parameter of the camera (C=34.00). The distance between the two optical centres T is 70mm. The disparity (disp) is the difference on the horizontal axis between the pixel in the left image and the right image.

6.4 Maps and path planning

All points corresponding to the faces detected are recorded and placed on a virtual metric map. This map allows the robot to record points in a perimeter of 10m2. This map is then displayed on a window on the laptop in real time thanks to the OpenCV library.

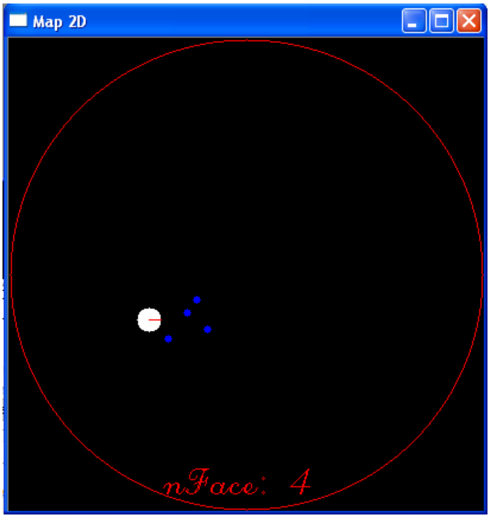


Figure 3: Virtual map 2D.

The idea of this algorithm is to move toward the group of people closest to the robot, then mark this location on the map by an area of one square meter. Thus the robot will know that this group has already been served.

Then the robot deviates slightly (one meter) from one of the groups, to scan the room again to find other faces and update its map. Then it repeats the same work, excluding the marked areas. When all the faces detected have been served, it returns to its starting point and clears all marked areas.

It is important to note that throughout its movement and rotation, the robot looks at the status of different sensors, and acts only in cases defined.

7 Conclusion

This project was proposed to give to the ButlerBot the sense of sight, so that it can independently move in a room to accomplish the task of serving beverages to people.

Various researches on stereovision allowed enormous amounts of progress to be made in intelligent vision over the last twenty years. Thus the world of robotics is now able to interact with its environment more accurately.

In this project a new method was tested to find the positions of people in a 3D space. This method shows good results, even if some points of the algorithm are still improving. The OpenCV library, with its simplicity of use, computational speed, and its robustness proved its power.

To complete the project ButlerBot to this end, future projects could improve the detection of faces and create a more efficient path planning system, with better management of sensors. Another project could be to remove the Atmega board to control the entire robot with the laptop.

This project is the result of a long time of work, which is soon coming to its end; it has helped participate in the process of development of the ButlerBot on its road to autonomy.

8 References

Forsyth, D.A. and Ponce, J. (2002), Computer Vision: A Modern Approach, Prentice Hall Professional Technical Reference,pages 321-344, ISBN:0130851981.

Harris, C. and Stephens, M.J. (1988), “A combined corner and edge detector”, In Alvey Vision Conference, pages 147–152.

Viola, P. and Jones, M. (2001), “Robust real-time object detection”, ICCV Workshop on Statistical and Computation Theories of Vision.

Bipedal Robot: Gaze Stabilization

R.K.Kozhissery and P.Culverhouse

Centre for Robotics and Intelligent Systems, Plymouth University, Plymouth, UK
e-mail: phil.culverhouse@plymouth.ac.uk

Abstract

The gaze stability is a requirement for steady image capture in locomotion. The idea of gaze stability came from animals. This research concentrates on the vertical movements of the eye in order to compensate the tilting of the eyes due to locomotion. The goal of this research is to develop a simple model for the gaze stabilization of the eye, which does not require much processing.

Keywords

Field Programmable Array, Pulse Width Modulation, VHSIC Hardware Description Language

1 Introduction

The goal of gaze stabilization is to maintain the eyes to stare at the fixed point, even during motion. Gaze stability is required for vision based processes and motion control for biped robot. Gaze stabilization is important for high resolution vision, mathematical simplification of the vision process and for facilitating stereo fusion (Coombs, Brown 1991).

The bunny robot platform is used for the research. The objective of this research is to develop a simple design, which can replace the present complex designs to maintain the gaze stability of the bipedal robot during locomotion. This paper deals with the different stages of designing the hardware for the gaze stabilization process in the bipedal robot. The bunny robot is used for this purpose. The sine relation of the accelerometer output and the corresponding degree has to be replaced by a simple equation which does not require much processing stages and the FPGA, the main control used for gaze stabilization also has to give control signal to the servo to compensate the tilt. This research utilizes the Quartus ii platform to design FPGA in VHDL.

2 Designing

Locomotion is linked with coordinated limb, body, head and ocular movements (Crane and Dmer 1997; Hirasaki et al.1999; Inmam et al.1981; Maurer et al. 1997; Mergner and Rosemeier 1998; Moore et al. 1999; Winter et al.1993). The idea about the design of gaze stabilization arrived from the natural gaze stabilization of animals. In animals The vestibulo-ocular reflex (VOR) and otolith-ocular reflex systems rotate the eyes to compensate the head and body motion that is detected by the vestibular and otolith organs in the inner ear (Coombs, Brown 1991). By imitating this functions the developed design should be able to do

1. Detection of tilt of robot with respect to the plane of earth
2. Find the angle to be rotated to compensate the tilt
3. Action to compensate tilt due to motion

This research is done on a mobile humanoid robot, the bunny robot. So it requires light weight and low power consuming hardware. The MXD2020E/F accelerometer is used for detecting the tilt of the robot. FPGA EP3C25F256C8 from the cyclone III family acts as the control and it control the SuperTec Digital Titch-44 servo motor of the eyes according to the signal from accelerometer.

For each axis, eye needs each motor. So each eye requires two motors for x and y direction tilts. For the experimental purpose, this research concentrates on vertical movement of the eye. So the devices have to be selected according to the requirement.

2.1 Accelerometer output

The output from the accelerometer is in the pwm format. It has to be decoded to find out the pulse width.

