Advances in

Communications, Computing, Networks and Security

Volume 10

Editors

Paul S Dowland
Steven M Furnell

Advances in Communications, Computing, Networks and Security Volume 10

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

2011 - 2012

Editors

Dr Paul S Dowland
Prof. Steven M Furnell

School of Computing and Mathematics
Plymouth University

ISBN: 978-1-84102-358-8

Preface

This book is the ninth 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 2011/12 academic year. A total of 25 papers are presented, covering many aspects of modern networking and communication technology, including security, mobility, coding schemes and quality measurement. Specifically contributing programmes are: Communication Engineering and Signal Processing, Computer and Information Security, Network Systems Engineering, and Robotics.

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, November 2013

COMPUTING
WITH
PLYMOUTH
UNIVERSITY

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 1500 students enrolled on its portfolio of taught courses, over 50 of which are at MSc level. In addition there are over 100 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 Environment, the School of Biological Sciences, the School of Geography, Earth and Environmental Sciences, and, the School of Marine Science and Engineering. There are research and teaching links across all four schools as well as with the rest of the University.

Prof. Steven Furnell
Head of School

COMPUTING
WITH
PLYMOUTH
UNIVERSITY

Contributing Research Centres

Centre for Robotics and Neural Systems

Head: Professor Angelo Cangelosi
Email: angelo.cangelosi@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

https://www1.plymouth.ac.uk/research/crns/

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

Signal Processing and Multimedia Communications

Head: Professor E Ifeachor BSc, MSc, PhD, DIC, CEng, MIEE
E-mail e.ifeachor@plymouth.ac.uk
Research interests:

1) Multimedia communications
2) Audio and bio-signal processing
3) Bioinformatics

http://www.tech.plymouth.ac.uk/spmc/

Contents

SECTION 1 Communications Engineering and Signal Processing

SECTION 2 Computer and Information Security

SECTION 4 Network Systems Engineering

SECTION 5 Robotics

Section 1

Communications Engineering and Signal Processing

On Trellis Structure of Error Correction Codes

S. Adishesh and M.A. Ambroze

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

Abstract

Error Correction Coding, a technique that is used extensively for efficient transmission of data bits in almost all fields of communication. A graphical representation of the code by constructing trellis diagrams has evolved as a valuable tool for reducing decoding complexities and improving the transmission efficiencies of the code. This project involves the study of Trellis diagrams, their construction, the encoding and decoding patterns and their implementation. The paper focuses on the trellis construction of single parity check codes and their coding/ decoding mechanisms using trellis diagrams. This implementation is carried out using C+ programming languages.

Keywords

Error Correction Codes, Single Parity Check Codes, Trellis Diagrams.

1 Introduction

Communication can be regarded as a simple process of transmission of information bits. The main aim of a communication channel is to transmit the information from the source to the sink over a channel which can be in the form of a physical cable, a wireless link or a storage device. The background of communication thus revolves around the concepts of transmission and reception. (Bhatacharya. A, 2006)

Any communication process involves the following three basic steps:

- Coding a message at its source.
- Transmitting the message through a communication channel.
- Decoding the message at its destination.

Error Correction Codes:

The communication systems strive to achieve error free transmission and reception of messages without errors by focussing on signal processing techniques like error correction codes. Error correction coding is a mechanism in which the errors introduced in the digital data during the transmission process are detected and corrected upon the reception of the data. It can be regarded as a signal processing technique which is used to improve the reliability and efficiency of communication on digital channels. The detection and correction of errors is carried out by the process of adding redundant bits into the string of messages that needs to be delivered. This technique of adding extra bits to the digital messages is termed as redundancy. Redundant bits have the ability to make each of the messages unique and maintain their unique structure even if some of the bits in the message are infected by various sources (Clark. G, 1981).These codes follow the concepts of Shannon's theorems that states that efficient transmission of bits can be attained if the transmission takes place as quick as possible with no or few errors. This fastness of the channel is guarded by channel capacity or the Shannon's limit which can be defined as the rate at which information is transmitted. This rate is nothing but the ultimate speed limit set for any communication system and is given by the notion: 'C'. (Ambroze. M. A, 2011)

Equation: **C = B log2 (1+SNR)**
Where: B = Bandwidth of the communication channel &
SNR = Signal to noise ratio.

Thus, error correcting codes can be of several variations like the hamming code, parity check code, goolay code, perfect code etc. In this paper we aim at the specific TRELLIS construction of single parity check codes

2 Single Parity Check Codes

Single Parity check codes form a part of the linear block codes for which each codeword consists of (N-1) information bits and a single parity check bit. These codes have the ability to detect any error patterns containing an odd number of errors. They are characterized as (N, N-1) codes, having $2^{(N-1)}$codewords and are used in various error detection operations. For a (3, 2) SPC code, the codewords can be written as: {0 0 0, 0 1 1, 1 01, 1 1 0}. The format of this codeword can be represented as | m1 m2 p|. Where: m1, m2 are the message bits and p is the parity check bit. The parity bits are inserted in the final column such that there exists an even number of 1's when one codeword in the row is considered. The generator matrix for this message block is formulated by selecting the identity matrix from the codewords.

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

3 Trellises and Viterbi Algorithm

Viterbi algorithm can be marked as a maximum likelihood decision device with efficient computational technique that can determine the probable path taken by the code to and output the correct transmitted codeword. It works on the principle of add- compare- select (ACS) to process a code trellis and to eliminate the less probable paths for further consideration. (Viterbi. A, 2006). A trellis code is a graphical representation of a code, conventional or block, in which every path represents a codeword. It can be defined as a directed graph which consists of levels of nodes (or vertices) and directed branches (or edges) that connect two consecutive nodes together. (Khchischang. F, 1995)

3.1 Construction of Trellises from the obtained Generator matrix:

- Each row in the generator matrix corresponds to the information bits of the code.
- The active span of each row is marked. The active span extends from the first 1 in the row to the last 1 in the row.
- The active spans in each row of the G matrix contribute to the number of states in each section of the trellis and the number of sections in the trellis is denoted by each column of the G matrix
- The information bits are matrix multiplied with the generator matrix.
- By considering the product and the active spans in each column of the G matrix, we determine the branch weights and the states respectively and thus construct the trellis diagram.

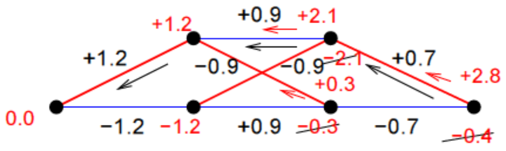
4 Illustration of the Viterbi decoding (soft decision) on (3, 2) SPC code

We consider the trellis diagram obtained for the (3, 2) SPC code and assign the codeword values to the three sections of the trellis.

i. In the first section, as a 1 is encoded by the vertical line, the received value remains the same. The received value undergoes a sign change on the horizontal line encoding a zero. Similarly, the weighting for each transitions are calculated in sections two and three of the trellis.
ii. The start node is always characterized by a node value of 0. The node values are calculated by adding the previous node value with the transition weight.
iii. The value of +1.2 in the top node of 1st section is obtained by: 0.0 + (+1.2)= +1.2.
The value of -1.2 in the bottom node of 1st section is obtained by: 0.0 + (-1.2) = -1.2.

Similar calculations are made for each of the nodes. For the node having two values, the largest value is considered and the smallest value is eliminated. The route through which the largest value is obtained is marked by an arrow mark as shown.

iv. Now if we trace back, we get:



The final decoded codeword by utilizing trace back technique is 101.

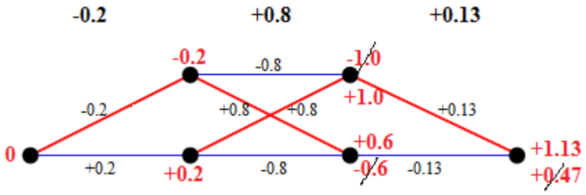
5 Results

SPC codes from (3, 2) to (6, 5) is considered and the results are produced for soft decision decoding. The addition of noise components on the received codeword is randomly added.

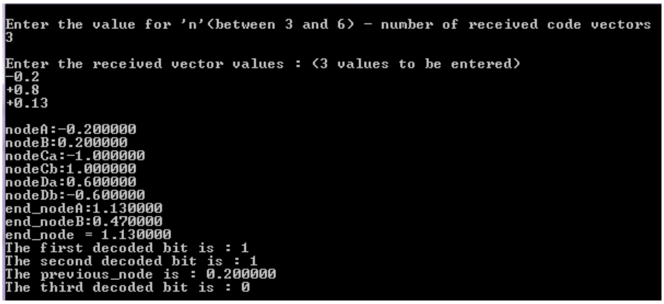
Transmitted codeword	Received codeword	Decoded codeword
0 0 0	-0.3 -0.5 -0.4	0 0 0
0 1 1	-0.2 +0.8 +0.13	0 1 1

Table 1: The decoded codewords of a (3, 2) SPC code:

Illustration 1: The received codeword is (-0.2, +0.8, +0.13)



The decoded codeword is [0 1 1].



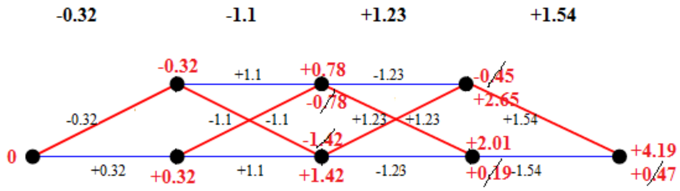
```
Enter the value for 'n'(between 3 and 6) - number of received code vectors
3

Enter the received vector values : (3 values to be entered)
-0.2
+0.8
+0.13

nodeA:-0.200000
nodeB:0.200000
nodeCa:-1.000000
nodeCb:1.000000
nodeDa:0.600000
nodeDb:-0.600000
end_nodeA:1.130000
end_nodeB:0.470000
end_node = 1.130000
The first decoded bit is : 1
The second decoded bit is : 1
The previous_node is : 0.200000
The third decoded bit is : 0
```

5.1 The decoded codewords of (4, 3) SPC code:

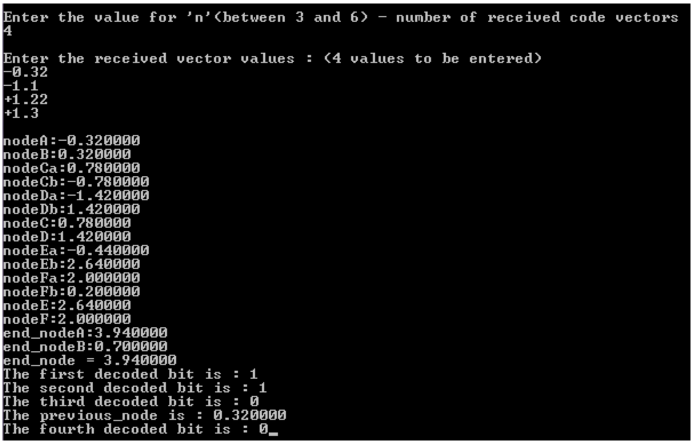
Transmitted codeword	Received codeword	Decoded codeword
0 0 0 0	-0.9 -0.34 -0.76 -0.1	0 0 0 0
0 0 1 1	-0.32 -1.1 +1.23 +1.54	0 0 1 1
0 1 0 1	-0.9 +0.5 -0.1 +0.67	0 1 0 1
0 1 1 0	-0.23 +0.9 +1.0 -0.12	0 1 1 0
1 0 0 1	+0.76 -0.2 -1.3 +1.3	1 0 0 1

Illustration 2:

The received codeword is (-0.32, -1.1, +1.23, +1.54)



The decoded codeword is [0 0 1]



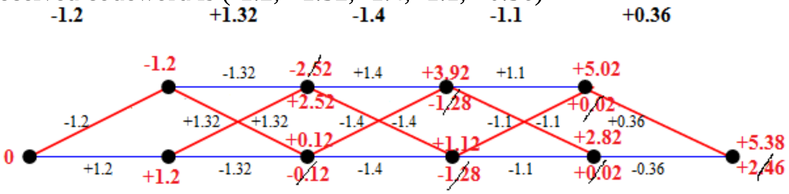
```
Enter the value for 'n'(between 3 and 6) - number of received code vectors
4

Enter the received vector values : (4 values to be entered)
-0.32
-1.1
+1.22
+1.3

nodeA:-0.320000
nodeB:0.320000
nodeCa:0.780000
nodeCb:-0.780000
nodeDa:-1.420000
nodeDb:1.420000
nodeC:0.780000
nodeD:1.420000
nodeEa:-0.440000
nodeEb:2.640000
nodeFa:2.000000
nodeFb:0.200000
nodeE:2.640000
nodeF:2.000000
end_nodeA:3.940000
end_nodeB:0.700000
end_node = 3.940000
The first decoded bit is : 1
The second decoded bit is : 1
The third decoded bit is : 0
The previous_node is : 0.320000
The fourth decoded bit is : 0_
```

5.2 The decoded codewords of (5, 4) SPC code:

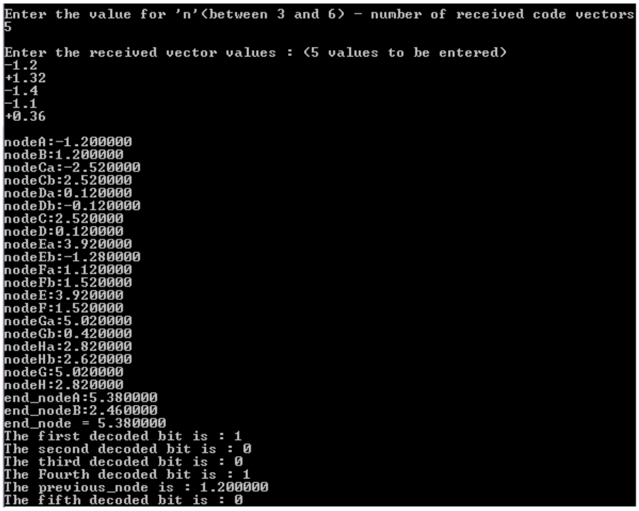
Transmitted codeword	Received codeword	Decoded codeword
0 0 0 0 0	-0.12 -0.7 -1.1 -0.98 -1.2	0 0 0 0 0
0 0 0 1 1	-0.23 -0.76 -0.4 +0.7 +0.2	0 0 0 1 1
0 0 1 0 1	-0.65 -0.9 +0.9 -0.123 +1.3	0 0 1 0 1

Illustration 3:

The received codeword is (-1.2, +1.32, -1.4, -1.1, +0.36)



The decoded codeword is [0 1 0 0 1]



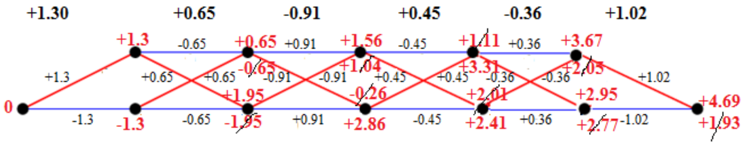
```
Enter the value for 'n'(between 3 and 6) - number of received code vectors
5

Enter the received vector values : (5 values to be entered)
-1.2
+1.32
-1.4
-1.1
+0.36

nodeA:-1.200000
nodeB:1.200000
nodeCa:-2.520000
nodeCb:2.520000
nodeDa:0.120000
nodeDb:-0.120000
nodeC:2.520000
nodeD:0.120000
nodeEa:3.920000
nodeEb:-1.280000
nodeFa:1.120000
nodeFb:1.520000
nodeE:3.920000
nodeF:1.520000
nodeGa:5.020000
nodeGb:0.420000
nodeHa:2.820000
nodeHb:2.620000
nodeG:5.020000
nodeH:2.820000
end_nodeA:5.380000
end_nodeB:2.460000
end_node = 5.380000
The first decoded bit is : 1
The second decoded bit is : 0
The third decoded bit is : 0
The Fourth decoded bit is : 1
The previous_node is : 1.200000
The fifth decoded bit is : 0
```

5.3 The decoded codewords of (6, 5) SPC code:

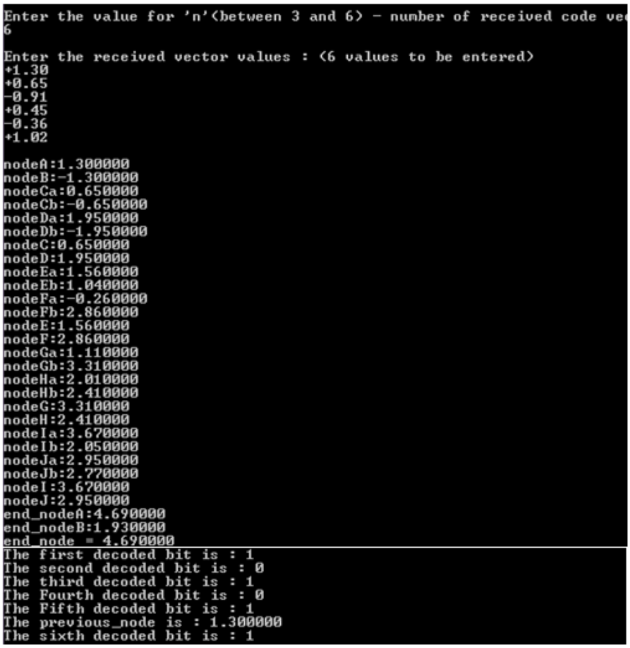
Transmitted Codeword	Received Codeword	Decoded Codeword
0 0 0 0 0 0	-0.1 -0.2 -0.1 -0.3 -0.2 -0.6	0 0 0 0 0 0
0 0 0 0 1 1	-1.2 -0.91 -0.13 -0.72 +0.12 +1.9	0 0 0 0 1 1
0 0 0 1 0 1	-0.23 -0.98 -0.43 +1.2 -1.8 +1.67	0 0 0 1 0 1
0 0 0 1 1 0	-0.12 -0.76 -1.2 +0.91 +1.1 -0.53	0 0 0 1 1 0
0 0 1 0 0 1	-0.43 -1.43 +0.63 -0.66 -0.75 +1.54	0 0 1 0 0 1

Illustration 4:

The received codeword is (+1.30 +0.65 -0.91 +0.45 -0.36 +1.02)



The decoded codeword is [1 1 0 1 0 1]



```
Enter the value for 'n'(between 3 and 6) - number of received code ve
6

Enter the received vector values : (6 values to be entered)
+1.30
+0.65
-0.91
+0.45
-0.36
+1.02

nodeA:1.300000
nodeB:-1.300000
nodeCa:0.650000
nodeCb:-0.650000
nodeDa:1.950000
nodeDb:-1.950000
nodeC:0.650000
nodeD:1.950000
nodeEa:1.560000
nodeEb:1.040000
nodeFa:-0.260000
nodeFb:2.860000
nodeE:1.560000
nodeF:2.860000
nodeGa:1.110000
nodeGb:3.310000
nodeHa:2.010000
nodeHb:2.410000
nodeG:3.310000
nodeH:2.410000
nodeIa:3.670000
nodeIb:2.050000
nodeJa:2.950000
nodeJb:2.770000
nodeI:3.670000
nodeJ:2.950000
end_nodeA:4.690000
end_nodeB:1.930000
end_node = 4.690000
The first decoded bit is : 1
The second decoded bit is : 0
The third decoded bit is : 1
The Fourth decoded bit is : 0
The Fifth decoded bit is : 1
The previous_node is : 1.300000
The sixth decoded bit is : 1
```

5.5. When the received codeword undergoes an error:

Received codeword with error/s for (3, 2) SPC Code:

Transmitted codeword	Received codeword	Decoded codeword

0 0 0	-0.3 -0.61 0.2
	+0.3 +0.61 +0.2
	+0.3 -0.61 -0.2
		0 0 0
		0 1 1
		1 0 1

0 1 0 1	+1.32 +0.3 -0.21 +1.1
	-1.32 -0.3 -0.21 +1.1
	-1.32 +0.3 +0.21 +1.1
		1 1 1 1
		1 1 0 0
		1 0 1 0

0 0 1 0 1	-0.65 -0.9 +0.9 +0.123 +1.3
	-0.65 -0.9 +0.9 +0.123 -1.3
	+0.65 +0.9 -0.9 -0.123 +1.3
		1 1 0 1 1
		0 1 1 0 0
		1 0 1 1 1

0 0 0 0 1 1	-1.2 -0.91 -0.13 -0.72 +0.12 -1.9
	+1.2 +0.91 -0.13 -0.72 +0.12 +1.9
	+1.2 -0.91 +0.13 -0.72 -0.12 +1.9
		0 0 0 0 0 0
		1 1 0 0 1 1
		1 1 1 0 0 1

6 Conclusion

This paper on Trellis structure on error correction codes involves a detailed working of the Single Parity Check codes, Viterbi Algorithm and the trellis construction of SPC codes. The soft decision coding is illustrated with various input parameters and the trellis is constructed for the same. Minimal trellis for (3, 2), (4, 3), (5, 4) and (6, 5) single parity check codes are constructed and Viterbi decoding algorithm is employed to decode the codes to obtain an output from the decoder. The software implementation for soft decision coding is carried out using C+ programming language, in which a decoded codeword is obtained on feeding the input bit values.

7 Limitations and Future work

The software implementation for encoding and the decoding is done for (N, N-1) Single Parity Check Codes where N = 3, 4, 5, 6. Viterbi decoding algorithm is implemented for the decoding purposes. Future scope is to upgrade the program to have a more concise program that would take care of (N, N-1) SPC codes.

8 References

Ambroze. M. A, 2010, *Digital and Wireless Communications notes*, School of Computing, and Communications Engineering (SoCCE), University of Plymouth. Available online: https://tulip.plymouth.ac.uk/Module/ELEC508/LectureNotes/notes.pdf Accessed on: 3.6.2011.

Bhatacharya. A (2006). *Digital Communication*. India: Tata Mc-Graw Hill. P3-6.

Clark. G, 1981, *Error Correction Coding for Digital Communication.* United States of America: Plenum Press. P7-15.

Khchischang. F, 1995, *On the Trellis Structure of Block Codes*, IEEE Transactions on Information Theory, Vol: 41. Available online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=476317. Accessed on: 4.7.2011.

Viterbi. A, 2006, *A Personal History of the Viterbi Algorithm*, IEEE Signal Processing Magazine, July. Available online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1657823. Accessed on: 18.10.2011.

Study of DCT Watermarking Methods

V. Buchaillet and M.A. Ambroze

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

Abstract

In digital watermarking, information are hiding into audio, image and video files with the main goal to be invisible at the human visual or hearing system and robust to some piracy attacks. Nowadays many technics of watermarking has been developed and are based on spatial domain (Least Significant Bit (LSB)) and transform domain (Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)). The basic DCT watermarking technics has been implemented in this project to study its strength and weaknesses and moreover how it is possible to improve a watermarking process and what does it cost.

Keywords

Digital watermarking, Discrete Cosine Transform, Improve a watermark process, Invisible.

1 Introduction

Since the creation of internet the availability of digital data has rapidly increase. Nevertheless, with this increasing of data, problem of protection and piracy appeared and protecting these data with copyright started to be a really important point for searchers. Indeed, to maintain the availability of digital files online and respect the owners of these files, a way to protect these files and their creators efficiently had to be finding.

One of method which is the most used to protect digital data as video, image or audio files is based on the steganography process and is named watermarking. The main goal of this method is to embed information data into the digital file to protect with an insensible form for human perception but in a way to protect it against some possible attacks against this information. Indeed, at the end of this process the data which has been protected will have to be exactly the same than the original one for the human perception but still offer the possibility of identification for the owner of the encrypting key.

In this paper, the method which has been studied is the DCT watermark method on images. This method is applied in the transform domain which is the most efficient domain to realise an invisible watermark (Mistry, 2010). Furthermore, this method has been applied to images to see easily the impact of the watermarking.

This study will only be focus on the performance of the DCT watermarking technic and study the factors which could affect the invisibility of the watermark. Nevertheless, by doing some amelioration in the second part of the research the watermark process developed will be protect against some attack even if creating a robust watermarking process is not the main goal of this research.

2 Discrete Cosine Transform Watermarking Studied

The principle of the DCT process is to break an image into different frequency bands (Mistry, 2010) in order to embed information into the middle frequency bands of the image to be invisible to the human perception which is sensible to the low frequencies. Furthermore, image compression systems affect more high frequencies so choosing the medium frequencies avoid a part of this problem.

A. Step of The DCT embedding method studied

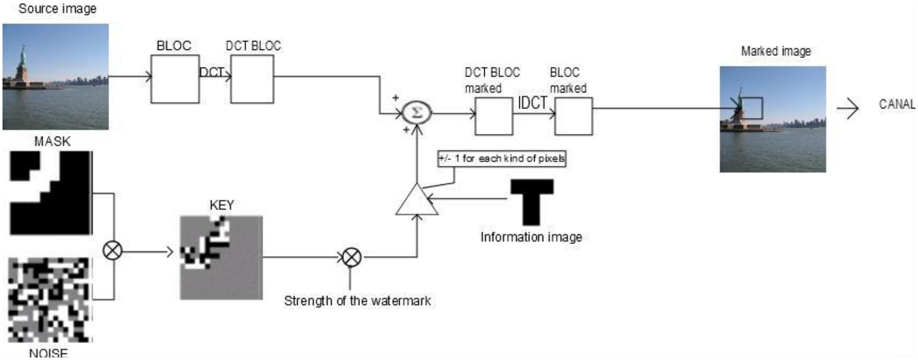


Figure 1: Scheme of the system studied

1) Isolate the blue component of the RGB colour of the original image because working on the blue component will increase the invisibility of the mark. Indeed, the human perception is less sensible to blue component that any other.

2) Divide the original image onto blocs of pixels which have a size proportional to the original and information image.

3) Transforms each bloc by using the DCT algorithm.

4) Encryption of the information using an encrypting key which will embed the information only on the medium frequencies.

5) Inversion of the DCT process and reassembling of each pixel blocs to have an image back which carry the mark.

B. Step of The DCT decoding method

To decode the information which has been encode the user will need the image where the information has been encoded and the encrypting key to decode this information. Then, if all the information is given to the receiver this one is able to decode it by following the scheme on figure 2.

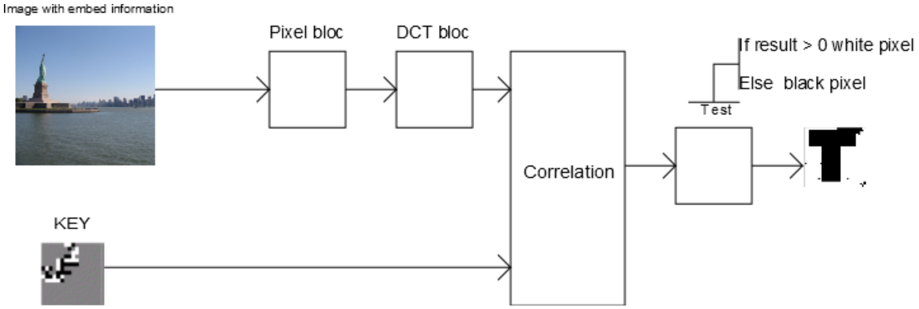


Figure 2: Scheme of the system studied

Indeed, the decoder will first take a bloc of pixels of the same size than the one which was taken by the encoder. Then, the DCT algorithm is applied to this bloc. Then, the DCT bloc and the encrypting key are comparing by a correlation system which will send back a value which will tell the dependency between this two blocs. The value sending back by the correlation system will be between -1 and 1.So, if the correlation system send a value superior to zero that’s mean that the correlation is high so a black pixel will be encode however a white one will be encoded. So, at the end by adding all this pixels together it will rebuild the information image.

C. Experiences applied to the DCT watermarking method

In the watermark process there is few things which can affect the visibility and the quality of the mark, like the strength of the watermark or the frequencies of a bloc. To analyses the efficiency of the method implemented three parameters have been test.

The first one is the difference between the original image and the mark image which is called distortion. Indeed, this allow us to see if the watermark is hide enough or if just by doing this simple manipulation a user can see which information has been mark. In the case of this study the following result has been finding.

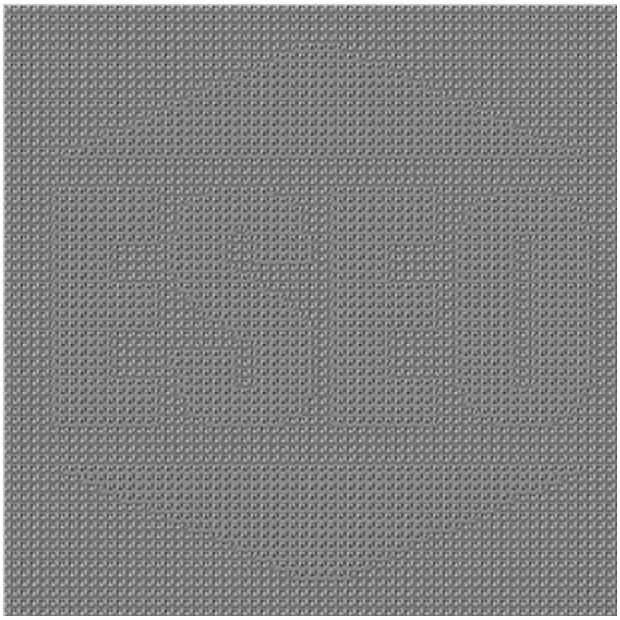


Figure 3: Distortion applied on images after applying the DCT watermarking

By analysing the result, it is possible to see that the mark can be seen. So the way to mark the information could be improved by for example find a way to scramble the information to be sure that the information will not be seen.

In a second analysis it has appeared that in some cases the retrieve information after the decoding process was noisy.

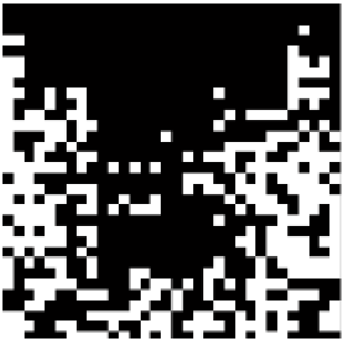


Figure 4: Example of noisy retrieved image

This noise was detected most of the time when the strength of the watermarking process was setting too low. To analyse how the strength was influencing the watermarking process a test has been done to show the influence that this parameter has on the error between the original image and the mark image and the peak signal to noise ratio.

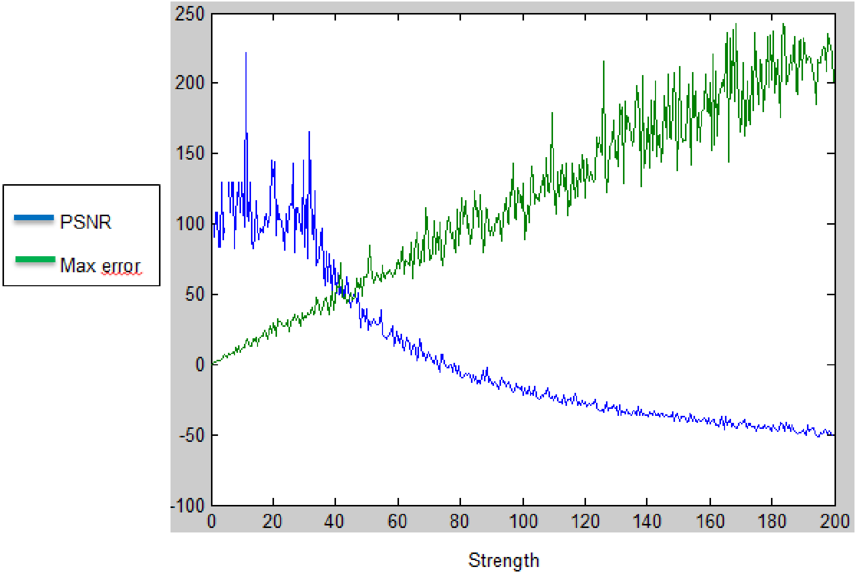


Figure 5: Influence of the watermarking strength on the peak signal to noise ratio and the error between the original image and the mark one.

So this experiment as shown that the strength of the process must be chosen well if the user want to retrieve the image without noise. Nevertheless, by testing on some images to use the best strength to embed the image another parameter has been finding. Indeed, when the watermarking process is applied to image with light colours the zones of the image will bring noise has it is possible to see on the following figure.

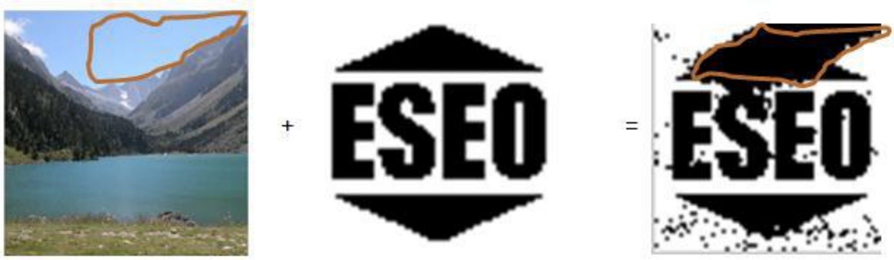


Figure 6: Influence of light colours on the watermarking process.

To conclude, the DCT watermarking which was studied was efficient to mark an image but not so efficient for hiding it or caring information without deteriorate it.

D. Improvement of the system

By doing the previous analysis an idea has come to deal with the light colours problem. Indeed, if a threshold value can be set on the DCT coefficient that have to be mark on each bloc, then the blocs which are not goodwill be dropped and the efficiency and the robustness of the watermark process will be increase.

To realise this improvement some step of the method has been modified. Indeed, each bloc taken from the original image will be 8X8 pixels bloc. This change has been made to be sure that even by dropping some blocs all the information to mark will fit in the source image. Furthermore, by dropping some blocs and taking some others this will scramble the mark during the process and increase the robustness of the mark.

The biggest modification of the process has been the bloc selection process. This step analyse DCT coefficients of the frequencies selected by the encrypting key and if there is less than half of them which are higher or equal to the threshold then the bloc will be dropped and the information will be marked in the next valuable bloc.

3 Conclusion

Digital watermarking can protect image from unauthorized modification done on an image by some noise or some person. The DCT system studied is better than a spatial domain watermark by the fact by the fact that it is more robust against compression or noise. Nevertheless, it can be improve to be more robust or even be secure but this can of improvement will take a long time to implement and will add some cost to the watermark process as computational or information cost.

4 References

Cox, I.J, Miller M, Bloom J, Fridrich J and Kalker T(2008), ‘Digital Watermarking and Steganography (second edition)’, Burlington: Morgan Kaufmann Publishers, ISBN: 978-0-12-372585-1.

Mistry, d., *comparison of digital watermarking methods*, International journal of computer science and engineering, vol.2, India: Gandhibagar, 2010.

Prediction of Electricity Consumption in France

R. Declerck and E. Ifeachor

Signal Processing and Multimedia Communications,
Plymouth University, Plymouth, UK
e-mail: E.Ifeachor@plymouth.ac.uk

Abstract

At any moment, the electricity that we consume has to be produced by any group of production because electricity produced cannot be stored. The aim is to satisfy the supply-demand balance to avoid any problem for the customers such as power outage, demand surge and, if necessary, to import electricity from another country. This publication describes some techniques used to predict the electricity consumption and shows some results obtained by them.

Keywords

Prediction, Electricity Consumption, Machine Learning, Multiple Linear Regression

1 Introduction

Electricity produced cannot be stored. At any moment, the electricity that we consume has to be produced by any group of production wherever they are situated in France or in a foreign country. In France, the company which predicts the electricity consumption is called « Réseau de Transport d'Électricité » (RTE). The consumption is predicted twenty-four hours in advance. The aim is to satisfy the supply-demand balance to avoid any problem for the customers such as power outage, demand surge and, if necessary, to import electricity from another country.

The possibility to predict the electricity consumption is possible thanks to Machine Learning. Machine Learning is a scientific tool that uses mathematical algorithms to solve a real problem. A lot of different kinds of Machine Learning algorithms exist. Machine Learning is used in many ways and different fields of activity such as medical diagnosis, audio-processing, automobile or multimedia communication.

In this paper, one example of Machine Learning is highlighted: the Multiple Linear Regression. The Multiple Linear Regression method is explained and some results obtained are compared with the best efficiency from RTE.

2 Electricity Consumption

Electricity consumption is sampled each half-hour. That is why data increases extremely rapidly. 48 samples per day are saved only for the consumption of electricity. Thanks to these data it is possible to visualize the previous electricity consumption. There are three kinds of cycle of electricity consumption (RTE, 2008), which are the annual cycle, the weekly cycle and the daily cycle. These various kinds of cycle are described hereafter.

2.1 2.1 Annual Cycle

The annual cycle shows clearly a peak of electricity demand in December during the winter and a low consumption around the 15th of August during the summer (RTE, 2008). It can be seen in figure 1.

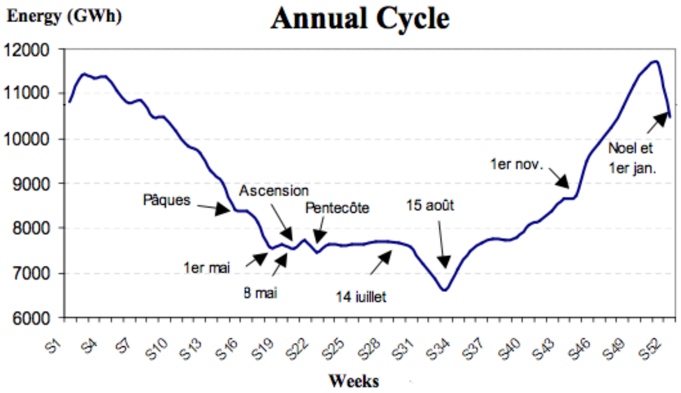


Figure 1: Annual Cycle Curve of Electric Load Consumption (RTE, 2008)

2.2 Weekly Cycle

The weekly consumption, in figure 2, shows that, in the weekend, less electricity is used than during the week. Indeed, most of the manufactures or companies are closed during the weekend (RTE, 2008). Moreover, a difference can be shown between the Saturday and the Sunday. As fewer shops are open on Sunday.

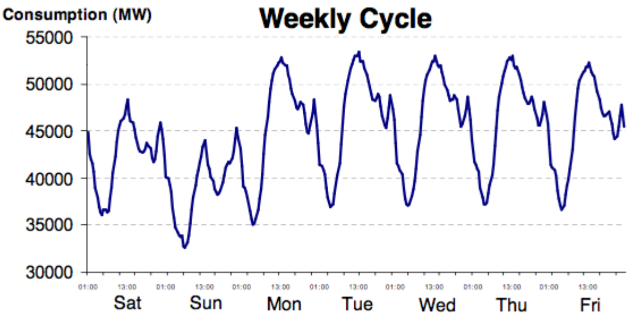


Figure 2: Weekly Cycle Curve of Electric Load Consumption (RTE, 2008)

2.3 Daily Cycle

The daily cycle shows that the peak of consumption during a day is around 8 p.m. the winter and around 1 p.m. the summer, time when people are cooking (RTE, 2008).

Logically, the low consumption happens during the night. This daily cycle can be seen in figure 3.

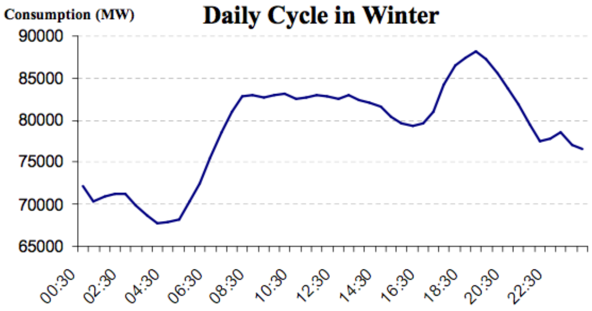


Figure 3: Daily Cycle of Electric Load Consumption in winter (RTE, 2008)

2.4 Electricity Consumption Forecasting

The quality of prediction depends on the accuracy of weather data. All error on these data will be transferred to the forecast of electricity consumption. So RTE is dependent of data provided by Météo-France. Then the historical consumption is used to calibrate the forecast of consumption taking into account the past and trends.

The quality of forecast can be evaluated through the discrepancy with the goal. Today, it is estimated the standard deviation between forecasts and realization of daily consumption to about 900 MW (RTE, 2008). An example, from RTE, of consumption forecast and the real consumption are shown in figure 4.

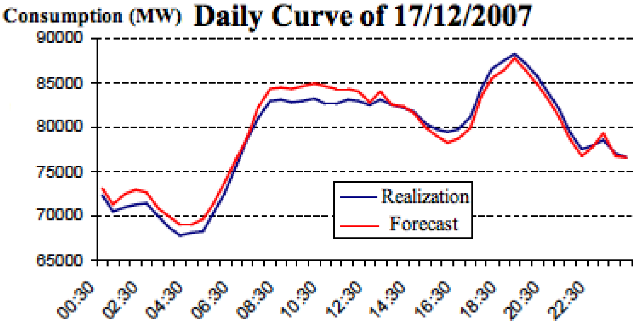


Figure 4: Forecast and the real electricity consumption of a day (RTE, 2008)

3 Data

Thanks to the visualization of the previous electricity consumption it is possible to have an idea of which parameters have an influence on the consumption of electricity. In this part some parameters that influence the consumption of electricity are explained. They are classified by their importance (RTE, 2008).

3.1 Meteorology

RTE uses two quantities, which are temperature and nebulosity.

Temperature, given by Météo-France, is measured thanks to a lot of sensors situated everywhere in France. Taking into account the assumptions of temperature and its variations coming quantifies the change in consumption induced by the use of heating electricity in the winter or air conditioning in summer. It is possible to calculate the correlation between the electricity consumption and the average temperature. This coefficient is the ratio of the covariance and product of their standard deviation. These standard deviations cannot be equal to zero. Figure 5 suggests that the electricity consumption depends on the temperature.

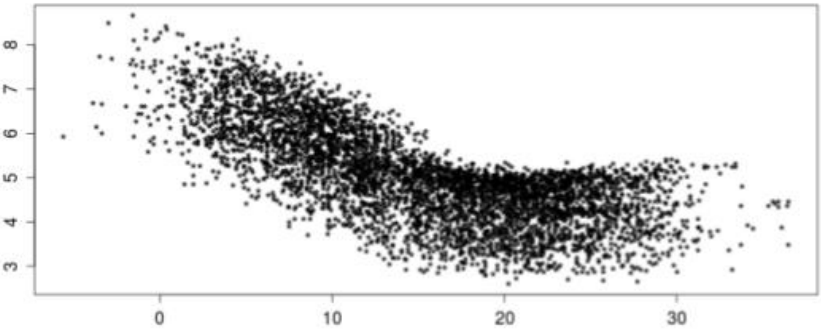


Figure 5: Electricity demand (in Gw/h) as function of temperature (in ° Celsius) (Cugliari, 2011)

Nebulosity represents the average rate of cloud cover. Nebulosity is also called cloudiness index. This quantity is expressed in Octa and varies from 0 to 8 (0 corresponds to a completely clear sky and 8 to an overcast sky). The cloudiness index is estimated thanks to an instrument that measures the illumination on a horizontal surface. The cloud has an influence on the use of lighting, but also by changing the heating effects of solar radiation in homes (RTE, 2008).