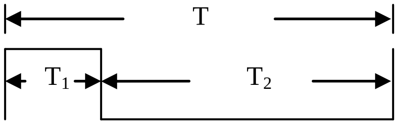


Figure 1: Accelerometer output

Where the output of the accelerometer can be related to A(g) by the equation,

A(g)= $(T_1/(T_1 + T_2 -0.5)/ 0.2$ -----------------------------(1) (MEMS 2007)

The accelerometer as gyroscope out binary signal with a pulse width varies from 1ms to 2ms. This pulse width has to be calculated from the binary signal and to be converted to terms of degree. The table 1 gives the observed data set of changes in tilt for X axes. These values are plotted to a graph with degree on X axes and X output in g in Y axes. From 0^o to 40^o the graph shows linear relation, thereafter it gradually becoming constant. So the gyroscope is more sensitive between 0^o and 40^o. This property can be used to resolve an equation for converting the Gyroscope output to terms of degree. The table 1 gives sine relationship. The X(g) = sin (X(degree)). But the implementation of sine function in FPGA is complex and time consuming. Implementation of look up table is also requires complex steps. So the linear relationship of the graph is explored for finding the angle from the output of accelerometer.

X Axis orientation to earth's surface (deg.)	X output (g)
90	1
85	0.996
80	0.985
70	0.94
60	0.866
45	0.707
30	0.5
20	0.342
10	0.174
5	0.087
0	0

Table 1: Changes in Tilt for X axis (MEMSIC 2007)

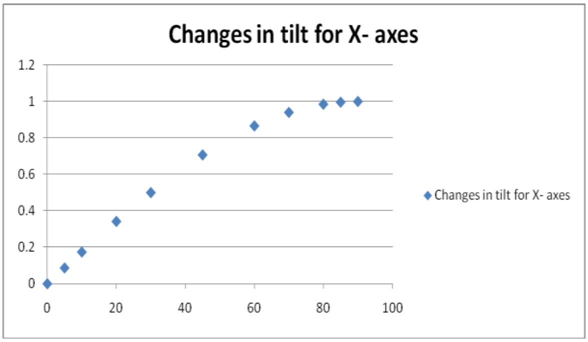


Figure 2: Graph plotted from table 1 with accelerometer output in y axis

Solving the linear property with values in the table 1, an average slope value of 0.017 can be find out for the angle 0 ^{o} to 30^{o}.

Degree = A(g) / 0.017 --(2)

After 30^{o}, it losses the linear relationship. So further part of the graph has to be solved with a different method. When the same graph is approached with the accelerometer output in x axis, and degree in y axis some of the parts of it represent the properties of parabola. So the remaining graph is divided into the parts of two parabolas and the constants with respect to those parts are found out.

From 30o to 70o the relation is considered to be the portion of first parabola. From 70o to 90o the second parabola piece is considered. In order to derive the equation, the constants a, b and c for each parabola has to be find out. For first parabola: from 30 to 70

$y= a_1x^2+b_1x+c_1$ -- (3)

when y = 30; $30 = a_1 0.5^2 + b_1 0.5 + c_1$ ------------------------------------ (3.a) when y = 45; $45 = a_1 0.707^2 + b_1 0.707 + c_1$ ---------------------------------- (3.b)

when y = 60; $60 = a_1 0.866^2 + b_1 0.866 + c_1$ --------------------------------- (3.c)

solving these three equation the constants $a_{1,}$ b_1 and c_1 can be resolved as

$a_1 = 59.618$; $b_1 = 0.532$; $c_1 = 14.83$

like the first parabola, the second parabola constants also can be found out by applying the values in the table to the equation $y= a_2x^2+b_2x+c_2$ -------------- (3)

when y = 70 ; $70 = a_1 0.940^2 + b_1 0.940 + c_1$ ------------------------------- (4.a)

when y = 80 ; $80 = a_1 0.985^2 + b_1 0.985 + c_1$ ---------------------------------- (4.b)

when y = 85 ; $85 = a_1 0.996^2 + b_1 0.996 + c_1$ --------------------------------- (4.c)

solving these three equation the constants $a_{2,}$ b_2 and c_2 can be resolved as

$a_2 = 4197.08$; $b_2 = -7854.82$; $c_2 = 3744.99$

Finally with three derived equations, the value of angle can be found out from the output of accelerometer.

From 0 ° to 30°, Degree = A(g)/ 0.17 -- (5)

From 30 ° to 70 °, Degree = $59.618\ A(g)^2 + 0.532\ A(g) + 14.83$------------ (6)

From 70 ° to 90 °, Degree = $4197.08\ A(g)^2 – 7854.82\ A(g) + 3744.99$--- (7)

2.2 Servo control

The servo requires a signal with the period of 20ms. The servo rotates 180°, when the pulse is 2ms long and 90 °, when it is 1.5ms. . So a change of ± 90 ° can be done with ± 0.5ms. From this relation the change in pulse width required for one degree can be find out as 5.556 microseconds. For more accuracy of detection and correction 1 microsecond is taken as the minimum pulse width, which response to a change of 0.18 °. So the calculated degree value can be converted to terms of how many microseconds by the equation:

N microseconds(change in degree) = (degree / 0.18) microseconds ----------(8)

When default N is 1500. Then it is equal to 1.5 ms, which is the required pulse for rotating the servo 90 °. The servo is always maintained at 90 ° with respect to the platform of the accelerometer. For other angles the N microseconds(change in degree) has to be added or subtracted to change the pulse width to servo.

N micro seconds (required pulse width)= 1500 ± N microseconds(change in degree)------(9)

The sign of the degree value determines the direction of turn of the servo.

2.3 Design

The design has two blocks ‘gyro_to_pwm’ for decoding the output of accelerometer and ‘pwmunit’ for outputting required signal to the servo.