3.2 Economic Activity

The economic activity of manufactures has a strong influence on consumption of electricity. These effects are directly observable on the curves of annual consumption (low consumption during the summer holidays) and weekly (consumption less on weekends). Thus, the day off such as Christmas, Easter, 1st of May and 14th of July change significantly profile of consumption on that day. The summer holidays have a strong influence.

3.3 Others parameters

Other parameters, less important, influence the electricity consumption:

- Commercial Offers Clearing The Electrical Power Consumed: There are several schemes to reduce the electrical power consumed.

- Approaches To Citizen Control Of Electricity Consumption: In some areas, which do not have many groups of electricity production, the RTE created devices call for restraint in case of high electricity consumption.

- The Legal Working Time: The legal working time (summer or winter) also influences the consumption of electricity by shifting from solar time.

- Exceptional Events: Some exceptional events can disrupt the pattern of consumption such as a final of a Football World Cup. However, most of the exceptional events cannot be expected. Indeed, no reference is available in the past.

4 Machine Learning

4.1 Brief Description of Machine Learning

According to (Mitchell et al., 1985), "The principle of a learning system is to determine a description of a given concept from a set of concept examples provided by the expert and from the background knowledge".

4.2 Multiple Linear Regression

In Italia (Bianco et al., 2009) and in Sardinia (Antoch et al, 2010) two different studies have been done using Multiple Linear Regression. The approaches gave good efficiency for short or mid term prediction of electricity consumption.

When a regression application depends on more than one independent variable, it is called a Multiple Linear Regression. The equation of a multiple linear regression model is (Littell, 2009):

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_k x_k + \varepsilon \tag{1}$$

- k is the number of independent variable such as temperature, nebulosity, previous electricity consumption in the case of electricity consumption.

- x_i is the independent variable.

- ε is a random variable with mean 0 and variance σ^2.

After the training session, the relation between the independent variable and the prediction of electricity consumption is found. The prediction equation obtained for the model is:

(2)

$$Y = b_0 + b_1x_1 + b_2x_2 + \ldots + b_kx_k + \varepsilon$$

- b_i means an estimate of β_i.

- Y means the predicted value so in this application the prediction of electricity consumption at a given moment.

The Multiple Linear Regression method fits a model using the least squares technique. Indeed, the method of least squares is used to estimate all b_i. The goal of this method is to find, through all the independent variables, all b_i that give the minimum $\Sigma(y-Y)^2$. So the best equation is obtained in order to predict y whatever the variables used in input.

5 Prediction of Electricity Consumption

5.1 Daily and Weekly prediction

The weekly prediction is several daily prediction put together. The consumption of two weeks is. One week that contains a day off and another without day off. The mean absolute difference of the prediction regarding the real electricity consumption is of 4,2531% when the mean absolute difference of RTE is 1,7384%. This efficiency does not reach the efficiency of RTE.

Firsty in figure 7, the prediction of electricity consumption from Monday 6th July 2009 to Sunday 12th July 2009 is shown. The electricity consumption of week day are more important than the week-end. The prediction (continuous curve) follows the real consumption (dotted curve). Indeed, during the week-end less electricity consumption is predicted as the real consumption.

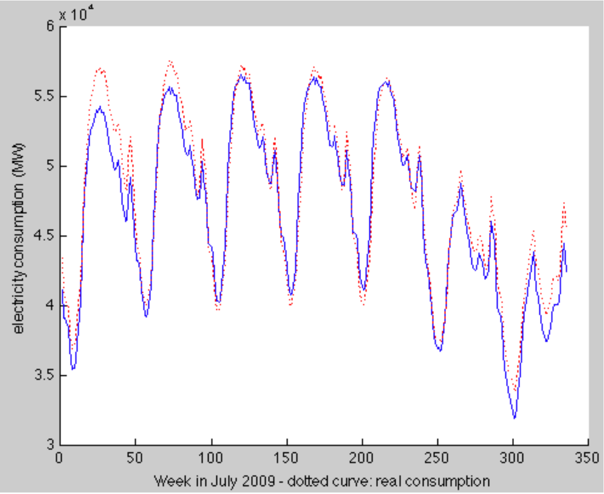


Figure 6: Electricity prediction of a week (without day off) in July 2009

Then in figure 8, the prediction of electricity consumption from Monday 4th May 2009 to Sunday 10th May 2009 is done. This week is special. Indeed, the Friday of this week is the 8th of May that is the armistice of the Second World War. In France, less people go to work this day. So the electricity consumption on this Friday should be less. The continuous curve, which is the prediction curve, follows the real consumption on Friday the 8th May 2009. The model considers if a day is a day off or not.

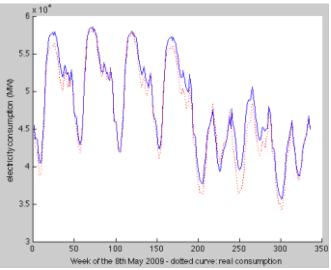


Figure 7: Electricity prediction of a week (with day off) in May 2009

5.2 Annual Prediction

For the annual prediction, the Multiple Linear Regression method has a mean absolute difference of 1.9621% regarding the real electricity. The mean difference between the real consumption and the prediction is 1.7216% (RTE, 2008). The results obtained are close to the efficiency get by RTE. The coefficients of the variables are in the following table in figure 9.

Definition	Coefficient	Values
1 day off - 0 if not	b(1)	-3.0263*10^5
Temperature	b(2)	-0.1187*10^5
Nebulosity	b(3)	-0.0258*10^5
1 Monday - 0 if not	b(4)	9.4700*10^5
1 Tuesday - 0 if not	b(5)	7.1837*10^5
1 Wednesday - 0 if not	b(6)	6.6188*10^5
1 Thursday - 0 if not	b(7)	6.5446*10^5
1 Friday - 0 if not	b(8)	6.2592*10^5
1 Saturday - 0 if not	b(9)	3.7759*10^5
1 Sunday - 0 if not	b(10)	4.4553*10^5
Value of the previous daily consumption	b(11)	0.8171

Table 1: Values of the various coefficients of the Multiple Linear Regression

The coefficient b(1) is negative because during a day off less electricity is consumed. b(2) is also a negative coefficient. Indeed, higher the temperature is less electricity is consumed. b(3) do not have a significant effect on the electricity consumption. The coefficients from b(4) to b(8) are quite identical. Indeed, they represent the different day of the week from Monday to Friday. b(4) is higher because the algorithm take into account the consumption of the previous day. On Sunday, the consumption is weak so the algorithm needs a higher coefficient for Mondays. b(9)-b(10): these coefficients are smaller than the coefficients corresponding to the other day of the week. Indeed, during the weekend, less electricity is consumed. The coefficient b(11) is very small compared to the others that are multiply by 10^5. But this coefficient is very important. Indeed, thanks to this coefficient the prediction can take into account the abnormal heat or cold waves. The visualisation of the annual prediction is shown in the figure 10.

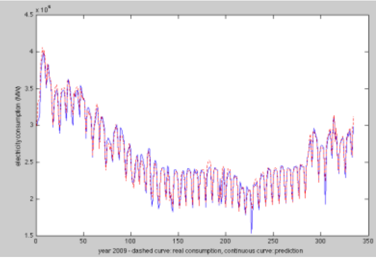


Figure 9: Annual electricity prediction of 2009

6 Conclusions and the Future

After some training and testing, with few algorithms good results have been obtained. Indeed, the Multiple Linear Regression has shown very good results: efficiency of 1.9621% instead of 1.7216% from RTE.

Currently, forecasting has a good efficiency. Nevertheless, it should improve their quality in order to avoid large forecast errors, which can be penalizing especially during periods of tight supply-demand balance. Furthermore, it should take into account new elements that may impact the electricity consumption such as the evolution of the electricity demand, the changing uses of electricity and the development of demand management of electricity. For example, the electricity consumption has stared to decrease in 2011 in France.

New algorithms will have to be found. Algorithms that take in account the evolution of the production of electricity by people thanks to solar panels and personal winds. Indeed, with the evolution of renewable energies, the countries will have to product less and less electricity. Because the electricity consumption of people are changing constantly, algorithms will have to be trained again and again until an algorithm that takes in account all the variables needed is found.

7 References

Antoch, J., Prchal, L., De Rosa, M.R., Sarda, P. (2010), Electricity consumption prediction with functional linear regression using spline estimators, Taylor and Francis, 2012.

Bianco, V., Manca, O., Nardini, S. (2009), Electricity consumption forecasting in Italy using linear regression models, Energy 34, 2009, pp. 1413–1421.

Cugliari, J. (2011) Prévision non paramétrique de processus à valeurs fonctionnelles, Cugliari, Université Paris-Sud 11, Faculté des sciences d'Orsay, [online] http://tel.archives-ouvertes.fr/docs/00/64/73/34/PDF/VD_CUGLARI_JAIRO_22112011.pdf (Accessed: August 26th 2012)

Littell, R. (2009), Linear Regression Analysis [online] http://www.stat.ufl.edu/CourseINFO/STA3032/Linear%20Regression%201.pdf (Accessed: August 26th 2012)

Mitchell, T.M., Carbonell, J.G., Michalski, R.S. (1985) Machine learning: an artificial intelligence approach, ISBN: 0-934613-09-5.

RTE (2008), Consommation française d'électricité, Caractérisitque et méthode de prévision, RTE, [online] http://www4.ac-lille.fr/~sphappli/IMG/pdf/methodologie_des_previsions_de_la_conssomation_electrique.pdf (Accessed: August 26th 2012)

Impedance Measurements of Magnetic Wires under the Effects of Stress and Temperature

G.S. Majin and L.V. Panina

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

Abstract

To gather, observe and analyse data from impedance measurements of amorphous wires at MHz frequencies for the possible use in the theoretical modelling of composite behaviour in arrays of magnetic wires and to develop a relationship between the impedance and the effective permittivity of the wires.

Keywords

Impedance, Amorphous Wires, Papers

1 Introduction

Amorphous magnetic wires became available some 20+ years ago. In that time, many interesting characteristics attributed to the wire have been investigated. They are unique to the wire geometry, its method of fabrication and to its amorphous nature. (Humphrey, 2002) And in that space, the wires have steadily grown from just an aspect of novelty, to something with established interest and demand. Many aspects of the wires have been looked and studied including methods of fabrication (Zhukov & Zhukova, 2009; Zhukov et al, 2004; Zhukov et al, 2000; Chiriac & Ovari, 1996).

The studies of the magnetic properties of amorphous glass coated microwires started in the 70s (Kraus et al, 1976) but those studies were limited to Fe-Ni compositions, measurements of hysteretic properties and ferromagnetic resonance. Recently though these tiny glass-coated ferromagnetic microwires have attracted new attention due to a number of unusual magnetic properties and potential applications in sensors (Mohri & Honkura, 2007, Ripka, 2001, Vazquez & Hernando, 1996) and multifunctional composites (Qin et al, 2010; Panina 2009; Phan & Peng, 2008). It is this field that provides the context of the project. The concept of GMI (Giant Magneto Impedance) was discovered in 1994, and since its discovery, *"the GMI effect has become a topic of great interest in the field of applied magnetism owing to the large sensitivity of the total impedance to the applied DC field at low field magnitudes and high frequencies*." (Panina & Mohri, 1994; Beach & Berkowicz, 1994). It is this high sensitivity of the wires at MHz and GHz frequencies that allowed for the concept of the wires as embedded sensors to be put forward. This paper shows the strong tunable characteristics of the wires based on the measurements of its impedance change over field. With this information and accurate modeling based on real data, new theories and behaviours of the wires can be extracted and based on the information; the wires can be configured and reconfigured to fit the specific sensory characteristics required of it.

2 High frequency impedance measurement setup

Below is the equipment setup used for the experiment:

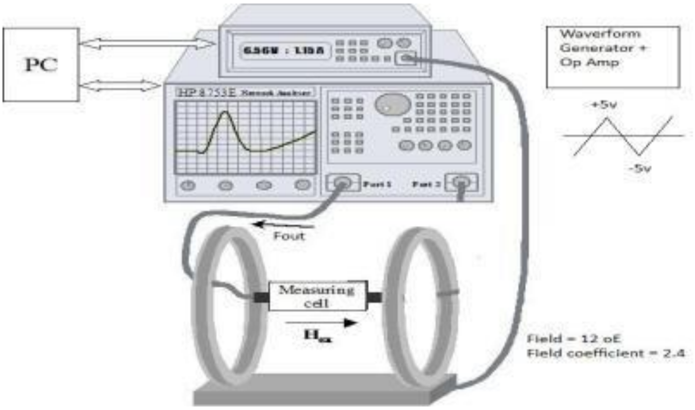


Figure 1: Experimental Set up for High Frequency Impedance measurements

A network analyser sends frequencies within the specified range of 50 – 150 MHz. A waveform generator set to +/- 5v ramps up and down, driving the field while measurements are taken over different field points. Each wire sample is placed in a measuring cell. The field was measured to be 12 oE (Oersted) giving a field coefficient of 2.4. This is necessary for the calibration of the software which measures the field dependence of the impedance Z(H) from the reflection coefficient when the dc magnetic field H changes from –H to +H. Table 1 below shows the specifications of the 8 wires sampled:

Serial no	**Type**	**d_m(μ *m*)**	**D_{gl} (μ *m*)**	**H_c(A/ *m)***
Wire 1	4924 (CF246)	19	19.4	Unknown
Wire 2	4918 (CM588)	21.6	17.4	Unknown
Wire 3	4918 CO	21	23.6	Unknown
Wire 4	MLCK-2	37.4	24.5	19.4
Wire 5	MWS-1	38.2	23.6	Unknown
Wire 6	Unknown	28.8	19.8	37.8
Wire 7	MWGMI 10	14	9.4	175
Wire 8	4918 (B437)	22.4	28.4	200

Table 1: Wire specifications

It is important to note that some details for the other wires are classified. The wires types are two in particular. Giant Magneto Impedance wires (GMI) with circular anisotropy; having almost linear saturation magnetisation loop and Bi-stable wires with axial anisotropy having rectangular magnetisation loop, in figure 2 below the typical magnetisation loop of the wires are demonstrated:

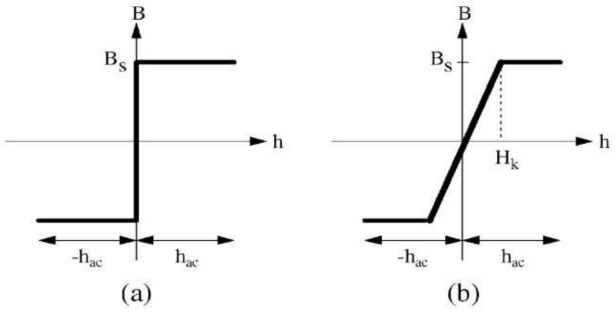


Figure 2: Showing the typical Magnetisation loop of Bi-stable and GMI wires respectively.

These different responses yield to widely different impedance responses of the wires and hysterisis loops. The GMI wires yield a greater impedance change over field than the Bi-stable counterparts and thus are decidely more sensitive under normal conditions. Below (Figure 3) is an example of the typical response for both wire types:

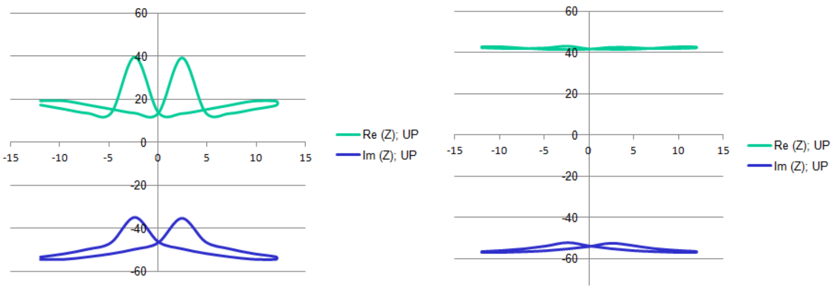


Figure 3: Showing the impedance change on both the real (top) and imaginary (bottom) for GMI and Bi-Stable wires respectively. Field (H) is -12 to +12 measured at 108 MHz.

Observable changes can also be looked into when the data is analysed at different frequencies simulateously. It appears that the percentage change in impredance is very observably different when looking at the real and imaginary data independently. A noticeable trend seems to be that the real part is much less sensisitve than the imaginary for the wire samples used. As the frequency increases, the general peak impedance and the slope of the change decreases, but the effect is much more pronounced with the imaginary side as shown in Figure 4.

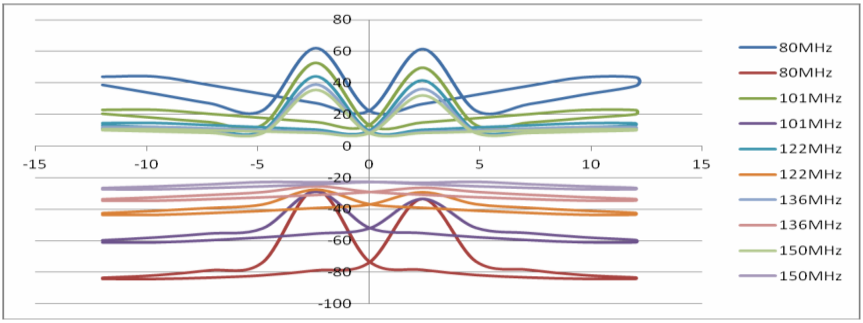


Figure 4: Impedance change appears to be more sensitive over different frequencies in the imaginary part than the real part. Frequency range 80 – 150MHz.

One possible way to look at this trend is to observe its effect on the actual impedance of the wires. To know the actual impedance, the formula is used to determine the values: $\sqrt{a^2 + b^2}$ *where a is the real impedance and b is the imaginary impedance*. At low frequencies the imaginary impedance has a greater presence, while that value dramatically reduces as the frequency increases. The effect this has on the actual impedance of the wires is that for some wires, there is sometimes a negative change in actual impedance at certain (usually lower) frequencies over field and a positive at higher frequencies, for example with wire sample 3 in Figure 5 below.

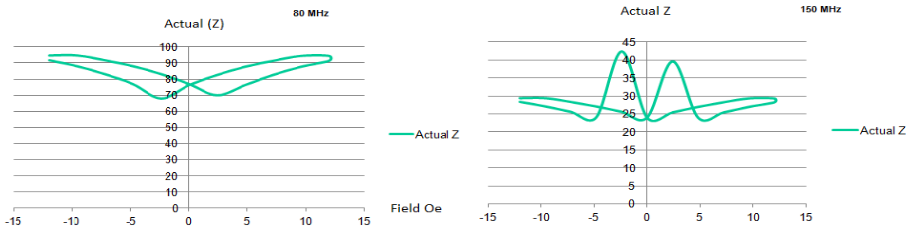


Figure 5: Showing negative to positive change in impedance over field as the frequency increases from 80 MHz to 150 MHz

Taking measurements of the impedance of the wires as a function of frequency gives a dispersion spectra in figure 6.

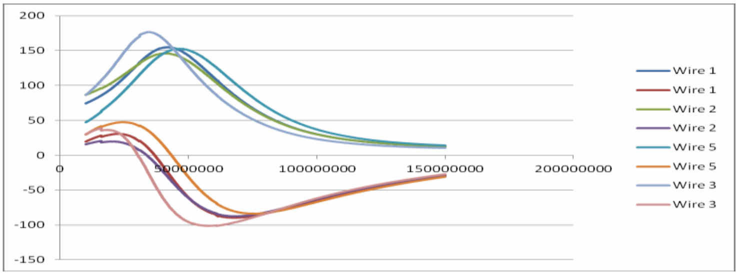


Figure 6: Impedance as a function of frequency, showing fairly common resonance in the wires.

Temperature measurements were applied to all the wires, however they did not come without limitations. Target temperature was 70 degrees for all wires. These are not the most temperature sensitive wires available but all the GMI wires still registered about a 5-15% change in peak impedance versus room temperature. The PCB of the measuring cell cannot allow for measurements realistically above 70 degrees coupled with the delay of the measuring hardware and software. Figure 7 below shows the typical response of a GMI and Bistable wire to temperature.

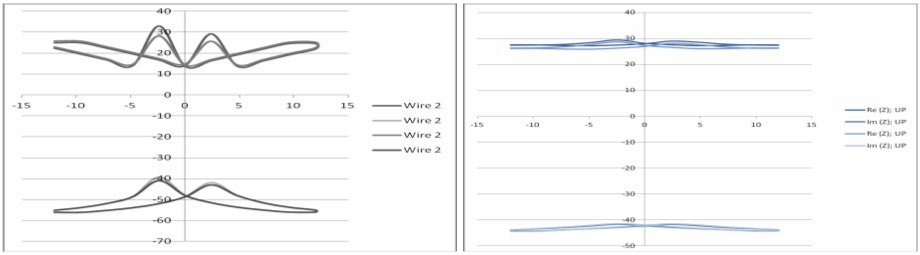


Figure 7: Showing that peak impedance value decreases with temperature. Real part appears to be more sensitive than imaginary for both GMI and Bi-Stable wires.

Generally the real part of the impedance is much more sensitive to the effects of temperature than the imaginary part. GMI wires are still predictably more sensitive in this test than Bi-stable wires. Limitations of equipment make it hard to see the effects at higher temperatures.

Stress measurements were also applied to the wires.Wires were taped and twisted before soldered into the cell. The effective number of twists applied to each wire was about three, so that bias can realistically be evened out and to give a sense of in impedance as shown in Figure 8.

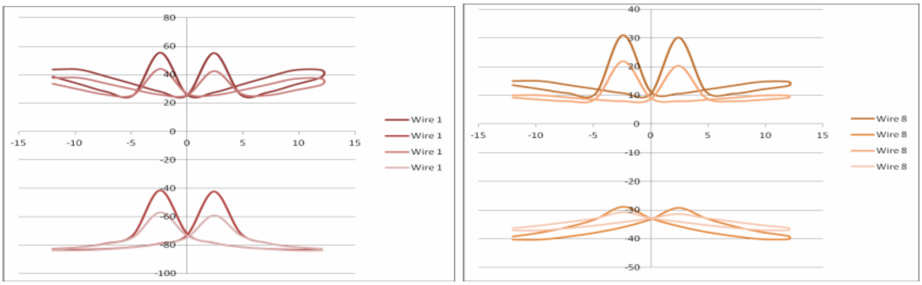


Figure 8: Showing the effects of stress on GMI wire samples 1 and 8. Both real and imaginary parts are equally sensitive and like with temperature, the peak impedance is reduced.

Like with temperature magneto-impedance (difference between peak and lowest impedance value) and sensitivity (slope of the rising curve) is reduced as a matter of fact, however there is an irregularity with the wire sample 5. At the lower end of frequencies the stress effect creates larger magneto-impedance effect in both the real and imaginary and at the higher end maintains a larger magneto-impedance effect in the imaginary as shown below in figure 9.

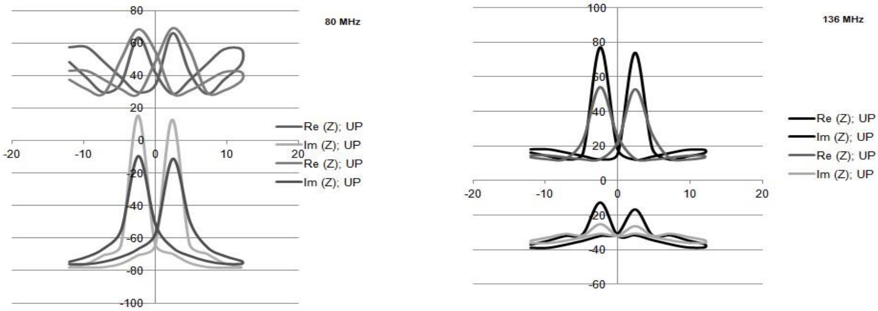


Figure 9: Showing irregularities against trend with wire sample 5.

The different response to stress for this wire can possibly be attributed to the method of applying stress but is more likely to do with the fabrication of the wires used.

For the Bistable wires at most tested frequencies, both wires experienced a complete shift in their normalised values of impedance in both real and imaginary planes. However in the real part the effect of stress is an increase in normalised impedance for Wire sample 6 and a decrease for Wire sample 4. Wire sample 4 generates a bigger curve as a result of stress while Wire sample 6 flattens as shown in Figure 10.

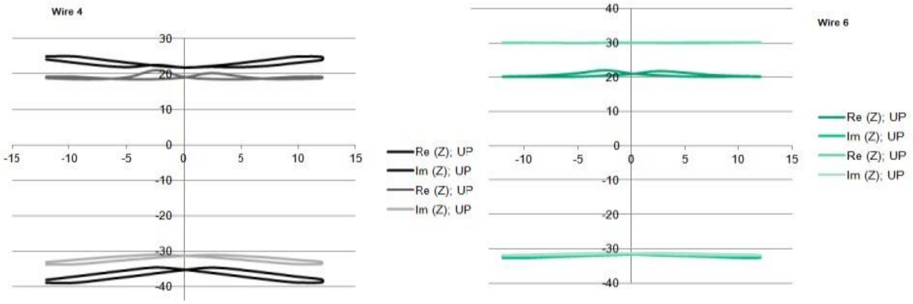


Figure 10: Comparing the bistable impedance response

Comparing the sensitivity of the GMI wires used, the values are normalised and we observe the difference in magneto-impedance effect and in sesitivity. These differences can be attributed to the diatemter or the wires, their glass coating, the comosite materials and possibly other un-indentified (classified) factors.

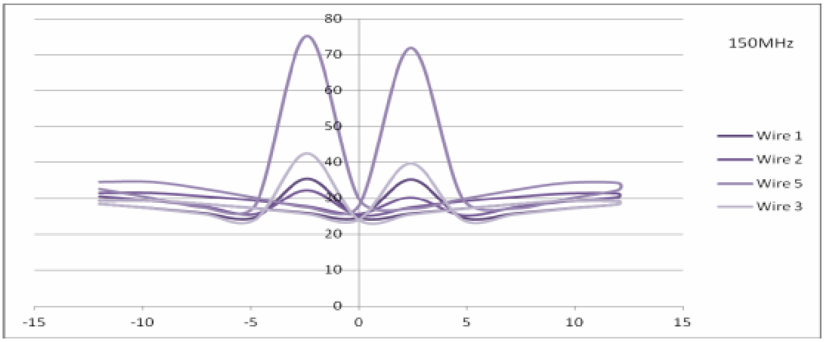


Figure 11: Normalised impedance values for GMI wires.

3 Theoretical modelling

Now that real data has been acquired for all the wires, a theoretical model can be conceived. By relating the impedance data that was gotten from the experiments with the “effective permittivity” (and relaxation parameters) of arrays of the magnetic wires, a theoretical model can be further developed to show that the losses are determined by the surface impedance depending on the wire’s magnetic properties. This is useful data for remote wireless monitoring of stress levels and strain related levels too. This is where on-going future research is heading towards (due to time constraints) and where desirable results are continually being targeted.

4 References

Beach, R.S. & Berkowicz, A.E. (1994). Giant magnetic field dependent impedance of amorphous FeCoSiB wire. *Appl.Phys.Lett.*, Vol. 64, No. 26, Jun 1994, pp. 3652-3654, ISSN0003-6951

Chiriac, H. & Ovari, T.A. (1996). Amorphous glass-covered magnetic wires: preparation properties, applications. *Progress in Material Science,* Vol. 40, No. 5, February 1999, pp. 333-407, ISSN: 0079-6425

Humphrey, F.B. (2002). 'Nearly 20 years of magnetic amorphous wire'. *Journal of Magnetism and Magnetic Materials,* 249(1-2*)*, 1-2 [online] doi: 10.1016/S0304-8853(02)00494-8 (Accessed November 22, 2011)

Kraus, L.; Schneider, J.; & Wiesner H. (1976) Ferromagnetic resonance in amorphous alloys prepared by rapid quenching from the melt. *Czech. J. Phys*. Vol. 26, No. 5. May 1976, pp.601-602, ISSN: 0011-4626

Mohri K. & Honkura Y. (2007). Amorphous wire and CMOS IC based magneto-impedance sensors --- Orign, topics, and future. *Sensor Letters*, Vol. 5, No. 2, March 2007 pp. 267-270, ISSN 1546-198X

Panina, L.V. & Mohri, K. (1994). Magneto-impedance effect in amorphous wires. Appl.Phys.Lett, Vol. 65, No. 9, August 1994, pp. 1189-1191, ISSN 0003-6951

Peng, H.X.; Qin, M.H.; Phan, F.X.; Tang Jie, Panina, L.V.; Ipatov, M.; Zhukova, V.; Zhukov, A. & Gonzalez J. (2009). Co-based magnetic microwire and field-tunable multifunctional macro-composites. *J. Non-Crystalline Solids*, Vol. 355, No. 24-27, August 2009, pp. 1380-1386, ISSN: 0022-3093

Qin, F. X. ; Peng, H. X.; Pankratov, N.; Phan, M. H. ; Panina, L. V. ; Ipatov, M.; Zhukova, V.; Zhukov, A.; & Gonzalez J. (2010). Exceptional electromagnetic interference shielding properties of ferromagnetic microwires enabled polymer composites. *J. Appl. Phys.*, Vol. 108, No. 4, August 2010, pp. 044510-044515, ISSN 0021-8979

Ripka P. (Ed). (2001). Magnetic sensors and magnetometers, Artech House Publishers, ISBN1-58053-057-5, Norwood, USA

Vazquez, M. & Hernando, A. (1996). A soft magnetic wire for sensor applications, *J Phys D: Appl Phys*, Vol. 29, No. 4, April 1996, pp. 939–949

Zhukov A. & Zhukova V. (2009). *Magnetic properties and applications of ferromagnetic microwires with amorphous and nanocrystalline structure*, Nova Science Publishers, ISBN:978-1-60741-770-400, Hauppauge, NY, USA

Zhukov, A.; Gonzalez, J.; Vazquez, M.; Larin, V. & Torcunov, A. (2004) Nanocrystalline and Amorphous Magnetic Microwires, In: *Encyclopedia of Nanoscience and Nanotechnology*, ed. Nalwa H. S., pp. 365-387), American Scientific Publishers, ISBN: 1-58883-001-2, Valencia, USA

Zhukov, A.; Gonzalez, J.; Blanco, J.M.; Vazquez, M. & Larin, V. (2000). Microwires coated by glass: A new family of soft and hard magnetic materials. *J. Mat. Res.*, Vol. 15, No. 10, October 2000, pp. 2107-2113, ISSN: 0884-2914

Spectral Analysis of Magnetic Wire Response for Non-Destructive Evaluation of Composite Structures

J.V. Martínez-Sapiña and L.V. Panina

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

Abstract

The magnetization processes in amorphous wires present non-linearity when excited by low magnetic fields, generating high order harmonics response. Furthermore, the magnetic configuration can be made very sensitive to external stimuli (for example, mechanical or thermal), and hence, the harmonic spectra will experience modifications depending on the state of the environment. If such microwires are incorporated inside a composite material, the harmonic spectra detection can be used for remote query measurement of stress and temperature. In this project, the voltage signals due to remagnetization of two different wires response (linear with saturation and bi-stable) under different conditions and substrates are analyzed to understand the effects of the external factors has on them. With this information, a spectral analysis of the voltage response is carried out. In the first place, a theoretical model to explain the origin and behaviour of the higher-order harmonics in response to temperature, stress and torsion effects is developed. In the second place, the analysis of the voltage signals is done by using the FFT to verify, among other things, the theoretical results. Finally, the FFT results are compared with direct harmonic measurements using a spectrum analyzer to study the viability of the FFT to obtain information based upon changes in the amplitudes of the higher-order harmonics.

Keywords

Sensor; FFT, Spectral Analysis, Amorphous Wires; Harmonic; Temperature; Stress; Torsion; Magnetically soft.

1 Introduction

The advancement of new composite materials with sensing properties that allow to obtain information on its current state are in high demand nowadays for structural evaluation and rehabilitation. Many structural failures are caused by stress and temperature related problems, such as formation of cracks, voids, deformation of the materials, etc. The development of new sensor materials permitting continuous condition monitoring (stress, strain, temperature, corrosion, etc.) is an important aspect to check and verify the health of structural components. Thus, miniature sensing systems are required to be bounded into a material without affecting its structural integrity (Mohri *et al.*, 2009). Amorphous wires are a new class of composite materials that meet the requirements above commented and they will benefit from low cost, very high sensitivities at low concentrations, consistency with structural integrity and remote wireless monitoring of stress with the use of microwave scanning techniques at low energies (Vázquez *et al.*, 2010).

The magnetization processes in amorphous wires present non-linearity when excited by low AC magnetic fields (Fetcher and Gershenfeld, 2000), generating high order harmonics response (Kim *et al.*, 2000; Ong and Grimes, 2002). Furthermore, the magnetic configuration can be made very sensitive to external stimuli (for example, mechanical or thermal), and hence, the harmonic spectra will experience modifications depending on the state of the environment. If the wires are incorporated inside a composite material, the harmonic spectra can be used for remote query measurement of stress, torsion and temperature because the harmonic generation is based only upon the magnetic properties of the wires (Ong and Grimes, 2002).

In this paper, the variations that the voltage response and its harmonic spectra suffer under tensile stress, torsion and temperature effects of eight different wires (linear with saturation and bi-stable responses) attached into four different materials (aluminium, paper, plastic and wood) are studied using the FFT analysis and a spectrum analyzer.

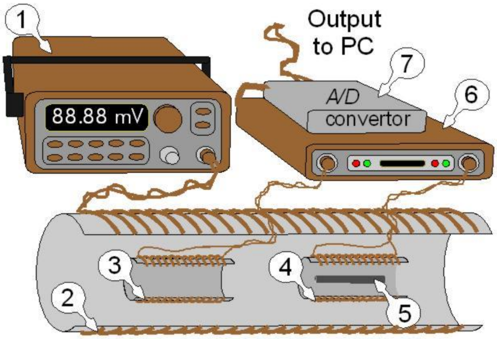


Figure 1: Experiment setup designed (Sandacci, 2004). The components are: (1) Signal generator, (2) Helmholtz coil, (3) compensation coil, (4) pick-up coil, (5) sample, (6) differentional pre-amplifier, and (7) A/D converter

The samples (5), which were created in the same way by attaching a wire into the material using cellophane, were placed in one of the pick-up coils (4), as shown in Figure 1. The effect of the uniform magnetic field generated by the Helmholtz coil (2), which was fed by using a 4 volts sinusoidal signal at 50 Hz produced by (1), was cancelled out inside the pick-up coils (3) and (4). The resultant voltage signal presented the magnetization changes of the sample. A differential detection system (6), which contains amplifiers and high frequency band-pass filters to suppress noise, is used to amplify and limit the input noise of the resultant voltage signal. Finally, the signals are displayed and stored in the computer after passing through the A/D converter (7).

All tests carried out in this research were performed in the same way. Normal tests were used as a reference. All the samples were introduced in the same coil with the wire facing up and after waiting some time, the signals were captured. In the stress tests, the samples were introduced in the same coil and a load was attached at the end of each sample. Then, the signals were stored. For the torsion tests, all the samples were twisted in the same direction and then introduced in the same coil. Then, the signals were stored in the computer. Finally, for the temperature tests, all samples were heated up until they reached 70º and then inserted in the coil. Finally the signals were captured.

2 Low frequency magnetization response.

When the wire is subjected to a mechanical or thermal stimuli, its magnetization changes and hence the amplitude and the shape of voltage signal varies as well (Fetcher and Gershenfeld, 2000; Kim *et al.*, 2000). By analyzing these changes, very useful information is obtained to study the harmonic spectra.

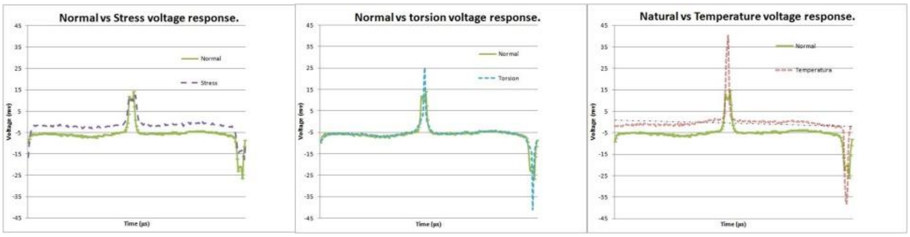


Figure 2: Voltage response under different conditions.

The first method to study these changes it is based on the variation of the shape of the voltage signal (figure 2) and it will be helpful to understand the changes in the harmonic spectra. When the samples are under stress, the voltage response amplitude decreases and the signal width increases. If the samples are under torsion, the amplitude of the signal increases and the width decreases. Finally, when the samples are under a temperature above the ambient one, the amplitude of the signal increases and the width decreases.

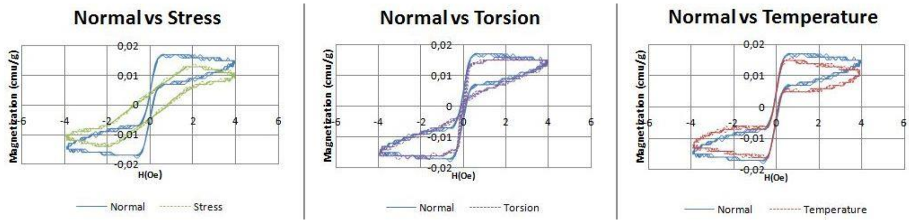


Figure 3: BH-loops under different conditions.

The second method consists in analyzing the changes that occur in the BH-loop of the wire. When the samples are under stress, the hysteresis shape is modified by increasing the coercivity, and hence, the magnetization decreases. If the samples are torsion, the distance between the BH-loop curves slightly decreases, and therefore, the coercivity decreases and the magnetization varies. Finally, in the temperature tests, the distance between the two curves decreases a little and consequently, its coercivity decreases.

3 Spectral analysis.

3.1 Theoretical model.

The higher order harmonic response the magnetic flux generated by the wire, at time t, can be modelled as follows:

$$B(t) = \sum_{n=1}^{\infty} a_n \cos(n\omega t + \phi_n) \quad (1)$$

where B(t) represents the magnetic flux, *n* is the number of the harmonic, a_n is the amplitude of the *n*th harmonic, ω is the fundamental frequency and ϕ_n is the phase between the direction of the magnetic field and the *n*th order harmonic. By applying the Fourier series decomposition to B(t) (Oppenheim *et al.*, 1983), it is obtained:

$$B(h) = C_0 + \sum_{n=1}^{\infty} 2|a_n| \cos\left(\frac{nh}{h_{ac}} + \phi_n\right) \quad (2)$$

where *h* is the applied ac field, h_{ac} its amplitude, C_0 the dc offset and b_n is the coefficient of the *n*th order:

$$b_n = \frac{1}{h_{ac}} \int_{-h_{ac}}^{h_{ac}} B(h) e^{-j\frac{n\pi h}{h_{ac}}} dh \quad (3)$$

For convenience and to simplify the calculations, the approximations given by Grensted (Grensted, 1953) and Ong and Grimes (Ong and Grimes, 2002) are going to be used, that is, it is assumed that h varies linearly with time whose value is $h_{ac}\omega t/2\pi$ and a_n is $|b_n|/\pi$.

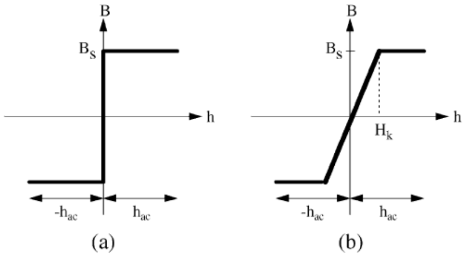


Figure 4: Bi-stable response (a) and linear with saturation response (b).

To calculate the theoretical response of **bi-stable wires**, it is applied equation 3 directly to the bi-stable response (Figure 4a). Using the linear approximation of h and doing some operations, b_n is 0 for even values and $\frac{2B_s}{n\pi}$ for odd values. The measured signal amplitude of the nth harmonic is determined by substituting b_n and a_n into equation 1 and taking the time derivate. Thus, the value of the measured amplitude, A_n, is $\frac{2B_s\omega L}{\pi^2}$, where L represents the detection circuit parameters.

On the other hand, to obtain theoretical response of **linear with saturation wires**, it is applied equation 3 directly to the linear with saturation response (Figure 2b):

$$b_n = \frac{B_s}{2h_{ac}}\left(\int_{-h_{ac}}^{-H_k} -e^{-j\frac{n\pi h}{h_{ac}}}dh + \frac{1}{H_k}\int_{-H_k}^{H_k} h - e^{-j\frac{n\pi h}{h_{ac}}}dh + \int_{H_k}^{h_{ac}} e^{-j\frac{n\pi h}{h_{ac}}}dh\right) \quad (4)$$

Using the approximations commented above, solving equation 4 and substituting b_n and a_n into equation 1 and taking the time derivate, the measured signal amplitude of the nth harmonic is obtained, whose value is as follows:

$$A_n = \frac{2B_r\omega L}{\pi^2}\left|\cos(n\pi) - \frac{h_{ac}}{n\pi H_k}\sin\left(n\pi\frac{H_k}{h_{ac}}\right)\right| \quad (5)$$

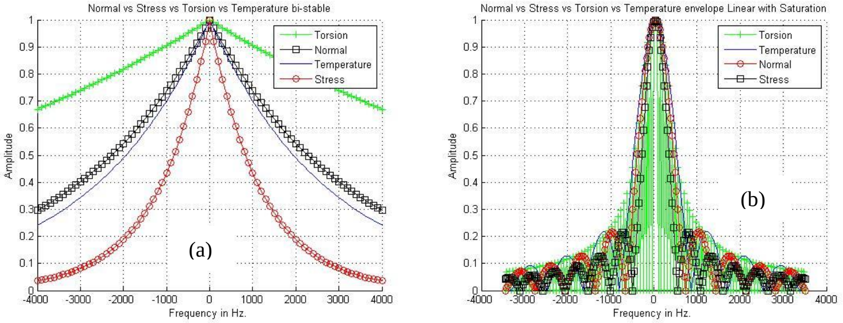


Figure 5: Plots for the theoretical bi-stable response (a) and linear with saturation response (b) under different conditions.

In figure 5 it is possible to find the plots for the different theoretical models. On the one hand, for the bi-stable response, although the result obtained said that the amplitude will remain constant, due to finite permeability and hysteresis losses it will decay when increasing the order number (Ong and Grimes, 2002) and the way the magnetization and the amplitude change was obtained in the low frequency magnetization response analysis. On the other hand, the amplitude of the harmonics decays when increasing the order because the second term of equation 5 reduces the value of the first term. In addition, the magnetization changes were obtained in the the low frequency magnetization response analysis.

3.2 FFT analysis.

In theory, the spectrum estimation is straightforward, simply calculate the FFT of the data sequence and plot it. In practice, the FFT has some limitations that were taken into account (leakage, number of points obtained, bandwidth available, etc.) (Ifeachor and Jervis, 2001). In addition, because it is know how the voltage signal varies under different conditions, it is possible to know how the spectrum is going to behave just by applying the basic time-frequency duality (Oppenheim *et al.*, 1983).

The FFT analysis of the bi-stable wires was not carried out because due to the equipment limitations used, it was impossible to capture a proper voltage signal to proceed to the analysis.

The FFT analysis of the linear with saturation wires is found in figure 6. As it can be seen, the results predicted by the theoretical analysis are very similar to the FFT ones. The size, position and amplitude of the lobes depend on the magnetic properties of the wire (which changes under different conditions) and the state of the material. Most of the spectrum energy is concentrated in the main lobe and the rest is spread into the side lobes. The attenuation suffered by the side lobes is bigger than the one predicted because the system introduces additional losses that were not taken into account such noise, connector cables losses, etc (Ong and Grimes, 2002). The results are normalized to the 3rd harmonic to ease the comparisons among figures.

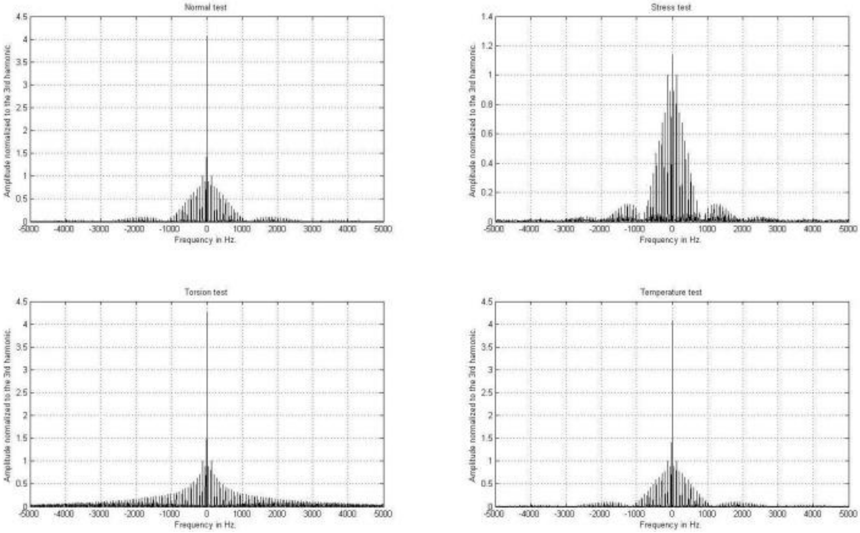


Figure 6: FFT analysis of one of the wires. Normal test (top right), Stress test (top left), Torsion test (bottom right) and Temperature test (bottom left).

3.3 Comparison between FFT analysis and direct harmonic measurements.

The spectrum analyzer of a lock-in amplifier was used to measure the amplitude of each harmonic to compare the performance of both methods. The number of harmonics obtained using the lock-in amplifier were 30 (it represents a bandwidth of 1500 Hz.) and no more were taken due to problems when carrying out the temperature tests (the lock-in amplifier was slow and the sample started to cool down).

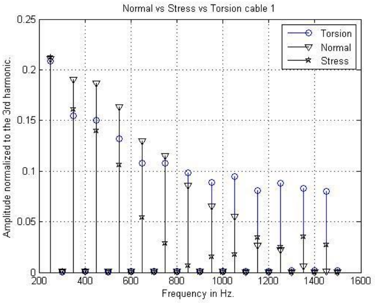


Figure 7: Plot of the direct harmonic measurement using the lock-in amplifier.

The behaviour and shape of spectra are the same when the wire is subjected under different conditions for both methods, as it can be seen in figures 6 and 7. In addition, the bandwidth of each lobe when using the same test is exactly the same for both. However, due to the differences of amplification from one method to the other, the value of the ratios is different although the information of the changes is available.

The noise level in the system is different from both methods. Whilst for the Lock-in amplifier method is almost negligible because it is cancelled out by the device, for the FFT depends on many parameters such as differentional pre-amplifier, connectors, etc. and it is bigger than the lock-in amplifier.

The speed for obtaining the harmonics is different. For the first method (FFT), it only takes a few milliseconds (with the computer used, MATLAB takes around 0.1 milliseconds to compute the FFT) to obtain the harmonics once the time signal is ready and digitalized. However, for the Lock-in amplifier method, it requires around one second to obtain one harmonic (the device needs time to cancel out the effect of the noise. Although this time can be reduced, it is going to be higher than the FFT method).

The system accuracy is different. The FFT method allows to obtain many harmonics in a quicker way but when increasing the order its amplitude will be affected by the noise. There is a point where is impossible to say if the amplitude corresponds to the harmonic or to the noise. On the other hand, the Lock-in amplifier is capable of measuring the signal amplitude even in noisy environments as long as is able to cancel the effect of the noise (the higher the harmonic is, the higher the time required to obtain its real value).

4 Conclusions

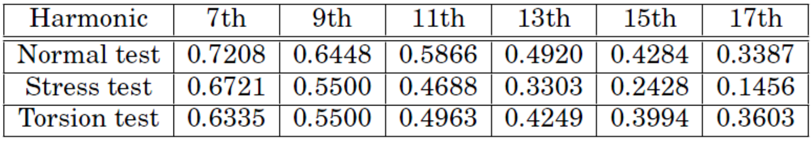
4.1 Low frequency magnetization processes.

The tests carried out over the samples used in the experiment have shown that amorphous wires can be used successfully to detect stress or temperature changes. In addition, the experiments have demonstrated that the wires response behave in a similar way when subjected under different conditions. This is because the forces applied in each test (torsion, tensile stress and temperature) act similarly in the wire's internal stresses. Thus, this implies that the BH-loop will also vary in a similar way.

4.2 Spectral analysis.

The theoretical model developed for linear with saturation wires corresponds with the measured spectra under different conditions.

The signals captured using the ADC have enough quality to be analyzed using the FFT. The spectrum obtained, whose bandwidth is 5 KHz and depends on the total number of points sampled by the ADC, has a very clear shape that allows to distinguish very high harmonics (over 40). The ratio of the amplitude for the nth harmonic varies under different conditions because there is change in the magnetization value. These variations are best seen when the higher the harmonic order is and therefore they allow to use amorphous wires as a stress/torsion/temperature sensors (table 1).



Harmonic	7th	9th	11th	13th	15th	17th
Normal test	0.7208	0.6448	0.5866	0.4920	0.4284	0.3387
Stress test	0.6721	0.5500	0.4688	0.3303	0.2428	0.1456
Torsion test	0.6335	0.5500	0.4963	0.4249	0.3994	0.3603

Table 1 – Ratios of from the 7th to 17th harmonics measured.

The results obtained by the lock-in amplifier by using its internal spectrum analyzer are equivalent to those obtained using the FFT method because the behaviour and shape of spectra is the same when the wire is subjected under different conditions. However, there are two main differences between both methods (see section: the first one is the noise level (the lock-in amplifier cancels out the effect of noise) and the second one is the speed to obtain the harmonics spectra (the FFT is faster than the lock-in amplifier method). For these reasons, it can be said that the use of FFT to analyze the time signals is very convenient because it allows to obtain the harmonic spectra in a quicker and cheaper way.

5 References

Fletcher, R. and Gershenfeld, N. (2000), "Remotely Interrogated Temperature Sensors Based on Magnetic Materials", IEEE Transactions on magnetics, Vol. 36, No. 5, pp. 2794-2795.

Grensted, P. E. W. (1955), "The frequency response analysis of non-linear systems.", IEEE, vol.102, pp.244-253.

Ifeachor, E. C and Jervis, B. C. (2001), Digital Signal Processing: A Practical Approach, 2º Edition, Prentice Hall, UK, ISBN: 0-20-159619-9.

Kim, C., Kim, H., Ahn, S., Cha, S. and Chang, S. (2000),"Magnetizing angle dependence of harmonics of magnetic induction and magnetostriction in electrical steel", Journal of Magnetism and Magnetic Materials, Vol. 215-216, pp. 159-161.

Mohri, K., Humphrey, F. B, Panina, L., Honkura, Y., Yamasaki,J., Uchiyama, T. and Hirami, M. (2009), “Advances of amorphous wires magnetics over 27 years”, Physical Status Solidi A, Vol. 206, No 4, pp 601-607.

Ong, K. G.; Grimes, C. A. (2002), “Tracking the harmonic response of magnetically-soft sensors for wireless temperature, stress, and corrosive monitoring”, Sensors and Actuators, vol.101, pp. 49-61.

Oppenheim, A. V.; Willsky, A. S.; Young, I. (1983), Signals and systems, Prentice-Hall, USA, ISBN: 0-13-809731-3.

Sandacci, S (2004), Dynamic magnetic effects in amorphous microwires for sensors and coding applications., University of Plymouth.

Vázquez, M., Chiriac, H., Zhukov, A., Panina, L. and Uchiyama, T. (2010), “On the state-of-art in magnetic microwires and expeted trends for scientific and technological studies”, Physical Status Solidi A, Vol. 208, No 3, pp 483-501.

Section 2

Computer and Information Security

Study of RSA Performance in Java Cards

G. Bernabé and N. Clarke

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

Abstract

In a near future smart card may have to use RSA 4096 bits on Java cards, so it may be interesting study the viability of RSA (both for private key and public key operations) in smart cards fopr such key lengths.

In this paper, some measurements of RSA performances carried out (using keys lengths from 512 to 2048 bits) for a recent Java card are presented and some regression analyzes as well as some statistical tests have been performed in order to calculate some estimations of performances for operations with RSA 4096 bits. This study shows that it may be realistic for smart cards' manufacturers to implement RSA 4096 bits in today's smart cards (notably Java cards), mainly for smart cards implementing TLS and certificate checking with public key operations.

Keywords

Smart cards, performance, RSA, Java Card, TLS

1 Introduction

Actually, different applications use RSA cryptosystem in smart cards: traditional applications such as banking (EMV protocol [EMV]), but also some Internet applications: particularly for Web authentication with TLS when the client is authenticated with his certificate and his private key (also called mutual authentication), in this case the smart card performs a RSA operation with its private key (e.g.: [Aussel J.-D., 2007], [PKCS11], [CAPI]). Some other applications (few for the moment) also implement the entire TLS Handshake protocol in the smart card for the client side (e.g.: [Urien P., 2009] and [Lu H.K., 2007]), therefore, some operations with the public keys of the certificate authorities (CA) are required so that the card can check the server's certificate. There are already some CA on the Internet that sign certificates with RSA 4096 bits, for a full list: see [List of CA, 2011], actually more than 10 CA using RSA 4096 are included in Web browsers, at least for *Firefox* and *Internet Explorer* (CA using RSA 4096 are mainly those of governments but also few others like *Microsoft Internet Authority*: used by services such as *Outlook* for emails).

However, it appears that no Java cards (name given to the smart cards implementing Java Card specifications [Java Card]) implement RSA up to 4096 bits today, at least it hasn't been possible to find the specifications of such a smart card on the Internet. In fact RSA 4096 is part of the version 3 of Java Card, but even some recent smart cards implementing Java Card 3 don't implement RSA up to 4096 bits (e.g.: *G&D SmartCafe expert 6.0*, Java Card 3.0.1: [G&D SC 6.0, 2011]).

So when considering certificate checking in the smart card for some Internet applications, this can cause a problem of compatibility between the server and the smart card, when the smart card has to check the server's certificate.

The aim of this study is to assess the viability of RSA cryptosystem for smart cards, and to determine if it makes sense to implement RSA 4096 in today's Java cards, in particular in the context of TLS and certificate checking in the card. Some measurements of the times of signature/verification and encryption/decryption (using both private key and public key) have been carried out for the card G&D SmartCafe 3.2 (Java Card 2.2.1), then an attempt has been performed to correlate these measurements with the theoretical time complexity of RSA, in order to estimate the performances of RSA for longer keys (4096 bits).

RSA 2048 bits in smart cards is pretty fast, but when increasing the length of the key, the time of private keys operations grows quite quickly.

Furthermore RSA 4096 will be probably required in a near feature (if it is not replaced by other cryptosystems) for the other applications that already use RSA in smart cards.

In order to estimate the times of operations for RSA 4096 bits, a regression analysis is conducted, however the extrapolation to a key length of 4096 bits is possible only if the size of the registers of the RSA coprocessor is big enough to store such lengths of data, otherwise the estimations for RSA 4096 for this chip will be distorted. The chip of the smart card used for the tests is *NXP P5CD144*, and it contains a FameXE RSA coprocessor. According to the specifications of this chip: [NXP P5CD144, 2008], this FameXE coprocessor supports RSA with an operand length of up to 8-kbit (up to 4-kbit with intermediate storage in RAM only). So it is very probable that an extrapolation using a regression analysis is valid.

This study is organized as follows: a review of theory and time complexity of RSA is presented in **2.**, then some measurements carried out for a recent smart card equipped with Java Card are analyzed and correlated in **3.** and **4.**. Finally, some estimations of RSA operations with keys bigger than 2048 are calculated in **4.**, and the viability of RSA for smart cards is discussed in **5.**.

2 Background

In this part, some theoretical concepts on RSA are reminded before presenting the analysis of measurements.

2.1 RSA cryptosystem

Below is the definition of RSA theorem:

p and q are two secret prime numbers and$N=p \cdot q$;
e is an integer satisfying: $\gcd(e,(p-1)(q-1))=1$; and $1<e<(p-1)(q-1)$;
d is an integer satisfying:$ed \equiv 1(\mathrm{mod}\ (p-1)(q-1))$;and $m \in \mathbb{Z}_N$;

encryption (using public key) **decryption** (using private key)

$$c \equiv m^e(\mathrm{mod}\ N) \qquad \textbf{(1)}$$

$$m' \equiv c^d \equiv m^{ed}(\mathrm{mod}\ N) \qquad \textbf{(2)}$$

with m the plaintext and c the ciphertext then m' equals m

The proof of this theorem can be found in many books, this one by example: [Hoffstein J., Pipher J. and Silverman J.H., 2008], which is generally quite detailed for the proofs of theorems, with many exercises for undergraduate students.

A speed improvement of RSA operations with private key can be done using the Chinese remainder theorem (CRT), a method has been introduced by J.-J. Quisquater in 1982. As explained in [Smart N., 2002], using CRT, operations with private key can be also calculated as follows (equivalent to formula (2)):

$$\left\{\begin{array}{l} m_1 \equiv c^{d_1}(\mathrm{mod}\ p) \\ m_2 \equiv c^{d_2}(\mathrm{mod}\ q) \end{array}\right. \text{where}$$

$$\left\{\begin{array}{l} d_1 \equiv d(\mathrm{mod}\ (p-1)) \\ d_2 \equiv d(\mathrm{mod}\ (q-1)) \end{array}\right. ⍰ m=m_1+((m_2-m_1)(p^{-1}(\mathrm{mod}\ q))(\mathrm{mod}\ q))p$$

d_1, $d_2$and $p^{-1}[q]$(the inverse of p modulo q), are likely to be pre-computed and stored with the private key.

This is equivalent to calculate$m \equiv c^d(\mathrm{mod}\ N)$.

Thanks tho the CRT, this method substitutes the main modular exponentiation for two sub modular exponentiations with smaller exponents, this permits to speed up the time of calculation by about 4 times (sizes of p and q are generally close).

(security considerations of RSA are not developed here, as explained before, the focus is on time complexity)

Time complexity of RSA

As we can see, the calculations done by RSA operations are some modular exponentiations, efficient methods for implementing this calculations have been introduced many years ago, “square-and-multiply” algorithm (also called binary exponentiation), combined with the method of Montgomery multiplication [Koç C. K., 1994].

Using these methods, the basic time complexity for RSA operations with CRT is about:

$$\frac{3k^3}{8} + \frac{k^2+3k}{2}, \quad \textbf{(3)}$$

k being the length (in bits) of the exponent. For RSA without CRT the time complexity is:$\frac{3k^3}{2}$.

According to some recent articles (e.g.: [Huang Z. and Li S., 2011]), today “square-and-multiply” combined with Montgomery multiplication are still the 2 algorithms the most used for RSA, including in smart cards. However many improvements of these 2 algorithms for speeding up the operations have been published this last decade (e.g.: [Alia G. and Martinelli E., 2002], [Sepahvandi S. *et al.*, 2009] or [Huang Z. and Li S., 2011]...), so it's not easy to know which ones exactly are implemented in a given smart card.

Moreover the history of smart cards is made of perpetual sophistication of algorithms in order to counter a variety of physical and logical attacks, this has begun in about 1996 after the first timing attacks of Paul Kocher, until now with more complex attacks combining physical and logical attacks (e.g.: [Sato H. *et al.*, 2005], [Amiel F. *et al.*, 2009], [Markantonakis K. *et al.*, 2009]).

There are also some alternatives to these two algorithms, by example this article: [Wu C.-L. *et al.*, 2006] reviews different other algorithms that are very efficient.

As a result, the basic algorithms have been enhanced, so the time complexity from **(3)** isn't the real one. However, as far as I know, when using square-and-multiply algorithm combined with Montgomery multiplication or some of their variants, the time complexity for private key operations stays in $O(k^3)$.So it is likely to be the complexity of the algorithm implemented in the smart card used for the tests of this study. According to the papers previously mentioned: because of the constraints of embedded devices like smart cards, square-and-multiply algorithm combined with Montgomery multiplication or some of their variants have been much more popular for smart cards until now. So the hypothesis is made that the time complexity of RSA operations with private key for the smart card used for these tests is of the order of $O(k^3)$.

Concerning operations with public keys, the time complexity is much more inferior, because a common practice is to use a small exponent e, generally equal to 65537 ([Hoffstein J., Pipher J. and Silverman J.H., 2008], page 121), this is possible because it is admitted that it doesn't weaken the security of RSA. Then, complexity with public key is in$O(k^2)$.

3 Measurements

3.1 Methodology of measurements

In order to measure the times of RSA operations, the method used for this study is sometimes used by researchers for measuring smart card performances. The measure is performed on the host PC using the Java API of OCF [OCF, 2003]. First it consists in measuring the time for the card to execute the“empty loop”: the empty loop is the program containing the operation we want to measure but without the line of code corresponding to the operation we want measure. Secondly it consists in measuring the time for the card to execute the “full loop”: the full loop is the same program but containing the line of code corresponding to the operation we want to measure. Finally we can subtract the time of “empty loop” from the time of “full loop” to obtain the time of the operation (method used by [Cordry J., 2009] and [Rehoui K., 2005]).

For this study, all the other methods of the framework from [Cordry J., 2009] have not been used, because the measures were precise enough. However using this framework could have permitted to improve precision of measures, by modifying the bytecode to isolate again more the operation to measure and by using other statistical tests to refine the measures.

The tests have been carried out for the card *G&D SmartCafe 3.2* (Java Card 2.2.1). The smart card reader used is *Gemalto GemPC USB-SL*, which is USB full speed: 12Mbps

The measurements are performed with the following Java code, using the Java API of OCF [OCF, 2003]:

```
start=System.currentTimeMillis();
sendAPDU(cmd,true);
time=System.currentTimeMillis();
```

These measurements are probably relatively approximate because of the work environment and the possible noise, furthermore due to the high level API of Java Card language, the lowest operation that it's possible to measure for RSA is the one corresponding to this line of code (Java Card):

```
cipherRSA.doFinal(data,(short)dataOffset,byteRead,data,(s
hort)dataOffset);
```

So it's not easy to know which operations are added by the API in addition to the RSA operation, but this factor of imprecision has been limited to its maximum because the RSA algorithm used is ALG_RSA_NOPAD, this algorithm (part of the API of Java Card) doesn't add any random number or padding to the data, so it only performs the modular exponentiation of RSA.

The card never sends the data resulting of its operations, so the measure is not affected by the time for the PC to display the result (of course it has been verified beforehand that when displaying the response of the card, the encrypted/decrypted or signed/verified data is correct).

The probable noise is potentially problematic (tasks, processes of the OS...), but when running the minimal number of programs necessary to perform the measures (basically none except the shell to run Java), it has been noticed that time measurements are minimalistic. Furthermore the time of the "empty loop" is so small in comparison with the time of the "full loop" (in the case of private key operations), that the noise should be negligible. Also, in the case of RSA operations with private key, the difference of times of operation between two lengths of keys is so important that it would have been probably not very useful to get more precise measures. However concerning public key operations, the measured times are very small, and using the framework from [Cordry J., 2009] could have been probably useful for a better precision.

It has been decided not to make more than 20 measures for each operation as the standard deviation and variance of the distribution are very small proportionally to the order of the measurements.

One pair of RSA keys (private key CRT + public key) has been generated for each length of key (the card supports 9 lengths of key, 8 of them have been used). For each pair, 20 measures have been carried out for each operation with a given key. This makes a total of: 20 measures for the signature with the private key RSA CRT, 20 measures for the encryption with the public key, 20 measures for the verification with the private key RSA CRT and 20 measures for the decryption with the public key (this makes 20*4*8=640 measures), in addition there is a test in empty loop for each measure (making a total of 2*640=1280 measures). The data to process is always the size of the key (modulus).

3.2 Results

Here are the results of the measurements:

key size (bits) / stat	512	768	896	1024	1280	1536	1984	2048
signature (ms) private CRT	63.9	95	115.9	142.7	210.1	304.3	543.2	585
encryption (ms) public key	14.1	15.5	16	16.7	18.1	19.9	23.9	24.8

Table1: Performances of RSA for ALG_RSA_NOPAD in *G&D SmartCafe 3.2,* Java Card 2.2.1

For a given key length, performances with private key for signature and verification (with ALG_RSA_NOPAD) are almost identical so only the results for signature are mentioned, the same for encryption/decryption.

The curve of RSA signature grows quite quickly, the more the length of the key increases the more the growth of the curve is important.

When changing the scale of the time axis and representing also the encryption with the public key, we can see that the blue curve is really soaring by comparison with the red one that almost stagnates: the time of encryption with the public key only inched up from 14.1ms to 24.8ms whereas the length of the key increased from 512 to 2048 bits.

Considering that the complexity of operations with private key CRT is in$O(k^3)$,and operations with public key in$O(k^2)$,according to the measurements, for k=2048: the time of operations with public key is more than 20 times faster than with private key CRT. Then if we want to estimate the time of operations for RSA 4096 bits with public key for this smart card, we know that it will be at least more than 20 times faster than with private key CRT of the same length.

4 Analysis of results

4.1 Estimation of the model: first approach

So under the hypothesis that the time complexity of RSA CRT operations with private key is$O(k^3)$,then the equation of the blue curve is of the form: $t=ax^3+bx^2+cx+d$ with a, b, c and d constants, and t the time of the operation.

In order to find the constants using the measurements of Table1, the following system has been solved with *Mathematica* software (4 points have been chosen, 4 are required as there are 4 unknowns in the system):

$$\begin{cases} t_1=ax_1^3+bx_1^2+cx_1+d \\ t_2=ax_2^3+bx_2^2+cx_2+d \\ t_3=ax_3^3+bx_3^2+cx_3+d \\ t_4=ax_4^3+bx_4^2+cx_4+d \end{cases}$$

$$\text{with } x_1=512;\ x_2=896;\ x_3=1280;\ x_4=1948;$$

$$\text{and } t_1;\ t_2;\ t_3;\ t_4$$

the corresponding time values from Table1

The result is: $a = 4.50537\times10^{-8}$; b = 0.000021989; c = 0.0358071; d = 33.7555; **(4)**

Using this model just found, we can observe that the estimations for the other points are quite close to the values of measurements:

x / value	768	1024	1536	2048
t measured	95	142.7	304.3	585
t from model	94.6	141.6	303.9	586.3

An estimation for x=4096 is t=3645.41 ms.

4.2 Least squares polynomial curve fitting

Now, using the method of least squares in the case of a polynomial curve, we may approximate better the model. So we apply directly the method of least squares to fit a distribution: considering a set of points $M_i(x_i, y_i)$, and $f(x)=c_0+c_1x+\ldots+c_px^p$; where p is the degree of the polynomial curve fit, and c_k the researched coefficients with $\{k \in \mathbb{N}, k \in [0, p]\}$.

So it consists in minimising Δ where:

$$\Delta=\sum_{i=1}^{n}\ [y_i - f(x_i)]^2=\sum_{1}^{n}\left[y_i - \sum_{k=0}^{p}\ c_k \cdot x_i^k\right]^2$$

We set out, $\{\square k \in \mathbb{N}, k \in [0, p]\}: \frac{\partial\Delta}{\partial c_k}(c_0,\ldots,c_k)=2\sum_{i=1}^{n}\ [y_i - f(x_i) \cdot -x_i^k]^2=0$

$\frac{\partial\Delta}{\partial c_k}(c_0,\ldots,c_k)$ is the partial derivative of Δ with respect to the variable c_k at the point $(c_0,\ldots,c_k)$.

This gives a system of p+1 equations: $\sum_{i=1}^{n}\ x_i^k \cdot f(x_i)=\sum_{i=1}^{n}\ y_i \cdot x_i^k$

We write $S_k=\sum_{i=1}^{n}\ x_i^k$ and $W_k=\sum_{i=1}^{n}\ y_i \cdot x_i^k$, then the matrix system can be written as follows:

$$\begin{array}{cccccc} n & S_1 & S_2 & \ldots & S_p \\ S_1 & S_2 & S_3 & \ldots & S_{p+1} \\ S_2 & S_3 & S_4 & \ldots & S_{p+2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ S_{p-1} & S_p & S_{p+1} & \ldots & S_{2p-1} \\ S_p & S_{p+1} & S_{p+2} & \ldots & S_{2p} \end{array} \cdot \begin{array}{c} c_0 \\ c_1 \\ c_2 \\ \ldots \\ c_{p-1} \\ c_p \end{array} = \begin{array}{c} w_0 \\ w_1 \\ w_2 \\ \ldots \\ w_{p-1} \\ w_p \end{array}$$

The proof that the result is minimalistic can be performed by calculating the Taylor series of Δ.

Here, we take p=3. Using the function “NonlinearModelFit” of *Mathematica* software we can solve this system. The model found is:

$$f(x)=4.39713\times10^{-8}x^{3}+0.0000247368x^{2}+0.0341446x+34.0995 \tag{5}$$

4.3 Estimations

Using *Mathematica*, the statistical ANOVA table generated for the model is:

	d.f.	sum of squares	mean squares
function	4	820935.	205234.
error	4	1.142	0.285501
sum	8	820936.	
corrected sum	7	290435.	

The estimated error variance is 0.285501.

The mean predicted values are in the table below with the corresponding confidence intervals for a probability of 95%:

Observed	Predicted	Standard Error	Confidence Interval
63.9	63.9679	0.518619	{62.528,65.4078}
95	94.8313	0.311777	{93.9657,95.6969}
115.9	116.182	0.315459	{115.306,117.058}
142.7	142.216	0.299743	{141.384,143.048}
210.1	210.548	0.314431	{209.675,211.421}
304.3	304.254	0.434188	{303.048,305.459}
543.2	542.609	0.346651	{541.646,543.571}
585	585.492	0.422988	{584.318,586.667}

Then, an estimation of t for x=4096 is: f(x)=3610.66.

5. Review

So an estimated value for private key's operations with RSA CRT 4096 bits is about 3.6 seconds (for the smart card used for these tests), and for k=3072, the estimation of t is about 1.6 second.

(to be noted that these are just some estimations, under the hypothesis set in the previous parts, the most probable source of imprecision of the estimations is due to the high-level API of Java Card, used for RSA operations. So even if the time complexity of RSA inside the coprocessor is$O(k^3)$,it's not easy to know exactly which operations are added by the Java Card API in addition to RSA)

In the context of TLS in the smart card for the client side (at least for the entire Handshake), the only time constraint is that the Handshake mustn't be longer than 10 seconds because it is the timeout set on most of the TLS servers, however for convenience reasons, much less is suitable.

For TLS without client authentication with certificate (optional), the client just performs some public key operations, so as explained previously: RSA 4096 bits operations with public key should be at least 20 times faster than with private key CRT. So based on the previous estimation, we can conclude that RSA is totally viable (as 3610÷20 < 200 ms) for the future of TLS in the smart card when the client is not authenticated by certificate. RSA 4096 bits having a key space of more than 128 bits of security, it is then considered secure for more than 30 years, according to the report on algorithms and key lengths ECRYPT II [ECRYPT II, 2011].

Also some other applications implement the server side of TLS protocol in smart card (according to the specifications of Java Card 3), in this case the card must perform an operation with its private key, so for cypher suites with RSA, private key's operations for RSA 4096 will be required in a near future.

We can suppose that in the future, with hardware improvements, the performances will be better, as RSA 2048 bits will be still secure for more than 10 years (according to [ECRYPT II, 2011]) and according to some reports [Briggs J.S. and Beresford R.A., 2001], smart cards seem to follow a kind of Moore's law, but not the same as computers, the period to double hardware performances is of the order of 5 years, rather than 18 months (for traditional computers).

However “some” physicians [Kaku M., 2011] point out that Moore's law should reach its limit by 2020, so cryptography adapted to smart cards will be likely an interesting challenge in the future for cryptographers and computer scientists. Also, the fact that the power of computers grows more quickly than the one of smart cards, presents another challenge for the future of smart cards because the key space of cryptographic algorithms grows in function of the performances of computers.

5 Conclusion

So this study shows that it can make sense for smart card manufacturers to implement RSA up to 4096 bits in today's smart cards, mainly for Java cards implementing TLS and certificate checking (given that some Ca on the Internet use now RSA 4096).

Also, the same study should be performed to estimate the time for the card to generate the 4096 bits key, because the time to generate the keys is noticeably much more longer than the times of signature/verification and encryption/decryption.

A credible alternative to RSA is elliptic curve cryptography (ECC), which provides better performances than RSA for private key operations, however in the case of public key operations, RSA is more efficient than ECC (according to different papers, but it would be interesting to do the test on recent Java cards).

Concerning TLS, some Web browsers actually support TLS 1.2 with cypher suites using ECC, servers as well should be compliant soon. From the server perspective, ECC is more suitable because RSA is more time consuming for calculations with private key, then a distributed deny of service (DDOS) is more efficient on a server implementing RSA than on a server implementing only ECC.

6 References

Alia G. and Martinelli E., 2002 G. Alia and E. Martinelli, (2002), “Fast modular exponentiation of large numbers with large exponents”, *Journal of Systems Architecture: the EUROMICRO*, volume 47, issue 14-15, page 1079-1088, http://dx.doi.org/10.1016/S1383-7621(02)00058-9

Amiel F. *et al.*, 2009 Frederic Amiel, Benoit Feix, Michael Tunstall, Claire Whelan, and William P. Marnane, (2009), “Distinguishing Multiplications from Squaring Operations”, *Lecture Notes In Computer Science*, Springer Berlin, volume 5381, page 346-360, http://dx.doi.org/10.1007/978-3-642-04159-4_22

Aussel J.-D., 2007 Jean-Daniel Aussel, (2007), “Smart Cards and Digital Identity”, *Telektronikk 3/4 2007*, ISSN 0085-7130, http://www.telektronikk.com/volumes/pdf/3_4.2007/Page_066-078.pdf

Briggs J.S. and Beresford R.A., 2001 J.S. Briggs and R.A. Beresford, (2001), “Smart cards in health”, *Report for the Department of Health*, University of Portsmouth

Cordry J., 2009 Julien Cordry, (2009), “La mesure de performance dans les cartes à puce”, French PhD, Conservatoire National des Arts et Métiers (CNAM)

CAPI Website, Microsoft cryptographic API, http://msdn.microsoft.com/en-us/library/aa380255(v=vs.85).aspx

David J.P. *et al.*, 2007 J.P. David, K. Kalach and N. Tittley, (2007), “Hardware Complexity of Modular Multiplication and Exponentiation”, *IEEE Transactions on Computers*, 56(10), page 1308-1319, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4302704

ECRYPT II, 2011 (2011), “ECRYPT II Yearly Report on Algorithms and Keysizes”, European Network of Excellence for Cryptology II, editor: Nigel Smart, available online: http://www.ecrypt.eu.org/

EMV, 2011 Website, EMV specifications, (2011), http://www.emvco.com/

G&D SC 6.0, 2011 Website, specifications of G&D SmartCafe Expert 6.0 (Java Card 3.0.1), http://www.gi-de.com/gd_media/media/en/documents/brochures/mobile_security_2/nb/SmartCafe-Expert.pdf

Hoffstein J., Pipher J. and Silverman J.H., 2008 Jeffrey Hoffstein, Jill Pipher and J.H. Silverman, (2008), “An Introduction to Mathematical Cryptography”, Springer, ISBN 9780387779935

Huang Z. and Li S., 2011 Zhen Huang, Shuguo Li, (2011), "Design and Implementation of a Low Power RSA Processor for Smartcard", *IJMECS*, vol.3, no.3, page 8-14

Java Card Website, Java Card specifications, (2011), http://www.oracle.com/technetwork/java/javacard/overview/index.html

Kaku M., 2011 Michio Kaku, (2011), "Physics of the Future: How Science Will Shape Human Destiny And Our Daily Lives by the Year 2100", Doubleday, ISBN 9780385530804

Koç C.K., 1994 Cetin Kaya Koç, (1994), "High-Speed RSA Implementation", Technical Report TR-201, version 2.0, RSA Laboratories

Koç C.K. *et al.*, 1996 Cetin Kaya Koç, T. Acar and B.S. Kaliski Jr., (1996), "Analyzing and comparing Montgomery multiplication algorithms", *IEEE Micro*, 16(3), page 26-33

List of CA, 2011 Website, list of certificate authorities on the Internet used by Windows root certificate program, http://social.technet.microsoft.com/wiki/contents/articles/2592.aspx

Lu H.K., 2007 H. Karen Lu, (2007), "Network smart card review and analysis", *Computer Networks*, volume 51 (Elsevier North-Holland), page 2234–224

Markantonakis K. *et al.*, 2009 Konstantinos Markantonakis, Michael Tunstall, Gerhard Hancke, Ioannis Askoxylakis and Keith Mayes, (2009), "Attacking smart card systems: Theory and practice", *Information Security Technical Report*, volume 14, page 46-56, http://www.sciencedirect.com/science/article/pii/S136341270900017X

Menezes A.J., Van Oorschot P.C. and Vanstone S.A., 1996 Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, (1997), "Handbook of Applied Cryptography", CRC Press, ISBN 0849385237

NXP P5CD144, 2008 Website, specifications of NXP P5CD144 with coprocesseur FameXE, (2008), http://www.nxp.com/documents/data_sheet/P5CX012_02X_40_73_80_144_FAM_SDS.pdf

OCF, 2003 OpenCard Framework, (2003), http://opencard.sourceforge.net/

PKCS#11 Website, PKCS#11 specifications, http://www.rsa.com/rsalabs/node.asp?id=2133

Rehoui K., 2005 K. Rehioui, (2005), "Java Card Performance Test Framework", Master thesis, Institute Eurecom and Université de Nice Sophia Antipolis, France

Sato H. *et al.*, 2005 H. Sato, D. Schepers and T. Takagi, (2005), "Exact Analysis of Montgomery Multiplication", *Progress in Cryptology - INDOCRYPT 2004, Lecture Notes in Computer Science*, publisher: Springer Berlin, ISBN 9783540241300, volume 3348, page 1387-1394, http://dx.doi.org/10.1007/978-3-540-30556-9_23

Sepahvandi S. *et al.*, 2009 S. Sepahvandi, M. Hosseinzadeh, K. Navi and A. Jalali, (2009), "An Improved Exponentiation Algorithm for RSA Cryptosystem", *International Conference on Research Challenges in Computer Science, ICRCCS '09*, page 128-132, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5401230&isnumber=5401177

Smart N., 2002 Nigel Smart, (2002),"Cryptography: An Introduction, 3rd Edition", publisher: Mc Graw Hill Higher Education, ISBN 9780077099879, available online: http://www.cs.bris.ac.uk/~nigel/Crypto_Book/

Sun H.-M. *et al.*, 2009 Hung-Min Sun, Mu-En Wu, M. Jason Hinek, Cheng-Ta Yang and Vincent S. Tseng, (2009), "Trading decryption for speeding encryption in Rebalanced-RSA", *Journal of Systems and Software,* volume 82, Issue 9, page 1503-1512, http://www.sciencedirect.com/science/article/pii/S0164121209000910

Tews H. and Jacobs B., 2009 Hendrik Tews and Bart Jacobs, (2009), “Performance Issues of Selective Disclosure and Blinded Issuing Protocols on Java Card”, *Proceedings of the 3rd IFIP WG 11.2: International Workshop on Information Security Theory and Practice*, Smart Devices, Pervasive Systems, and Ubiquitous Networks, Springer Berlin, Heidelberg, http://dx.doi.org/10.1007/978-3-642-03944-7_8

Urien P., 2009 Pascal Urien, “TLS-tandem: a smart card for web applications”, (2009), *Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference*, page 3-4

Wu C.-L. *et al.*, 2006 Chia-Long Wu, Der-Chyuan Lou and Te-Jen Chang, (2006), “Computational complexity analyses of modular arithmetic for RSA cryptosystem”, *23rd Workshop on Combinatorial Mathematics and Computation Theory*, page 215-224

Improving Online Collaboration within the IFIP Working Group on Human Aspects of Information Security and Assurance

O. Burton and N. Clarke

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

Abstract

In this paper a study into online collaboration methods has been carried out. Starting with the types of online collaboration, research was carried out into the existing methods of collaboration for the International Federation for Information Processing (IFIP) working group on the Human Aspects of Information Security. Further research was conducted into the field of online collaboration focussing on wikis, social networks and bespoke tools. Based on this it was decided that a bespoke online collaboration platform would be designed and built taking into account the requirements of this working group. Feedback on the bespoke platform was provided continually by the working group and helped to create a solution that exceeded their requirements and expectations. It was also highlighted that the solution would be adopted by the working group as their primary means of online collaboration.

Keywords

Online collaboration, collaborative tools, social networks

1. Introduction

The growth of the Internet has enabled people to communicate quickly across large geographic distances and access huge quantities of information. Before this time if researchers wanted to collaborate with their international colleagues they would have to communicate by telephone, post or by regular on site visits. Each of these methods has issues such as; the time differences when considering telephone calls, the delay in postal delivery and the cost of on-site visits. It can therefore be seen that the internet can help to overcome these problems and provide an effective solution for collaborating with geographically distributed colleagues.

The topic of online collaboration is becoming more important in the modern world, as technology progresses and computers are able to produce more complex data file size have increased and it has become less feasible to rely on email as the primary method of collaborating online. File size limits imposed by email service providers have made it impossible to attach certain file types to emails. In addition to this the growth of social networking has given rise to improved online collaboration software.

This paper will cover the topic of online collaboration, providing examples and literature relating to this. It will continue to present the case study of a working group within IFIP in which they migrated from a system with no collaborative elements to bespoke collaborative software. The case study will explain why it was decided that the software would be bespoke, what features of the software make it ideal for encouraging collaboration and will end with a discussion on the feedback provided by the members of the working group.

The paper will end with a discussion on the importance of online collaboration in the research environment and how bespoke software solutions could provide the best fit for this. It will further discuss the importance of user requirements in the development of online collaborative tools and how these tools can become an important part of daily working.

2. Online Collaboration

There are many examples of online collaboration that takes place in unique ways for example, the re-captcha system which makes use of massive scale online collaboration in order to digitise the world's books (Ahn, 2011.) The open source movement has produced software that rivals and in some cases exceeds its commercial rivals (Bird, 2011). This project however looks at some of the more regular methods of collaboration such as wikis, social networks and bespoke software platforms as these are more closely related to the aims of the project. There are some disadvantages to online collaboration such as the issues present in emails where a user is relying on the other user to answer before they can continue the discussion. This poses a particular problem when it takes one party some time to reply to their emails. Further issues arise with users treating this mode of communication informally which can negatively affect their professional relationships.

One method of collaboration is through the use of a wiki, there are many open source software packages available for the creation of this. A wiki is interactive software that allows members to create and edit articles about a subject as part of a collaborative conduction. This allows for the rapid creation of a large knowledge base by a community of members however does suffer from issues related to the quality of information in the articles. Furthermore as articles go through various iterations it is difficult to tell whether an article is complete when reading through it.

The modern age of mass communication and sharing online has given rise to a new type of social website known as social networks. These websites allow users to connect with people they know and share information. There are hundreds of millions of members worldwide which have become an important part of modern internet usage as they allow rapid sharing of information and in some cases they can spread news more quickly than through traditional news channels (Murphy, 2012.)

Github is an example of a code repository that has evolved to enable faster and more efficient sharing of code between developers. It allows users to create their own profile page and (Github, 2012) claims that "many developers have started referring to GitHub Profiles as the new résumé." This highlights the importance of member profiles and shows how social networking can be used within a research environment. One disadvantage with social networks is that users often expect other users to be available instantly D'andrea et al. (2012, p.151). However this is often not the case for researchers and developers who may not have much time to devote to social networking.

Another method for online collaboration is provided by bespoke software solutions, these solutions overcome the file size limits imposed by e-mail providers by providing their own file uploading and sharing facilities. ActiveCollab is one such software that allows users to upload the software on their own server which gives them control over the software and the security of the system (ActiveCollab, 2012). This means that the users are not tied to the updates and changes made by the software provider as would happen with social networks however it does mean that they have to implement any features or purchase additional modules to extend the functionality of the software.

Other methods of online collaboration based on cloud technology are now in existence. Google docs and skydrive allow users to create and edit files online and share them with others, the cloud technology means that the software is not run on the local machine; this provides them with the ability to access and edit their files from any computer. This is useful for sharing information and work between researchers who may not have compatible software which is often a problem found in online collaboration. Further solutions exist such as video conferencing software and instant messaging programs. With websites such as Facebook adding instant chat and video calling features (BBC, 2011) it is clear that the future of online collaboration lies in the integration of different collaborative software.

3. Case Study – IFIP working group 11.12

A particular example of an implementation of online collaboration software is presented by the case study of the IFIP working group on human aspects of information security. In this case study the IFIP working group had a public facing website with membership functionality however it maintained no facilities for collaboration between members. Furthermore, the website suffered from frequent SQL injection attacks and spam which had to be manually removed from the database by the administrator. From this and several consultations with the working group a very clear set of requirements was created.

In this situation it was decided that a bespoke online collaboration platform would be created that would include aspects from social media, wikis and bespoke software to create a solution that was fit for purpose and met the working group's requirements. It was considered to be important to implement social networking features into the software in order to help build relationships between the researchers which would in turn lead to more productive collaboration efforts. The decision to create a bespoke platform was due to some very specific pieces of functionality that the working group required, this overall set of features was not present in an existing system. Furthermore, the effort involved in tailoring an existing platform to include these features would have been similar to that of developing a bespoke solution.

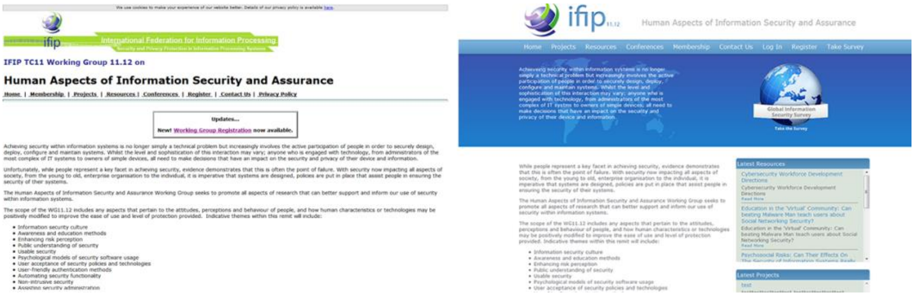
Using an agile development methodology and modular approach to design it was possible to work closely with the working group to regularly deliver functionality and reduce the risk of the user's requirements not being met. Furthermore the agile methodology also allowed the focus of the project to be on delivering functionality rather than on documentation.