2.3.1 ‘gyro_to_pwm’ block

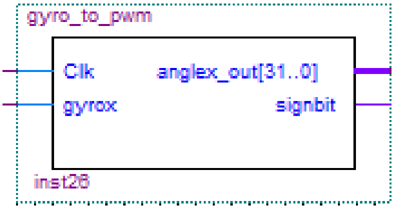


Figure 3: ‘gyro_to_pwm’ block

The accelerometer reading is given in the form of pulse width modulated signal. This signal width has to be identified and converted to corresponding angle in degree. In the gyro_to_pwm block the output of the accelerometer is converted to the terms of degree. The block is run by a 50 MHz clock. There are three inputs and two outputs for this block. Where one output and one input is for later expansion of the program. The converted angle in degree is outputted in the 32 bit signed format. There are 5 variables used in Architecture. These entire variables are initialized as zero. The variables t1x are t2x are acting as counters. T1_x and T2_x acts a storage variable for storing the final values of t1x and t2x respectively. The variable g_x stores the calculated integer value of angle in degree. The output level of accelerometer has to be checked in each clock cycle. The pulse width and period is find out using the variables t1x and t2x. Thus in each clock cycle, corresponding variable is incremented. After detecting the first ‘0’ after ‘1’, the value in t1x is passed to T1_x and t1x gets initialized. For the first ‘1’ in each period the value in t2x is passed to T2_x and t2x gets initialized. So T1_x contains the pulse width value and sum of T1_x and T2_x gives the period of the accelerometer output. This process continues until the program runs in the robot and accelerometer continue to give the output.

The period of the accelerometer is 10 ms from the observation of the output. The A(g) is calculated first and its values are compared with the values with respect 30 ^{o}, 70 ^{o} and 90^{o} by applying the equations (5) (6) and (7) respectively. The calculated angle value is assigned in the variable g_x and converted to 32-bit logic and passed to the ‘pwmunit’ block. A sign bit, s also out to represent the direction of tilt.

2.3.2 ‘pwmunit’ block

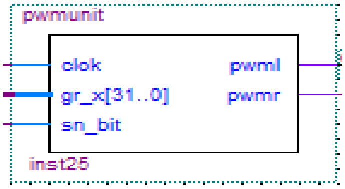


Figure 4: ‘pwmunit’ block

In this block the angle of tilt from gyro_to_pwm is inputted and this value is converted to number of microseconds required for that tilt. The observation reveals that the accelerometer is fixed with a tilt on the bunny. Moreover the tilt of the platform it situated also effects the default angle. It can be varied from 22 to 27. 27 is taken as the default angle. The equation (9) is applied and the value is stored in the variables oxl for the left and right eye. So the default value 1350 is used. The variables c1and c2 act as inbuilt timers. c1 increments in each clock cycle. So c1 gets incremented in each 20 nanoseconds. The sensitivity of the reaction of motor with respect to the accelerometer signal is manually limited to 1 microsecond in the program. 50 clock cycles is equal to 1microseconds. When c1 becomes 50, the variable c2 is incremented and c1 gets initialized. c2 give the number of microseconds; ie N . The signal in pwml and pwmr will ne high until the count of c2 reaches oxl.

2.4. Results and Analysis

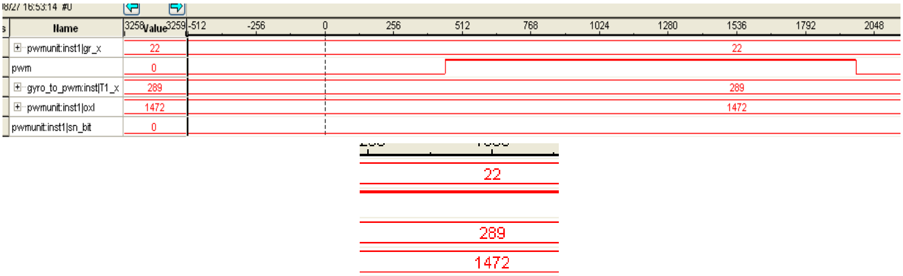


Figure 5: Precision of the system with positive sn_bit

An overall analysis of the input from accelerometer to the output of servo can be done with the above signal tap view. T1_x gives the pulse width of the signal from the accelerometer. It can be substituted in eq (1) to get the value of A(g). Here T1_x is 289.

So A(g) = ((289/500) – 0.5) / 0.2 = 0.39

This value is less than 0.5. so linear relationship is used to find the angle. Angle in degree = 0.39 / 0.017 = 22.9 ≈ 22 (due to truncation to integer, the floating part gets cancelled.)

The calculated angle is same as the observed angle in the figure as gr_x. its sign is also positive. So sign bit will be zero. The sn_bit indicates zero. In the pwmunit the angle value is converted to change in number of microseconds required for the pulse width of servo to compensate the tilt.

Change number of microseconds required = 22 / 0.18 = 122

When sign bit is positive, the above value is added for the left eye and subtracted for the right. Here the left eye value is indicated.

Total number of microseconds required to get required tilt = 1350 + 122 = 1742

The observed value of oxl also gives 1742.

The accelerometer output was decoded at the same moment, when the signal falls to low. These are converted to the angle values with the help of derived equations. The observation of the working of the design shows that the combined action of linear equation and two parabola equations gives accurate angle values for the tilting of the robot. These values were same as that of actual calculated values except the fractional part. The designed system effectively responds for all the angle of tilt detected by the accelerometer. The observations exhibited that the observed value and the actual value are approximately same with a maximum tolerance of ±0.9. The maximum delay observed from the design is 20.2 microseconds.

One of the defects of this design is the presence of an error signal in between the original values, which is originating from the calculation of the width of pulse from the accelerometer or from the accelerometer output itself. The accurate reason of this error pulse is not identified yet.

3 Conclusion

The objective of this research was to develop a simple model for gaze stabilization. The design developed is capable of giving the same output in the hardware as well as from the theoretical point of view. So it is easy to compare the results of this design and find the errors, if there is. The main part of research was to develop a new solution for converting the output of accelerometer to an angle value in degree, where its real relation is sinusoidal. This was solved with the help graphical representation of the sine values and with the help of basic geometry. This replaced the requirement of sinusoidal function in the design. Moreover the model developed for gaze stabilization in this research is simple and compact. It is easy to add new features to this design.