The bespoke solution was delivered on time and to specification and contains particular features that help to encourage collaboration through the system. The software itself does not present any novel features however the combination of features provides a novel and interesting example of online collaborative software. One key element of this solution is the inclusion of a profile for each user with a profile picture, this idea is expanded by including the user's name and profile picture whenever they post or message on the site. By using a profile and a profile picture in this way it helps to make the website feel more personal and social, by doing this it helps to accelerate the forming of new social and professional bonds. In turn this helps to encourage collaborative working and the sharing of information.

The messaging system on the IFIP working group's website has taken its design from social media website and in particular Facebook. Instead of each user having an inbox, sentbox and an outbox, a user has a conversations list showing the latest received message and the number of new unread messages in the conversation. The advantage of this is that a user is then able to open the conversation and see all of their previous messages with the user in reverse chronological order. This feature helps to reduce the risk of messages being lost, as often happens with email inboxes. This is like a wiki as it allows a user to quickly see the information related to the message they are seeing and provides a way for members to easily view the historical trail of a discussion. Furthermore, this feature helps to make the process of collaboration more simple and organised by removing unnecessary complications and features.

The key point of collaboration for the IFIP working group's website is the projects feature. This allows members on the site to create a new research project which other website members can then join and contribute to. The creator of a project can select whether the project is open to anyone or whether they will need to be approved; they can also choose to allow any file uploads or to approve those also. Furthermore, each project page has a discussion area on which users can post their ideas and thoughts on the project. This is not deleted and as such provides a record of the discussion and development throughout the project. A further collaborative element is provided through the uploading of files to the project page, these are then shown in reverse chronological order. This provides a record of the development of documents related to the project and allows members to share their findings and resources.

As part of the IFIP project a questionnaire was distributed and feedback was sought, in this the members were asked to contrast the new website to the old one and provide feedback on the collaborative potential of the software. The response to the question 'Do you think that this website will bring more people to join your collaborative research efforts' was very positive and consisted of the following statement 'Yes, insofar as it creates a very professional impression of the WG, and will consequently present a more encouraging, credible shop window aspect to encourage engagement.' This is a key finding as it emphasises the success of the website in promoting collaboration and ensuring involvement in the research group. Further feedback was stated that 'I think it will allow a much more effective relationship with the WG membership and a direct opportunity to involve them in project activities and other participation". This response emphasises the success of the website in delivering online collaboration functionality.


We use cookies to make your experience of our website better. Details of our privacy policy is available here.
ifip
International Federation for Information Processing
Security and Privacy Protection in Information Processing Systems
Home | Membership | Projects | Resources | Conferences | Register | Contact Us | Privacy Policy
ifip 11.12
Human Aspects of Information Security and Assurance
Home
Projects
Resources
Conferences
Membership
Contact Us
Log In
Register
Take Survey
Global Information Security Survey
Take the Survey
Latest Resources
Latest Projects

IFIP TC11 Working Group 11.12 on

Human Aspects of Information Security and Assurance

Updates...

New! Working Group Registration now available.

Achieving security within information systems is no longer simply a technical problem but increasingly involves the active participation of people in order to securely design, deploy, configure and maintain systems. Whilst the level and sophistication of this interaction may vary; anyone who is engaged with technology, from administrators of the most complex of IT systems to owners of simple devices, all need to make decisions that have an impact on the security and privacy of their device and information.

Unfortunately, while people represent a key facet in achieving security, evidence demonstrates that this is often the point of failure. With security now impacting all aspects of society, from the young to old, enterprise organisation to the individual, it is imperative that systems are designed, policies are put in place that assist people in ensuring the security of their systems.

The Human Aspects of Information Security and Assurance Working Group seeks to promote all aspects of research that can better support and inform our use of security within information systems.

The scope of the WG11.12 includes any aspects that pertain to the attitudes, perceptions and behaviour of people, and how human characteristics or technologies may be positively modified to improve the ease of use and level of protection provided. Indicative themes within this remit will include:

- Information security culture
- Awareness and education methods
- Enhancing risk perception
- Public understanding of security
- Usable security
- Psychological models of security software usage
- User acceptance of security policies and technologies
- User-friendly authentication methods
- Automating security functionality
- Non-intrusive security
- Assisting security administration

Achieving security within information systems is no longer simply a technical problem but increasingly involves the active participation of people in order to securely design, deploy, configure and maintain systems. Whilst the level and sophistication of this interaction may vary; anyone who is engaged with technology, from administrators of the most complex of IT systms to owners of simple devices, all need to make decisions that have an impact on the security and privacy of their device and information.

While people represent a key facet in achieving security, evidence demonstrates that this is often the point of failure. With security now impacting all aspects of society, from the young to old, enterprise organisation to the individual, it is imperative that systems are designed, policies are put in place that assist people in ensuring the security of their systems.

The Human Aspects of Information Security and Assurance Working Group seeks to promote all aspects of research that can better support and inform our use of security within information systems.

The scope of the WG11.12 includes any aspects that pertain to the attitudes, perceptions and behaviour of people, and how human characteristics or technologies may be positively modified to improve the ease of use and level of protection provided. Indicative themes within this remit will include:

- Information security culture
- Awareness and education methods
- Enhancing risk perception
- Public understanding of security
- Usable security
- Psychological models of security software usage
- User acceptance of security policies and technologies

Cybersecurity Workforce Development Directions

Cybersecurity Workforce Development Directions

Read More

Education in the 'Virtual' Community: Can beating Malware Man teach users about Social Networking Security?

Education in the 'Virtual' Community: Can beating Malware Man teach users about Social Networking Security?

Read More

Psychosocial Risks: Can Their Effects On The Security of Information Systems Really

test

Figure 1 The Old and New Website Interface

Figure 1 contrasts the old website with the new website; this in particular highlights the improvement in the professional appearance of the new website. Furthermore there is more dynamic data and content displayed on the home page that is user-generated; this allows the users to share information rapidly with the public and other members through the website.

4. Discussion

Collaboration is becoming increasingly important in the modern working environment and online collaboration is a key driver behind distributed software development, a methodology that has been adopted by large companies such as Microsoft. These kinds of projects tend to suffer from issues related to collaboration including lost emails and lengthy delays in communication. The case study of the IFIP project has created a software environment that can aid collaboration and build professional bonds between researchers. The key feature in the project was that the software was a tool that could be used for collaboration but also allowed members to collaborate outside of the tool using methods that they prefer such as email. This is important as it provides multiple points of contact which can make collaboration easier and more efficient. Furthermore this project could be taken and applied to distributed development projects to help introduce team members to each other and develop sub-projects.

The IFIP case study also demonstrated the success that an agile development methodology can have when combined with regular close contact with the end use. In doing this it ensures that the software is on course to meet the user's requirements and also allows any major design issues to be overcome or removed from the project during its lifetime. Furthermore, the project demonstrated the fact that a bespoke platform can often provide the best solution to an organisation's requirements rather than trying to retrofit existing software.

A key finding of this paper is that online collaboration is a growth area and that the future of this lies in the integration of elements from existing software solutions. It is important to integrate social elements into any collaborative solution in order to build social bonds between the users of the system. Furthermore, integrating elements of wikis can be useful as it can provide a way for members to look back over previous discussions and to review the progression of ideas and work. This is important as it helps to build a deeper understanding of the thread of discussion and also provides a reference point for the future.

The rise of software companies such as facebook, twitter and dropbox are testament to the fact that sharing online is becoming a central part of internet usage. With the rise of mobile and cloud computing this is going to become even more prominent in the coming years, therefore complex collaboration software will be required. Software such as that produced in the IFIP case study is a very useful way to facilitate the sharing of information and the building of a community based around a particular subject. Forums can be thought of as a similar method of building online communities however they lack the functionality provided by the bespoke software solution and therefore do not provide the same level of collaboration.

From the review of the IFIP case study, feedback was provided by the chair and co-vice chair of the working group. Feedback such as “Prior to this site, collaboration was a time consuming and difficult task – both in finding interested parties but also then undertaking the collaboration. This will no longer hold true,” helps to highlight the success of the project and the improvements that will be delivered to the online collaboration of the working group. Further feedback “Yes, whilst other systems such as email will be used to contact members and enable a level of collaboration, I would expect all primary collaboration to published via the site.” helps to highlight the fact that whilst the system will be an enabler for the working group. Whilst it will be the primary means of collaboration for the working group it will be an enabler and not impede the working group from collaborating through other means.

The rapid sharing of information can become a vital feature in the work environment as it will allow people to have access to data in near real-time, this will reduce the time spent waiting for information and therefore help to improve efficiency in the work place. Website projects such as the IFIP case study highlight the importance of online collaboration and how the application of user’s requirements can lead to bespoke software solutions that are a good fit. These software solutions can act as enablers for collaboration and also help to improve existing collaborative efforts.

5. References

ActiveCollab, 2012. Welcome. [online] Available at: http://www.activecollab.com/ [Accessed 24 Jan 2012].

Ahn, L., (2011) TEDxCMU: Massive-scale online collaboration.[video online.] Available at: http://www.ted.com/talks/luis_von_ahn_massive_scale_online_collaboration.html [Accessed 7 December 2011]

BBC, 2011. Facebook Adds Skype Video Chat Feature. [online] Available at: http://www.bbc.co.uk/news/technology-14054860 [Accessed 30 January 2012].

Bird,C.,2011, " Sociotechnical coordination and collaboration in open source software", IEEE,27th IEEE international conference on software maintenance, (p.p.568 – 573)

D'Andrea, A., Ferri, F., Grifoni, P., Guzzo, T., 2010 , "Multimodal Social Networking for Healthcare Professionals," Database and Expert Systems Applications (DEXA),(p.p.147-153)

Garrison,D.,2006, "Online Collaboration Principles",[online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.4536&rep=rep1&type=pdf [Accessed 12 Jan 2012]

GitHub, 2012. The Company Information. [online] Available at: https://github.com/about [Accessed 29 Jan 2012].

Murphy, S., 2012. Twitter Breaks News of Whitne Houston Death 27 Minutes Before Press. Mashable.com Entertainment blog, [blog] 12 Feb. Available at: http://mashable.com/2012/02/12/whitney-houston-twitter [Accessed 20th August 2012].

Developing a Mobile WiFi Tracking Unit

M. Dagnall and N.L. Clarke

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

Abstract

Modern mobile and portable devices such as laptops and smart phones are often WiFi enabled. In the event that they are lost or stolen, it is desirable to recover them and their contents if possible. This research focuses on the development of a mobile system for locating WiFi enabled portable devices via the WiFi signal emanating from them. A mobile localisation system utilising a combination of a directional Yagi antenna and the received signal strength was developed and shown to be effective at locating WiFi sources at ranges from 45m to 500m away depending on the environment.

Keywords

Mobile, WiFi, Tracking, Localisation, Yagi Antenna, 802.11g, Directional, WLAN

1 Introduction and background

WiFi enabled portable devices such as smart phones and laptops are regularly targeted by thieves or misplaced by their users with 850,000 mobile phones stolen across the UK in 2007 (Flatley, et al, 2009). In the event of theft of loss, recovery is desirable either to recover the device or its contents. The physical value can be in the region of hundreds or thousands of pounds but its contents such as confidential, commercial or classified information in some cases could far exceed the physical value of the device. During a recent study of major European organisations, the average value of a missing laptop averaged €35,000, with the total impact totalling €1.29 billion (Ponemon Institute, 2011). Due to the items portable nature, once it has been stolen in could conceivably be secreted in numerous environments. There is therefore a justifiable need to track and locate WiFi enabled portable devices in the event that they are stolen.

Current solutions employed in the tracking location of lost or stolen devices typically employ a combination of some of the following technologies:

- GSM – The mobile cell can be used to locate the portable device
- GPS – The GPS coordinates can be broadcast by a GSM module
- RF 173Mhz – Localisation via traditional wildlife tracking Tx/Rx

GSM cell location cannot always be relied upon to provide sufficient resolution to recover the device on its own. Typically, GPS does not perform well inside buildings (Bakhru, 2005; Bajaj et al, 2002) and in the event that the GPS signal is lost an alternative method of locating the device is required. Traditional RF tracking solutions (i.e. those used for tracking wildlife) can be employed, but this is with a cost penalty as this is additional functionality to be incorporated into the device. Some devices contain an 802.11g WiFi module and if this signal can be repurposed in order to locate the box instead of traditional RF methods then cost savings can be achieved.

There are existing applications of WiFi for localisation but these are principally focused on some form of triangulation which requires multiple receivers in order to do so. Generally the location of the receiver is known and so are the expected path losses. RADAR is an established tracking system based on RF for locating individuals or object in buildings. It relies on multiple access points with overlapping coverage in order to function. The combination of received signal strength measurement and signal propagation modelling facilitates location (Bahl & Padmanabhan, 2000). Due to the varied environments that the cash boxes necessarily operate in signal propagation modelling is not viable. The tracking unit should be capable of being used for tracking in isolation so more established triangulation methods are not suitable.

In this paper, we focus on localising 802.11g signal sources using a directional antenna. Section 2 of this paper illustrates how the tracker was developed. The 3rd section summarises the results from a number of differing environments and the 4th section discusses them. The final section contains the conclusions.

2 Development of the WiFi tracker

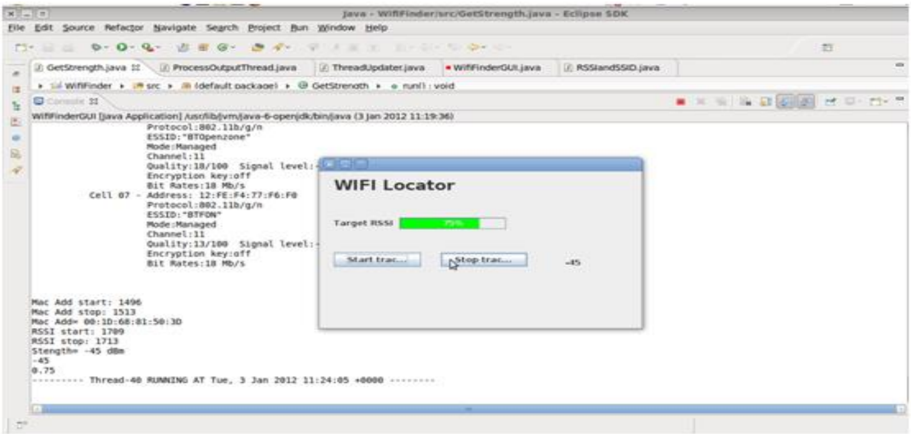
In order to facilitate tracking the WiFi signals back to their source the tracker required 3 basic components:

1. A directional antenna for obtaining a vector to the target
2. A method of obtaining WiFi signal metrics that are suitable for tracking
3. A method of displaying the metrics in a manner usable for tracking

These components were developed and employed as follows:

1. The Pheenet ANT-120YN 2.4 GHz Yagi antenna was used as Yagi antennas typically provide high gain with a narrow focus (Rosham & Leary, 2004). This narrow focus facilitated the directional nature of the antenna.
2. The RSSI (Received Signal Strength Indicator) and MAC address of can be obtained from a WiFi adapter connected to a directional antenna. This allows the strength of the received signal to be captured along with its identity. The output from the Linux command *iwlist scan* provides a list of WiFi sources and their RSSIs available to the WiFi adapter. This output was programmatically captured and filtered in order to obtain the RSSI for a specified MAC address (i.e. the target's MAC address). The sample rate achieved was 0.3Hz, that is the RSSI and list of WiFi sources to be filtered was updated every 3 seconds. A GUI was developed in Java and a signal strength bar was used to display the signal strength associated with the

target's MAC address. This provided a simple hot and cold measure of RSSI VS. Direction when utilised in combination with 2 and 3.


Java - WifiFinder/src/GetStrength.java - Eclipse SDK
File Edit Source Refactor Navigate Search Project Run Window Help
GetStrength.java
ProcessOutputThread.java
ThreadUpdater.java
WifiFinderGUI.java
RSSIandSSID.java
WifiFinder ▸ src ▸ (default package) ▸ GetStrength ▸ run() : void
Console
WIFI Locator
Target RSSI
75%
Start trac...
Stop trac...
-45

```
WifiFinderGUI [Java Application] /usr/lib/jvm/java-6-openjdk/bin/java (3 Jan 2012 11:19:36)
                    Protocol:802.11b/g/n
                    ESSID:"BTOpenzone"
                    Mode:Managed
                    Channel:11
                    Quality:18/100  Signal level:
                    Encryption key:off
                    Bit Rates:18 Mb/s
          Cell 07 - Address: 12:FE:F4:77:F6:F0
                    Protocol:802.11b/g/n
                    ESSID:"BTFON"
                    Mode:Managed
                    Channel:11
                    Quality:13/100  Signal level:
                    Encryption key:off
                    Bit Rates:18 Mb/s


Mac Add start: 1496
Mac Add stop: 1513
Mac Add= 00:1D:68:81:50:3D
RSSI start: 1709
RSSI stop: 1713
Stength= -45 dBm
-45
0.75
--------- Thread-40 RUNNING AT Tue, 3 Jan 2012 11:24:05 +0000 --------
```

Figure 1: Screen shot of GUI displaying high RSSI

The antenna was connected to a USB WiFi adapter with an external antenna connected. This was connected to a Linux Ubuntu OS laptop which was used to host the RSSI capture and GUI functionality.

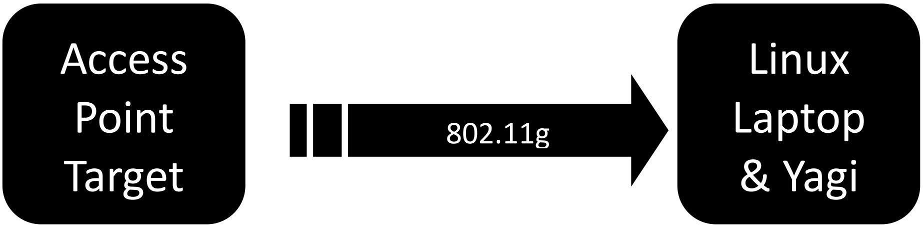


Figure 2: System architecture

3 WiFi tracker test results

A range of environments were chosen for experimentation and testing of the WiFi tracker, those discussed in this paper are:

1. Clear countryside
2. Urban terraced
3. Urban City Centre
4. Large building, analogous in layout to a shopping centre

In order to simulate a WiFi enabled target, a simple 802.11g domestic access point (AP) was used.

The RSSI was captured as a power and the units are measured in dBm accordingly. A note on the difference between 0 signal strength (no signal) and 0dBm (1mW power): Where a signal was lost in its entirety, that value has been changed from 0 to -100dBm (effectively no signal). This is because a strength of 0dBm (1mW) was not measured, being high signal strength/power and would have misrepresented the results.

1. *Clear countryside*

The AP was placed at the edge of an open space and the maximum distance at which the target's signal could be recorded with direct line of sight was 560m

2. *Urban Terraced*

For this experiment the AP was placed centrally on the ground floor of a double glazed, terraced property with the windows closed. Scanning was initiated and RSSI readings were taken at increasing distances after turning left out of the property until the signal was lost at 45M. Turning right out of the property resulted in a maximum distance of 112M being reached prior to the signal being lost. The experiment was repeated with the windows open but it had no significant impact on the range with identical distances being recorded at which the signal was lost.

3. *Urban City Centre*

The access point was placed on the 4th floor of an office block in a large city centre. The total area of the 4th floor was 1438 $m^{2.}$ The maximum distance at which the target's signal could be recorded with direct line of sight was 200m away. The front of the building was surveyed by sweeping the antenna from side to side on each floor. The signal was significantly stronger on the right hand side of the 4th floor, which cut down the most likely search area to $448m^2$. Upon entering the building, no further signals could be detected on the preceding floors until entering the 4th floor. Once it was confirmed that the 4th floor contained the target, it was located by sweeping the antenna and following the strongest signal within 3 minutes. In figure 2 below, the signal strength can be seen increasing as the tracker gets closer to the target.

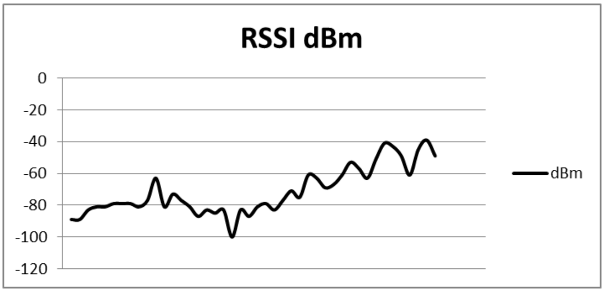


Figure 3: 4th floor RSSI over Time during search

There were 15 windows of the 4th floor and they were coated in a heat reflective film. Two of the windows were open, 20 signal strength readings were taken from the front of the building with the windows open and then closed in order to determine if the open windows were significant. The RSSIs measured are shown in Figure 3 below.

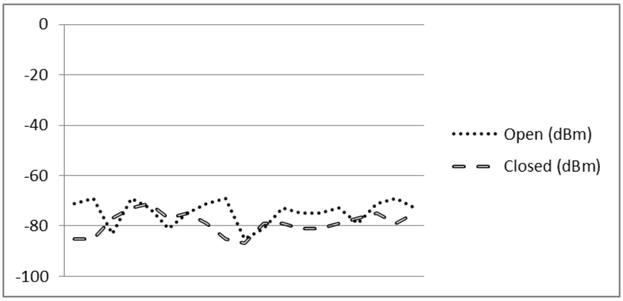


Figure 4: RSSI(dBm) Open heat reflective windows VS Closed

4. *Large Building*

This site is a large office building with accommodation for 2000 employees and a total floor space of 35,000m^2. It contains a large central atrium with stairs and lifts giving access to floor plates on each side of the atrium, a lay out common to many shopping centres. The AP was hidden by an assistant in an unknown location and locating the target was attempted from outside the building. It took 12 minutes to find the target. After surveying the exterior of the building, the location of the target was approximated to be on the second floor in the west quadrant of the building. Upon entering the building the signal was lost but following the building layout and ascending the stairs resulted in the signal being required and traced back to its source. The AP was found located in a room with an area of 990m^2. The signal was subject to reflections and in places, ghosting was encountered. However this was easily eliminated by taking readings in other directions and following the strongest RSSI.

4 Discussion of results

The objectives of the experimentation were as follows:

1. How far away from a target can the tracking solution start reading the RSSI?
2. Is it possible to locate a target using the tracking solution?
3. Is it possible to locate a target using the tracking solution in a variety of environments?

The maximum range in clear line of sight possible with the equipment used for the research in the environments available was 0.5km. Clear line of sight may be useful in a situation where the target is not in an urban environment. The maximum effective distance achieved was 200m from an elevated position and from between

45m and 112m from at ground level. It is therefore possible to cover a larger area without obstructions to line of sight to the 802.11 scanner than in an urban environment where there are obstructions. However this does not necessarily lessen the effectiveness of the tracker. A range of a 100m or so within a built up area is acutally quite effective as due to its very nature large open spaces are few and far between. Streets and building layouts can be used as visual guides for the tracker to follow in combination with the RSSI and vector prodivded by the directional antenna.

If the WiFi source is placed in an elevated position, then this range can be at least doubled. Ideally, an environment with a building surrounded by clear line of sight for up to a kilometer would be used for ascertaining the exact range but such a bulding was not available at the time of research. Also from an ideal perspective a range of building types would be used and a range of elevations but there has to come a point where the practical benefits would be outweighed by the logistics of this approach to the research.

During experiment 2, maximum range was less than expected. The signal propagation was approximately 50% on the west side of the property than the east side. Although such a marked delta is initially surprising, further investigation of the construction of the building may explain the results. The walls on the north and west side of the property are unusual in being in excess of 450mm thick and solid. The wall on the east side is double skinned brick and significantly thinner.

According to (Ohrtman & Roeder, 2003) a window in a brick wall will reduce signal strength by 2dB and the brick wall by 3dB. However the attenuation caused by windows did not prove to be significant when testing the tracker in operation during experiments 2 and 3. The distances maximum tracker range was unaffected by opening of closing the properties windows and doors.

For line–of-sight (LOS) propagation the transmitting and receiving antennas must be in effective line of sight of one another. The qualifier *effective* is used as the atmosphere can refract signals and objects in the signals path may reflect, refract or scatter them (Stallings, 2005). Although reflections may result in false positive readings and could in theory make it very difficult to localise the target, testing has shown that reflection, refraction and scattering actually help the singal propogate. This means it is possible to follow the signal to its strongest source such as in a building where without this propogation, it may not have been picked up at all.

Being in a bulding, with lots of potential for ghosting, was not the issue it was orginally thought to be. This is because by applying a little common sense, the tracker can follow the building layout. By using the building corridors and doorways to guide the tracker, it is possible to locate targets even in larget buildings. This was demonstrated in experiments 3 and 4 when upon entering the building, it was sufficiently large that the signal found outside was lost. However because the signal was strongest when pointing up at a specific part of the bulding from the outside, the tracker can use the layout of the building to guide them to likely places to pick up the signal again.

The maximum range of the tracker is affected by its environment, the environment of the target and its sensitivity/gain. The environmental factors are not possible to control as the intended target when in use (a mobile device) is by design portable. In order to increase the effective range, the gain could be improved by using a more sensitive WiFi adapter or an antenna with higher gain. However this would need to be balanced against the impact of cost on the tracker and its portability.

5 Conclusions

The WiFi tracker developed for this research can be used in order to locate a WiFi enabled target such as a smart phone or laptop.

The effective range of the tracker developed for this research is between 45m and 200m when the target is place in a building. The effective range is affected by environmental considerations such as the thickness of walls. Elevation has a significant impact on range, the range increases with elevation. With uninterrupted line of sight of the target, the range increases to approximately 500m.

Refraction and multipath interference was more of a help than a hindrance. The refraction of the signal around buildings allowed the signal to be followed back to the source by following the path of corridors and stairs.

Due to the limited range of the WiFi tracker, it is highly unlikely that it could be effectively deployed on its own in the field without the help of alternative tracking technologies such as GPS to guide operator to an effective start point.

In order to establish if WiFi is an effective tracking technology for commercial application as an alternative to more established technologies, consultation with the security industry will be required. The effective ranges and recovery times offered by WiFi will need to be compared with currently employed solutions and its effectiveness judged.

If a tracker was to be constructed for commercial use it would ideally be as compact as possible. The tracker developed for this research required two hands to operate which made opening doors and operating lift controls difficult. Weather proofing of the tracker would also be desirable as would some resistance to impact as it is likely that the tracker will be subject to both at some point during day-to-day use.

6 References

Bahl, P., & Padmanabhan, V. M. (2000). RADAR: an in-building RF-based user location and tracking system. NFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE , 2 .

Bajaj, R., Ranaweera, S. L., & Agrawal, D. (2002). GPS: Location-Tracking Technology. Computer , 4, 92-94.

Bakhru, K. (2005). A Seamless Tracking Solution for Indoor and Outdoor Position Location. International Symposium on Personal, Indoor and Mobile Radio Communications , 3.

Britsh Retail Consortium. (2011). Cash and Valuables in Transit: Best Practise Guidlines for Retailers. 2, 14. British Retail Consortium.

Flatley, J., Moon, D., Roe, S., Hall, P., & Moley, S. (2009). Home security, mobile phone theft and stolen goods: Supplementary volume 3 2007/08 - British Crime Survey. Home Office.

Ohrtman, F., & Roeder, K. (2003). Wi-Fi handbook: building 802.11b wireless networks. NY, US.

Ponemon Institute. (2011). The Billion Euro Lost Laptop Problem: Benchmark study of European organisations. Ponemon Institute.

Rosham, P., & Leary, J. (2004). 802.11 Wireless LAN fundamentals. Indianapolis, US: Cisco Press.

Stallings, W. (2005). Wireless Communications and Networks (2nd Edition ed.). Upper Saddle e River, NJ, USA: Pearson Education.

A Crime Depended Automated Search and Engine for Digital Forensics

J.P. Fizaine and N.L. Clarke

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

Abstract

As the number of cybercrime is rising up, time and accuracy in digital forensic become more complex to handle. This phenomena is due to the large amount of data to be investigate hence requires more time to analyse. In the meantime the technology is more and more complex and it more skills are necessary to be able to investigate such complex system. Existing tools like EnCase or DataAccess could tackle the complexity of new technologies by adding scripts which also allow some automation. But those are not built to face large amount of information in restricted amount of time. During the investigation there is always the same tasks to do. In addition each crime has a pattern. So common pattern where found for the same type of crime. The idea is to build a module that take advantage from the common pattern to automate the analysing process of evidence. This fact would help in model as a response to automate the investigation process. This paper aims to present a simple concept of file identification determined by a crime profile.

Keyword

Automated tool, automated investigation process, automated forensic tool, digital forensics, digital formalization formation, automated forensic model, file carving, data hiding.

1 Introduction

Digital forensic, a part field of forensic science, is specialised in crimes investigation where computers, electronic devices and computer networks are involved in. In response to the increasing threats of crime involving computers and the complexity of information technology, appropriated software are being developed such as Encase (http://guidancesoftware.com/) or FTK(http://accessdata.com/products/forensic-investigation/ftk).

Computers are now involved in various nature of crime such as child pornography, fraud, identity theft, as well as there are weapons of crimes. Spreading computer virus, hacking computers and networks to gained unauthorized access, performing deny of service are some other examples. The U.S Justice Office of Justice Programs (2008) had categorised each crime based on involved information. Where most of researches work about new models and frameworks which is detailed in section 2 they focus on the current approach used by FTK and Encase.

Those tools are widely used in industries, governments, agencies as well for law enforcement. There are highly specialised tools that require experiences and solid knowledge in operating systems and networks. Therefore they can only be used by technical and skilled investigators. Still they are efficient tools with large panel of features required in digital investigation. Their approach is to let the investigator officer manages his own investigation process. As a example Encase has it own script engine to give the opportunity to automated the most common task.

During the first step of the investigation, the investigator is aware of the suspected crime and so he must look for specific information which are liable for the crime or to dismiss the accusation. Lets take as an example a case of child pornography. He will be looking for Images and websites. However in case of financial fraud he would be instead looking for bank account number, financial documents, etc. If it the case of unauthorized access as computer intrusion, program, logs, would then be the information he would look for. At the end of the first step of investigation he will performed a deep analysis of what he found, to prove are not the crime.

This first step of collecting useful information can be automated because each crime is defined differently as regarding the information it involves. Such a process is not performed by Encase and FTK or even other forensic tools. Even if the research in digital forensic is active, must of them focus on models and frameworks to analyse the data more efficiently. Some attempt to automate the investigation process is also part of the research area.

This paper is about a new approach in digital forensic. The tool fits in the first step of investigation. Its purpose is to perform an automated process for collecting information related specifically to one crime. And to prepare this set of information for further deep analysis by appropriated program. Therefore the global architecture and general process would be detailed.

The section 2 regroups relevant models, frameworks and tools and explains why there are interesting. The next section 2.2 quickly discuss about related work and background. Base and requirement are detailed and explained in section 3. Then the novel approach is detailed in the following section 4. The paper continue through the section 5 where it explains the extraction process in more in detailed and with in section 6 the heart of the core with the formalization of the triage. At last future work and improvements are introduced in section 7.

2 Survey on forensic tools, frameworks and models

Novel frameworks, new tools and models are hot topics in computer forensic science. Several sort of technologies and different approaches had being introduced but the community agreed on the necessity to have a suitable tool for an appropriate use. This section first presents previous researches and works that explain necessities and need in computer forensic. It is followed by a second section where a background is given.

2.1 Needs in digital computer forensics

The fist attempt to automated forensic is found 2004 with the work from Slay et al. (2004) and Gladyshev & Patek (2004). The work from Slay et al. (2004) expresses the necessity of developing new tools. Despite the fact that the work is about Australian usage and requirement, they argue that the most widely used software, Encase (from Guidance software system) have an expensive cost and it requires skilled investigators. They also claim, the tool is not available for police officer. But Gladyshev & Patek (2004) had another approach based on finite state machine. Their work consist of automate the reconstruction process whereas Slay et al. (2004) really focus on a whole automated model and tool.

Peisert et al. (2007) has expressed some principles and qualities a good forensic model should have. The goal of their work is to build a rigorous approach based on attack profiles formalise by graph. Practical forensic is based on logged data from various tool which do not constitute a rigorous model. The authors had highlighted five principles:

- The whole system must be considered;
- To log as much as possible without considering the attack or the failure;
- The effect of events must be considered and not only the action;
- The interpretability and the understandability of events must suit the context.
- Work on conditions from before and from after the event.
- The event must be presented in a way, they can be analysed and be understandable by the forensic investigator.

The authors also spotted other requirements, forensic tool must have. The data should be logged from different layer of abstraction. And a limit must be set to prevent collecting to much data.

Andrew (2007) had establish in his work a model to perform rigorous analysis of digital devices and media storage. His paper focuses on requirements to perform such analysis. The basis of his model are the principle of consistent result and the principle of static storage. Forensic software are put on the top. followed by the concept of *individualization* from Dr Paul Kirk and *identification*.

2.2 Background and related work

EnCase from guidance software, is the most spread forensic tool. Garber (2001) in his case of study about the tool concluded that it is a tool for who know what he is doing. It is a very complete tool. Even if it as a script engine to give the capability to used automated process, the tool is still for skilled people. This point is argued by Slay et al. (2004) and they claimed the fact that it is still an expensive solution reserved to forensic laboratory.

Since a few years, research on model, tool and framework is a hot topic and significant work as been published. Slay et al. (2004) has argued the need of a more simple tool then Encase to give the ability to perform forensic investigation in the industries Marrington et al. (2010) expressed in there work the necessity of an automated tool to handle the quantity problem and the complexity problem developed by Carrier (2003a).

Most of the new models focus on the analysing aspect as Bhat et al. (2010) and Marrington (2010). Bhat et al. had developed a new approach based on data mining but Marrington based his work on an accurate framework. Bhat et al. had a non-forensic approach and a non-rigorous approach as Hunton (2011a) defined it. And the work of Marrington has a general and rigorous approach with significant features. Hunton (2011b) has noticed the existence of technical challenged and a gap between examiner and non-technical people. As a response he developed a model composed of several layer to process cybercrime investigation.

As the response to give the ability to perform forensic investigation, with the lowest cost, by non-technical and non-skilled people and for the world of industry, the challenge is to develop a tool with automated process investigation. Such a process first have an extraction process and make the extracted data available for further deep analysis by appropriated tools. The automated process is based on the fact that cybercrime can be ordered in a taxonomy Casey (2004).

The tool would be based on a rigorous approach with a scientific approach and based on science forensic concepts. Therefore evidences which are exposed in court can’t be argued. Works from Andrew (2007), Carrier (2003a), Marrington et al. (2010) and Hunton (2011a) would be the foundation of a such rigorous approach.

3 Requirements Analysis

The research consist of developing a new forensic tool. Therefore the tool must fit some requirements and it must follow a rigorous approach. The tool would fit the general investigator process described by Casey (2004). The investigation process starts with acquisition of data, a process to prevent the integrity of data to change or be altered. It consists of make an exact duplication of the digital media which results in a file called image. It is simply a file contained raw data from digital media. The image is the basis to perform an investigation.

In order to perform deep analysis by other tools, data must be collected and stored in a secure location. A database is the best solution. Because it has security feature and can handle a huge amount of data. Every software with a database interface and the specification of the table can access easily to data. The design of the storage must take in consideration the concept of individualization from Dr. Paul Kirk Andrew (2007). Individualization is an important concept because it is the basis of re-construction. To perform the re-construction process, relevant information must be collected and extracted. The quantity problem orders to take care during the process of extraction, but there must be enough information to allow the re-construction.

Forensic science orders to analyse deeply the evidence. In our case the evidence is a digital media storage which stores files in organised structured. Such a concept is called file system, a feature of a modern operating system. But in order to solve the quantity and the complexity problem from Carrier (2003b), the tool is based on layer of abstracted. This approach would cover only files from the file system and thus introduces errors. Slack space analysing and data carving are important feature as well. Some old deleted or hidden file can be find in slack space. It is hence important to detect their location within the evidence in order to apply data carving techniques to extract deleted file. Detecting and extracting hidden file is a far more complex problem.

Sometime criminals can be very skilled in technology. They are aware of anti-forensic techniques. They would use cryptography, steganography techniques and even more advanced data hiding techniques. The tool would consider possibility with in two points. A profile of the suspect would give an average idea of its skills. This profile would be a measurement of the skill. The value is calculated by analysing all the software found in the evidence.

In all the possible crimes involving computers, networks, or electronic devices, the investigator should be able to perform keyword research. This feature is based on engine that first collect all text pattern. This is an indexing process of words found in the devices. And a list of keyword is given by the investigation. Such keyword could be names, phone number, ip address.

A preliminary report would give a summary of what was found. The investigator knows hence which files request it attention. It would be on those flagged files that he must performs the deep analysis. Those new results would be summarized in final report. This last document is specially to be present to the court. But the preliminary report is not suitable for the court because the individualization concept is not applied. Moreover the facts are not linked together to re-construct the crime. So any piece of evidence are linked together regarding the action and the time. Thus the crime cannot be proven.

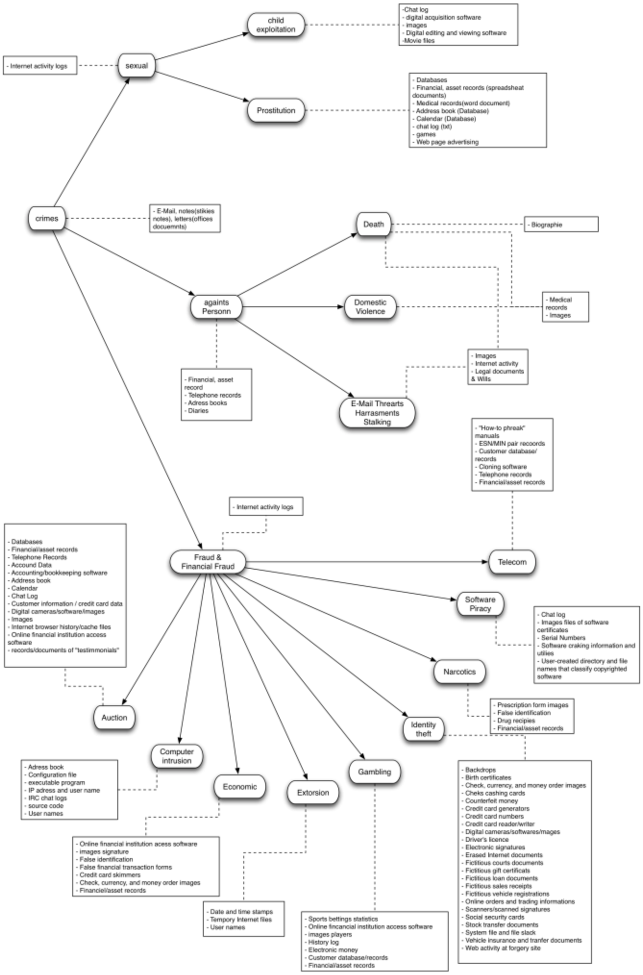
EnCase is an expensive and a proprietary solution. It has the consequence that the tool can only be extended by the presence of the scripting engine which brings some flexibility. It has not the ability to communicate properly with other software. From the view of the development, an open-source solution would give the tools lots of possible contribution in the future. And more a deep review by the community of the sources would gives trust in the tool. The essence of opensource software gives the capacity to fully evaluate the software. Carrier (2002) opensource explains in his work that open sourced software are more likely to suit *Daubert*’s principals than closed source tool would.

4 The crime taxonomy

A cybercrime tree taxonomy is the foundation of the triage process. It defines which files must be look for during the triage process. But it needs the help of layer of abstraction to identify properly different nature of data. The last point explain the need of a database to store data.

4.1 The foundation of the extraction process

In our knowledge all the existing automated process of forensic software, models and framework concentrates on the final analysis. EnCase software has no native automated process, despite the fact it could be added with the script engine. Actually it is the script engine that give the capability of automating some tasks. But the software remains mainly conducted by the investigator. To give our tool this capacity to automate an investigation process with a minimal interaction of the investigator, the automated engine is based on the taxonomy of cybercrime. Casey (2004) explained than each crime first affects different files. With the *Locard Exchange Principal* from Dr. Edmund Locard itself, the criminal would interact with the environment, here in operating system Andrew (2007), causing some changes in it. In a case of crime involving computer devices, it would alter some files and the environment, the operating system.



child exploitation
-Chat log
- digital acquisition software
- images
- Digital editing and viewing software
-Movie files
- Internet activity logs
sexual
Prostitution
- Databases
- Financial, asset records (spreadsheat documents)
- Medical records(word document)
- Address book (Database)
- Calendar (Database)
- chat log (txt)
- games
- Web page advertising
crimes
- E-Mail, notes(stikies notes), letters(offices docuemnts)
Death
- Biographie
againts Personn
Domestic Violence
- Medical records
- Images
- Images
- Internet activity
- Legal documents & Wills
- Financial, asset record
- Telephone records
- Adress books
- Diaries
E-Mail Threarts Harrasments Stalking
- "How-to phreak" manuals
- ESN/MIN pair recoords
- Customer database/ records
- Cloning software
- Telephone records
- Financial/asset records
- Internet activity logs
- Databases
- Financial/asset records
- Telephone Records
- Accound Data
- Accounting/bookkeeping software
- Address book
- Calendar
- Chat Log
- Customer information / credit card data
- Digital cameras/software/images
- Images
- Internet browser history/cache files
- Online financial institution access software
- records/documents of "testimmonials"
Fraud & Financial Fraud
Telecom
Software Piracy
- Chat log
- Images files of software certificates
- Serial Numbers
- Software craking information and utilies
- User-created directory and file names that classify copyrighted software
Narcotics
- Prescription form images
- False identification
- Drug recipies
- Financial/asset records
Auction
Identity theft
Computer intrusion
- Adress book
- Configuration file
- executable program
- IP adress and user name
- IRC chat logs
- source code
- User names
Economic
Extorsion
Gambling
- Backdrops
- Birth certificates
- Check, currency, and money order images
- Cheks cashing cards
- Counterfeit money
- Credit card generators
- Credit card numbers
- Credit card reader/writer
- Digital cameras/softwares/mages
- Driver's licence
- Electronic signatures
- Erased Internet documents
- Fictitious courts documents
- Fictitious gift certificats
- Fictitious loan documents
- Fictitious sales receipts
- Fictitious vehicle registrations
- Online orders and trading informations
- Scanners/scanned signatures
- Social security cards
- Stock transfer documents
- System file and file slack
- Vehicle insurance and tranfer documents
- Web activity at forgery site
- Online financial institution acess software
- images signature
- False identification
- False financial transaction forms
- Credit card skimmers
- Check, currency, and money order images
- Financiel/asset records
- Date and time stamps
- Tempory Internet files
- User names
- Sports bettings statistics
- Online fincancial institution access software
- images players
- History log
- Electronic money
- Customer database/records
- Financial/asset records

Figure 1: Cybercrime tree taxonomy

From this, a taxonomy of cyber crime is built. Figure 1 shows the result of the classification based on work from U.S. Office of Justice programs (2008).

The nodes represent nature of crime and the leaves represent the type of crime. The tree is enriched at each node and leave, with file extension names and type of data. The extraction process would only focus on files extension name and data that characterized one crime. In fact the file signature would be used because it is more relevant than file extension name which can be easily modified.

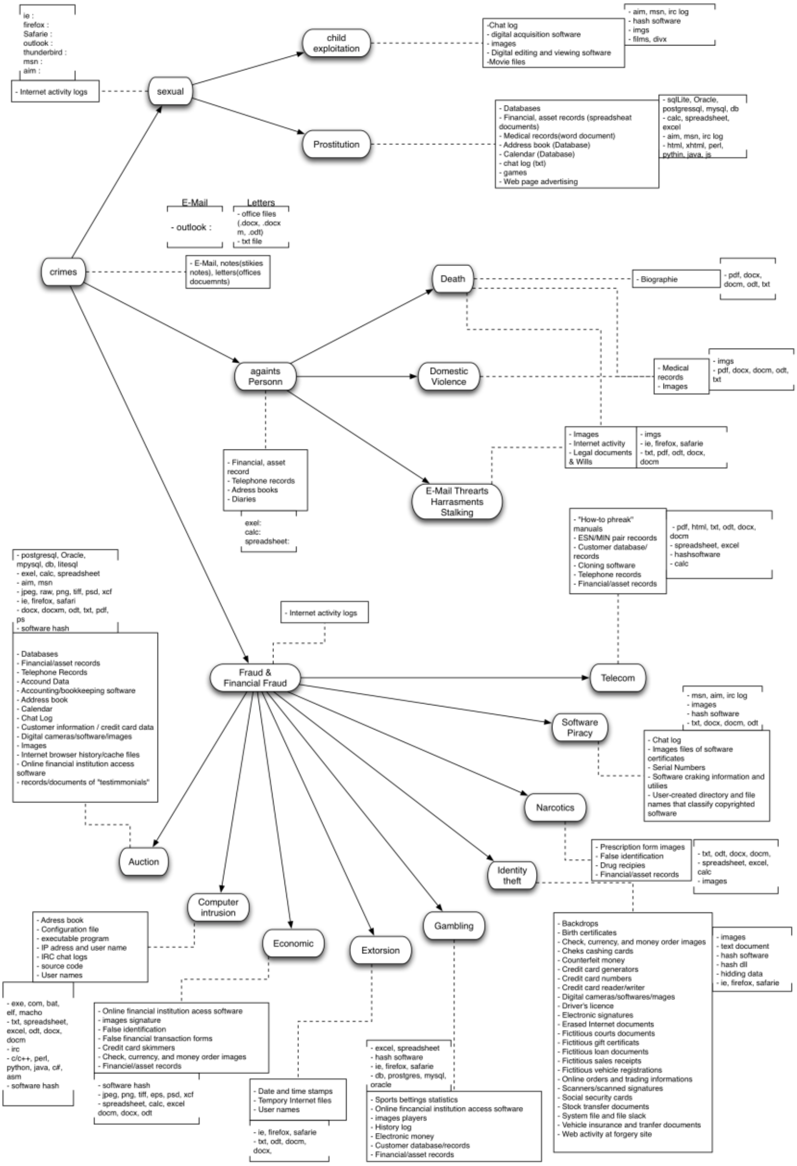

ie :
firefox :
Safarie :
outlook :
thunderbird :
msn :
aim :
- Internet activity logs
sexual
child exploitation
-Chat log
- digital acquisition software
- images
- Digital editing and viewing software
-Movie files
- aim, msn, irc log
- hash software
- imgs
- films, divx
Prostitution
- Databases
- Financial, asset records (spreadsheat documents)
- Medical records(word document)
- Address book (Database)
- Calendar (Database)
- chat log (txt)
- games
- Web page advertising
- sqlLite, Oracle, postgressql, mysql, db
- calc, spreadsheet, excel
- aim, msn, irc log
- html, xhtml, perl, pythin, java, js
E-Mail
- outlook :
Letters
- office files (.docx, .docxm, .odt)
- txt file
crimes
- E-Mail, notes(stikies notes), letters(offices docuemnts)
Death
- Biographie
- pdf, docx, docm, odt, txt
againts Personn
Domestic Violence
- Medical records
- Images
- imgs
- pdf, docx, docm, odt, txt
- Images
- Internet activity
- Legal documents & Wills
- imgs
- ie, firefox, safarie
- txt, pdf, odt, docx, docm
- Financial, asset record
- Telephone records
- Adress books
- Diaries
exel:
calc:
spreadsheet:
E-Mail Threarts Harrasments Stalking
- "How-to phreak" manuals
- ESN/MIN pair recoords
- Customer database/ records
- Cloning software
- Telephone records
- Financial/asset records
- pdf, html, txt, odt, docx, docm
- spreadsheet, excel
- hashsoftware
- calc
- postgresql, Oracle, mpysql, db, litesql
- exel, calc, spreadsheet
- aim, msn
- jpeg, raw, png, tiff, psd, xcf
- ie, firefox, safari
- docx, docxm, odt, txt, pdf, ps
- software hash
- Internet activity logs
- Databases
- Financial/asset records
- Telephone Records
- Accound Data
- Accounting/bookkeeping software
- Address book
- Calendar
- Chat Log
- Customer information / credit card data
- Digital cameras/software/images
- Images
- Internet browser history/cache files
- Online financial institution access software
- records/documents of "testimmonials"
Fraud & Financial Fraud
Telecom
Software Piracy
- msn, aim, irc log
- images
- hash software
- txt, docx, docm, odt
- Chat log
- Images files of software certificates
- Serial Numbers
- Software craking information and utilies
- User-created directory and file names that classify copyrighted software
Narcotics
- Prescription form images
- False identification
- Drug recipies
- Financial/asset records
- txt, odt, docx, docm,
- spreadsheet, excel, calc
- images
Auction
Identity theft
Computer intrusion
- Adress book
- Configuration file
- executable program
- IP adress and user name
- IRC chat logs
- source code
- User names
- exe, com, bat, elf, macho
- txt, spreadsheet, excel, odt, docx, docm
- irc
- c/c++, perl, python, java, c#, asm
- software hash
Economic
- Online financial institution acess software
- images signature
- False identification
- False financial transaction forms
- Credit card skimmers
- Check, currency, and money order images
- Financiel/asset records
- software hash
- jpeg, png, tiff, eps, psd, xcf
- spreadsheet, calc, excel docm, docx, odt
Extorsion
- Date and time stamps
- Tempory Internet files
- User names
- ie, firefox, safarie
- txt, odt, docm, docx,
Gambling
- excel, spreadsheet
- hash software
- ie, firefox, safarie
- db, prostgres, mysql, oracle
- Sports bettings statistics
- Online fincancial institution access software
- images players
- History log
- Electronic money
- Customer database/records
- Financial/asset records
- Backdrops
- Birth certificates
- Check, currency, and money order images
- Cheks cashing cards
- Counterfeit money
- Credit card generators
- Credit card numbers
- Credit card reader/writer
- Digital cameras/softwares/images
- Driver's licence
- Electronic signatures
- Erased Internet documents
- Fictitious courts documents
- Fictitious gift certificats
- Fictitious loan documents
- Fictitious sales receipts
- Fictitious vehicle registrations
- Online orders and trading informations
- Scanners/scanned signatures
- Social security cards
- Stock transfer documents
- System file and file slack
- Vehicle insurance and tranfer documents
- Web activity at forgery site
- images
- text document
- hash software
- hash dll
- hidding data
- ie, firefox, safarie

Figure 2: Enriched taxonomy tree

The U.S Department of Justice Office of Justice programs (2008) details each sort of information which caracterised one crime. Pedo-pornography requires image whereas financial fraud requires documents like financial report, bank account number or credit card number. For example images are stored in jpeg, bmp, or png file, and user documents are files created with office software like Microsoft Office or Openoffice. Therefore each information is listed with the exact file extension. From this fact we enriched the previous taxonomy tree with file extension name. Figure 2 presents the results.

4.2 Layer of Abstraction

The input of the tool is raw data, produced from the acquisition process. A tool such as *dd* would performed such task. There are no logical reading, which means if data are directly read they are no structure. Files and directories or operating system information as the registry in windows case cannot be accessed. Moreover the tools must handle various file-system ands the most spread one, linux's , macintosh's and window's file system. The tool must keep the ability to access different layer, from the hardware to the operating system. Blocks, cluster and file and directory are all the different layer it needs.

Sleuth kit offer this capacity. It is a set of open-source tools developed by Carrier to give investigator the ability to work at various abstraction layer Carrier (2003b). It handles and retrieves information and file from NTFS, FAT, EXT2-3 and HFS+ file-system. The set of tools make also possible the extraction of information at the partition level. Therefore different type of slack space can be define and deep analyse can be accomplish to detect hidden data, deleted file or encrypted data.

4.3 Storing the data and case management

Sleuth-kit is set of tools which makes possible to deal with abstracted layer of data. In a matter of accuracy the software needs to store all the abstracted layer as well as all the information which were extracted. The first objective is to limit the quantity problem. The size of extracted data and information is function of the size of the digital media. A database system would accomplish this task. It is an excellent solution to share the data.

The database system would be organised databases. Each case would be stored in it own database because they are no relation between data of several cases. So each case would be described by a sets of abstracted sets of data. Only relevant information would be stored to prevent huge size of data, especially when the investigation is performed on tetra-bytes amount of data. Generally offset and size are stored for partitions as well as files. In the last case, metadata of files are stored because they contain relevant information as last access time, creation time, etc... Such information are useful to perform the chronological analysis or data correlation analysis where it would use file owner, hash of file.

The abstraction layer has a layer for hidden and encrypted data. The database would stored as much information as possible. A special part is dedicated to slack space information. Those information are significant to detect hidden data. In case of supposed encrypted data, only the offset and the length are stored but the database would have the ability to stored information found after a deep analysis.

In order to make possible an analysis of digital media by several programs, Alink et al. (2006) had developed a integrated approach named XIRAF. It uses a XML and a database system to wrap together different tools. Alink et al. focus their work on the analysing process where their developed an automated process. The XIRAF approach is an interesting approach for our software.

5 The working flow

The tool fit in a classic investigation process explained and detailed in the working flow as a iterative process. The next point gives the details on how to make the process efficient by selecting and avoiding defined sets of information. Then the paper focuses on the filter as a recursive function.

5.1 The general workflow, an iterative process

The tool does not follow a defined model from various work. It follows the digital forensic approach, acquisition, extraction, deep analysis and report as explain by Casey (2004). Still the extraction process follows a model which takes into consideration hidden and deleted data and the crime profile. The model is drawn out in the figure 3.

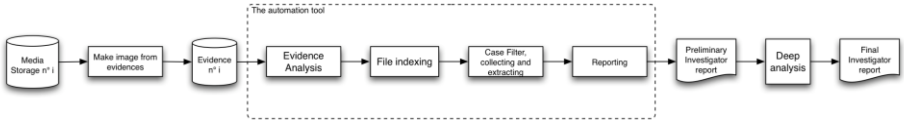

The automation tool
Media Storage n° i
Make image from evidences
Evidence n° i
Evidence Analysis
File indexing
Case Filter, collecting and extracting
Reporting
Preliminary Investigator report
Deep analysis
Final Investigator report

Figure 3: General working flow

The investigator enters all the digital media as evidence to the case and gives the type of crime. Then the process starts by analysing the evidence to determine the general structure of the evidence. The operating system would try to be guessed if it was not given by the investigator. For Each partition on the digital media, it performs file indexing. It is the second level of abstraction where it enables the software to sort out files by their nature. In the following the tool filters files that would be reliable for the case according to the crime profile. At the end of the process it produces a preliminary report, a starting point for the investigator to build the deep analysis.

5.2 A more efficient process

The filtering is based on the cyber crime tree taxonomy but it still need to look through entire evidences. To prevent time consuming, during the analysis step of each evidences, the environment, in fact files issued the operating system, are not analysed in filtering process. The reason is that not all cybercrime requires such a deep analysis of the evidence. The level of analysis is function of the suspect profile and the installed tools.

We need to understand what to analysed and how. For that purpose we developed a an formalization of the storage media. It is a model to reprensation how the data are organized on the disk. It helps on the process of the triage.

The structure of an image can be formalized with the help of the theory of set. The difference between sets are conceptual differences.

$$E=FS \cup MBR \cup PT \cup fAS \cup uAS$$

where

- E = $\{ci, i \geq 0$ and $i \leq EvidenceSize/ClusterSize)\}$ and $E \neq \emptyset$ is the image, is the set of all clusters. Size are in bytes.
- MBR = $\{b_j, 0 \geq j \geq 1\}$, where b is a block of size 512 bytes. It defines the set of clusters allocated to the master boot record.
- *FS* is the set of clusters used to store file system information, $FS = \{fs_i, i \in \{1, 2, 3, 4\}\}$, where fs_i is a file
- *PT* is the set of cluster to store information about the partition table, $FS \cap PT= \emptyset$
- *fAS* is the set of file allocated space from file system, e.g. allocated clusters and $(FS \cup PT) \cap fAS=\emptyset$
- *uAS* is the set of unallocated space, e.g. unallocated clusters.

Each set can be process by an appropriate function. We need for each of sets to define functions processing them and their domain of result. Analysers of the Evidence are formalise as function:

- Evidence analyser:
$$EA: E \times MBR \rightarrow FS$$
- File indexing:
$$FI: FS \rightarrow fAS$$
- Slack space analyser:
$$SSA: E \cdot\times MBR \cdot\times fAS \rightarrow uAS$$
- Data analyser:
$$DtAn: sE \in (fAS \cup uAS) \rightarrow St$$

  where *sE* is the subset of clusters build from the allocated and unallocated cluster. It can also be view as a partition of the union of allocated and unallocated cluster. And *St* is the set of possible status defines as $St=\{encrypted,fileFragment,file,unknown\}$

- Triage:
$$T: CR \times\cdot fAS \rightarrow SF$$

  where *CR* is the set of crime profile, *IF* is the set of indexed file and $SF \in E$ is the set of suspected data.

- Deep analysis:

$$DA: SF \rightarrow CL$$

where $CL \in E$ is a set of clues.

We cannot consider file slack space in the modelization. The reason is data extracted from there are unstructured data. But need to be able to index them for future analysis. As indeed to keep the formalization simple it was not considered.

We first start to define file slack space as:

$$fAS = RD \cup FSS$$

where

- RD is the set of bytes of the file and
- FSS is the bytes that are not used by the file.

A file is defined regarding a given file system *fs/inFS*. File can be formalise as a function over *fAS*:

$$file : fAS_{fsi \in FS} \rightarrow \mathrm{F}$$

where F is the set of all file inside a file system. We do not need to considerer directory as there are either a file or a meta data for the file system.

Now we can formalized other kinds of abstraction as file produced by the user, file from the operating system and file from program. The set F of all files from the file system is therefore define as:

$$F = uF \cup sF \cup pF$$

where

- $uF \in F$ is the set of files produced by the user.
- $sF \in F$ is the set of files from the operating system.
- $pF \in F$ is the set of files from programs.

The Environment checker can than be defines as:

$$Ec: (pF \cup sF) \cdot \times NSRL \rightarrow \{sane, unsane\}$$

where *NSRL* is the set of checksum of program file and from operating system file. This database allows to gain trust on some sets of data. We can therefore avoid any analysis on that space. But in the case of unauthorized access this set must be analysed to find any rootkits, malware and other malicious tools.

6 Formalization of the core and basic of the triage process

The filter and the extraction are recursive functions where one of the argument is the profile of the suspect and the crime profile. The profiling would be first initiated by the investigator. It first analyses program which are installed to detect known tools and software for securing data, performing hacks or penetration computer system. It also involves cryptographic techniques as steganography.

If no such tools are found the software does not try to look for encrypted or hidden data more deeply. In the opposite it would try to make available such data by looking for password and try then to decrypt the data. This part of the process depends on the operating system and on the user. For example an accurate acknowledged user in information security would not stored his passwords in the environment but a less accurate user would effectively stored them in his account. For the moment any procedure nor algorithm have been yet developed whereas detection of slack space, therefore possible hidden data, in windows environment exist Carrier (2005).

The triage process can be seen as a function to selection particular data within a set. The selection is based on some condition. A logical approach could be used but we preferred a vectorized approach because it gives the ability to tune and to give weight on some parameter. Let recall the definition of the triage function:

$$T{:}CR \cdot \times fAS \rightarrow SF$$

Now let give a formal definition of the set of crime profile CR. We define an element $cr \in CR$ as a vector of n independent vectors c_i, $0 \leq i \geq n$, hence we have $c_r = (c_0, c_1, \ldots, c_n)$. A vector c_i is one characteristic of the crime. The value 0 means the parameter is not considered whereas the value 1 considered it in the triage process. As an example of an arbitrary crime profile is defined by the following vector *crime*=(1,1,0,0,1,0,1). The number of field is not yet defined here.

The triage process is based on the characteristic of crime. The following function maps the file and the crime profile. The definition is:

$$p{:}F \rightarrow CR$$

For any files there is a mapping with the type of information it represents. Table 1 gives some examples.

Extension name	Type of information
jpeg	image
bmp	image
png	image
xls	spreadsheet
docx	office document
odf	office document
exe	applications
com	applications
pdf	office document
text	office document

Table 1: Examples of extension file maps to type of information

The definition of the triage function is now very simple. It needs two inputs, the crime profile and the file. But the file is mapped before the triage process beginnings. The result is either the value 0 or 1. The value 1 express the file is selected.

$$T(cr, p(f)) = \begin{cases} f \in SF & \text{if } p(f) \times cr^T > 0, \\ f \notin SF & else. \end{cases}$$

In fact vectors can be translated into matrix with allow us to describe the operation.

If the multiplication of matrix of file type by the transpose matrix of crime profile then the file is considered as suspected. We need to use the transpose of the matrix of crime profile so the multiplication of matrix makes sense.

Here some example of triage process in case the file is not suspected and in the case it is. Let defines an arbitrary crime profile *cr*=(0,0,1,1,0) and two files f_1 and f_2. Their profile is hence $p(f_1) = pf_1$ = (0, 0, 1, 0, 0) and $p(f_2) = pf_2$ = (0, 1, 0, 0, 0). File f_1 is suspected because

$$p_{f_1} \times cr^T = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$= 1$$

whereas f_2 is not because we obtain

$$p_{f_2} \times cr^T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$= 0$$

7 Future work and improvements

The interface of this tool was not yet discussed yet which is still in development. But here are some guideline to design the software interface. It must remain as simple as possible and the more intuitive as possible. So the design would care about what is the more suitable for human.

Cryptographic aspects were introduced in the process but it represents a big part of development. As we meant previously, this aspect would first start by look stored password. An appropriate algorithm must be developed to extract and validate automatically the password. It represents another big challenge.

The keyword search engine was also briefly mentioned. This is one of the next point to work on.

The interaction with other tools was mentioned. It his challenging to give the ability to the software to communicate and interact with external program on shared data. The constraint is to be able to nicely add, update a external tool without modifying the architecture. As it was late introduced in the research, XIRAF solution is not yet integrated even if it remains a nice solution. If not, a XML based protocol sound like a nice alternative. The challenge here remains in the ability to extend, change, update easily parts of the software without having the necessity to re-develop it from scratch. It is to give an interface to allow such manipulation.

8 Conclusion

This paper introduces foundation and requirements for our novel automated tool. It aims to fill the need of a complete tool for non-technical investigator. Therefore the investigator could focus only on the case without having to matter about technical difficulties. The software has not the purpose to replace a power tool such as EnCase but it is an alternative tools for non-technical and for industries and police officer for example.

The first priority is to develop the search engine and the interface. Still many aspect of the tool are not yet covered in this paper they are planned in the core of the workflow. The core of the process would be developed in Python. It was chosen for its portability and for its fast coding capability it gives. The first step would be to check and to validate the workflow process.

As based-mobile device treats are growing such issue should be surveyed and potential modification may be added to the software. The nature of mobile technology is different from computer even if they share same foundations and principles. The functionality and the behavior would get closer to computer but still differences would remain and it would give new challenges in digital forensic.

9 References

Alink, W., Bhoedjang, R. A. F., Boncz, P. A. & de Vries, A. P. (2006), 'Xiraf - xml-based indexing and querying for digital forensics', Digital Investigation 3(Supplement-1), 50–58.

Andrew, M. W. (2007), Defining a process model for forensic analysis of digital devices and storage media, in Huang & Frincke (2007), pp. 16–30.

Bhat, V., Rao, P. G., V, A. R., Shenoy, P. D., R, V. K. & Patnaik, L. M. (2010), 'A novel data generation approach for digital forensic application in data mining', IEEE Computer Society pp. 86 – 90.

Carrier, B. (2002), 'Open source digital forensics tools: The legal argument'.

Carrier, B. (2003a), 'Defining digital forensic examination and analysis tools using abstraction layers', International Journal of Digital Evidence 1(4).

Carrier, B. (2005), File system forensic analysis, Addison-Wesley.

Carrier, B. D. (2003b), 'Defining digital forensic examination and analysis tool using abstraction layers', IJDE 1(4).

Casey, E. (2004), Digital evidence and computer crime, forensic science, computers and the internet, Elsevier.

Garber, L. (2001), 'Computer forensics: High-tech law enforcement', IEEE Computer 34(1), 22–27.

Gladyshev, P. & Patel, A. (2004), 'Finite state machine approach to digital event reconstruction', Digital Investigation 1(2), 130–149.

Huang, M.-Y. & Frincke, D. A., eds (2007), Second International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2007, Seat- tle, Washington, USA, April 10-12, 2007, IEEE Computer Society.

Hunton, P. (2011a), 'A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a uk law enforcement environment', Digital Investigation 7(3-4), 105 – 113.

Hunton, P. (2011b), 'The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation', Computer Law & Security Review 27(1), 61 – 67.

Marrington, A., Mohay, G. M., Morarji, H. & Clark, A. (2010), A model for computer profiling, in 'ARES', IEEE Computer Society, pp. 635–640.

U.S Department of Justice Office of Justice Programs, U. D. (2008), 'Electronic crime scene investigation: A guide for first responders, second edition', a Accessed Online on 15/07/2010, http://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

Peisert, S., Bishop, M., Karin, S. & Marzullo, K. (2007), Toward models for forensic analysis, in Huang & Frincke (2007), pp. 3–15.

Slay, J., Hannan, M., Broucek, V. & Turner, P. (2004), Developing forensic computing tools and techniques within a holistic framework: an australian approach, in 'Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC', pp. 394 – 400.

Assessing the Feasibility of Security Metrics

B. Heinzle and S.M. Furnell

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

Abstract

Security metrics are used to measure the effectiveness of an organisation's Information Security Management System (ISMS) as well as the sub-processes, activities and controls of the ISMS. Guidelines and example metrics have been published, but it is still difficult for an organisation to select metrics that are feasible for their environment, i.e. their ISMS.

This paper proposes a self-assessment framework that allows a user to determine security metrics that are feasible specifically for the user's ISMS. To achieve this, a metric catalogue containing 95 metrics from different sources was created. For each metric, requirements that need to be fulfilled in order to be able to use the metric, and ISO 27001 clauses and controls whose effectiveness is being measured by the metric, were ascertained and assigned. By this, a list of requirements was generated that can be used to describe an organisation's ISMS. During an assessment, the user indicates which requirements from the list of requirements are fulfilled. After conducting an assessment, a list of feasible metrics, the number of metrics per ISO 27001 clause and control, and other information are generated as assessment results. A software prototype was created and shows a proof of concept of the self-assessment framework. The results of the study were evaluated by external experts, which has shown the usefulness of the study and helped to identify areas of improvement and future work.

Keywords

Security Metrics, Security Measurement, Feasibility, Effectiveness, ISMS

1 Introduction

The term metric in general stands for the process and methods of quantification of a given attribute, aspect or characteristic (Savola, 2007; Jansen, 2009). Savola (2010) states that metrics “[...] simplify a complex socio-technical system into models and further to numbers, percentages or partial orders”. According to this definition, information security metrics measure aspects of information security.

While security metrics are defined differently and can be categorised differently (Chew *et al.* 2008; COBIT5, 2012; Savola, 2007; Saydjari, 2006; Jansen, 2009), this study focuses on security metrics according to ISO 27004 (2009): Metrics that measure the effectiveness of an ISMS and its sub-processes and controls. A variety of frameworks and guidelines on how to set up a so called information security measurement programme exist (ISO 27004, 2009; Chew *et al.* 2008; COBIT5, 2012; Payne, 2006), although these publication only give little or no guidance on how to select the most feasible or adequate security metrics.

Further publications in the area of security metrics mostly agree that security metrics are a difficult area and further research is strongly needed (Bellovin, 2006; Hinson, 2006; Jansen, 2009; Rosenquist, 2007; Saydjari, 2006). Two approaches for determining feasible security metrics were reviewed. Savola's (2010) approach is a set of evaluation criteria with a scheme how to evaluate candidate metrics according to this scheme. Fruehwirth *et al.* (2010) published an approach that tries to determine feasible metrics by considering the organisation's capabilities according to the Systems Security Engineering Capability Maturity Model (SSE-CMM).

2 Possibilities to describe an ISMS

For the self-assessment framework that was developed during this study a formal method to describe an organisation's ISMS is vital in order to enable the determination of feasible security metrics. Rather than evaluating a list of security metrics from a catalogue and determine the best suitable or most feasible metrics according to an evaluation scheme such as Savola's (2010) approach, a method to describe an organisation's ISMS and determine feasible metrics with the information about the ISMS was researched.

Similar to the approach published by Fruehwirth *et al.* (2010), the maturity model used in CobiT 4.1 (2007) and the ISO/IEC 15504 based process capability model used in COBIT5 (2012) were reviewed. One further possibility to describe an organisation's ISMS offer catalogues of possible elements of an organisation's ISMS such as the "IT-Grundschutz Catalogues" (BSI IT-Grundschutz Catalogues, 2005). It was evaluated how the existence of specific components could indicate that specific metrics are feasible.

While reviewing process capability or maturity models and modelling catalogues towards their usefulness to describe an ISMS with the aim of determining feasible security metrics, both possibilities were not considered suitable for the self-assessment framework. This was mainly because establishing a link between metrics and certain elements of the reviewed possibilities or attributes of these elements seems to be difficult. Also using these possibilities would limit organisations that can use the self-assessment framework to those organisations that use the relevant method to describe an ISMS or manage IT in general.

It was decided to use a method that is closer oriented to metrics and less bound to ISMS frameworks like ISO 27001 (2005) or the COBIT process capability and maturity model (CobiT, 4.1 2007; COBIT5, 2012). To describe an organisation within the self-assessment framework, requirements of each metric were worded without using a predefined model or formal language. Requirements are described as a condition that needs to be fulfilled by components of the ISMS or information that needs to be reported by components of the ISMS, e.g. "Inventory of assets indicates number of applications that are classified as critical to the organisation". The list of recorded requirements can then be used to build an organisational model. An organisation shall be described by the list of fulfilled requirements, which will be a subset of the overall list of requirements.

3 Metrics Catalogue

A metric catalogue was created and contains the following information:

- Source of the metric
- Title of the metric
- An identifier which is unique within the source
- Brief description, e.g. “Percentage (%) of information systems that have conducted annual contingency plan testing”
- ISO 27001 processes and controls that are measured by the metric: At the end of an assessment, this allows to determine which controls are measured.
- Requirements of the metric, i.e. a condition that needs to be fulfilled for the metric to be feasible.

An overview of sources and the number of metrics used from each source is shown in Table 1.

ISO 27004 (2009)	13
NIST SP 800-55 (Chew *et al.* 2008)	16
Steve Wright (2006)	7
The CIS Security Metrics (The Center for Internet Security, 2010)	28
Scott Berinato (2005)	5
Robert Lemos (2012)	4
COBIT5 (2012)	13
security metametrics blog (Brotby and Hinson, 2012)	9
total number of metrics	95

Table 1: Number of metrics per source

The list of ascertained requirements was grouped into categories of requirements. Categories were made based on the area of the ISMS or the IT activities that are addressed. Categories are similar to ISO 27001 control sections or control objectives. Furthermore, for each ISO 27001 clause and control the number of metrics that measure it can be determined, as relevant clauses and controls were assigned to each metric.

4 Self-Assessment Framework

Figure 1 shows an overview of the developed self-assessment framework, the data that is being used and how this data correlates.

As initial data the framework uses the metrics catalogue, the list of requirements, a list of ISO 27001 clauses and controls and the relationships between these three items, which are again stored in the metrics catalogue.

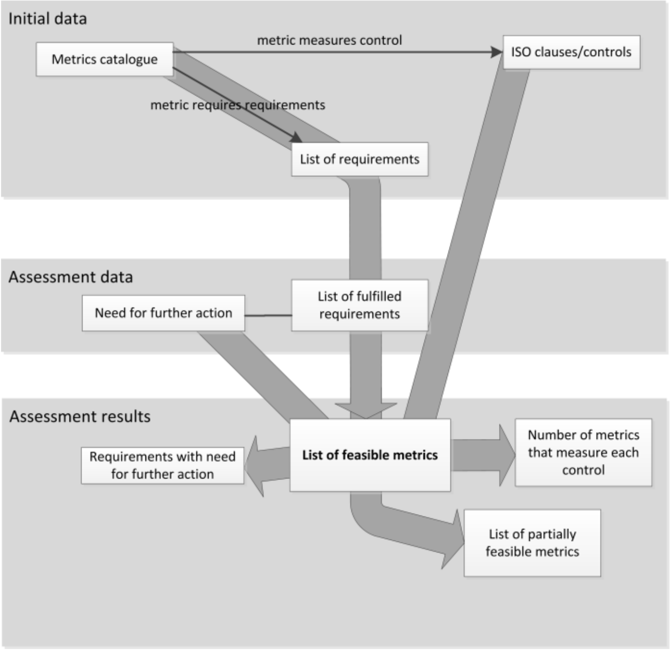

Initial data
metric measures control
Metrics catalogue
ISO clauses/controls
metric requires requirements
List of requirements
Assessment data
Need for further action
List of fulfilled requirements
Assessment results
Requirements with need for further action
List of feasible metrics
Number of metrics that measure each control
List of partially feasible metrics

Figure 1: Self-assessment framework

During an assessment, the user is asked to indicate which of the requirements are fulfilled within the ISMS. It might occur that a requirement is currently not fulfilled properly, but fulfilment can be achieved in near future. If this is possible with a reasonable effort and the user is willing to do so, the user can indicate this for each fulfilment of a requirement. In this case, the requirement is considered as fulfilled to the effect that the metrics that rely on this requirement are considered feasible as long as the metric’s other requirements are fulfilled. Comments on how the requirement will be fulfilled in future should be added for documentation purposes. The opportunity to add comments on the possibilities and modalities of data collection related to each requirement is given to the user.

Once the user has walked through the list of requirements and has indicated which requirements are met, the following assessment results can be determined: (1) A list of feasible metrics, i.e. metrics that have all their requirements fulfilled. If one or more requirements of a metric need some further action in order to be fulfilled properly, the metric is still considered feasible. (2) A list of requirements that need further action to be fulfilled properly, i.e. all the requirements for those it was indicated the requirement is currently not fulfilled but fulfilment will be achieved with reasonable effort in near future. All issues on this list should be addressed by the user of the framework. (3) A list of partially feasible metrics, i.e. some but not all the requirements were fulfilled. This list indicates which metrics could be used if more requirements were fulfilled. (4) A list showing ISO 27001 clauses and controls with the number of feasible metrics per clause and control is generated. In this way, the user of the framework sees at a glance of which clauses and control the effectiveness can be measured.

With the aim of providing an example how the self-assessment framework could be used in practice, a software prototype was implemented. This was achieved using Microsoft Access 2010. The software prototype offers functionalities for editing the metrics catalogue and the list of requirements as well as conducting assessments. Reports for metrics (i.e. the metrics catalogue), requirements and assessments can be generated as well.

5 External Evaluation and Discussion

The results of the study were evaluated by 11 external experts. Evaluators are working in the following positions: Professor at University of Applied Sciences Upper Austria, CISO at Domestic & General, Manager at a leading Security Consulting Company in London, Sr. IT Auditor at General Motors UK, Security Manager at HCL Great Britain Ltd, GRC Consultant in InfoSec at RNG Conseil Limited, Digital Security Risk Consultant at BP, Information Security Manager at Marie Curie Cancer Care, Audit Manager at Cofunds Limited, Security Manager at Hermes Fund Managers Limited as well as a Risk and Compliance Manager from a further UK-based company. The evaluation was done by asking for the evaluators' opinions about the metrics catalogue, the list of requirements, the self-assessment framework (as a theoretic description) and the software prototype via 13 questions.

In general, the evaluated components were found very useful. Some proposals for improvement were made. Besides different presentation formats and grouping for the catalogue and the list of requirements, a more detailed description of the self-assessment framework and improvement of the prototype's usability, comments mostly proposed new metrics as well as new functionalities and ways how the framework and the software prototype could be developed further. However, many of these proposals were related to extending the software to support data collection and calculation of metric results as well. The results of the study leave room for further development, but these proposals address functionalities that were not part of the original aims of the study. It was also commented that metrics should be linked to business objectives and then be selected according to the metric's ability to fulfil relevant objectives, as it is done by other publications (Chew *et al.* 2008; Fruehwirth *et al.* 2010; ISO 27004, 2009). Nevertheless, metrics are linked to control objectives, which can be seen as a certain type of business objectives. Although the framework in its current version does not select metrics according to a list of ISO 27001 control objectives that shall be achieved, it is possible to adapt both framework and software prototype to allow this.

Some metrics were found as infeasible or very unlikely to be fulfilled. This is known and shall not be considered as a weakness. Metrics can be added to the catalogue, even though their requirements are very infeasible, as long as their requirements were ascertained and worded correctly. This solely results in the metrics being feasible during hardly any assessment.

In order to draw a line between the framework and the software prototype, in can be said that the framework is the theoretic approach of using the metrics catalogue (including the requirements per metrics) and determining feasible metrics for a customer by using the entire list of requirements and indicating which metrics are fulfilled. The prototype is a software implementation of the framework, but the idea behind it resides with the framework. That means that it is not necessary to use the software prototype in order to use the framework, one could make a different implementation or do it manually with paperwork. The self-assessment framework and the software prototype are not the same thing but the software prototype is strongly linked to the framework.

While ascertaining requirements it was found that the feasibility of metrics depends heavily on the support given by software used for patch, asset, incident, identity, etc. management. This finding also reflects that some of these software solutions fully integrate the calculation of security metrics.

6 Conclusion and Future Work

The metrics catalogue delivers an extensive set of metrics for measuring the effectiveness of an ISMS or processes and controls of an ISMS. The catalogue's use is not limited to the self-assessment framework; it can be used independently as a collection of security metrics. The catalogue is not only a collection of security metrics, also ISO 27001 clauses and control were assigned to each metric if their effectiveness is being measured. As essential information for the self-assessment framework requirements were ascertained for each metric. The metrics catalogue does not and could never claim completeness. As used sources can change or new sources can appear, constant monitoring of existing sources and updating of the catalogue is needed.

The self-assessment framework defines how feasible metrics can be determined. An assessment is conducted by presenting the list of requirements to the user, who indicates which requirements are fulfilled by the user's ISMS. Results of the assessment are not only feasible metrics: a list of partially feasible metrics can be created together with an action plan indicating which requirements need further action to be fulfilled properly and the number of feasible metrics per ISO 27001 clause and controls, which has the benefit that the user of the framework sees at a glance which parts of the ISMS have their effectiveness measured. With the self-assessment framework, anybody can determine feasible metrics; no special knowledge regarding security metrics is needed. The only requisite is being sufficiently informed about the ISMS or having enough information about the ISMS at disposal so that one can indicate which requirements are fulfilled.

The software prototype provides a proof of concept of how an assessment according to the self-assessment could be conducted with tool support. Additionally, the software prototype allows management of all data needed by the self-assessment framework and generates documents such as the metrics catalogue. The software prototype is rather a proof of concept than a piece of software that is ready for release. Further work is needed before releasing it to the market. The framework and the software prototype could be developed further by adding graphical charts to the reports, allowing users to adapt metrics, include processes from data collection to presentation of metric results and offering more interactive methods than PDF files to explore data like the metrics catalogue or the assessment results.

The external evaluation showed the usefulness of the results of the study and additionally helped to identify limitations and future work.

Similar as the reviewed other approaches for selecting metrics, this approach still relies on subjective perceptions of individuals. The ascertainment of requirements for each metric involves subjectivity. In addition, the assignment of controls to security metrics was done mainly based on the perception of the researcher. The metrics catalogue and in particular mappings to controls and requirements could be revised in a peer review process.

The reviewed frameworks and guidelines for establishing an information security measurement programme offer little guidance on how to select metrics. Therefore, the self-assessment framework could be integrated into those frameworks. Any source of metrics could list the requirements per metric and enable users to determine feasible metrics via the self-assessment framework and the software prototype.

7 References

Bellovin, S. (2006), ‘On the brittleness of software and the infeasibility of security metrics’, *Security & Privacy* **4**(4), 96–96.

Berinato, S. (2005), ‘A few good information security metrics’. http://www.csoonline.com/article/220462/a-few-good-information-security-metrics [Accessed 5 May 2012]

Brotby, C. and Hinson, G. (2012), ‘Security metametrics: SMOTW: Security metrics of the week’. http://securitymetametrics.blogspot.co.nz/search/label/SMotW [Accessed 23 Jun 2012]

BSI IT-Grundschutz Catalogues (2005), Bonn. Federal Office for Information Security (BSI). https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html [Accessed 12 Dec 2011]

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. and Robinson, W. (2008), *NIST Special Publication 800-55: Performance Measurement Guide for Information Security*, National Institute of Standards and Technology, Gaithersburg. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf [Accessed 15 Dec 2011]

CobiT 4.1 (2007), Illinois. IT Governance Institute. http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf [Accessed 10 Dec 2011]

COBIT5 (2012), Illinois. A Business Framework for the Governance and Management of Enterprise IT. ISACA. http://www.isaca.org/COBIT/Pages/Product-Family.aspx [Accessed 16 May 2012]

Fruehwirth, C., Biffl, S., Tabatabai, M. and Weippl, E. (2010), Addressing misalignment between information security metrics and business-driven security objectives, *in* ‘Proceedings of the 6th International Workshop on Security Measurements and Metrics’, MetriSec ’10, ACM, New York, pp. 6:1–6:7.

Hinson, G. (2006), ‘Seven myths about information security metrics’, *The Information Systems Security Association ISSA Journal July 2006* (July), 1–6.

ISO 27001 (2005), Genf. ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization (ISO).

ISO 27004 (2009), Genf. ISO/IEC 27004:2009 – Information technology – Security techniques – Information security management – Measurement. International Organization for Standardization (ISO).

Jansen, W. A. (2009), *Directions in security metrics research*, National Institute of Standards and Technology, Gaithersburg. http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf [Accessed 25 Dec 2011]

Lemos, R. (2012), 'Five strategic security metrics to watch'. http://www.darkreading.com/security-monitoring/167901086/security/perimeter-security/232601457/five-strategic-security-metrics-to-watch.html [Accessed 20 May 2012]

Payne, S. C. (2006), *A Guide to Security Metrics*, SANS Institute. http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55 [Accessed 17 Dec 2011]

Rosenquist, M. (2007), 'Measuring the return on it security investments'. http://communities.intel.com/docs/DOC-1279 [Accessed 12 Feb 2011]

Savola, R. (2007), Towards a taxonomy for information security metrics, *in* 'Proceedings of the 2007 ACM workshop on Quality of protection', QoP '07, ACM, New York and NY and USA, pp. 28–30.

Savola, R. (2010), 'On the feasibility of utilizing security metrics in software-intensive systems', *IJCSNS International Journal of Computer Science and Network Security* **10**(1), 230–239.

Saydjari, O. S. (2006), Is risk a good security metric? , *in* 'Proceedings of the 2nd ACM workshop on Quality of protection', QoP '06, ACM, New York, pp. 59–60.

The Center for Internet Security (2010), 'The CIS Security Metrics'. https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf [Accessed 29 Nov 2011]

Wright, S. (2006), 'Measuring the effectiveness of security using ISO 27001'. http://wwww.iwar.org.uk/comsec/resources/iso-27001/measuring-effectiveness.pdf [Accessed 1 Jul 2012]

Firewall Rulebase Analysis Tool

P. Jain and P.S. Dowland

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

Abstract

Research has shown that majority of network penetration attacks is likely because of poor implementation of firewalls; which are actually meant to protect the network at perimeter. The Firewall Rulebase Analysis Tool analyses the inapt firewall rules and helps you defend against penetration attacks. The aim of this project is to highlight that the offline rulebase analysis has more to offer and should be considered in cost-cutting measures and by SMEs. This tool does an intensive analysis on each rule against a pre-defined checklist, and generates a report mentioning necessary actions required.

Keywords

Firewall rules, rulebase analysis, rulebase automation tool, Netscreen, Cisco ASA

1 Introduction

Firewalls are meant to protect the network by analyzing traffic packets against pre-defined rulesets, and thus its significant implementation is extremely crucial. This includes physical configuration, location in network architecture, and managing rules within. A single inappropriate rule is enough to provide an entry point for hackers to penetrate the network.

These rules are created by firewall administrator based on whitelist or blacklist pattern to allow/deny traffic. The objective of having such rules is to create a bottleneck for only authorized packets to enter the network and block all other unnecessary traffic.

With such critical job, managing firewalls is equally critical. Large organizations have multiple firewalls and large rulebase. Firewall management products from leading vendors do real-time analysis with combination of logs and firewall rules. However, such products are heavy and come at a costly price, which SMEs cannot afford or don’t actually need. SME’s have mostly 1 or 2 firewalls and comparatively less rules within.

The objective of this tool is take a passive approach and use the configuration file to perform rulebase analysis. Configuration file is a file that has entire settings related to the device; from users’ passwords (can be masked or unmasked), to hardware configuration settings and all other working parameters. This will help the firewall administrators, and also security auditors to assess their rulebase configuration. This will help them save the cost of integrating firewall management suites and at the same time help out with compliance audits.

In this paper, we look at the overview of existing products and its limitations; the developed tool’s working features, tool-generated reporting structure and tool evaluation.

2 An overview of existing products

Tools like Algosec’s firewall analyzer, RedSeal’s Network Advisor are active tools that need to be integrated with the firewalls. “AlgoSec supports firewall policy management, including the automation of firewall operations, auditing and compliance, change management, and risk analysis”. (Algosec, n.d.). From policy management perspective, we need to perform the similar task using configuration file, an offline approach.

There are tools like NII’s Firesec, 360 Anaytics’ 360-FAAR, and earlier versions of Nipper. However, Nipper and 360-FAAR only helped in interpreting configuration file and present it in a more readable manner. Firesec is the only tool that does some offline analysis, but the checks are very limited as compared to active tools and the reporting format is not user-appealing. The report does not give any specific reason for marking a rule as ‘Unsafe’. In such scenario, the user is left clueless on the modifications required in the rulebase and the next step to be taken.