The precision of this model can improved in the future works by improving the arithmetic calculations. The vergence control of the eye also can be added to this design for better performance. The exact source of the error signal has to be identified and eliminated. But compared to the advantages of this model, the only dis advantage is the presence of error signal and it can be rectified in future works.

4 References

Coombs, D.J, Brown, C.M, (1991), "Cooperative Gaze Holding in Binocular Vision", *IEEE*

Crane, B.T, Demer JL (1997) "Human gaze stabilization during natural activities: translation, rotation, magnification, and target distance effects", *Journal of Neurophysiol* vol:78, pp2129–2144

Hirasaki, E, Moore, S.T, Raphan, T, Cohen, B (1999) "Effects of walking velocity on vertical head and body movements during locomotion" Exp Brain Res 127, pp117–130

Inman, V.T, Ralston, H, Todd, F (1981) "Human walking" Williams and Williams, Baltimore

Mergner, T, Rosemeier, T (1998) "Interaction of vestibular, somatosensory, and visual signals for postural control and motion perception under terrestrial and microgravity conditions – a conceptual mode". Brain Res Rev 28, pp118–135

Moore, S.T, Hirasaki, E, Cohen, B, Raphan T (1999) "Effect of viewing distance on the generation of vertical eye movements during locomotion" Exp Brain Res 129, pp347–361

Winter, D.A, MacKinnon, C.D, Ruder, G.K, Wieman, C (1993), "An integrated EMG /biomechanical model of upper body balance and posture during human gait. In: Allum JMJ, Allum" Macklenburg DJ, Harris FP, Prohst R (eds) Progress in brain research. Elsevier, Amsterdam, pp359–367

New Titch44 Servo Controller

V.Mérelle and P.Culverhouse

Centre for Robotics and Intelligent Systems, Plymouth University, Plymouth, UK
e-mail: phil.culverhouse@plymouth.ac.uk

Abstract

The aim of this paper is to present the results of an MSc Robotics thesis on the new design of a small servo controller with a permanent ironcore DC motor. In a first paragraph it will explain the control method chosen to control the motor in position an presents the simulation. The other section will focused on a new rotary Hall Effect chip available since last month. The last section will discussed about the architecture of the software.

Keywords

Control theory, DC motor, PID Controllers, rotary Hall effect sensor, Bunny Robot, microcontroller, ATmega16, SPI connection, bioloid bus, embedded software, rotary Hell Effect sensor, AS5055, serial connection.

1 Introduction

This paper is related to an MSc robotic thesis on the new controller for a servo controller of The Bunny robot (Culverhouse et al. 2004) which is a research and teaching platform of Plymouth University. To simplify the platform, the actuators communication means tends to be uniformed on the base of the serial protocol of the Dynamixel servos. This requires building new electrical design for smaller servo like the Titch44 of Supertec Digital which received only the information through a PWM signal coding the setpoint position.

The plan is to make this new servo on the mechanical base of the small servo controller Titch44 of the Super Tec Digital Company. To investigate new technologies, it will use a rotary Hall Effect sensor instead of a potentiometer. The new electrical parts of the servo will be based on a microcontroller and provides the regulation loop and the serial communication on the bioloid bus.

2 Control of the motor

The motor used by the Titch44 servo controller is an iron core motor with permanent magnets. These kinds of motor are made to have high torque regarding their size their works at a high velocity speed (Gieras and Wing 2002).

To make a controller for this motor, the way chosen id to make a model based on the theoretical equation of the motor completed by the measurement of its features.

The electrical equation of the motor contains an electrical part and a mechanical one. The Laplace transfer function of the angular velocity and the motor's voltage is a second order function (1) where Ke is electromotive force, B the Viscous friction constant, J the inertia of the motor, R the resistance of the rotor coils and L is inductance.

$$\frac{\omega_m(s)}{U(s)} = \frac{K_e}{(B+Js)(R+Ls)+\ K_e{}^2} \qquad (1)$$

We consider that the inductance of the rotor is small, so the electrical time constant of the motor is neglected behind the mechanical one. Thus, this transfer function can be approximated by a first order system.

Then, the Total transfer function of the motor and the gearbox is:

$$H(s) = \frac{K_{gear}\ * K'}{s(1+\ \tau s)} \qquad (2)$$

Where Kgear is the gearbox ratio, τ the mechanical constant time and K' a parameter to measure. The time constant has been identified with measurement on the scope and an optical tachometer has provided the value of the gain K'. The gear box ratio has been identified by disassembling the gearbox and counting the tooth of each sprocket:

- Kgear = 3/1600
- τ = 10 ms
- K'=150.

The block diagram of this system with Matlab Simulink software is represented in figure 1.

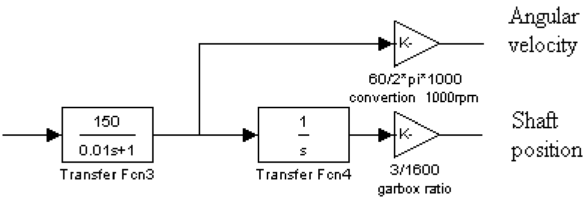


Figure 1: Simulink model of the motor and gearbox.

This system is unstable in position, so a feedback controller has been made to obtain the wanted position in the output of the system. The controller to implements is executed by a microcontroller, so the transfer function of the controller is in discreet time. Some zero holders have been added on the input and output of the system.

The design method used the Ziegler-Nichols in the temporal domain (Åström and Hägglund 1995).The transfert function of a discreet PID controller is composed by the addition of the intégral , proportional and dérivate terms weight by they respectiv gain K_p , K_i and K_d.

$$C(z) = K_p + \frac{K_d}{Ts} * \frac{z-1}{z} + K_i\,Ts * \frac{z}{z-1} \qquad (3)$$

The simulation of the contoller are unrevealing that only a proportional controller can provide a good result. The temporal methode of Ziegler-Nichols for a proportional controller define the parameter α as shown on the figure 2.