The need of the hour is to have an interactive report, additional number of checks, further granular analysis to avoid false positives, highlighting unsafe rules with proper analysis comments, and reduce manual effort. This will help users prepare for compliance standard requirements.

3 Firewall Rulebase Analysis Tool

The tool developed is on the grounds of passive analysis and so it is important to understand the basic rule structure. Following this, the tool working and report will be discussed.

3.1 Basics of Rulebase Analysis and the approach used

Before going ahead with rulebase analysis, it is important to understand the basic structure of a ‘rule’. Basically, a rule is a combination of source, destination and service. However, it has some more elements:

Rule no|Rule name | Source | Destination | Service | Allow status | Protocol | Logging

Rule no: Each rule may be associated with a rule number or rule id for reference. This is an optional field, as what matters is the position of the rule. Generally the preceding rule has higher priority unless there is a global policy set.

Rule name: This is used to give information about the interface and the direction of traffic (Inbound or Outbound), the rule is applied for. The approach may vary, but ultimately the information provided is the same.

Source, Destination: Address objects or Group Address objects which are binded with IP address(es)

Service: It defines Service objects or Group Service objects with port numbers/services (e.g. ‘port 53’ or ‘service DNS’)

Protocol: This field mentions the IP protocol number/name which determines the nature of the traffic (e.g. tcp/udp/icmp/ip)

Allow status: The action to be taken, if a packet matches the rule. It can be ‘allow’ or ‘deny’

Logging: Irrespective of the action taken, this field defines whether the packet details that match the rule should be logged or not. Each rule will have to specify this option individually. The logs can be stored locally in a log file or in a central syslog server.

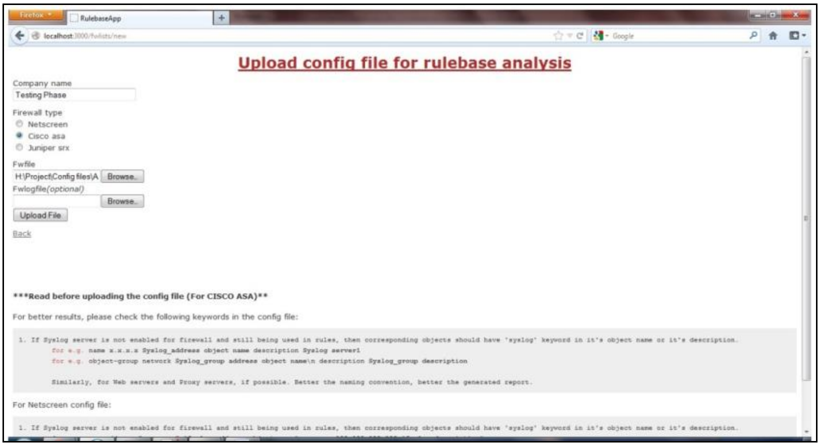
Since, a rule is associated with interfaces, address objects, and service objects; all this data along with rules also need to be collected from the configuration file. If logging is enabled, then generated logs will be useful to count the number of hits on a particular rule, which proves useful.

Thus, a checklist was created that would assess different unsafe patterns of rule settings, which will be discussed in section 4. After surveying the demand for leading firewall vendor products, Juniper’s “Netscreen” and Cisco’s “ASA” firewalls were chosen to be used as experiment models for the tool. The tool is developed using ‘Ruby on Rails’ framework.

3.2 Tool working and its features

The target users of this tool are firewall administrators of SMEs and security auditors. Focusing the criticality of data within configuration file, this tool will have to be installed locally, rather than on internet. Once the tool is installed, and rails server is started; typing ‘localhost:3000’ in the browser URL will load up the application. 3000 is the default port number used by rails server. This will show a page, indexing all the previous uploaded configuration files and associated form details. Click on ‘New Fwlist’ to upload a new file.

Step 1: Fill the form details and upload the config file and log file (optional). Only one check depends on log file and the user may not want to upload such a huge file (size can be in MBs).



Upload config file for rulebase analysis

Company name
Testing Phase

Firewall type
○ Netscreen
● Cisco asa
○ Juniper srx

Fwfile
H:\Project\Config files\A

Fwlogfile(optional)

***Read before uploading the config file (For CISCO ASA)**

For better results, please check the following keywords in the config file:

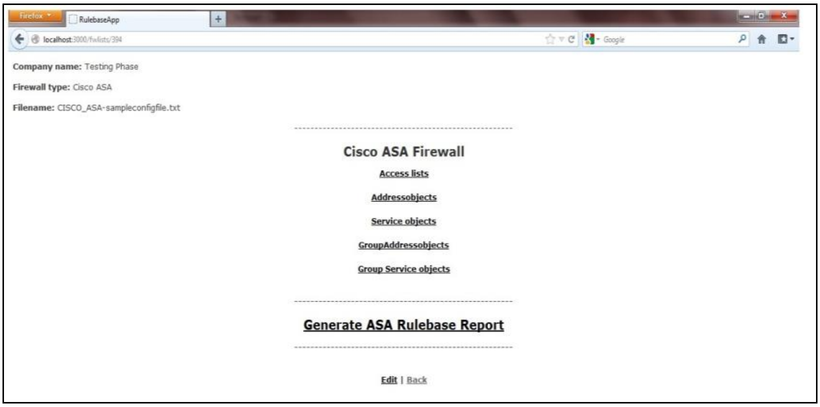
```
1. If Syslog server is not enabled for firewall and still being used in rules, then corresponding objects should have 'syslog' keyword in it's object name or it's description.
        for e.g. name x.x.x.x Syslog_address object name description Syslog server1
        for e.g. object-group network Syslog_group address object name\n description Syslog_group description

        Similarly, for Web servers and Proxy servers, if possible. Better the naming convention, better the generated report.
```

For Netscreen config file:

```
1. If Syslog server is not enabled for firewall and still being used in rules, then corresponding objects should have 'syslog' keyword in it's object name or it's description.
```

Figure 1: Form to upload new file

Step 2: Clicking on Upload file and the Firewall Type chosen, scripts run in the background to parse the data from the uploaded files and store it in database tables. In this case, it's Cisco ASA.



Company name: Testing Phase

Firewall type: Cisco ASA

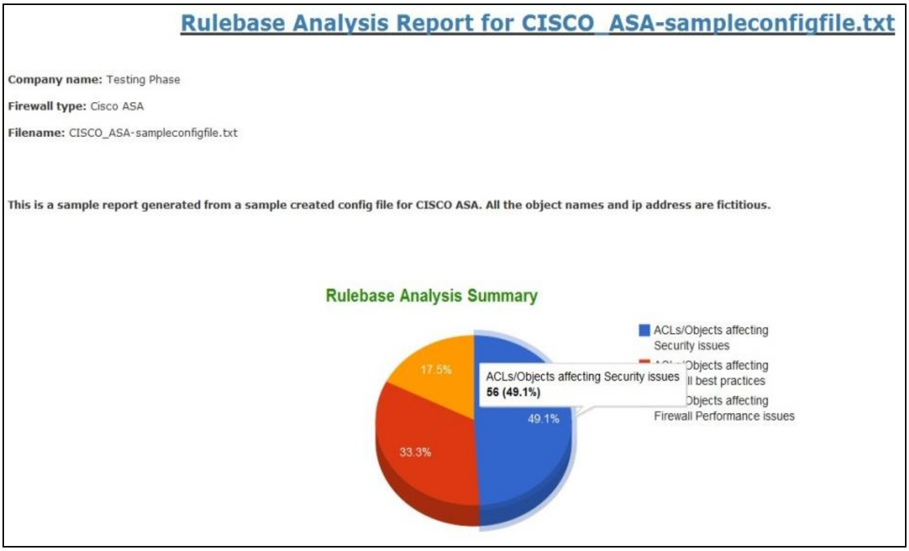
Filename: CISCO_ASA-sampleconfigfile.txt

Cisco ASA Firewall

Figure 2: List of database tables for uploaded file and link to generate report

Step 3: Cross check if all the tables; "Accesslists", "Service Objects", "Address Objects" and "Group Objects" have correct data. If not, then edit/delete options are provided for each row.

Step 4: Click on 'Generate ASA report'. This will run scripts for all rulebase checks on the above tables and generate an evaluation report. Each section of the report is discussed in SECTION 4 along with the checklist.



Rulebase Analysis Report for CISCO_ASA-sampleconfigfile.txt

Company name: Testing Phase

Firewall type: Cisco ASA

Filename: CISCO_ASA-sampleconfigfile.txt

This is a sample report generated from a sample created config file for CISCO ASA. All the object names and ip address are fictitious.

Rulebase Analysis Summary
ACLs/Objects affecting Security issues
ACLs/Objects affecting ...ll best practices
...Objects affecting Firewall Performance issues
ACLs/Objects affecting Security issues
56 (49.1%)
17.5%
33.3%
49.1%

Figure 3: Tool-generated report

3.3 Tool-generated Report structure

After researching through firewall management products, PCI DSS standards and NIST considerations, a checklist was prepared, which could be used to determine inapt rules using configuration file. These checks were then converted to scripts, with the intention of reducing manual effort and present a sensible and valuable report. To be more interactive, these ruby scripts are integrated with rails framework so the tool has a User Interface and the user could use it without any knowledge of scripts or commands.

Following are the tests that run against the rules/objects of the uploaded file. Severity levels determine the criticality of the check (in [] brackets).

Check name	Description
Reverse/ Bidirectional rules [Security]	Reverse rules are the ones in which the source object of one rule is present in destination of another and vice-versa. For stateful firewalls, such access might not be needed, except for some special applications. Once the TCP handshake is done and the state is established, the firewall would refer to the state table for allowing incoming traffic.
Rules allowing cleartext services [Security]	Cleartext protocols send data in clear text, without any encryption. This means that the data sent through these protocols are susceptible to network sniffing attacks. Commonly known clear-text protocols are HTTP, Telnet, IMAP, POP, FTP, and NETBIOS. Avoid using such protocols.
Deny-All-Log rules [Security]	This rule rejects and logs all the traffic patterns not covered in the rules. This gives a whitelist approach, where only required traffic is permitted. With the amount of security, this single rule provides, it is required to have an explicit 'deny-all' rule (with

	logging enabled) at the end. If an implicit 'deny-all' rule already exists, then the explicit one would act as an additional layer of defense.
Entire Network access [Security]	Many-a-times, firewall administrators mention 'any' in address objects, normally under pressure, to avoid business interruption. This rule exposes full network for the corresponding firewall interface. Always have specific addresses in the ACLs.
Large Port Range access [Security]	Ports and services may have associated vulnerabilities running. Hackers outside, malicious insiders or compromised devices may try to port scan the network. Unnecessary ports, especially large range of port access should be avoided.
Invalid IP addresses [Security]	A valid IP address format is: **x.x.x.x** (IP address) **x.x.x.x** (Netmask)**; where x<=255.** Any address that does not fit in this format is invalid. Generally, these are typo-errors by administrators. If such address is used in permit rule, may cost business interruption. If present in deny rule, may prove the rule invalid; thereby allowing traffic which meant to be rejected.
Inappropriate access rules [Security]	**Connecting to any DNS server on internet:** DNS service resolves queries for domain names into IP addresses to locate devices on the internet. In order to stay protected from malicious DNS servers on the internet, make sure to connect to a dedicated DNS server instead of 'any'. **Connecting Syslog and Web server to Internet:** Syslog and Web servers are very critical servers in terms of information they hold. They should never be connected to the internet. Such rules will also be reported by the tool. This tool will take different approaches to determine presence of such servers from configuration file.
Access to 127.0.0.1 and 0.0.0.0 IP addresses [Security]	127.0.0.1 is a loopback (or localhost) address and presence of this IP address, would give access from/to all ports bound to loopback interface. '0.0.0.0' is an unspecified address. Presence of this address in destination, gives access to all network interfaces of a device (Network Working group, 2002)
Management Interface access [Security]	Management interface should be isolated from any traffic except management traffic and also the number of management hosts should be limited. Rules are not required to provide management access, as firewall has other features to enable mgmt access. This tool will determine the management interface and list down all the related rules present. The user has to decide on whether the rules are required or not.
Redundant / Shadow rules [Performance]	Redundant rules are the ones, when one rule is a subset of the other rule. If the parent rule exists, then the other rule composing of its child objects with similar access proves to be redundant.
Covered rules [Performance]	If two rules have any two of; source objects, destination objects and service objects in common, then those rules can be merged to form one rule. Lesser the number of rules, easier it is to manage the rulebase.

Duplicate rules [Performance]	If two rules are exactly similar, they get reported here in this section. One of the two rules should be removed.
Unused rules and top 10 used rules [Best Practice]	If logging is enabled, one can use the valuable information to increase firewall performance. Firewall's efficiency can be increased by bringing the most used rules at the top and removing all unused rules from the rulebase.
Unused Objects [Best Practice]	Unused objects are the objects which are created, but not used in any of the rules.
Inactive rules [Best Practice]	These are disabled rules and prove no use of staying in the rulebase.
Orphan rules [Best Practice]	These ACLs are the ones which have obsolete objects present. Sometimes, systems are removed from the network infrastructure, but the corresponding rules are not removed. It is not possible to get the list of such objects from the config file. However, presence of certain objects might create doubts, for e.g. generally, there would be only one external proxy server in the network. The tool will check for keywords 'proxy' or 'proxies' in address objects and it's descriptions, to determine presence of a proxy server. If more than one external proxy server is found, all related rules will be reported.

Table 1: List of rulebase checks with description

Each check is presented with a generic description in the report followed by a list of unsafe rules under that check. Each rule is given an appropriate audit comment and presented with line number of the rule within the configuration file. This information will help user to locate the rule in configuration file and make suitable changes. Moreover, if the user wants to check the effect of changes being made, before applying to the config file, then the user can scroll down to the APPENDIX of the tool-report. The APPENDIX of the tool-report has the list of database tables, as discussed in previous section, which will help to edit values, and the effect can be observed by regenerating the report. When all the checks are completely executed, a graph is presented which gives a statistical analysis on the number of unsafe findings being reported.

Thus, the user is given a complete interactive report with graphs, proper comments, description of each rule check, location of rule in file, and additional rule-edit options to test before implementing changes.

4 Conclusion and Future Scope

The tool built is really useful for firewall administrators and security auditors to assess their rulebase offline. Most of the checks relevant to PCI DSS and NIST standards have been covered. Thus, using this tool will aid in preparing for these standards. This tool is developed for Netscreen and Cisco ASA firewalls, and has been tested for performance up to 1000 rules. However, lesser the number of rules, better it is to manage the rulebase. The tool will help boost user’s confidence in managing firewall configuration.

With the configuration having so much information to offer, a full vulnerability assessment of configuration file should be targeted. At present, the tool assists in compliance, but, in future, the report should itself be a compliance standard report. Moreover, this being a prototype, only 2 firewalls were used for analysis, and in future, the support should be extended for maximum firewalls.

5 References

ALGOSEC (n.d.) *Algosec Security Management Suite* [WWW] Algosec Inc. Available from: http://www.algosec.com/en/products/firewall_analyzer [Accessed 18/1/12].

Network Working Group (2002) *Special-Use IPv4 Addresses* [WWW] The Internet Society. Available from: http://www.ietf.org/rfc/rfc3330.txt [Accessed 20/07/12]

Snort IDS Ability to Detect Nmap and Metasploit Framework Evasion Techniques

Z. Jammes and M. Papadaki

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

Abstract

Detecting exploit and port scan disguised by evasion technique is a challenge for IDS. This research examines the evasion technique provided by Nmap, a port scanner and Metasploit Framework, an exploit launcher against a famous IDS named Snort. The result tends to prove that Snort has the ability to detect port scan and exploit on condition to have a good configuration of Snort and signature for the exploit.

Keywords

IDS, Snort, Nmap, Metasploit Framework, evasion techniques, resilience

1 Introduction

Nowadays, information systems are increasingly open Internet. This opening is beneficial but is poses nevertheless a major problem: it brings a number of new attacks and requirement. The first effect is the implementation of a security policy around these systems. In addition to the implementation of firewalls and authentication systems are also necessary. To complete this security policy, it is also important to have monitoring tools to detect possible intrusions in the system. The solution is intrusion detection system but like each software, the IDS have also some weakness named: evasion techniques. Hopefully, over the time, the IDS are improved bringing new functionalities but therefore, they are become powerful but also difficult to configure. Today, the slightest error in configuration can then let go of thousands of intrusion without being alerted.

2 Evasion techniques

The evasion techniques were firstly introduced by Ptacek and Newham (1998). They explained that they described three evasions which are the foundations: the insertion, the evasion and the denial of service.

The insertion attack is an attack where IDS does not detect anything although on the target system, the attack does occur and the target system ignored the packets. The evasion attack is an attack where the target system accepts the packets although the IDS refused the packets. The aim of these evasion techniques are the packet content in the traffic was differently interpreted between the IDS and the end system; this being due to the different system implementation. Finally, the denial of service attack is an attack is an attack with the aim of makes unavailable the IDS. This known evasions techniques target specific layers of the TCP/IP protocol stack and use their weakness (for instance fragmentation). Nowadays, these techniques have also spread to other different protocol as SMB, DCERPC and HTTP.

In 2010, Stonesoft (Boltz, Jalava, & Walsh, 2010) shared findings on a new evasion threat. Indeed, they discover this year new techniques to evade IDS named Advanced Evasions Techniques (AET). The AETs target multiple layers of the protocol TCP/IP stack and combine multiple evasion methods. Furthermore, they can be changed or modified during the exploit. The problem is that they do not conform to the rules used by IDS today.

Nowadays, many tools used to test the security implements different technical evasion. For instance, Nmap (2012) is designed to detect open ports, identify hosted services and information about the operating system of a remote computer but provided some evasion techniques. Metasploit Framework (Maynor , 2007) is a tool that allows launching different exploit against a remote host while also providing different evasion techniques. An exploit is a computer program to “exploit” a security flaw or vulnerabilities.

Snort (2012) is a signature-based IDS e.g. it uses signatures of known attack to detect the attack in the network traffic. It is very dependent signatures and therefore required to be updated regularly. Snort is also considered like anomaly-based IDS. It is able to detect some anomalies in the different protocol.

Snort is therefore based on the preprocessors to normalize traffic and detecting anomalies and on the rules to detect in this study exploits. preprocessors and rules will be put to the test.

3 Snort configuration against Nmap’s evasion techniques

The experiences made with Nmap can be easily redo because it does not necessary have specific equipment. The only requirement is to have 2 computer or virtual machine. The most important is to have one host which launches the scan and another which is scanned. It could be useful to prefer to target a Linux distribution rather than a windows system.

Nmap offers different scan techniques based on the TCP and UDP protocol. The sfPortscan is the preprocessor that is able to detect different port scan in function of its configuration. Most of the evasions are based on changes to the UDP, TCP and IP protocol. For this part, the experience uses different scans provide by Nmap.

The most efficient evasion technique provided by Nmap to evade this module is the fragmentation. Usually, fragmentation occurs when datagrams are larger than the allowable size, this limitation is called MTU (Maximum Transmission Unit). Each fragmented packet has an IP header for linking fragments together during the reconstruction.

Type of scan	With Frag3	Without Frag3
Syn scan/regular scan	OK	NO
Fin scan	NO	NO
Null scan	NO	NO
Maimon scan	NO	NO
Xmas scan	NO	NO
Connect scan	OK	NO
Ack scan	NO	NO
IP protocol scan	NO	NO
Intensive scan	OK	NO
Intensive scan plus UDP	OK	NO
Intensive scan all tcp	OK	NO
Slow comprehensive scan	OK	NO

Table 1 - Port scan detection with fragmentation

In this case, despite that the sfPortscan is enabled, Snort is unable to detect any port scan. Snort needs the frag3 preprocessor which performs the defragmentation of IP packets in order to prevent attack packets intentionally fragmented can escape detection. Snort is not able to detect some scans provided by Nmap. Indeed, the Fin, Null, Xmas, Maimon scan are not detected because this type of traffic does not exist normally on a network. In this case, it is important to add some rules to Snort such as:

```
alert tcp any any -> $HOME_NET any (msg:"FIN Scan";
flags: F; seq:1;)
alert tcp any any -> $HOME_NET any (msg:"NULL Scan";
flags: 0;)
```

The stream5 preprocessor is also an important piece to detect Nmap scan technique detection. It reconstructs TCP flows and it is also capable of reconstructing the UDP sessions. It allows rules to be executed on the data stream. Without it, once again, Snort cannot detect port scan.

SYN Scan	Detected
T5	OK
T4	OK
T3	OK
T2	OK
T1	OK
T0	NO

Table 2 - SYN scan detection with different timing

Another evasion technique, it is the possibility to choose the timing between sending two probes. Nmap provide different default template. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). The first two are for IDS evasion. The paranoid mode waits 5 minutes between sending each probe where the sneaky mode waits 15secondes. Without any difficulty, snort was able to detect the sneaky, polite, normal, aggressive and insane mode but it is not able for the paranoid mode. The problem is that sfPortscan analyse the packet on a windows of 60 second when the low sense level is selected. The best chance is to use the High level because it continuously track active host but it requires adjustments.

Nmap gives the possibility to change the TTL value in the different packet created. One thing to notice is if the TTL is set to 0, Snort is not able to detect any scan because it ignores each packet that has a TTL of 0. This evasion can be difficult to put in place in a real network because with a TTL of 0, it is impossible that a scan reaches their target, the different will be dropped before it happens. The only possible is to scan a computer in the same network so the attacker is inside the company or via a disgruntled employee.

Stream5, Frag3 and sFportscan are complementary and the best way to detect port scan with or without evasion techniques. After their effectiveness in detecting scans depend on their configuration.

4 Snort configuration against Metasploit's evasion techniques

In this part, it is important to configure this option like this: `config checksum mode: none.` Otherwise, the entire exploits tested are not detected because Snort seems to assume that the traffic with the bad checksum has no effect on the target.

For Metasploit Framework, the majority of the experiences needs different version of windows, old software version, and some specific software configuration. It is really difficult or impossible to retrieve older versions of software that some exploits target (Luckily it is impossible to find, in this way the average user is protected). Hopefully, the majority of exploits that target the browser (Internet Explorer) or some versions of OS are easily to recreate.

The evasion techniques used by the Metasploit Framework are evasions that are focus on HTTP, DCERPC, SMB, TCP protocol and HTML. In this part, Snort relies more on the rules than the preprocessor. The preprocessor are here to normalizes the traffic and make information that transits understandable and decipherable to ensure and increase the chances of detection.

Snort has static signatures so the different evasion techniques try to transform the exploit for that it stay understandable for the target but not for Snort e.g. the exploit does not match the signature of the rule.

Evasion	Netapi Exploit detection	Wkssvc Exploit detection
Without evasion	OK	OK
DCERPC::max_frag_size	OK	OK
SMB::pipe_evasion	OK	OK
SMB::pad_file_level	OK	OK
SMB::pad_data_level	OK	OK
TCP::max_send_size	OK	OK
TCP::send_delay	OK	OK

Table 3 - Exploit DCERPC/SMB detection

OK: Snort detects the exploit
NO: Snort does not detect the exploit

A first part of the evasion techniques take the advantage on some specificity of DCERPC, SMB and TCP protocols.

On the DCERPC protocol, it is possible to force the fragmentation of packet. In this condition, Snort is unable to understand the DCERPC protocol. Hopefully, the DCERPC2 preprocessor is able to defragment.

On the TCP protocol, it is possible to limit the size of the TCP segment. In this case, the packet are segmented and to be able to still see the exploit, Snort needs to have the stream 5 preprocessor activated.

A second part of the evasion techniques take the advantage on some specificity of HTTP protocols. This evasion allows changing some value in the HTTP header and encoding the HTTP body.

On the HTTP protocol, it is possible to compress the HTTP page to gain in bandwidth. The problem is that the IDS will not be able to detect the signature include in the HTTP body compressed. It is important to activate the inspect_gzip option. This options specifies the HTTP inspect module to “uncompress” the compressed data (in gzip/deflate) in HTTP response. With this option, Snort is able to still detect the exploit.

Metasploit framework is able to encode the HTTP body with different language such as base64,Unicode and JavaScript, Snort is not able to detect the exploit anymore because the rule does not recognize this type of encoding but Snort provides an alert if it detects the use of Base64 and JavaScript in the payload: “POLICY-OTHER base64-encoded uri data object found” and “Obfuscation JavaScript”. Normally, Snort is able to normalise the Unicode like the JavaScript but it could be difficult for Snort to refund the original code.

Evasion	IE Exploit detection	Mozilla Exploit detection
Without evasion	OK	OK
HTML ::base64	NO	Rejected
HTML::JavaScript::escape	NO	Rejected
HTTP::chunked	NO	NO
HTTP::compression	OK	Gzip:OK Deflate: Rejected
HTTP:junk_header	OK	OK
HTTP::server_name	OK	OK
SSL implementation	NO	NO

Table 4 - Exploit HTTP header and body detection

OK: Snort detects the exploit
NO: Snort does not detect the exploit
Rejected: the result obtained by the evasion technique is not sufficient

One of the weak points of Snort is its inability to detect an exploit in a traffic encrypted.

A third part the evasion techniques is more focus on the modification of URI, these evasions incorporate some evasion available with Nikto. Snort is able to send some alerts based on the anomalies found in the URI.

The problem is that Metasploit Framework according to the exploit offers different evasion options but it is important to highlights that in some case, when an evasion option is activated, it seems that the evasion option is not implemented and so did not make the modifications expected in the main packet of the exploit. Sometimes, the modifications worked but the exploit did not work anymore. The modification made prevents the exploit to work correctly due to changes too important. Certainly, it is possible that the exploit or the vulnerable software is not suitable for certain evasions but Metasploit Framework could at least warn users instead of proposing default evasion.

5 Conclusion and future work

Snort has the ability to detect most of the port scan made by Nmap and the exploit launched by the Metasploit Framework. For Nmap, Snort relies heavily on these preprocessors (Frag3, Stream5 and sfPortscan).

It is important to note with the default configuration provided on the official website of Snort that by default the sfPortscan is not activated. In this case, Snort is unable to generate an alert about port scan activities. An inexperienced user may believe to be protected but, in this case, Snort will not be able to generate alerts concerning scans Otherwise, the configuration provided for Stream5 and frag3 is sufficient to protect and detect port scan with or without evasion technique. However, it is always important to check the traffic and not only rely on Snort.

For Metasploit, Snort relies more on the rules than the pre-processor. The pre-processor (DCERPC2 and HTTP inspect with the support of Stream5) are here to normalizes the traffic and make information that transits understandable and decipherable for the detection engine to ensure and increase the chances of detection for the rules. Each preprocessor has its purpose but it is important to see all the preprocessor as a whole because each preprocessor depends on the other.

By default, the default configuration of the DCERPC2 preprocessor is sufficient it is especially useful for its ability to defragment DCE/RPC. On the other side, the http inspect pre-processor may need some changes. Indeed, some useful options need to be activated such as multi_slash, iis_unicode, apache_whitespace and so on. It really depends on the structure and the type of the server that use the company (IIS, Apache). The administrator may needs to make some choices to adapt the alert that he wants.

The real weak point is that Snort is unable to detect exploit in an encrypted communication and when the code of exploit are encoded by others language, there is still a risk.

The simple way to avoid to be targeted by an exploit from Metasploit, it is to patch the different software on a network regularly or otherwise create a rule the time that the patch comes.

Snort can be considered as one the best solution to protect a SME because its first advantage is that it is free. Large companies will promote solution-based IPS and SIEM but Snort offers a great flexibility and unparalleled scalability through rules. The only inconvenient is that it requires knowledge and basic configuration requires some modification to be really efficient.

For the future, it could be interesting to remake these experiences but in a testing environment where the hardware is limited and the traffic includes not only the traffic of attacks but also some other traffic such as streaming. Snort will be still able to detect the port scan and the exploit. It could be also interesting to test these evasion techniques against other IDS.

6 References

Boltz, M., Jalava, M., & Walsh, J. (2010). "New Methods and Combinatorics for Bypassing Intrusion Prevention Technologies": Stonesoft. available online: http://storage.pardot.com/1912/77027/content_CTA_Technical1_AET.pdf (accessed on 15/01/12)

Maynor, D. (2007). “Metasploit toolkit for penetration testing, exploit development, and vulnerability research”:Syngress. ISBN-10: 1597490741

Nmap, (2012), “Description of Nmap” Available online: http://nmap.org/docs.html (accessed on 17/05/2012)

Ptacek, T. H. (1998). “Insertion, evasion, and denial of service: Eluding network intrusion detection”: DTIC Document. Available online: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA391565 (accessed on 15/01/12)

Roesch, M., Green, C., Sourcefire Inc, (2011), “SNORT Users Manual 2.9.2”, available online: http://www.snort.org/assets/166/snort_manual.pdf (accessed on 17/05/2012)

Snort (2012) "Description of Snort", available online: http://www.snort.org/snort

Evading IDS Detection

P. Jarmak and M. Papadaki

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

Abstract

Intrusion Detection Systems (IDS) is software capable of monitoring incoming and outgoing traffic. The project is to provide a benchmarking study in order to find a trade-off between performance and level of detection as well as to show how it is easy to evade an IDS. This publication describes the evasion techniques, the structure of the experiments as well as the trade-off between performance and level of detection. The results show the necessity of several pre-processors, the resources required by the IDS to guarantee a high level of detection as well as advice to configure Snort.

Keywords

Intrusion Detection System (IDS), Evasion Techniques, Snort, Pre-processors

1 Introduction

During the last years, multiple threats such as new virus or worms have been discovered. An IDS is become essential and should be used in every network where private and critical data flow.

Furthermore, new mechanisms called evasion techniques are able to bypass the security settled by the IDS. Indeed the new evasion techniques consist of combining multiple basic techniques used by the past in order to create new ones. The problem is that the available IDS software is usually not able to detect them. According to Stonesoft (2011) we have only seen "*the tip of the iceberg and over 90% of that iceberg is still unexplored. The theory and practice of evasion techniques needs to proceed hand-in-hand with leaps, not steps*".

In this paper, we focus on the mechanisms deployed by the IDSs to detect the threats but also on a benchmarking study in order to provide results of the resources required as well as the level of detection possible if configured with cautious and reliability.

The paper is divided in three sections. Section two is going to explain the background of the project such as the evasion techniques, Intrusion Detection System (IDS). Section three is going to discuss about the experiments. Therefore the methodology as well as the results will be presented. Finally, Section four is a conclusion of the research and discuss about the aims achieved.

2 Background

2.1 Intrusion Detection System (IDS)

IDS or Intrusion Detection System "*is the process of monitoring computers or networks for unauthorized entrance, activity, or file modification*" (Innella *et al.*, 2001).

Snort is one example of open-source IDS. It provides the basic techniques of threats detection. Snort is able to detect and alert an administrator when an intrusion is detected (Roesch *et al.*, 2011).

2.2 Evasion techniques

It is the ability "*to fool the IDS into seeing data different from what the target host will see"* (Oh *et al.*, 2007). Therefore the IDS system and the host will see different things. There are three kinds of evasion techniques:

- Insertion: The IDS "*makes the mistake of believing that the end-system has accepted and processed the packet when it actually hasn't*" (Ptacek & Newsham, 1998). It is what we call Insertion.

- Evasion: The IDS rejects a packet that the host accepts. It is what we call Evasion. As the previous techniques the IDS and the host will not see the same things.

- Denial of Service: This attack consists to overwhelm the IDS. Thus, it cannot detect the attack contained in a packet. In order to launch the kind of attack the attacker usually uses different hosts, generally a botnet. It is a computer infected by a program. According to Microsoft (2011) a botnet is "*malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it*".

Example of basic evading techniques:

- String matching, IDS can search a specific pattern in a packet. However this technique is very weak because it is easily to change the pattern without changed the meaning. For sample the IDS searches the pattern /etc/passwd but the packet contains /etc/rc.d/.../passwd. The two patterns have the same meaning but not the same words.

- Fragmentation attack which consists of fragmenting the piece of code containing the attack in several packets.

- Fragmentation overlap, this technique consists to send a packet followed by a second packet which overwrites a part of the first one.

- Bad Header fields (No IP addresses set or header length too small, bad “DF” (Don’t fragment) flag…)

- End system fragmentation bugs depending on the Operating system, the packet will not be reconstructed into the same way

Source: Ptacek & Newsham, 1998; Timm, 2006

As treated in the introduction, the evasion techniques evolved much faster than the security community thought. Stonesoft (2011) found new kind of evasion techniques. They are completely different than the precedent evasion techniques. They call it, Advanced Evasion Techniques (AET). The mechanisms to detect them are completely different and the techniques used to detect the other evasion techniques do not work. Therefore it is really important than the techniques evolve fast to be able to handle these new threats.

3 Experiments

The experiments conducted, have been divided in two objectives, one to show of how it is easy to evade an IDS and the roles of the pre-processors and another one to find the trade-off between performance and level of detection.

3.1 Influence of the pre-processors

In this experience, one configuration file of Snort has been used. That configuration file has been modified to identify the different threats (Scan, vulnerability scan, exploits, etc.). Then for different dataset such as scan, exploits, vulnerability scanner, Snort has been launched with different modification in its configuration file. Indeed some of the pre-processors have been deactivated to show their influences. These conditions have been reproduced for each dataset tested. Here, one example of the result obtained:

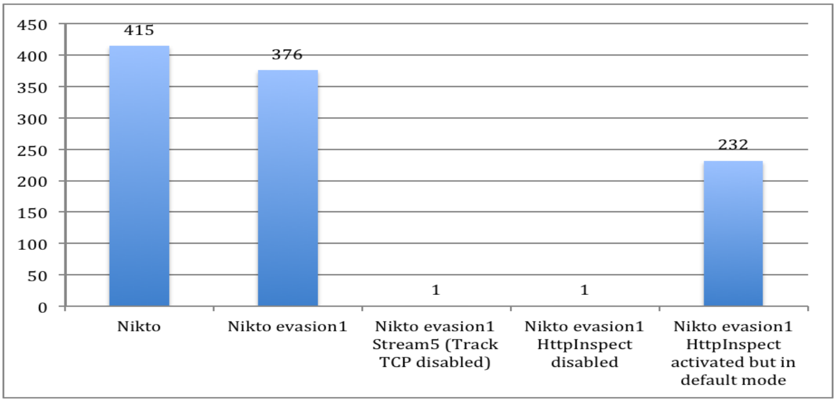


Figure 1: Influence pre-processors on vulnerability Scan detection (URL encoding evasion)

As we can see, the configuration of the pre-processors is essential in the detection. One modification change completely the number of alert found. Of course the modifications have been made to show the influence. Therefore the modifications have been done on the pre-processors essential for the detection of the evasion techniques.

One conclusion can be drawn for these experiments, is that some of the pre-processors are essential for the detection of the threats and without them it is straightforward to fool Snort. These pre-processors are Frag3, Stream5, HttpInspect, Sfportscan. Basically they contribute to provide the mechanisms capable of handling the defragmentation or tracking the connection as well as detecting the evasion techniques. These mechanisms are able to detect most of the evasion techniques which usually use fragmentation, delay, etc.

3.2 Trade-off between performance and level of detection

A second experiment has been done to observe the performance and level of detection according to three different configurations of Snort. These configurations are:

- A modified configuration according to the Snort manual to optimize Snort
- A configuration provided by the Snort website
- A configuration where all the options are by default

These configurations have been tested on a “test-file” regrouping several threats such as scans, vulnerability scanner, exploits, etc. Different parameters have been measured such as the CPU usage, the memory used, the number of alert detected and the time spent of analysing the file.

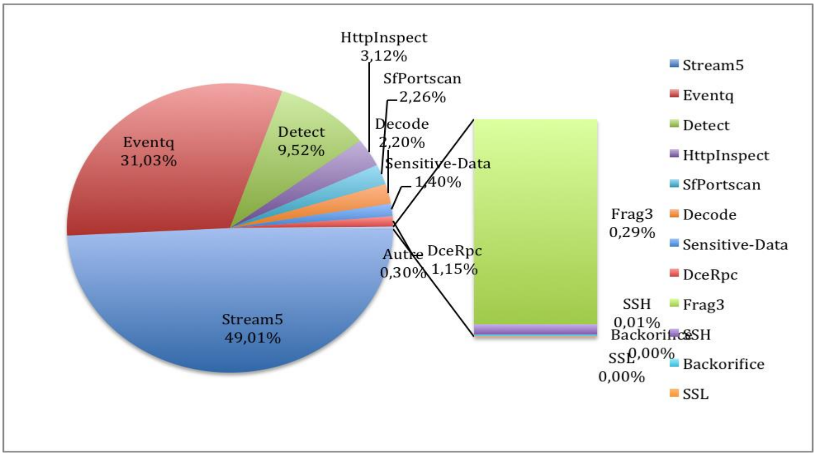


Figure 2: Percentage of time spent for each pre-processor

As we can see, three pre-processors take almost all the resources during the detection step. There are Stream5, Eventq, Detect and I can add also HttpInspect. These pre-processors take the majority of the resources and times because there are the pre-processor able to deal with the evasion techniques.

Moreover the pre-processors Eventq is responsible to generate the alerts. Therefore the way of how the alert are generated should be optimized in order not to take too much time in generating the logs and alerts even if it is a critical part for a later analyse by the administrator. Another solution could be to generate the alerts by another module speratated of Snort. That kind of software already exists such as Barnyard (Securixlive, 2012) which allows unifying the alert as well as improving the time spent to generate the alert. This allows Snort to focus on the detection of intrusion.

The graphs below show the trade-off between performance and level of detection. It shows the results of the three previous configuration files according to different parameters such as the number of alerts, the time spent and the memory usage. A table has also been provided to be more readable:

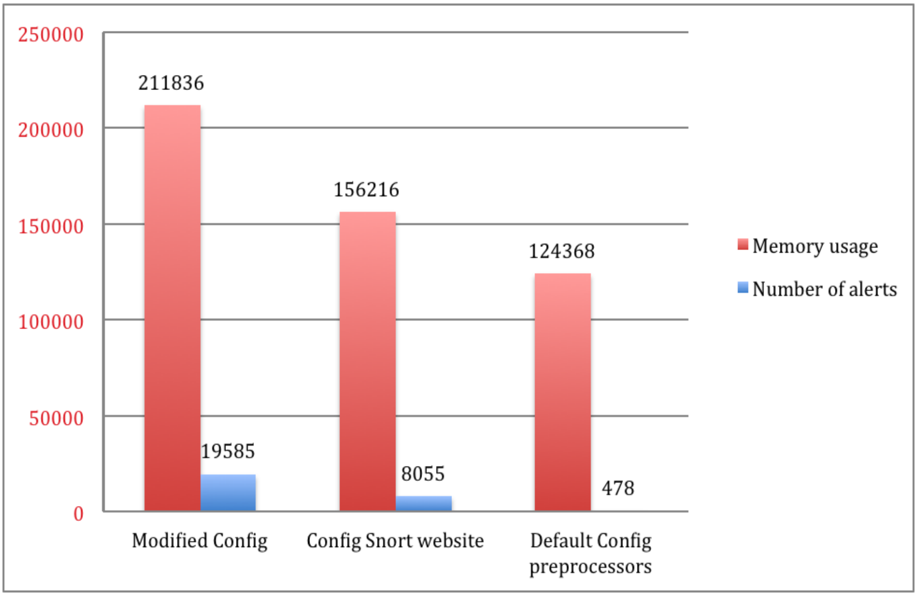


Figure 3: Memory usage versus number of alerts

As shown in the table and the graphs, the modified configuration provides better results in terms of detecting the intrusions but required as well more resources. However the resources stay reasonable. The level of detection is more accurate for the detection of the suspicious traffic.

Indeed the modified configuration file takes more time because it contains more options activated which required more time when Snort checks a packet.

Furthermore because Snort generates more alerts it spends more time to analyse the packets and write the logs.

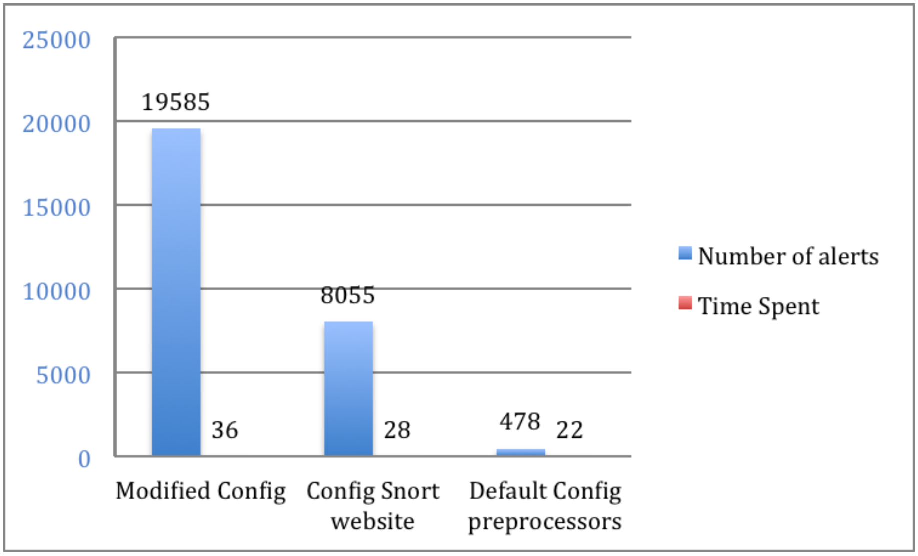


Figure 4: Time spent versus number of alerts

The table shows also the importance of properly configure the IDS. The default configuration found in the Snort website even if it is able to detect some of the threats, it is not enough to secure correctly the network. The same conclusions can be drawn with the third configuration. A default configuration should not be used, because it is not optimized and specific for a particular network. Moreover because a default configuration aims to be used by a large number of users, it contains a lot of flaws and therefore the network is not secured and easily fooled.

The experiments conducted show the importance of an IDS. Evasion techniques are something natural nowadays and therefore should be taken seriously. The paper has shown that Snort is able to detect the majority of them. However this level of detection requires resources and time. These requirements could be too high for certain network or company. Indeed a huge company with a high bandwidth, thousand of hosts, dozens of software could be asked enormous resources. Therefore a network monitor has to be optimized in order to be able to do its work and avoid being overwhelmed which could mean missed intrusion or threats. This is the last thing a company want. It could be interesting to conduct these experiments in a busy environment to number the resources and performance of an IDS.

The paper focused on the configuration of the pre-processors. Another lead could be to optimize the number of rules as well as the way to write them. Indeed too many rules will slow down the IDS. Furthermore a rule poorly written could cause a misunderstanding from the administrator who will read the log. A rule poorly written could cause as well false positives. These false positives may participate as well to slow down Snort if they are too many.

4 Conclusion

The research tried to investigate the resilience of Snort in term of evasion techniques as well as show its performance and level of detection. The experiments conducted, have shown that Snort if properly configured, is able to detect the majority of the evasion techniques. The pre-processors Frag3, Stream5 and HttpInspect play an essential role in the detection of the evasion techniques as well as different threats such as scans or exploits. The experiments have shown that if they were bad configured the level of detection can decrease and therefore miss threats.

Furthermore the experiments showed as well that the resources and the time required increase due to the number of options activated in the configuration of Snort. It is perfectly normal since the number of checking and computation increase as well. However the resources required stay reasonable and the level of detection increases. Therefore according to the resources available the user can obtain good performance with Snort.

However in the experiments conducted, the traffic was not overloaded and it explains why the resources required stay reasonable. In a busy network the results could change and it could be interesting to investigate that question but it should not change a lot. Furthermore it could be interesting as well to compare the results with other IDS for instance with commercial IDS.

The results are strongly linked to the network used in this paper. Therefore one configuration can be optimal for a network and inappropriate for another. The trade-off between performance and detection is sensible to the network and the technologies used. It means that simply copy the security measures for a network would not be efficient for a another network even in the same company using different networks. Each network should be considered with the same importance and level of protection and examine with strong attention.

To conclude the results identified in this paper show the importance of an IDS and its danger if not configured properly as well as the variety of threats nowadays. These threats are in a constant evolution and therefore the security controls must evolve as well in order no to get left behind.

5 References

Innella, P., McMillan, O., Tetrad Digital Integrity, LLC, (2001), '*An Introduction to IDS*', Available at: http://www.symantec.com/connect/articles/introduction-ids (accessed on 22/05/2012)

Micorsoft, (2011), '*What is a botnet*', Available at: http://www.microsoft.com/security/resources/botnet-whatis.aspx (accessed on 22/06/2012)

Oh, J., Park, S., Jeon, Y., (2007), '*Detection of DDoS and IDS Evasion Attacks in a High-Speed Networks Environment*', Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.9533&rep=rep1&type=pdf (22/05/2012)

Ptacek, T., Newsham, T., (1998), '*Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*', Available at: http://insecure.org/stf/secnet_ids/secnet_ids.html (accessed on 22/05/2102)

Roesch, M., Green, C., Sourcefire Inc, (2011), '*SNORT Users Manual 2.9.2*', http://www.snort.org/assets/166/snort_manual.pdf (accessed on 22/05/2012)

Securixlive, (2012), '*A unified output system for Snort*', http://www.securixlive.com/barnyard2/download.php (accessed on 30/08/2012)

Stonesoft, (2011), '*Anti-evasion*', Available at: http://www.antievasion.com/principles (accessed on 22/06/2012)

Timm, K., (2006), '*IDS Evasion Techniques and Tactics*', Available at: http://www.symantec.com/connect/articles/ids-evasion-techniques-and-tactics (accessed on 22/06/2012)

Web-based Risk Analysis for SMEs

R. Kunder and N.L Clarke

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

Abstract

Information technology has made its present felt everywhere around the world. Organisations too heavily depend on information technology for carrying out their day to day work. Hence it is of utmost importance that the IT infrastructure must be guarded against the various threats that are looming over every other organisations infrastructure. Today, large organisations are taking every step to see to it that their assets are protected from the various threats by doing various risk assessments. Unfortunately but true, various survey and researchers have found out that small and medium enterprises (SME) hardly ever follow security practices. Although there are many solutions available in the market for SME to carry out risk assessment but due to lack of in-house expertise and budget constraints they are unable to carry out such security related assessments since the available tools and other solutions either have high costs or require some expertise to use those solutions.

The purpose of this research is to identify all the problems that act as a hurdle for the SMEs when it comes to performing risk analysis and come up with a novel methodology that can be implemented into a web based risk analysis tool which in return be an useful solution for the SMEs as the tool would be available free of cost, user friendly and most importantly suggest cost effective controls which would ensure the balance between the control implementation cost and also keep the threat levels under check. The designed methodology was then implemented into a working prototype called ERAS (Effective Risk Analysis Solution). The prototype was put under test by involving users from Information security background to check if the tool was successful in achieving the aims with which it was developed. It was clear from the users feedback that the tool was easy to use and understand and also the organisation profiling which is employed by the tool proved to be better than the time consuming questionnaire based approach used by other RA tools and solutions.

Key words

Risk Analysis, SME, Security, Risk Management

1 Introduction

SMEs are organisations where there are less than 250 employees and have an annual turnover of not more than € 50 m (European Commission, 2003). In order to protect the IT infrastructure unlike the SMEs, large organisations spend a considerable amount of money which in turn ensures safety of their critical assets. Whereas SMEs they do not hold such security practise. The managers of the SMEs are least cared about the security of their IT related assets. ISBS(2010) claims that SMEs are more vulnerable to security related attacks and this comes as no surprise because in the same survey it has been stated that on an average only 10% of IT budget is spent by SMEs on their security (ISBS, 2010). The main problem of SMEs when it comes to risk assessment is the lack of technical expert staff and less amount of budget is available (Kelleher, 2009). As per the ISBS (2012) only 5% of the total SME spent more than 25% of their budget for information security, which is lower than in the year 2010 which was 8%. There are different RA solutions and tools available in the market (e.g. CRAMM, COBRA) but SMEs find it difficult to understand or use them in a more effective manner (Dimopoulous et al., 2003). The problem with using this tool is the lack of skills to interpret the results given in the output by these tools. According to the ISBS (2012) survey, contingency plans were in place by majority of the SMEs when it came to virus infection, staff misuse of information system, confidentiality breach and access control. but the real problem lies in the fact that although there are still cases where contingency plan is in place but not that effective, 23% organisation failed when it came to system failure or data corruption. Hence, this clearly indicates that due to poor selection of controls SMEs still face a problem in having an effective solution to minimise the risk that they face.

Considering the problems of SMEs relating to the Risk analysis this research would focus mainly upon understanding the main root cause of the problem and coming up with a novel methodology which would be best suited for the SMEs and when this methodology would be implemented into a working prototype then it should meet all the requirements of the SMEs so that they can perform risk analysis without much problems..

2 Risk Analysis and SMEs

Risk analysis is a major concern for all organisations, especially small and medium sized enterprises which are particularly sensitive to business risk and competition (Alquier and Lagasse, 2006). According to (McKierna and Morris, 1994), SMEs are characterized with the central role of the owners and multiplicity of duties and close identity with employees. Enterprises in their start-up phase often underestimate risks or even ignore them completely (Smith, 1998). Start-up SMEs usually face a high degree of uncertainties and the necessity to make quick decisions. Henschel (2008) states that risk management is a challenge for SMEs in contrast to larger firm they often lack of the necessary resources, with regard to human capital, data base and specificity of knowledge to perform a standard and structured risk management. Most of SMEs do not have the necessary resources to employ specialists at every position in the firm (Matthews and Scott, 1995). They rather focus on their core business and have generalists for the administration function. In contrast to larger organisations, very few SMEs have one of the owners as a part of the management team. His intuition and experience are important for managing the firm (Dickinson, 2001). Therefore, owner manager in SME is often more responsible for many different tasks and important decisions. Although risk analysis principles are common to all types of enterprises, the manager’s risk perception and his attitude towards risk analysis influences the adequacy of the enterprise’s risk analysis actions deployed (Ntlhane, 1995). In SMEs, the risk analysis function usually resides with the owner’s assessment of threats and opportunities pertaining to the enterprise (Watt, 2007). Implied in SME, risk analysis is the core principle that management focus should be focussed at recognising future uncertainty, deliberating risks, possible manifestations and effects, and formulating plans to address these risks and reduce or eliminate its impact on the enterprise (Ntlhane, 1995). One of the skills required of entrepreneurs is the ability to identify and analyse risks to ensure that advantage is taken of calculated risks (Watson, 2004).

The fact that a risk is beyond the control of the managers, does not absolve the manager from the need to anticipate the risk, and reducing the impact of the risk occurrence to achieve organisational goals. Managers should be educated in risk management principles, risk handling techniques available and risk control programmes that can be used, but care should be taken in the application of risk management principles, as although risk principles are common to all types of enterprises, the application thereof differs substantially between small and larger enterprises. However, many SMEs practice intuitive risk management when they assess the risk involved in decisions (Ntlhane, 1995). SMEs do not tend to use special techniques to optimize significant risks. Empirical studies show that the attitudes of SMEs towards risks and their risk assessment differ significant from that of large firms.

2.1 Existing RA solutions for SMEs in the market

There are many numbers of tools and standard baseline guidelines available for carrying out risk analysis specially designed for SMEs. Few of the solutions that have been selected for this research purpose are discussed below.

The OCTAVE-S which is specially developed for the SMEs but it is more of a self assessed, streamlined process and produces similar results and also it includes only a limited exploration of the computing infrastructure (CERT, 2008). Small and Medium sized companies do not have the ability to run or interpret the results of vulnerability tools all by themselves due to lack of expertise hence OCTAVE-S is not suited for SMEs. Speaking about COBRA then, it is a process that takes the risk assessment more as business issue rather than a technical one. The tools are not available for free downloads. Theses tools help in self-assessment of the risks (Riskworld, 2011). SMEs refrain from using this tool due to its cost and it also takes long time to fill up the questionnaire thus increasing the analysis time. (Dimopoulous, 2007).

There are other solutions available like the ISO/IEC 27002:2005 Code of Practice which is intended to provide a framework for international best practice in information security management (IS027002, 2012) and NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems is the US Federal Government’s standard. This methodology is designed primarily to be used for qualitative approach, it relies on the skill set and experience of the security analysts working with system owners, and technical experts to thoroughly identify, evaluate and manage risk in IT systems (NIST SP 800-30, 2011). But again both these standards require some amount of expertise to understand and apply the same to the organisation. Hence SMEs abstain from using these solutions too.

3 The Prototype: Effective Risk Analysis Solution (ERAS)

After researching on the problems of the SMEs the main obstacles in the path of effective risk analysis were determined and using this, a new methodology was deigned to suit the SME risk analysis process. The new methodology would take care of the following issues.

- The process of new methodology would be short in length.
- The tool would be simple to use and understand.
- The tool shall be hosted over internet thus it would be freely available to the users.
- Proper assistance would be provided while the user selects assets and controls so as to help the user to get a proper understanding about the relation between the assets, threats and the controls that they need to apply.
- Cost effective controls would be suggested to maintain a balance between the control implementation cost and the threat value level.
- The new methodology should be such that even after RA is finished the tool should give further support in terms of determining effectiveness of controls and allow the user to make further changes.

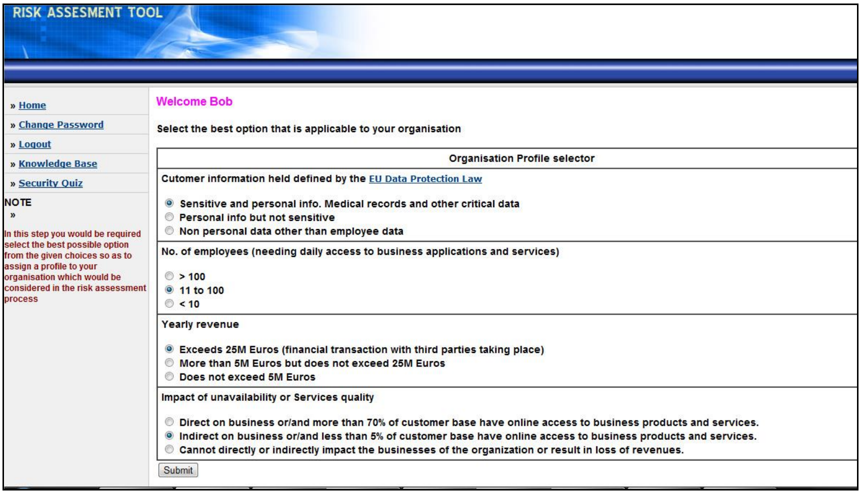
3.1 Overview of methodology

As shown in figure 1 instead of using a traditional questionnaire based approach here the tool would make use of the organisation based profiling. The organisational profile evaluation table would be used to identify their risk context. The organisational risk context is derived from the business and the external environment of an organisation and can be divided into four risk areas: Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability (ENISA, 2007). Figure 2 shows you the prototypes user interface which is implemented using the current methodology. Once the organisation profile is selected (Figure 2.) then the controls are mapped corresponding to the assets identified. The controls are of two types namely, Organisational based controls and Asset based controls.

- Organisational based control cards are that which contain controls applicable to the organization horizontally and are concerned with practices and management procedures.
- Asset based control cards that are applicable to critical assets and are asset-category-specific.

As shown in the figure 2 below data is asked from the user related to the four risk areas and hence from the input of the user the profile is decided. Each area is classified in three classes: High, Medium and Low (corresponding to Medium size, Small size and SOHO respectively). These classes express quantitative criteria for the organisation in question with regard to the risk area and help identify a risk level. "As a rule of thumb the highest risk identified in a risk class defines the overall business risk profile. A high risk carried in the financial risk class marks a high risk profile. Equally, a medium risk leads to a medium risk profile and low risks to low risk profiles" (ENISA, 2007). For example a low risk carried in the reputation and confidence, in legal and regulatory compliance and productivity but a high risk in financial stability risk class concludes to a high organization risk profile. Organisational based profiling (risk profiling) should be considered as a very important decision which subsequently leads to the risk related selection of assets and their protection via control.

Once the organisation profile is selected then users selects the corresponding organisational based controls.



NOTE
»

In this step you would be required select the best possible option from the given choices so as to assign a profile to your organisation which would be considered in the risk assessment process

Welcome Bob

Select the best option that is applicable to your organisation

Organisation Profile selector

Cutomer information held defined by the EU Data Protection Law

- ● Sensitive and personal info. Medical records and other critical data
- ○ Personal info but not sensitive
- ○ Non personal data other than employee data

No. of employees (needing daily access to business applications and services)

- ○ > 100
- ● 11 to 100
- ○ < 10

Yearly revenue

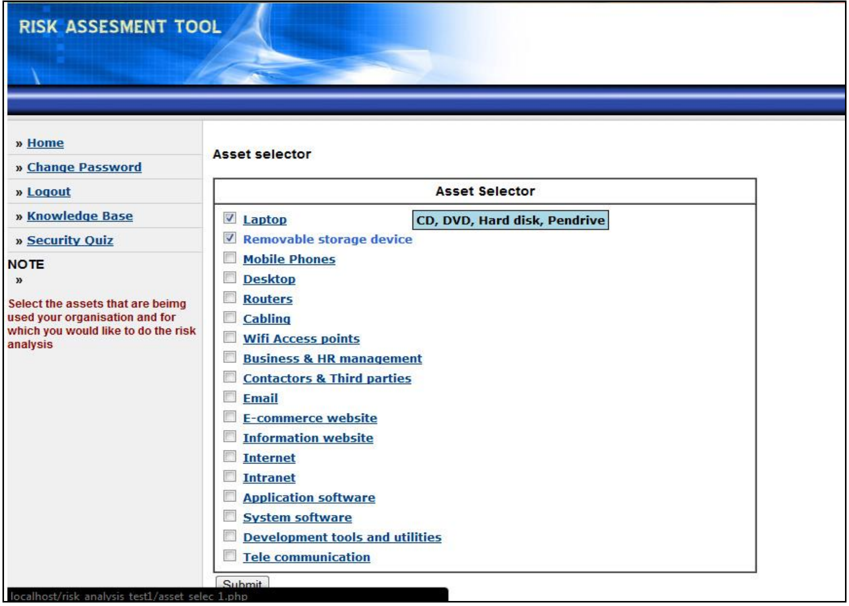
- ● Exceeds 25M Euros (financial transaction with third parties taking place)
- ○ More than 5M Euros but does not exceed 25M Euros
- ○ Does not exceed 5M Euros

Impact of unavailability or Services quality

- ○ Direct on business or/and more than 70% of customer base have online access to business products and services.
- ● Indirect on business or/and less than 5% of customer base have online access to business products and services.
- ○ Cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

Figure 1: Selection of organisation profile

After choosing the applicable assets the user is then presented with the asset based controls for each asset and also the user has to rank the assets as per their importance (Figure 3). The user selects and submits the controls along with the asset ranking to the system.



NOTE
»

Select the assets that are beimg used your organisation and for which you would like to do the risk analysis

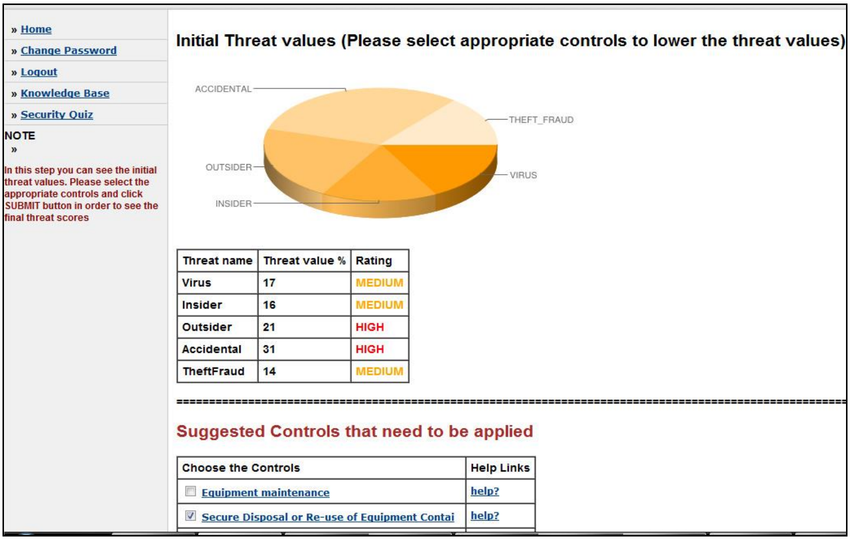
Asset selector

Asset Selector

- ☑ Laptop — CD, DVD, Hard disk, Pendrive
- ☑ Removable storage device
- □ Mobile Phones
- □ Desktop
- □ Routers
- □ Cabling
- □ Wifi Access points
- □ Business & HR management
- □ Contactors & Third parties
- □ Email
- □ E-commerce website
- □ Information website
- □ Internet
- □ Intranet
- □ Application software
- □ System software
- □ Development tools and utilities
- □ Tele communication

localhost/risk analysis test1/asset selec 1.php

Figure 2: Asset selector and ranking



NOTE
»

In this step you can see the initial threat values. Please select the appropriate controls and click SUBMIT button in order to see the final threat scores

Initial Threat values (Please select appropriate controls to lower the threat values)

Threat name	Threat value %	Rating
Virus	17	MEDIUM
Insider	16	MEDIUM
Outsider	21	HIGH
Accidental	31	HIGH
TheftFraud	14	MEDIUM

Suggested Controls that need to be applied

Choose the Controls	Help Links
☐ Equipment maintenance	help?
☑ Secure Disposal or Re-use of Equipment Contai	help?

Figure 3: Initial threat value display along with suggested controls

After this step the initial threat values for the organisation are then displayed. This threat level can be brought under control by selecting the specific cost effective controls that have been displayed to the user. The user can select as much controls as possible until the threat level has decreased to a safe level. This calculation is done using the control effect value that is associated with each control. This value is used as a diving factor either the threat value. Thus as long as control specific to a threat are selected the particular threat value would decrease. Eventually after we have selected the controls keeping in mind the budget of the organisation, we get the final threat value. At present the prototype is not considering the economical values like ROI and ALE,

3.2 Evaluation

The prototype was put under test to investigate whether the aim with which the development of prototype was achieved to what extent. The main purpose of taking feedback from selected users was to get feedback on the tools ease of use, how effective and useful is the output of the tool and the overall functioning and process flow of the tool. Participants who had some background in information security or may be working for an SME carried out the evaluation. The feedback obtained revealed that ERAS prototype's user interface was easy to use and even a person who is not trained in RA could easily use it. The organisation profiling approach was considered far better than using the tradition time consuming questionnaire approach. More users would try it as the tool would be available free of cost. However there is still room for improvement as the users desire more detailed and descriptive output and also more should be included in the output so as to make it more descriptive. Also more informational links and help text should be provided which would help in raising the security awareness among the users of the tool.

4 Conclusion

The methodology discussed above in the research is very easy to understand and also it is not time consuming. Help links are provided for every control in the prototype so as to help the user to implement those controls. Future work on this prototype would be to include a feedback system which would assist the user even after the assessment is over by suggesting controls that might still be required to implement to reduce certain threats.

5 References

Alquier, B. and Lagasse, T. (2006). *Risk management in small- and medium-sized enterprises.* Prod. P. & C., 17(3): 273-282

CERT(2008) OCTAVE [WWW] CERT. Available from: http://www.cert.org/octave/ [Accessed 19/01/12].

Dickinson, G. (2001) Enterprises risk management; its origins and conceptual foundation, The Geneva Papers of Risk and Insurance, 26(3), pp. 360-366.

Dimopoulos, V., Furnell, s.m., and Barlow, I.M. (2003).Considering IT Risk Analysis in Small and Medium Enterprises. Proceedings of the 1st Australian Information Security Management Conference 2003 (InfoSec03), Perth, Australia, 24 November 2003

ENISA (2007), *ENISA deliverable: Information Package for SMEs* [WWW]. Available from: http://www.enisa.europa.eu/activities/risk-management [Accessed 29/05/2012].

European Commission (2003), *COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises* [WWW] Accessed from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF [Accessed 12/01/2012].

Henschel, T. (2008), “Risk management practice for SMEs; Evaluation and implementation effective risk management system”, Berlin Erich Schmidt, 2008.

ISBS (2010) *Information Security Breaches Survey 2010, April 2010*. Technical Ed. PricewaterhouseCoopers LLP.

ISBS (2012) *Information Security Breaches Survey 2012, April 2012*. Technical Ed. PricewaterhouseCoopers LLP.

ISO27002 (2012) *ISO/IEC 27002* [WWW]. Available from: http://www.iso.org [Accessed 30/05/2012].

Kelleher, D. (2009) SME security: SME mindset must change [WWW]. Available from : http://www.scmagazineus.com/sme-security-sme-mindset-must-change/article/136052/ [Accessed 11/01/12].

Matthews, C.H., Scott, S.G. (1995) Uncertainty and planning in small and entrepreneurial firms; an empirical assessment. Journal of Small Business Management, 33(4), pp. 34-52.

McKieranan, P., Morris, C. (1999) Strategic planning and financial performance in UK SMEs: Does formality matter. British Journal of Management, 5, pp. 31-41.

NIST SP 800-30(2011) *Guide for Conducting Risk Assessments.* United States: Joint Task Force Transformation Initiative, SP800-30.

Ntlhane, K.E. (1995). *The application of risk management principles to smaller enterprises*. Research report (Masters of Business Administration in the Faculty of Management), University of the Witwatersrand.

Smith, J.A. (1998) Strategies for startups. Long Range Planning, 31(6), pp. 857-872.

Watson, G.E.H. (2004). *A situational analysis of entrepreneurship mentors in South Africa.* Dissertation submitted (Masters of Commerce in Business Management), University of South Africa.

Watt, J. (2007). *Strategic risk management for small businesses*. In: Reuvid, J. (ed.). *Managing Business Risk.* 2nd ed. a practical guide to protecting your business. London – Philadelphia: Kogan Page.

E-Safety in the Mobile Context

A. Legunsen and S. Atkinson

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

Abstract

The research aims to develop practical strategies which can be used to curb dangers and risks associated with children going online through mobile devices. The research identified that stakeholders have a role in ensuring e-safety so a multi-stakeholder practical approach was employed and it entailed using a data survey conducted by Plymouth Safeguarding Children‟s Board. A risk model was also developed for the purpose of implementing practical strategies to minimize online risk. The data from the survey was analysed and the risk model was implemented on the outcome of the survey. The risk model discovered inherent problems in particular situations and the different stages of the risk model are applied to the problem until a positive feedback resolved the problem.

Keywords

Mobile, E-Safety, Risk Model

1 Introduction

The primary essence of technology, of which the internet and mobiles are by-products, is to add positive effects to life. The internet, which can now be accessed from a range of mobile devices including mobile phones, handheld game consoles like the Nintendo DS, Sony‟s PSP, and Apple‟s iPod touch, has become an integral part of modern family living. The use of technologies on mobile platforms has increased tremendously and children are increasingly having their own internet enabled mobile devices. Although these devices present children with opportunities in learning, socialising and entertainment, they also expose them to certain risks. Of note are the likes of cyber bullying, identity theft, access to pornographic images and videos, sexting, exposure to strangers, spam, viruses, abuse of intellectual property and even excessive use (Livingstone et al., 2011).. Internet safety measures are often implemented in schools and homes to guide young people online but managing the implementation of such safety measures within the mobile content has proved to be a daunting task.

This research aims to develop practical strategies which can be used to curb the dangers and risks associated with children going online through mobile devices. The research will investigate the present modalities in place for ensuring e-safety in the mobile context, the shortcomings of such modalities, and finally, a risk model will be designed to aid the implementation of practical strategies that end users can follow in order to minimize the risks.

2 Background

Surveys on e-safety started as early as 1999 when Finkelhor et al. (2008) conducted the first youth internet safety survey (YISS-1) with 1,501 youths within the age range of 10 to 17 years. Of recent, there have been diverse researches on cyber-bullying, online sexual harassment, and exposure to pornographic materials amongst adolescents. Researches have also considered the ways in which the society is making efforts to reduce these online risks, especially through parents and schools.

Major concerns have also risen based on the increase in statistics of mobile device ownership and usage amongst children. 50% of 10 year olds in most EU countries already have a mobile phone while 75% of 6 – 17 year olds are already active online (EC, 2008a; Livingstone et al., 2009). Recent statistic for the EU Kids Online project show that 60% of kids between 9 – 16 years go online daily, spending an average of 88 minutes online per day, and 33% of these kids go online via a mobile phone or other handheld devices (Livingstone et al., 2011). These show the extent of growth in the use of mobile amongst children in recent years and forecasts by Cisco (Cisco, 2011) showing further growth is inevitable necessitates the need for adequate e-safety measures in mobiles.

Mobiles and online technologies present young ones with opportunities for learning, socialising, and entertainment but exposure to risks such as cyberbullying, meeting online contacts offline, giving out personal information, sexual and online harassments, hacking, and mobile malware attacks also accompany these opportunities (Donoso et al., 2009). With these risks comes the need to ensure e-safety.

2.1 Who is to ensure e-safety?

To ensure e-safety, the question of who is responsible for e-safety needs to be clarified. Livingstone et al. (2009) and Byron (2010) agreed that the responsibility of ensuring e-safety lies with the multiple stakeholders involved. This includes the young ones that use the mobile device, the companies that manufacture the devices, mobile network operators and ISPs, security community and web programmers, governments, teachers and also parents.

2.2 Byron Review

The Byron Review (Ofcom, 2007) identifies a similar set of stakeholders and places them in a value chain. Two types of control were identified and implemented along the value chain. These are – controlling the availability and controlling the access to potentially harmful contents. Byron provided an update to these control measures in 2008 (Byron, 2008) by adding children‟s resilience to harmful and inappropriate content online.

3 Adopted Practical Approach

An area of the Byron review was considered in choosing a practical approach to ensuring e-safety in mobiles. Byron mentioned a list of education-based initiatives to help promote e-safety awareness. One of these initiatives is the need to have Local Safeguarding Children Boards (LSCB). Their objective is to "coordinate and to ensure the effectiveness of their member agencies in safeguarding and promoting the welfare of children" (Ofcom, 2007). LSCB are also expected to deploy a multi-agency approach to e-safety. This makes this adopted practical approach robust as the board can provide details about other stakeholders.

The adopted practical approach uses an Early Years Survey carried out by the e-safety group of the Plymouth Safeguarding Children Board (PSCB) in collaboration with Plymouth University. The survey was conducted in April 2010 by Dr Shirley Atkinson from the School of Computing and Mathematics, Plymouth University. The aim of the survey was to gain an accurate picture of the online use of children under the age of 5.

The survey was implemented using questionnaires. This was made available in hard copy during an e-safety training session. The data gathered was analysed using both quantitative and qualitative methods.

4 Risk Model for E-Safety in Mobiles

The primary innovation of this research is the design and development of a risk model for e-safety in mobiles. The research carried out reveals there is presently no risk model designed specifically for the purpose of e-safety in mobile devices. The solutions available are models geared towards e-safety in general such as BECTA"s PIES model (BECTA, 2008) and the 360 degree safe self review tool by SWGfL (SWGfL, 2011).

The main aim of these models is to help develop and review policies and practices regarding online safety for children and young ones. These policies are instructions to guide the users and also to educate the guardians on how to ensure that young ones are safe online. However, the success of policies lies in its adherence. Therefore having policies in place does not necessarily guarantee acceptance and adherence by the users. Also, risks inherent in mobile situations are unique and not easily guarded by general policies but specific practical strategies. The models, therefore, need to be further backed up by practical strategies, and this research aims at achieving this with the implementation of the developed risk model.

The essence of the risk model is to capture a measure of the reality of risks inherent in the mobile context. Figure 1 show the risk model designed towards putting a check in the e-safety process in mobiles. This model takes changes in technologies into consideration as this is a common occurrence in the case of mobiles.

In a bid to develop and design this risk model, the models presented by BECTA and SWGfL were considered as guidelines but streamlined to a mobile-inclined perspective.

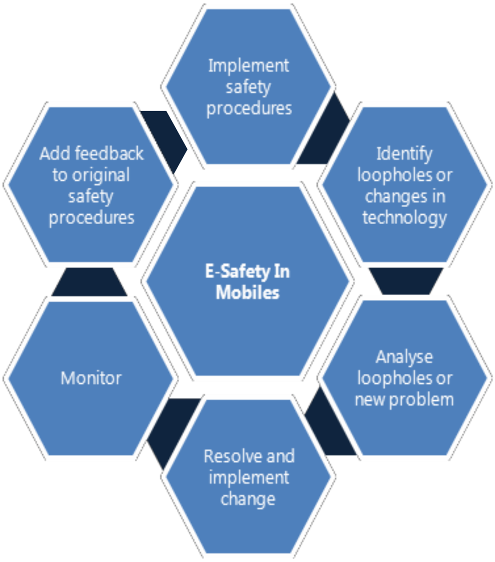

Implement safety procedures
Identify loopholes or changes in technology
Analyse loopholes or new problem
Resolve and implement change
Monitor
Add feedback to original safety procedures
E-Safety In Mobiles

Figure 1: Risk Model for E-Safety in mobiles

The policies and practices advised by these models form a part of the first step in the model. The set of safety procedures that apply to mobiles are highlighted and implemented. This model examines the present effects of the implementation of these safety procedures and proceeds into considering the loopholes that might exist in these procedures. Afterwards, the identified loophole, which could be as a result of change in use patterns or even a new technology, is analysed in depth.

Based on the outcome of the analysis, suggestions are worked out with the aim to achieve a safe procedure once again. This could necessitate an adjustment in the e-safety policy, the need to provide further training, or other measures. The change is then implemented and a period of monitoring is stipulated. During this period, the effect of the change implemented against the identified loophole is observed closely.

The feedback obtained can be treated in two ways. If it is positive, it can be fed directly into the original safety procedure and a more secure e-safety measure is attained. On the contrary, if the feedback obtained is negative, it can be fed back into the „analyse" or „resolve and implement" sections. This is further reviewed, the result is implemented and monitored, and when the feedback becomes positive, it is added to the original safety precautions.

5 Survey Results and Implementation of Risk Model

The result obtained from the Early Years survey is analysed using quantitative and qualitative research methods. An Early Years toolkit developed by the PSCB and the final policy recommendation for EU Kids Online project by Dr Sonia Livingstone and the EU Kids Online network are used as a check on the outcome of the survey"s data analysis. The outcome of the data analysis is discussed as a means for the implementation of the risk model.

5.1 The Early Years Survey

There were a total of 151 respondents to the survey in 106 days between 7 July 2010 and 20 October 2010. The survey required the participants to fill a questionnaire with about 15 questions addressing the use of technologies such as mobile devices and internet in their Early Years settings. The questionnaire also inquired about their practice of online safety, mobile phone usage staff"s ability to use online technologies safely, how secured their ISPs are, and the awareness and adoption of an Acceptable Use Policy.

5.2 Discussion and Implementation of the Risk Model

5.2.1 ISPs

ISPs can play a major role in achieving e-safety in mobiles by blocking illegal contents, filtering services, and providing useful information about online safety to parents and children (Ofcom, 2007). End users need to verify that the services provided by their ISPs are secured, and in this regard, the different means of connectivity should be considered. If the ISPs carry out the responsibility of blocking and filtering adequately, then a secured connection can be provided to end users which in turn promotes e-safety.

The first step of the risk model is to implement safety procedures and considering ISPs, data from the survey shows that most settings have a secured internet connection. 91% confirmed that there ISP is a recognised name and 82% of these mention that their internet connection is also secured. This information suggests that most of the ISPs have implemented suitable safety features in their services. With the first level of the risk model satisfied, this area of e-safety can be judged satisfactory. However, the services by the ISPs need to be monitored still as updates on services or upgrade of equipment could open up new vulnerabilities.

5.2.2 Acceptable Use Policy

The availability and awareness of an Acceptable Use Policy (AUP) is deemed as the minimum level of adoption by the settings towards online safety but the survey revealed only half of the settings have an AUP. The absence of an AUP means there is likely to be no agreed way of handling situations within the setting which could in turn affect other online safety requirements in the setting. This is further proven by the data survey as 51% mention that they have no designated person for online safety. In the same light, the awareness of the AUP by all staff and parent is not satisfactory with just 23% strongly agreeing to the question.

BECTA‟s PIES model and the 360 degree safe models are built on developing policies and practices but having a standard policy does not guarantee its successful implementation. Acceptance and adherence by users is prime. This being a shortcoming of these models is proven by the survey, with 24% stating out rightly that they have no AUP and 20% do not know if one exists in their setting or not.

However, haven identified an unsatisfactory state in the implementation of the Acceptable Use Policy as a safety procedure, and also recognized the loophole as being an absence of the policy or lack of awareness by staff and parents, this loophole is analysed further. The reason for the absence of the AUP or lack of awareness needs to be investigated and corresponding measures taken to resolve the problem. With respect to policy development and implementation, Albrechtsen and Hovden (2010) recommend a workshop approach which involves the parties concerned. Rather than presenting a „finished‟ document and presenting it to the parties to accept and adhere to as the AUP, Albrechtsen and Hovden recommend that the parties adopt dialogue, participation and collective reflection during the policy development. Such approach can be implemented as a measure to resolve the problem. A monitoring period is stipulated to monitor the use of the new AUP and appropriate feedback is carried out on the process. The risk model can also be applied in the same manner to policies that fails to address a situation appropriately.

5.2.3 Mobile Phone Usage

Another area of concern raised by the survey is the management of mobile phone in the Early Years settings. Most of the settings do not permit the use of mobile phones in their settings with 60% stating this clearly. This step is taken by some settings in a bid to ensure safety, but as discussed in the technology use section, taking extreme measures such as completely banning mobile phones to reduce risk can in turn prevent opportunities. Banning technology could have a negative impact on learning. Children are supposed to be educated and trained on the use of technology and not denied its use.

Also, the use of mobile phones has become an integral part of daily living and placing a ban on its use in settings might result into members of the setting trying to get around the rules. This can yet have further impacts on learning in the setting. The implementation of the risk model in this case helps to identify the loophole and implement safety procedures unique with each setting.

5.3 Scenarios of the Risk Model Implementation in Mobiles

The implementation of the e-safety risk model in mobile-specific scenarios shows how the risk model can help to further check inherent risks after the implementation of standard policies. Present day mobile operating systems are now being accompanied with online application stores. Examples include Apple‟s App Store, Google‟s Android Market, BlackBerry‟s App World and Windows 7 Marketplace. Young ones can download resources such as games, music and software from these stores but these exposes them to the risk of downloading malicious applications or their financial information might be stolen and used for fraudulent purposes. Kaspersky (2011) reported the detection of over 50 malicious Android OS applications which were written and distributed through the Android market by cybercriminals. The implementation of the risk model in such situation identified loopholes with the content producers.

Another scenario is the use of social networking sites (SNS) on mobiles by young ones. SNS often carry out upgrades on their sites, bringing in new features which leave the user"s settings to the default state set by the SNS. These changes often happen without prior notification and users, especially young ones, might likely continue to use the SNS"s new features without considering if new risks are associated with such features. Usage on mobile devices sometimes makes these changes unnoticeable. Dangers associated with such changes needs to be examined to prevent young users from being exposed to the associated risks.

6 Conclusion

This research was carried out with the aim of developing practical strategies which can be used to curb the dangers and risks associated with children going online through mobile devices.

Analysis of the data gathered was criticized with the Early Years toolkit and the final recommendation policy, and the results were discussed and used to evaluate the designed risk model. Results showed that even though the Early Years settings that participated in the survey were aware of the policies and practices available in the Early Years toolkit to help ensure online safety in their settings, they still did not adhere to some of the prescribed practices.

Rather than a policy which is developed after carefully considerations of, supposedly, all possible scenarios, the developed risk model addresses the situation in accordance with its present context. Policies provide instruction and guidelines to help in the decision-making process of problem solving. The e-safety risk model, however, helps to check inherent risks in mobile situation after the implementation of the policies. As shown from the scenario, policies can guide young ones in the general usage of social networking sites for example, but addition of new features which is not covered by the present policy in place can introduce new vulnerabilities and risk. The e-safety risk model can be used to analyse such situations and implement new safety procedures within a short period rather than the daunting task of reviewing the policy.

6.1 Future Work

This research gives room for further evaluation and implementation of the risk model. Effort can be made to implement the risk model in a setting or institution working towards improving the state of e-safety in mobiles. Another area of further research is the opportunity to carry out surveys with other stakeholders, using the data collated to examine the implementation of the risk model.

7 References

Albrechtsen, E. and Hovden, J. (2010) „Improving information security awareness and behaviour through dialogue, participation and collective reflection - An intervention study‟, Computers & Security, 29(4), pp. 432-445. [online] doi:10.1016/j.cose.2009.12.005 [Accessed 10 December 2011].

BECTA (2008) Safeguarding children in a digital world: developing an LSCB e-safety strategy. Available at: https://www.education.gov.uk/publications/standard/_arc_SOP/ Page11/BEC1-15535 [Accessed 28 December 2011].

Byron, T. (2010) Do we have safer children in a digital world? A review of progress since the2008 Byron Review. Available at: http://www.education.gov.uk/ukccis/about/a0076277/ the- byron-reviews [Accessed 26 December 2011].

Byron, T. (2008) *Executive summary of the 2008 Byron review*. Available at: http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews [Accessed 26 December 2011].

Cisco (2011) Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010–2015. Available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ ns537/ns705/ns827/white_pape r_c11-520862.html [Accessed 22 April 2011].

EC (European commission) (2008a) Towards a safer use of the internet for children in the EU – a parent‟s perspective, Analytic Report. [online] Available at: http://ec.europa.eu/ information_society/activities/sip/docs/eurobarometer/analyticalreport_2008.pdf [Accessed 6 June 2011].

Finkelhor, D., Mitchell, K.J., and Wolak, J. (2008) *First Youth Internet Safety Survey (YISS-1),* National Data Archive on Child Abuse and Neglect, Cornell University, Ithaca, New York.[online] Available at:http://www.ndacan.cornell.edu/NDACAN/ Datasets/UserGuidePDFs/134user.pdf [Accessed 3June 2011].

Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011) *Final Report, LSE, London: EU Kids Online*. [online] Available at: http://www2.lse.ac.uk/media@lse/ research/EUKidsOnline/Home.aspx [Accessed 30 September 2011].

Livingstone, S., and Haddon, L. (2009) „Introduction‟ In: Livingstone, S. et al. (ed.), *Kids Online: Opportunities and risks for children*. Policy Press, Bristol: pp. 1-15.

Ofcom (2007) *Annex 2: Current tools and approaches to protecting children from harmful content online.* Available at: http://stakeholders.ofcom.org.uk/market-data-research/telecoms-research/byron/ [Accessed 23 December 2011].

SWGfL (2011) 360^{o} Safe: *The self-review tool, South West Grid for Learning.* Available at: http://www.360safe.org.uk/ [Accessed 17 October 2011].

Web-Based Risk Analysis for Home Users

R.T. Magaya and N.L. Clarke

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

Abstract

The advancement of the Internet has seen more home users becoming connected to superfast broadband. It has also provided access to a wide variety of online services such as banking, e-commerce, social networking and entertainment. The wide availability and popularity of the Internet has also led to the rise in risks and threats to users, as criminals have taken an increasingly active role in abusing innocent users, giving rise to attacks such as unauthorised access, malware attacks, denial of service attacks and identity theft.

Current risk analysis tools, techniques and methods available do not fully cater for home users but are tailored for large organisations. The tools require expertise to use them, expensive to purchase or simply provide general awareness information. As such a tool is required that can bridge the gap between bespoke risk assessment approaches that provide bespoke information and broad-spectrum approaches that simply provide all information regardless of its relevance.

The paper proposes a web-based risk analysis tool for home users that is based on well-accepted standards (such as the ISO 27002, NIST SP800 and SANS 20 Critical Security Controls guidelines). The tool assists the user in performing risk analysis in an extremely user-friendly fashion and not requiring any prior knowledge and provides tailored information indicating any controls missing, with guidance also on how to implement the recommended tools. In addition the tool will also educate the user by providing information about safe user behaviour. A prototype was developed and evaluated by a sample of home users. 93% of the participants found the tool to be easy to use helpful and very informative.

Keywords

Risk Analysis, Risk Assessment, ISO 27002:2005, NIST SP 800-30, SANS 20 Critical Security Controls, Home User, Information Security Awareness.

1 Introduction

According to the latest Ofcom report 80% (eight in ten) UK households now have access to broadband internet (Ofcom, 2012). As home users are now always connected to fast broadband internet, they have come to depend on the internet for their daily activities with at least 73 % adults in the UK spending approximately 8.3 hours per week the internet (Ofcom, 2011).

This increased dependence however exposes users to numerous risks and threats (Furnel *et al.*, 2007). A computer connected to the internet without protection maybe infected with malicious software in under a minute (Postnote, 2006). Most threats now operate without the user's knowledge, stealing personal details or using a user's computer for malicious purposes (GSO, 2010).

Several threats exist in different forms; these include but are not limited to malware, spyware, Trojans etc. These threats result in attacks such as denial of service attacks; fraud; identity, data and service theft, unauthorised access, destruction of data and systems. In UK, 1 in 5 users have been victims of phishing scams, while 40% have experienced virus attacks, and 19% have been victims of online identity theft (GSO, 2010).

There is a need for a risk analysis tool designed for home users which will provide guidance and support with the aim of identifying missing controls and assisting the user on how to implement recommended controls to reduce risks. The tool should do this in a simple, user-friendly and non-technical manner.

This paper will look at the development of a web-based risk analysis tool for home users. The next section will provide a background about risk and risk assessment. Current tools, standards and techniques available will be discussed. Section 3 describes the web-based risk analysis tool methodology. The design and appearance of the tool will be discussed section 4. Section 5 will discuss the evaluation of the tool by users. Conclusions and recommendations will be in section 6.

2 Background

2.1 Risk and Risk assessment

Risk is the likelihood of a given threat exploiting a particular vulnerability. It is a combination of threats and vulnerabilities that may have adverse impact if they occur (HIPAA, 2010). Risk can lead to a compromise in confidentiality, integrity and availability of systems and or data (Elky, 2006). Risk assessment identifies, quantifies and prioritises risks using a risk acceptance criterion. Risk assessment helps set priorities for managing risks and implementing controls to mitigate identified risks (ISO 27002). It helps focus security activities on important assets.