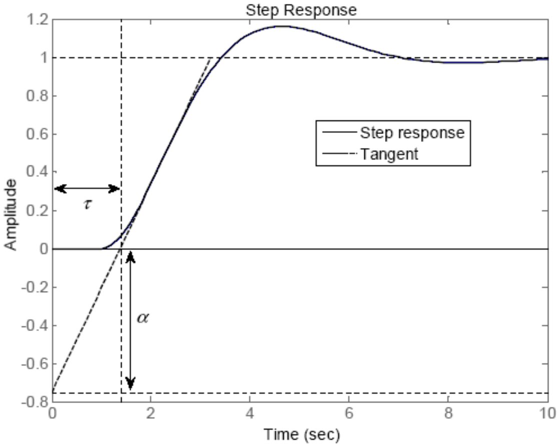


Figure 2: Ziegler-Nichols parameter’s identification, temporal method with generic features.

The table gives Kd= 1/ α. In our case α=0.022, so Kd≈45.5.

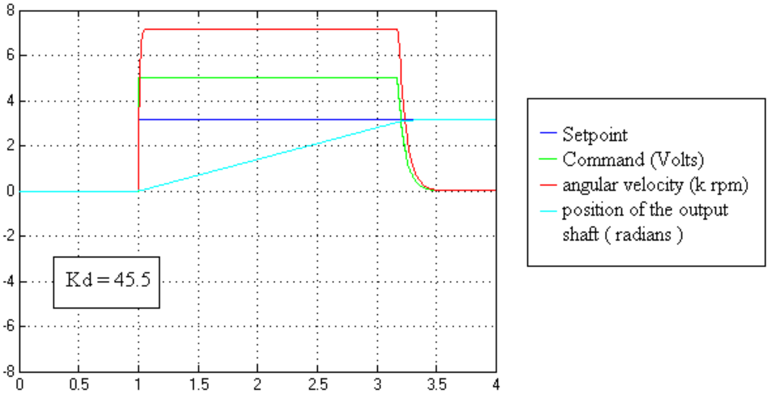


Figure 3: output response of the system with feedback controller.

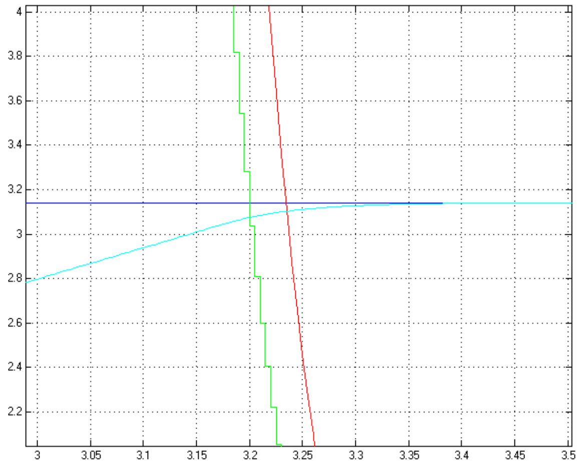


Figure 4: Zoom of figure 3

The result with the Ziegler-Nichols parameters provides a good enough control of the system: There are no oscillations, no overshoot, and the capture of the setpoint position cannot be very much faster because of the five volts saturation of the command. Moreover, this design is easily implementable in a microcontroller.

3 Rotary Hall Effect sensor (Janisch 2006)

The rotary all effect sensor chips used to measure the position of the output shaft is the new smallest chip on the market: the AS5055 by austriamicrosystems.

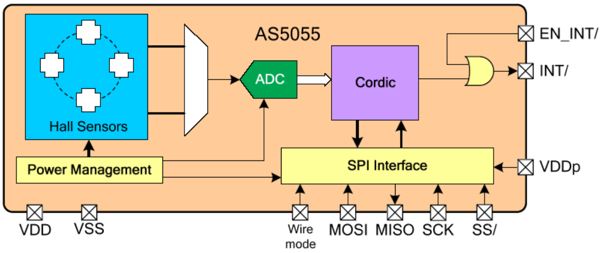


Figure 5: AS5055 block diagram (AS5055 Datasheet)

The principle of the angle measurements is based on fourth linear Hall Effect sensor dispose in a square shape. This configuration permits to give back the sine and cosine values of the angle of a tow pole magnet by an amplitude factor relative to the magnet fields. The CORDIC algorithm (coordinate rotation digital computer) deduces the angle and the strength of the magnetic field.

A serial peripheral interface deals with a synchronous communication with the microcontroller in a master/slave pattern. The AS5055 is ready to used for simple angle measurements application in a tree wire mode where it always returns the angle measurement in a 16 bits frame format.

4 Embedded software design

The embedded software developed for the ATmega16 is dealing with the bioloid bus based on a half duplex asynchronous serial link and the control algorithm. This program is executed with a clock frequency of 8 MHz. The software must respect the time features of the serial link as well as the sampling period of the regulation algorithm.

The important actions to do for the serial link are:

- Stock the data when they are received to avoid overwriting the incoming bytes. So an interrupt routine service (ISR) is trigged when a byte is received by the microcontroller UART and is stoked in a buffer.

- Respond to the bus controller after an appropriate time called Return delay time. During this time, the some data can be received and the UART must stay in reception mode. The solution chosen is to put the data to send in another buffer and make the activation / sending /desactivation of the transmission with interrupts. Another timer ISR activates transmission mode, the UART interrupts send the data until there are no left on the buffer and then return in reception mode. In this way, the transmission time of the servo is reduces and the regulation process can be computed in the main loop.

The important actions for the regulation loop are:

- To respect the sampling period of the regulation loop, i.e always make the measurements spaced of the same time interval. This is perform by another timer ISR which make a the hall sensor request, change the PWM value and update the tick to inform the main loop that the regulation process have to be run another time.

Advantages of the main loop architecture (figure 6):

If there are lots of information on the bioloid bus, the packet parsing time can exceed the sampling period, the code are just missed a regulation step and the controller will deals with it on his one in a few sampling period. If the regulation process has the priority on the packet parser, a new position instruction can be missed and the error can be more complicated to detect and restore.

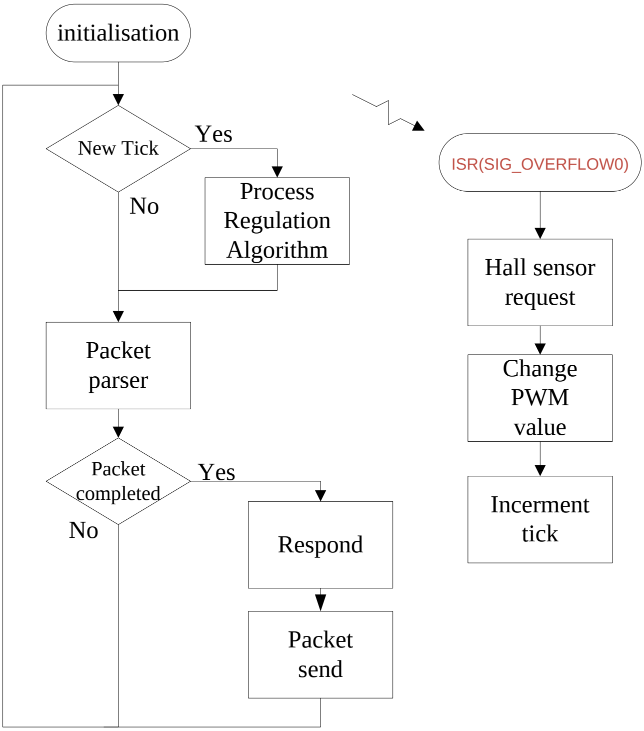


Figure 6: main algorithm

5 Results and Conclusion

Some hardware a problem on the AS5055 chip has prevents us to make a working controller on the real motor system. These problems may come from the miniaturization of the chip (QFN 16-pins package, of 4x4x0.85mm). This problem has not been resolved yet and so the accuracy of this rotary Hall Effect sensor has not been tested. Happily the software in the Atmel has permits to identify this new servo by his ID controller which validate its serial link part. The miniaturisation of this controller is not achieved either, due to the time spent trying to make the AS5055 working.

6 References

Åström, K. J. and Hägglund, T. (1995), "*PID Controllers – theory, and Tuning*", Research Triangle Park, North Carolina.

Gieras, J., Wing, M. (2002), "*Permanent Magnet Motor Technology: Design and application"*, Marcel Dekker, New York.

Janisch, J, (2006), "*Understanding Integrated Hall Effect Rotary Encoders*", http://www.sensorsmag.com/sensors/position-presence-proximity/understanding-integrated-hall-effect-rotary-encoders-1254?page_id=1 (Accessed 25 August 2010)

Wolf , J., Vicente, A., Gibbons, P., Gardiner, N., Tilbury, J., Bugmann, G. and Culverhouse, P. (2009), *"BunnyBot: Humanoid Platform for Research and Teaching ",* Proceedings of FIRA RoboWorld Congress 2009, pp25-33

Implementing Fast Human-Robot Interaction on the iCub Humanoid Robot

J.Rose and T.Belpaeme

School of Computing and Mathematics, Plymouth University, Plymouth, UK
e-mail: tony.belpaeme@plymouth.ac.uk

Abstract

In an effort to design a fast human-robot interactive demonstration for potential usage as an experiment on the sociability of robots and humans past research indicated that the most suitable form of demonstrative interaction would be in the form of a competitive game. Therefore a game of rock, paper, scissors was chosen for its quick time of play as well as its long-term strategic side. The iCub humanoid robot platform was chosen to be the platform for demonstration and so a method of interaction was developed utilising a multi-coloured glove as a hand input device by utilising the iCub's stereoscopy vision to track moving colours and determine hand positions game moves based on colour. The project operated as designed and performed well at rapid successions of playing rock, paper, scissors. Key errors discovered included misinformation due to the nature of human hand movement. future work included utilising the designed demonstration for actual human-robotic interactive experimentation.

Keywords

iCub, HRI, robotics, interaction

1 Introduction

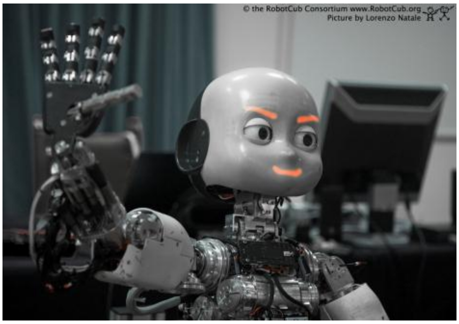
The goal of this project is to develop a fast interactive human-robot interaction demonstration, focusing on the use of the robots physical non-verbal actions to convey a sense of communication to a human observer.

Much work has already been accomplished in the field of human-robot interaction (HRI) not only for scientific and engineering purposes, but also for psychological and social interaction studies on humans too. As such there is a wide range of theories on how to approach the same problem of non-verbal communication.

This paper therefore shall set its focus on designing the demonstrative system that would be required to perform these experimental studies for HRI and through investigation of previous work, determine the most suitable design for a fast human-robot interaction experiment.

2 Background

The iCub is a 5 year long open source project funded by the European Commission through Unit E5 "Cognitive Systems, Interaction & Robotics". The iCub project is determined as an open project based on the open distribution of iCub units and open source software development. An example of the iCub robot can be seen pictured in Fig1.



© the RobotCub Consortium www.RobotCub.org
Picture by Lorenzo Natale

Figure 1: Example of iCub hardware.
(http://www.robotcub.org/index.php/robotcub accessed 2009)

3 HRI Design

It can be determined that in order to design a sociable human-robot interactive demonstration the robot must be able to control the environment with which the robot is viewed in order to direct what form of social interaction the human counterpart can expect. It is also important that the robot be capable of drawing the human counterpart into a close enough proximity to the robot as to maximise the degree of anthropomorphism the human will place on the robot without increasing the factor of fear.

This is why a most suitable form of interactive demonstration would not be that of a co-operative task but rather a competitive task. in a competitive task such as that of a simple game the human is directed by the environment factor of the game (such as the games rules and conduct) to determine that the robot is to be seen as an equal player to the game. With the robots abilities of playing said game unknown to user, the user can not view the robot as superior (and thus simply declassed as a machine or tool) nor can the robot be seen as inferior until completion of the game where the results of the game begins to show the robots ability at playing. In order to maintain anthropomorphism however the act of playing the game must be smooth and quick as to distract the human counterpart from ascertaining the robots true intelligence.

It is for this reason that the game most suitable for this form of interaction, that would both act as a method for controlling the environment the human views the robot in as well as drawing in the humans attention to a proximity to maximise anthropomorphism, and requires a simple rule base to allow for quick rapid play succession is the simple game of rock, paper scissors.

With the analysis of past research complete and a viable scenario for a fast HRI demonstration determined as rock, paper, scissors (RPS) the main design of the physical setup of the scenario is determined by what needs are required for such a game in terms of actual programming on the iCub hardware and how to create the interactive environment desired for playing.

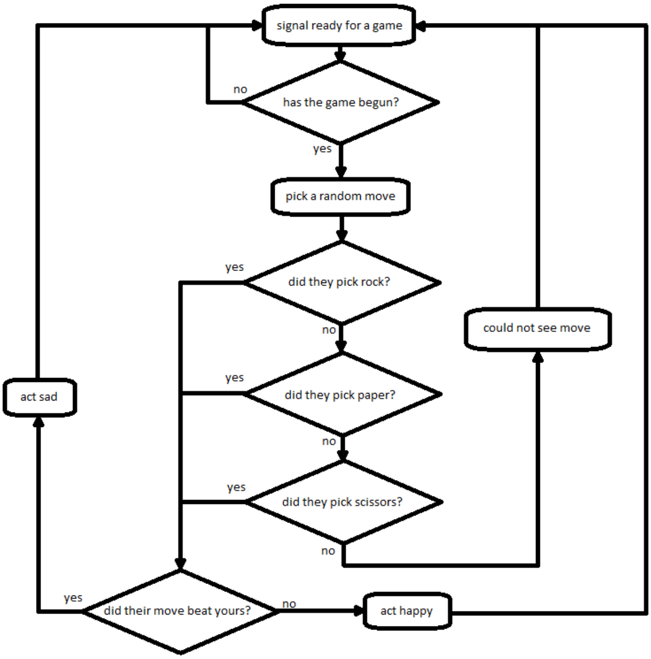


Figure 2: RPS game program flow chart

The flow chart design as shown in Fig2 demonstrates a good representation of the RPS game dynamics that will be implemented into the program. The first stage therefore is to ensure that the human players hand motions and positions can be tracked and understood in order to ensure smooth game play on the robots end.

4 Vision analysis

Utilising one camera each pixel can be read in one after the other. as the pixels are read in each pixels colour information is read in as an RGB value as shown below:

255,0,0 = RED 0,255,0 = GREEN 0,0,255 = BLUE

255,255,255 = RED, GREEN, BLUE = WHITE

By altering these values a variety of colours can be created but by setting a threshold level, if a pixel read in goes beyond the threshold then it can be determined to be a specific colour. for example if the pixel read in is determined to fall between the range 200,0,0 and 255,0,0 then if the threshold was set as 200 the pixel would be classified as a red pixel.

This threshold system allows for error and noise tolerance when dealing with the real world data as no object in the real world will always be completely red or green or blue etc due to lighting, or noise in the camera. now that pixels can be read in and colours can be specifically determined with error tolerances in place it is possible to start tracking colours to an extent.

The system begins by going through each pixel and looking at the colour information, if the colour information falls into the range of a desired colour then the pixels X coordinate (from 0 to 340) and Y coordinate (from 0 to 250) is added to a variable and a counter will increase by one, this process will continue until the entire cameras array of pixels have been viewed. The theory is that the counter is effectively counting the total number of pixels that fall into the desired colour range and with this information the stored variable containing the totals for the X and Y coordinate pixels can be divided by the total number of pixels of the desired colour in order to locate the mean average pixel of the desired colour. This can be shown demonstrated as an example in Fig3 with the black pixel representing the average centre of the red object.

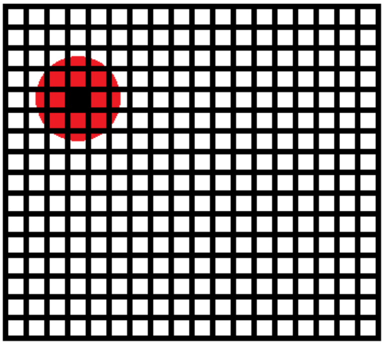


Figure 3: Example of locating average pixel of red object

What this means is that if the camera sees an image with a coloured object in its view that possess most of the pixels of that colour. then the average pixel can be located and thus the average centre of the object can also be located. With this information it become an easy task later of assigning action response based on the general pixel locations of the average centre of coloured objects. however this system only mainly works with one object of one colour, if two separate objects were to be present and both in the same desired colour range then the average pixel will be of all the pixels that fall in the colour range meaning that the average point might be exactly between the coloured objects. This error effect can be seen in Fig4 where there are two objects of the same colour, with one object bigger than the other and so the average pixel coordinate as shown by the black pixel is located near the edge of the larger red object.

It is because of this potential error in multiple colours that the iCub design will only be actually physically tracking only one colour whilst simply taking note of the colour surrounding its vision for other purposes. this way the colour chosen can be of a specific and highly contrasting background to most environment to ensure maximum success.

With the iCub however this is not the end as the iCub possesses two camera eye inputs in order to truly simulate human stereoscopic vision. If one eye was only utilised then errors would be discovered as the iCub would possess a tendency to track the object more to one side than the other depending on which eye was utilised. In order to overcome this error a virtual "third eye" must be created in the middle of the iCub's two already existing eyes, and to utilise this third camera as the basis for object colour tracking. This third eye however is very simple to create as it simply requires performing the tracking analysis on both eyes individually and then taking an average of the two average pixel coordinates for the same colour. this effectively takes an average of both perspectives of the iCub's eyes and thus a third nonexistent virtual eye is created effectively sitting equidistant from the two real eyes.

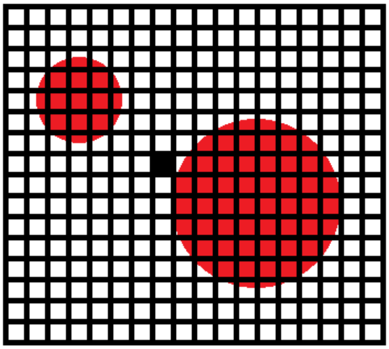


Figure 4: Example of locating average pixel of multiple red objects

In order for the iCub to effectively play RPS the iCub will need to be capable of viewing and tracking the relevant information vital to hand position movement. Of course the use of a data glove input is far too laborious and unwieldy for such a task as well as adding on extra cost. Therefore by building on what has been developed in terms of colour tracking, the most suitable form of data input via the hand is by utilising a coloured glove as seen in Fig5

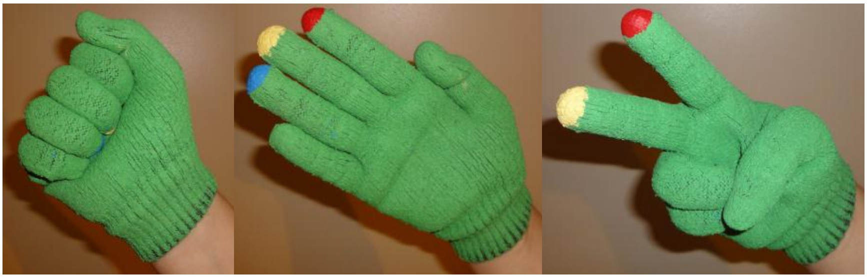


Figure 5: left rock, middle paper, right scissors in real world

5 Results

After many trials of calibration the robot was capable of performing not only fast colour tracking over small distances but large distances too allowing the head and eyes to move as effectively as intended. The results to this rapid movement of eyes without disturbing major head movement can be seen in Fig6.

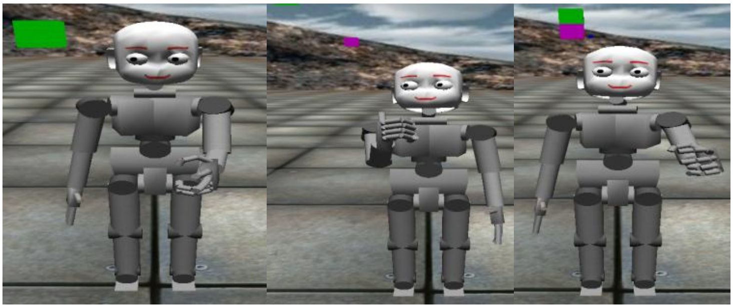


Figure 6: evidence of rapid eye movement

6 Conclusion

The main factor that was determined by this project was the fact that it is possible even with today's minimally intelligent robots to design an HRI experiment that can place the machine on the same competitive level as a human. this allows more of a focus to be made on fine tuning that interaction and determining what are the best and worst aspects to remember when design such advanced robots in today's environment.

6.1 Future work

Of course the next major step for this project is for it to be fine tuned for a much wider error correction but more importantly to develop a gradual emotional response in terms of winning and losing the game. This could be performed by setting general movements towards emotions and having them be made far more randomly by having certain variable factors determine their emotional extent.

Once those aspects are taken care of the most important factor is actually running the designed demonstration as an actual experiment with human participants in order to determine a much wider range of perceptions on the interactive design. The results could then be used to develop a brand new system utilising more complex interactions.

7 References

http://www.robotcub.org/index.php/robotcub (Accessed November 2009)

http://eris.liralab.it/wiki/Main_Page (Accessed November 2009)

http://eris.liralab.it/wiki/Manual (Accessed November 2009)

http://eris.liralab.it/yarpdoc/index.html (Accessed November 2009)

http://eris.liralab.it/wiki/ODE (Accessed November 2009)

http://eris.liralab.it/wiki/Simulator_README (Accessed November 2009)

Author Index

Advances in Communications, Computing, Networks and Security

Volume 8

Edited by
Paul S Dowland & Steven M Furnell

This book is the eighth in a series presenting research papers arising from MSc/MRes research projects undertaken by students of the School of Computing and Mathematics at Plymouth University. These one year masters courses include a significant period of full-time project activity, and students are assessed on the basis of an MSc or MRes thesis, plus an accompanying research paper.

The publications in this volume are based upon research projects that were undertaken during the 2009/10 academic year. A total of 30 papers are presented, covering many aspects of modern networking and communication technology, including security, mobility, coding schemes and quality measurement. The expanded topic coverage compared to earlier volumes in this series reflects the broadening of our range of MSc programmes. Specifically contributing programmes are: Communications Engineering and Signal Processing, Computer and Information Security, Computer Science, Network Systems Engineering, Robotics, and Web Applications Development.

The authorship of the papers is credited to the MSc/MRes student in each case (appearing as the first named author), with other authors being the academic supervisors that had significant input into the projects. Indeed, the projects were conducted in collaboration with supervisors from the internationally recognised research groups within the School, and the underlying research projects are typically related to wider research initiatives with which these groups are involved. Readers interested in further details of the related research areas are therefore encouraged to make contact with the academic supervisors, using the contact details provided elsewhere in this publication.

RESEARCH
WITH
PLYMOUTH
UNIVERSITY

ISBN 978-1-84102-293-2
90000
9 781841 022932