The tool developed in this research will use qualitative risk assessment methodology for assessing risks which involves determining the probability of an outcome using an interval scale which is represented by non-numerical labels such as High, Medium and Low. The risk rating will be based the SANS 20 Critical Security Controls, a well-recognised industry standard for control prioritisation. The tool will not use complex calculation to assess risk as the same can be achieved qualitatively with simplicity.

The web-based risk analysis tool will use a questionnaire to gather information about the assets the user has and the currently controls in place. The answers to the questionnaire will determine the user's level of risk and the tool will recommend any missing controls to reduce the risk; also providing assistance to the user in selecting and implementing the controls.

2.2 Awareness

A significant number of users are still unaware of their exposure to security risks (ENISA, 2009). Lack of awareness makes users vulnerable to online threats. Awareness involves educating the user with the aim of focusing the user's attention on security by changing user behaviour and pattern (ENISA, 2010; NIST SP 800-16). Awareness is a pre-requisite for adequate protection (Spears and Barki, 2010). The effectiveness of any security measures hugely depends on users' awareness of risks and countermeasures.

Websites like Get Safe Online, Microsoft Security Centre provide awareness and security guidance information to help users stay safe online. They are however not well structured making it difficult for the user to search for and find specific information. They assume a certain level of computer security knowledge and do not provide adequate information or assistance about selecting and implementing controls.

2.3 Current state risk assessment standards and techniques

There are several tools and standards available to help identify and manage risks. They however have a number of weaknesses. The available tools such as CRAMM, OCTAVE and COBIT require expertise and are tailored for large organisations. Standards such as the ISO 27002 and NIST SP 800 act as guidelines for reference; they do not provide information on how to implement controls. Most of the processes outlined in the standards are not applicable home users. They also require a certain level of expertise making them less suitable for home users.

As Home users lack expertise and awareness, there is need for a tool that performs risk analysis for the user and provides relevant recommendations that are tailored to their assets whilst also educating them. The tool will address the weaknesses of existing websites, tools and standards

3 WEBRA tool

The web-based risk analysis (WEBRA) tool framework used the ISO 27002, NIST SP 800 – 30 standards base guidelines to identify assets and formulate questions. This was to ensure all important security areas outlined by industry accepted standards are covered.

The tool will consist of a two-part questionnaire which is tailored for a home user environment. Help will be provided throughout the tool in the form of mouse overs, links and pop up description boxes to provide guidance to the user. There will also be a full glossary page with explanations of risk and security terms. The tool unlike existing tools will cater for all home users without requiring any prior knowledge of security. The tool will have three main processes:

- **Asset selection**: the user selects assets they have, data stored on the assets, services used and controls currently implemented.
- **Control ranking**: the system analyses the missing controls and determines risk level based on a control priority ranking system.
- **Output/Recommendations**: The tool will provide an overall risk rating for each asset and will recommend missing controls that are required to mitigate the risks. Additional guidance will be provided through a description of each control and links provided to direct the user where they can get the controls or guidance on how to implement them.
- **Behavioural practice**: the user answers a series of questions regarding their use of systems. The WEBRA tool will recommend safe practice behaviour to the user such as regular updates, scanning removable media, changing passwords etc. In addition the tool will educate the user providing explanations and links to other useful websites. The information on the recommendations page is presented in a simple and comprehensive manner.

The web-based risk analysis tool will be made up of a two part questionnaire divided into section 1 (assets and controls) and section 2 (user behaviour).

3.1 Assets and countermeasures

This section forms the core part of the risk analysis tool. The questions will enable the tool to assess the user's risk level and recommend appropriate controls. Section 1 questions will help identify the user's exposure to risks based on the missing controls.

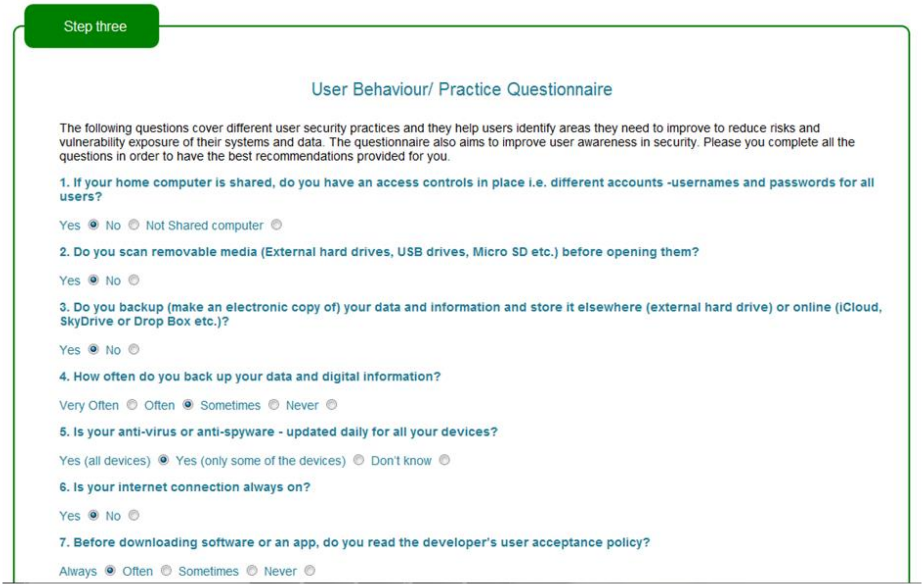
The tool begins by building an asset profile for the user by identifying the assets they have. The tool will also ask the user to provide key information about the assets such data stored on the assets, internet services used. The user will also be asked to indicate the current security controls they have in place. The system ranks all controls according to priority based on the SANS 20 Critical Security Control List (SANS, 2011); any controls missing will be highlighted as recommendations and links to relevant websites provided.

All questions in section 1 are in tabular form. This was done to simplify the user input process and for a good interface that makes navigation easier and quicker for the user.

3.2 User behaviour

The second part of the web-based risk analysis questionnaire aims to inform and educate the user about staying secure. The questionnaire evaluates user behaviour and awareness. The questions are in multiple choice form and assess existing security practices in a number of areas outlined in both the ISO 27002 and NIST SP 800 – 30 standards.

The 18 questions cover user behaviour in the home environment; for example how regularly a user updates their security software, change passwords, perform backups etc. Several other topics are covered including security policy, authentication, encryption and privacy. See Figure 1 below for sample questionnaire.



User Behaviour/ Practice Questionnaire

The following questions cover different user security practices and they help users identify areas they need to improve to reduce risks and vulnerability exposure of their systems and data. The questionnaire also aims to improve user awareness in security. Please you complete all the questions in order to have the best recommendations provided for you.

1. If your home computer is shared, do you have an access controls in place i.e. different accounts -usernames and passwords for all users?

Yes ● No ○ Not Shared computer ○

2. Do you scan removable media (External hard drives, USB drives, Micro SD etc.) before opening them?

Yes ● No ○

3. Do you backup (make an electronic copy of) your data and information and store it elsewhere (external hard drive) or online (iCloud, SkyDrive or Drop Box etc.)?

Yes ● No ○

4. How often do you back up your data and digital information?

Very Often ○ Often ● Sometimes ○ Never ○

5. Is your anti-virus or anti-spyware - updated daily for all your devices?

Yes (all devices) ● Yes (only some of the devices) ○ Don't know ○

6. Is your internet connection always on?

Yes ● No ○

7. Before downloading software or an app, do you read the developer's user acceptance policy?

Always ● Often ○ Sometimes ○ Never ○

Figure 1: Behavioural Questionnaire.

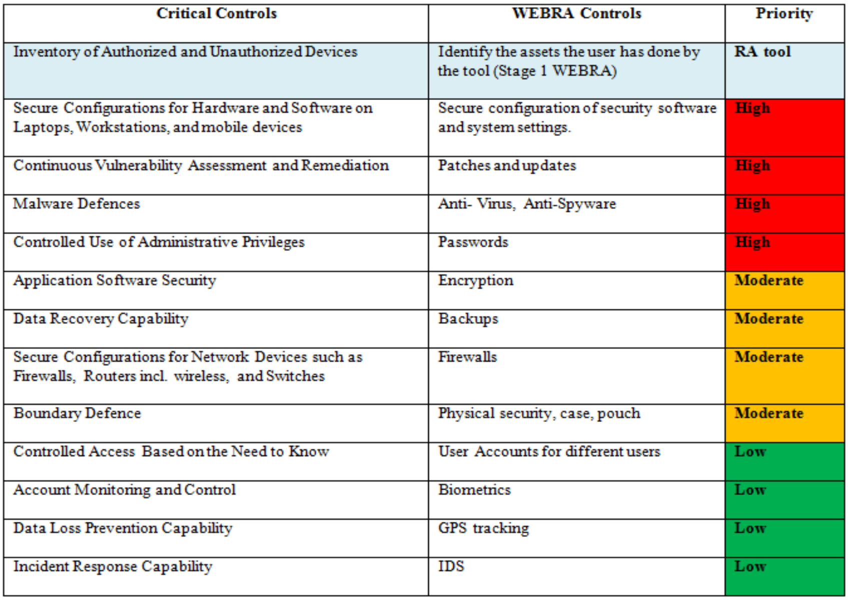
Once the user has completed all the questions in this section the tool will give recommendations for best practices. Links are provided to websites that offer best practice guidelines which will address any insecure user behaviour.

3.3 Determining the risk level

The web-based risk analysis tool uses a modified control prioritisation list tailored for home users (shown in Figure 2). All controls listed apply to home users. The 20 Critical Security Controls takes into consideration the latest threats and vulnerabilities.

The process allows controls in place to be mapped to the assets and indicate areas where controls need to be implemented. The tool will rank each control in order to give a view of relative importance (IRM, 2002). The controls are ranked according to their importance in keeping assets secure.

The WEBRA will use a simple rating scale of High, Medium and Low to represent the degree of risk. The rating will be based on the prioritisation of controls in terms of their effectiveness and potential impact in reducing common threats and vulnerabilities. This will help user prioritise resources and efforts on critical areas in order to prevent attacks and intrusions. It will also help ensure that systems have the most critical baseline controls in place.



Critical Controls	WEBRA Controls	Priority
Inventory of Authorized and Unauthorized Devices	Identify the assets the user has done by the tool (Stage 1 WEBRA)	RA tool
Secure Configurations for Hardware and Software on Laptops, Workstations, and mobile devices	Secure configuration of security software and system settings.	High
Continuous Vulnerability Assessment and Remediation	Patches and updates	High
Malware Defences	Anti- Virus, Anti-Spyware	High
Controlled Use of Administrative Privileges	Passwords	High
Application Software Security	Encryption	Moderate
Data Recovery Capability	Backups	Moderate
Secure Configurations for Network Devices such as Firewalls, Routers incl. wireless, and Switches	Firewalls	Moderate
Boundary Defence	Physical security, case, pouch	Moderate
Controlled Access Based on the Need to Know	User Accounts for different users	Low
Account Monitoring and Control	Biometrics	Low
Data Loss Prevention Capability	GPS tracking	Low
Incident Response Capability	IDS	Low

Figure 2: Asset Priority List. (Adapted from SANS, 2011).

The reason for using this methodology was to eliminate the subjectivity inherent in qualitative analysis methods while ensuring the score reflects the importance of controls based on statistics (such as the SANS 20 Critical Security Controls) that reflect vulnerabilities and threats affecting users today. The result of the risk assessment questionnaire will lead to recommendations tailored to the user's assets. An overall risk rating for each, missing controls and their priority ranking will be displayed on the recommendations page.

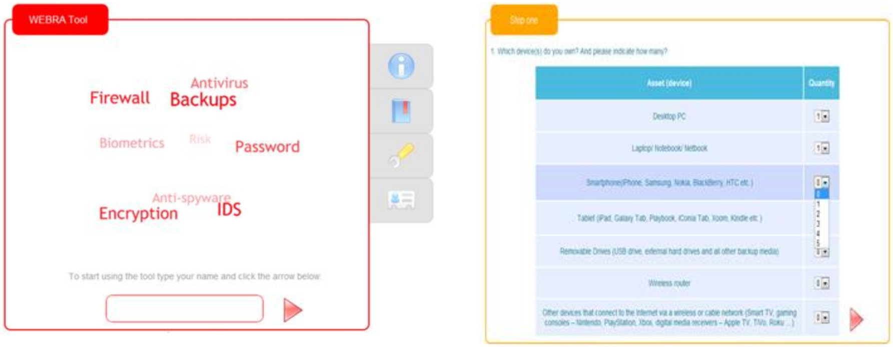
3.4 Overall risk rating

The tool will give the overall risk rating as High (Red), Medium (Amber) and Low (Green). If one of the missing controls has a High priority ranking in the controls list then the overall risk is High. The same is true for Medium risk rating, if one of the controls missing has a Medium priority then the overall risk rating for the asset is Medium. If all missing controls are Low priority, then the overall risk rating will be Low. For example, if patches and updates (ranked High priority) are not installed the system can be easily compromised even if all other controls are in place. Patches and updates cover vulnerabilities and loopholes attackers can use to compromise the system.

4 WEBRA Design

The web-based risk analysis tool prototype was developed to demonstrate functionality, usability and the suitability of the tool to home users. The tool consists of a front-end website for the user interface, and a back-end database that stores all the input data, asset lists, countermeasures and priorities.

4.1 The interface

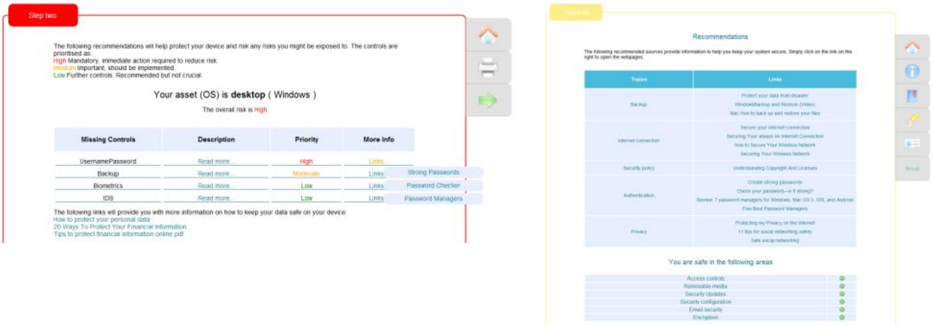


To start using the tool type your name and click the arrow below

1. Which device(s) do you own? And please indicate how many?

Asset (device)	Quantity
Desktop PC	1
Laptop/ Notebook/ Netbook	1
Smartphone(iPhone, Samsung, Nokia, BlackBerry, HTC etc.)	0
Tablet (iPad, Galaxy Tab, Playbook, iConia Tab, Xoom, Kindle etc.)	
Removable Drives (USB drive, external hard drives and all other backup media)	0
Wireless router	0
Other devices that connect to the Internet via a wireless or cable network (Smart TV, gaming consoles – Nintendo, PlayStation, Xbox, digital media receivers – Apple TV, TiVo, Roku ...)	0

Figure 2 & 3: Main Page and Assets questions



The following recommendations will help protect your device and risk any risks you might be exposed to. The controls are prioritised as:
High Mandatory, immediate action required to reduce risk.
Medium Important, should be implemented.
Low Further controls. Recommended but not crucial.

Your asset (OS) is **desktop** (Windows)

The overall risk is High

Missing Controls	Description	Priority	More Info
UsernamePassword	Read more...	High	Links
Backup	Read more...	Moderate	Links
Biometrics	Read more...	Low	Links
IDS	Read more...	Low	Links

Strong Passwords
Password Checker
Password Managers

The following links will provide you with more information on how to keep your data safe on your device:
How to protect your personal data
20 Ways To Protect Your Financial Information
Tips to protect financial information online pdf

Recommendations

The following recommended sources provide information to help you keep your system secure. Simply click on the link on the right to open the webpages.

Topics	Links
Backup	Protect your data from disaster WindowsBackup and Restore (Video) Mac: How to back up and restore your files
Internet connection	Secure your internet connection Securing Your always on Internet Connection How to Secure Your Wireless Network Securing Your Wireless Network
Security policy	Understanding Copyright And Licenses
Authentication	Create strong passwords Check your password—is it strong? Review: 7 password managers for Windows, Mac OS X, iOS, and Android Five Best Password Managers
Privacy	Protecting my Privacy on the Internet 11 tips for social networking safety Safe social networking

You are safe in the following areas

Access controls	●
Removable media	●
Security Updates	●
Security configuration	●
Email security	●
Encryption	●

Figure 4 & 5: Recommendations for Assets and User behaviour

Usability helps users use the tool, completing the process quickly and easily. The interface determines whether the user can quickly learn to use the tool. Functionalities like navigation through menus, colours for different risk levels and priorities, mouse over and hovering makes the tool more usable and easy to follow. Figure 2 to 5 above illustrate the tool's interface.

5 Evaluation

The prototype was evaluated to test its suitability for home users and to see if it addressed the problems of existing tools. Two types of evaluations were undertaken.

The first one involved evaluation by sample of 50 home users. The aim was to gather users' perceptions, attitudes and opinions about the tool. The second evaluation involved a focus group of information security professionals. The group tested the WEBRA tool alongside a number of existing tools such as Secunia PSI, Get Safe Online, and Microsoft Baseline Security Analyser (MBSA). The usability of the tool, help provided, recommendations and links to other information were some of the criterion used to evaluate these tools.

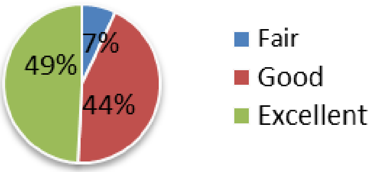


Figure 6: Usability of the tool (Ease of use)

Feedback from the users indicated that most (93%) users found the tool very easy to use and the interface was user friendly (as shown in figure 6 above).

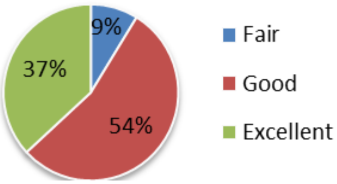


Figure 7: Provided implementation assistance

The majority of users (91%) felt the tool had provided adequate assistance and links to help them select and implement recommended controls. Users also found the recommendations to be helpful because they were tailored to their needs.

Overall the users liked the friendly user interface which made the tool easy to follow and use. Users found the questions easy to understand and the tool improved their security awareness. The tool risk analysis process took reasonable time to complete. Issues pointed out by the users included the need for more detailed explanation for terms like Intrusion detection systems and digital certificates which most users are not aware of.

Focus group feedback was the tool was comprehensive covering all aspects from risk assessment, control recommendation and implementation guidance to educating the user; unlike other tools which only covered a few areas like awareness and patches. The group also noted that WEBRA supported different devices and platforms; and had a simple and which provided a comprehensive report specific to the user’s assets.

Overall the group concluded that the WEBRA tool was *“excellent and offered tailored recommendations to the user.”* Tool was also easy to use for users with little experience, taking reasonable time to complete and very educational making it more suitable for home users than other tools. Areas the group felt could be improved include adding more controls and automatic detection of some controls like firewall.

6 Conclusion and Future work

This research looked at risk analysis and how it affects home users. This paper proposes a tool which is designed based on industry wide standards such as ISO 27002 and NIST SP 800. A web-based risk analysis tool was designed and developed to help users analyse and assess their security requirements; providing information in a simple manner to the user about how to solve identified security problems. In addition the tool also educated the user about risks and security.

The tool identifies missing controls and recommends them to the user together with educational information about safe practices. It also improves user behaviour by proving links to safe practices. The tool was evaluated by users who found it very easy to use, helpful and informative.

The prototype needs to be improved to include more controls and should be regularly updated to reflect latest threats, vulnerabilities and countermeasures. Detailed explanation of controls and auto detection of controls are other improvements to make the tool better.

7 References

Elky, S (2006). *An Introduction to Information System Risk Management*. SANS Institute. InfoSec Reading Room.

ENISA (2009). *Awareness Raising. European Network and Information Security Agency.* Available at: http://www.enisa.europa.eu/media/key-documents/fact-sheets/Awareness-1.pdf [Accessed: 25 August, 2012].

ENISA. (2010). *The new users' guide: How to raise information security awareness.* Available at: http://www.enisa.europa.eu/ [Accessed: 25 August, 2012].

Furnell, S. M., Bryant, P. & Phippen, A. D. (2007). *Assessing the security perceptions of personal Internet users.* Computers &amp; Security, 26 (5). pp 410-417.

GSO. (2010). *UK Internet Security: State of the Nation. The Get Safe Online Report.* November. Available at: http://www.getsafeonline.org/media/ Get_Safe_Online_Report_2010.pdf [Accessed: 26 25 August, 2012].

HIPAA. (2007). *Basics of Risk Analysis and Risk Management.* HIPAA Security Series. Volume 2: 6/2005: rev. 3/2007

IRM (2002). *A Risk Management Standard.* The Institute of Risk Management (irm). Available at: http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf [Accessed: 18 August, 2012].

IS0 27002. (2005). *Information technology. Code of practice for information security management.* British Standards Institution. BS ISO/IEC 27002:2005. ISBN 0 580 46262 5.

NIST SP 800 – 30. *National Institute of Standards and Technology (NIST) Special Publication 800-30. Risk Management Guide for Information Technology Systems.* Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [Accessed: 03 January, 2012].

NIST SP 800-16. *Information technology security training requirements: A role- and performance-based model.* Available at: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf [Accessed: 25 August, 2012].

Ofcom. (2011). *Communications Market Report: UK*. Available at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/UK_CMR_2011_FINAL.pdf [Accessed: 03 December, 2011].

Ofcom. (2012). *Communications Market Report: UK*. Available at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf [Accessed: 25 August, 2012].

Postnote. (2006). *Computer Crime.* The Parliamentary Office of Science and Technology Available at: http://www.parliament.uk/documents/post/postpn271.pdf [Accessed: 12 July, 2012]

SANS (2011). *20 Critical Security Controls - Version 3.1*. Available at: http://www.sans.org/critical-security-controls/guidelines.php [Accessed: 25 July, 2012].

Spears, J. L. and Barki, H. (2010). *User Participation and Information Systems Security Risk Management.* MIS Quarterly. Vol. 34 No. 3, pp. 503-522/ September.

Education in the 'Virtual' Community: Can beating Malware Man Teach Users about Social Networking Security?

A. Sercombe and M. Papadaki

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

Abstract

Social Networks have become part of daily life for millions of people and by their very nature they encourage information sharing, which poses a significant security challenge. 2011 has seen numerous targeted "Spear Phishing" attacks in which the attackers have gained knowledge about victims before carrying out the attack. Social media has been utilised as the source for this information so therefore it is even more important that users are educated against the risks (Symantec, 2011).

This paper looks the current threats and awareness strategies. It describes the design and evaluation of an online game to help educate users. The game has a central 'Malware Man' character and a firewall which burns him if the player answers correctly. The success of the game was then evaluated using an experiment with a group of participants who had played the game, and a control group who had not. 101 users participated in the study. The results showed that the game was successful in educating users, as the average percentage of correct answers was 77% for those who had played the game, compared to 55% for those who had not.

Keywords

Social Networking, Social Networks, Phishing, Spear Phishing, Education, Awareness, Game, Interactive

1 Introduction

Social Networks are defined as 'networks of social interactions and personal relationships' (Oxford Dictionary, 2011). They are used to build online communities of people who share interests with one another (Shin, 2010). Facebook alone, reports that it has over 800 million active users, of which more than 50% logon every day (Facebook, 2012). This makes social network sites a very lucrative target for attackers. There is a large amount of data to mine and a plentiful supply of users that can be targeted.

These threats not only affect individuals, but also pose a risk to organisations and even governments and infrastructure. 2011 has seen a decrease in the amount of spam detected, but an increase in targeted attacks (Symantec, 2011). It is suggested that attackers may be moving away from spam and choosing to use social networks to mine information so they can perform more targeted attacks.

In the last week a security company called Stratfor has been hacked and has released an announcement on Facebook stating that they have evidence that users or employees who have posted messages of support on the social networking site are being specifically targeted (BBC, 2011). This is further evidence that information on social media sites is being used by hackers as a standard information gathering tool, and can also be used to target individuals.

2 Social Networking Threats

Before you can start to design a game to educate users you need to understand the threats. The following is a list of the main threats against social networks.

2.1 Spam

Spam can be defined as 'unsolicited messages propagated through a medium' (Hogben, 2007 p11). It is one of the oldest, simplest and most common attacks and it is very quick to adapt to new technologies. Social networks are usually free to use and free to send messages, which mean that they are an ideal candidate for spammers.

2.2 Social Engineering

One of the ways that social networks have been targeted is by the use of social engineering attacks. These attacks often take advantage of the fact that there is pressure on social networking users to have the most ‘friends’ or ‘followers’ (Symantec, 2010, p3). Phishing is a common type of social engineering attack and is used against social networks. In a study by Jagatic, Johnson, Jakobson and Menczer (2007), they used freely accessible social networking information to create crafted emails that appeared to be from friends of the victim, and they found that the targets were much more likely to give away information to a friend than to a stranger.

2.3 Trojans/Malware

The W32 Koobface worm was one of the first large scale malware attacks targeting social networks and is said to still be active today. It is very successful and relies on social networking users link opening behaviours. (Symantec, 2010, p3).

2.4 Applications

Some social networks allow active content to be embedded in pages. Examples of applications include daily horoscopes and quizzes. Some social networks allow remote code to be included, but most larger networks use APIs to restrict the access that these applications have.

2.5 Content threats

There are various content threats that have been used against social networking users. Some of the most serious include utilising vulnerabilities in the underlying software to embed malicious content inside profiles. One of the easiest ways to perform an attack is to use malicious links. URL shortening makes it hard for even savvy users to check if a request is genuine.

2.6 Privacy

Privacy is a serious concern for social networking users. It is important that the user has control and can easily restrict information. Once a message is posted, it is almost impossible to delete it because of the nature of internet caching. Information disclosure such as location data and private information is also a concern. (West 2010, p26).

3 Awareness Strategies

There are a number of different strategies used to raise awareness about security threats, and there has been considerable research in this area. The U.K. government, law enforcement and a number large organisations sponsor a Get Safe Online initiative (www.getsafeonline.org) (Furnell, Bryant & Phippen, 2007). The web site offers videos, guides, reports and help for users and small businesses to raise their security awareness.

Globally there are numerous initiatives, for example the European Network and Information Security Agency (ENISA) have an awareness raising program which consists of workshops, conferences, literature.

4 Malware Man Design

A number of requirements were collated as a result of learning and education research and literature review. The key requirements are listed below:

4.1 Non-functional Requirements

- Captivate player attention (Dondlinger, 2007)
- The game design must promote and foster learning (Dondlinger, 2007)
- Use design elements from video games to encourage game play (Dondlinger, 2007)
- Narrative context is key to making the game engaging and fun (Sheng et al., 2007)
- A strong character and story will help motivate players. (Sheng et al., 2007)
- An emphasis on skill as there must be a challenge to prevent players getting bored

- Stimulate desired learning outcomes using goals and rewards (Dondlinger, 2007)

4.2 Functional Requirements

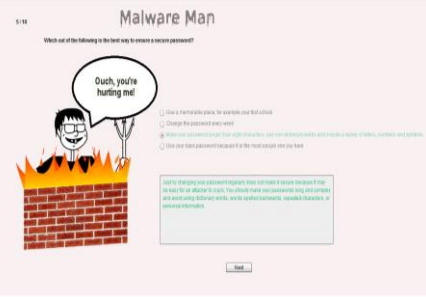
- The game should be dynamic and easily configurable for different types of Social Networks. The game will be more relevant to users if it can be customized.
- Platform independence. It is important that the game is available to as wide a group of users as possible.

4.3 Design

The game was developed using Adobe Flash Builder 4.5 using the flex development language which builds a .swf file. This ensures that the game will run on any browser as long as it has Flash Player 10 or above installed.

There are three game states; 'Start', 'InGame' and 'End'. If the user answers correctly, a flickering animated firewall increases in size and a speech bubble appears giving the impression that Malware Man is being hurt.

Help information appears providing the user more information about the question and the correct answer after they have submitted their answer. If the user answers correctly then the text will be coloured green.



5/10

Malware Man

Which out of the following is the best way to ensure a secure password?

○ Use a memorable place, for example your first school
○ Change the password every week
● Make your password longer than eight characters, use non dictionary words and include a variety of letters, numbers and symbols
○ Use your bank password because it is the most secure one you have

Just by changing your password regularly does not make it secure because it may be easy for an attacker to crack. You should make your passwords long and complex and avoid using dictionary words, words spelled backwards, repeated characters, or personal information.

If the user answers incorrectly then the firewall stays the same size, and the wrong answer and hint text are coloured red. The right answer is coloured green, so that the user can immediately see where they went wrong.

The design of the questions in the game was centred around the main threats outlined earlier in this paper. The questions were all multiple choice based with four possible answers. Some questions used images from social networks, for example a wall posting from a Facebook feed to make the question more relevant to the user. Three sets of ten questions were created for three different versions of the game.

5 Evaluation Design

The game needed to be evaluated to assess how successful it was in educating users. This assessment was done by carrying out a user study. The study consisted of one group of users who had played the game, and a control group who had not. Both groups were given the same survey to complete and the hypothesis was that the users that had played the game would answer more questions correctly.

There was also an informal feedback field in the survey for participants to give some qualitative feedback on the game.

The two sample groups included Plymouth University Masters and Undergraduate students and Met Office employees in the Technology and Information services department. All participants were over 18 years old and the study did not include vulnerable adults. An invitation email and a consent page outlined the aims of the research, contact details, a clear description of the right to withdraw at anytime and a reinforcement that participation if voluntary.

6 Results

104 participants took part in the study, of which three results had to be discarded due to the fact that all the answers were blank. The overall percentages are 32% female, 65% male and 3% undisclosed. 51% of participants were aged between 26-35 and 32% were between 36-45. The other 17% were either 18-25, 46-55 or 56-65.

The results indicated that the percentage of correct answers for those users who played the game was 77% as opposed to 55% for those who did not. These results relate to the first 8 questions in the survey as these were the same for all users. The other questions were Facebook or Twitter specific and only appeared if users played those specific versions of the game but also gave very similar results.

It was also found that users did not do as well on the number based statics questions compared to those that were more descriptive. This is interesting as it suggests that the participants may learn better when the question answers are more descriptive in nature.

The informal feedback on the game showed that participants found the game to be generally good and informative, but there were some concerns over the clarity of the colours for users who may suffer from colour blindness. One participant suggested that a leader board may have added to the experience so they could see how they performed compared to other users.

7 Conclusions and Future Work

This paper has given an overview of the current social networking threats and awareness campaigns and has then presented the design and evaluation of the Malware Game.

The results suggest that the game was successful in educating users as there was a large difference between the number of correct answers for those that had played the game compared to those who had not. The sample size was not sufficient to be conclusive and the participants belonged to quite a specific demographic.

Future research could include looking at different cultures and demographics of users, as well as using a larger sample size. It could also include extensions to the game for different levels and could give forms of reward to see if this improves the user experience.

Trialing the game against other forms of online educational material and carrying out a study to determine how well the game performed comparatively would give a better understanding of how effective the game is in educating users in comparison to other techniques.

8 References

BBC, 27/11/2011, 'Anonymous' hack victims face repeat attacks, BBC. Available from: <http://www.bbc.co.uk/news/technology-16338680>. [27/12/2011].

Dondlinger, MJ 2007, 'Educational video game design: A review of the literature', Journal of Applied Educational Technology, vol. 4, no. 1, pp. 21-31.

Facebook, Statistics - Facebook, Facebook. Available from: <https://www.facebook.com/press/info.php?statistics>. [05/01/2011].

Furnell, SM, Bryant, P & Phippen, AD 2007, 'Assessing the security perceptions of personal Internet users', Computers &amp; Security, vol. 26, no. 5, pp. 410-417.

Hogben, G 2007, 'Security issues and recommendations for online social networks', Position Paper ENISA European Network and Information Security Agency, vol. 80211, no. 1.

Jagatic, TN, Johnson, NA, Jakobsson, M & Menczer, F 2007, 'Social phishing', Communications of the ACM, vol. 50, no. 10, pp. 94-100.

OxfordDictionary 2011, Oxford Dictionaries - Definition of Social Network in Oxford Dictionaries, Oxford University Press, [01/06/2011].

Sheng, S, Magnien, B, Kumaraguru, P, Acquisti, A, Cranor, LF, Hong, J & Nunge, E 2007, 'Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish', in, ACM, pp. 88-99.

Shin, D-H 2010, 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption', Interacting with Computers, vol. 22, no. 5, pp. 428-438.

Symantec, CW- 2010, 'The Risks of Social Networking', Symantec - Security Response[12/05/2011].

Symantec, PW- 2011, Symantec Intelligence Report: November 2011, Symantec, [20/12/2011].

Section 3

Network Systems Engineering

Performance Analysis of Video Calls Using Skype

A. Asiri and L. Sun

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

Abstract

The widespread use of the Internet has had a significant impact on the world of communication, leading to the development of new technologies. One of these new technologies, VoIP (voice/video-over-Internet protocol), has revolutionised contemporary communication. Skype is undoubtedly the most well-known VoIP application in the current spectrum. Its features, capabilities and successes have attracted the research community and telecommunication companies, which have become interested in illustrating Skype's performance, characteristics, quality and end user experience. This paper focuses on investigating Skype's responsiveness mechanism toward bandwidth variation. Skype's sending bit rate and packet size when experiencing different levels of packet loss will be studied as well. In addition, we focus on how Skype shares its available bandwidth with other cross-traffic such as TCP traffic. Moreover, we measure end user quality of experience (QoE) under different packet loss conditions. This paper offers a number of key findings, including the fact that Skype responsiveness to bandwidth variation very dependent on the speed motion of the video calls. In addition, Skype is robust regarding minor packet loss. We also found that Skype is indeed TCP-friendly and reacts effectively to congestion. Furthermore, we have determined that the acceptable quality for the end user when Skype video calls experience different levels of packet loss is 8% of loss; beyond that, the user will not tolerate poor quality.

Keywords

Skype, video call, Quality of experience, VoIP.

1 Introduction

Communication among people has been fundamentally revolutionised by the Internet. Text messages and emails are still the traditional means of communication; however, we are now at the cutting edge, welcoming the next generation of communication: voice/video telephony. Several vendors have provided applications that support online video chat, such as Facetime, MSN messenger and Skype. The most popular example of these applications is Skype, which provides high quality voice/video transmission in a variety of network conditions. Due to the nature of video calls, which require real time communication between users, its quality can be more sensitive to network impairments, such as bandwidth variations and packet loss. In addition, as video calls demand more bandwidth than do voice calls, their traffic and quality can be also affected by other cross traffic. It is therefore of central importance for researchers, application developers and users to evaluate Skype's video call behaviour and quality under a variety of network conditions. However, to date, there has been very little research conducted in this area.

In this paper, we present our recent study of Skype's performance under adverse network conditions such as bandwidth variation and packet loss. In addition, we will investigate how Skype will compete for bandwidth with other traffic. Finally, the end user quality of experience (QoE) will be measured.

2 Related work

Evaluating Skype's performance can be categorised into two areas: studying protocol network characteristics and investigating VoIP aspects. Baset and Schulzrinne (2006) first examined Skype's traffic, peer-to-peer technology and NAT crossing mechanism. Since then, several papers have been released on Skype's P2P technology, architecture and traffic (Bonfiglio et al., 2008; Guha et al., 2006). In the second area, some researchers concentrated on Skype voice quality, providing extensive investigation into its voice service only (Chen et al., 2006; Te-Yuan et al., 2009). Some papers have been published regarding Skype video calls. Boyaci et al. (Boyaci et al., 2009) studied Skype's sending rate under different network conditions and then compared its performance with other video chat applications. They found that Skype, under adverse network conditions, performed better than other VoIP applications. In a recent paper, De Cicco et al. (De Cicco et al., 2011) investigated Skype's responses to bandwidth variation; they determined that Skype's responsiveness mechanism is too slow. The most recent investigation was conducted by Xinggong et al. (Xinggong et al., 2012), who studied Skype performance under different network conditions such as pocket loss, propagation delay and bandwidth variation. They also developed several models, such as Skype video calls' rate control and FEC redundancy. They concluded that Skype adapts well to bandwidth variation and can perfectly combat mild loss. Identifying whether Skype is TCP friendly or not was a controversial issue among some researchers (Boyaci et al., 2009), (De Cicco et al., 2011) and (Xinggong et al., 2012). In our paper we will study Skype performance under adverse network conditions using different video motions. In addition, we will investigate how Skype shares bandwidth with TCP traffic. Finally, we will measure the end user experience regarding Skype video quality.

3 Measurement Testbed Setup

A controlled testbed that consists of several components was used to study Skype video call performance, as shown in Figure 1. This testbed consisted of two clients on which the Skype program was installed. These clients were connected by NAT wireless routers where each host has a private IP address and connects to the Internet via these routers. In addition, a software-based network emulator was used to emulate the different network conditions (NEWT) (Microsoft.Resarch.Asia, 2010). To emulate video calls, we used three standard video sequences with different motions—Akiyo, Foreman and Stefan. This can comprehensively determine Skype's video adaption mechanism. Video sequences are injected into Skype using ManyCam (Manycam, 2012), which provides a constant and repeatable transmission of the video content. The measurement data are captured using Wireshark and then analysed using Matlab.

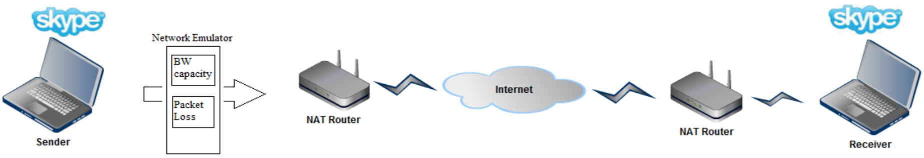


Figure 1: Testbed architecture

4 Measurement Results

In this section, we will illustrate Skype performance under adverse network conditions. This includes reporting on Skype's response to bandwidth variation when various video sequences with different speed motions are used; discussing how Skype's sending rate and packet size behave under different packet loss conditions; identifying whether or not Skype is TCP-friendly; and examining the acceptable quality for the end user when the application experiences different packet loss conditions.

4.1 Impact of available bandwidth

To examine Skype's responsiveness mechanism toward changeable network conditions such as plunge/soar available bandwidth, the capacity of bandwidth was varied according to a square wave form. The network emulator was used to change bandwidth to rates ranging from 1,000 Kbps to 160 Kbps. The measured results of Skype sending rates are demonstrated in Figure 2, which shows that Skype effectively reduced its sending rate as the available bandwidth plunged, and increased its sending rate when the bandwidth rose. This increase varied as per the speed motion of the video call.

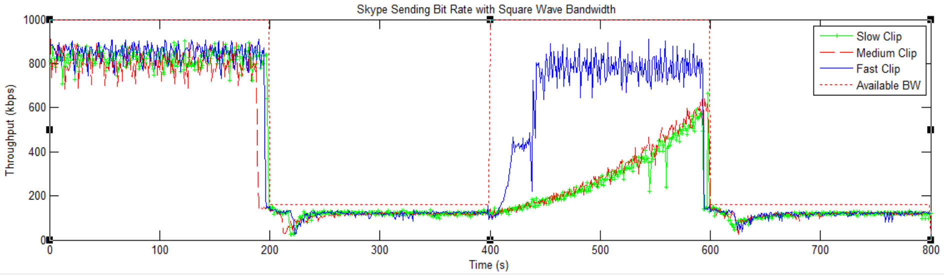


Figure 2: Skype sending bit rate per second with the square wave bandwidth

In the time interval [400,600], where the available bandwidth was increased suddenly to 1000, it was noticed that Skype adapted to the sudden increase by increasing its sending bit rate for fast, medium and slow calls. However, Skype's responsiveness mechanism for the fast video call was more effective and quicker than for the other video calls, which were medium and slow. Skype sending bit rate for the fast video call took approximately 50s to adapt to the sudden bandwidth increase, and then it increased its sending bit rate again to up to 800 Kbps. This can be explained in that due to the fact that the fast video call contains the most complex scene and the highest motion, thus; it need more bandwidth to deliver the call in high quality. In the medium and slow video calls, Skype's adaptive mechanism was too slow with respect to the sudden increase in bandwidth and this conclusion was also achieved by (De Cicco et al., 2011) . Skype's sending bit rate for medium and slow calls increased gradually over the period, reaching roughly 600 Kbps at the end of the period.

In conclusion, Skype can adapt its sending bit rate with respect to sudden decreases/increases in bandwidth. Skype video calls' adaptive mechanism for fast motion was more effective and quicker than those of the other video calls.

4.2 Impact of packet loss

We investigated how Skype behaves in term of sending bit rate and packet size when packet loss is introduced at different levels. This is particularly crucial in assessing Skype reactiveness toward different levels of packet loss. Using a network emulator, we varied the packet loss rate from 0% to 14%.

The measurement results of Skype's sending rate are illustrated in Figure 3. We found that Skype adapts its sending bit rate toward packet loss in three manners. First, when the rate of packet loss is ≤ 6%, Skype's sending bit rate remains almost constant. Second, in the range of the packet loss 6%-10%, Skype's sending rate decreases gradually. Third, when the level of packet loss is larger than 10%, Skype's sending rate is flatted at a lower value. These behaviours were also observed for the different video calls that were used in this experiment (fast, medium and slow).

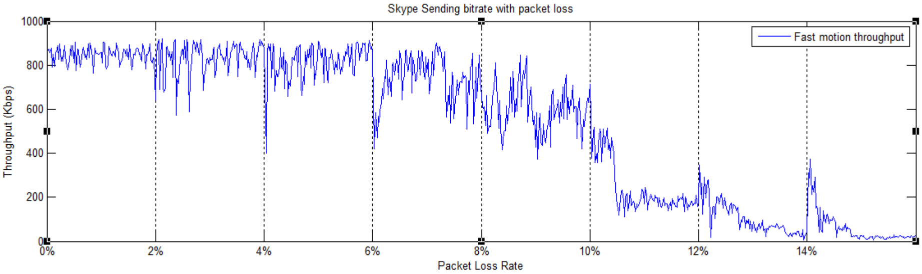


Figure 3: Skype Average sending bit rate with different rate of packet loss

To summarise, the adaptation point for Skype, when it combats different packet loss level, is 6%. Skype adapts to the packet loss via three behaviours. First, Skype functions normally when the packet loss is ≤ 6% and its sending rate becomes loss-ignorant. Second, in the range of 6% to 10% loss, Skype start reacting to the different packet loss condition by reducing its sending bitrate gradually. The third behaviour is that Skype turns to conservative behaviour when the packet loss is larger than 10% and it significantly keeps its sending rate flat at a low value. Skype follows these behaviours for fast, medium and slow video calls.

The measured results of Skype's packet size show that Skype adapts to minor packet loss by increasing its packet size proportionally as the minor packet loss rate increases. However, when the level of packet loss is significantly large, Skype relatively adapts by reducing its packet size. This is illustrated at Figure 4.

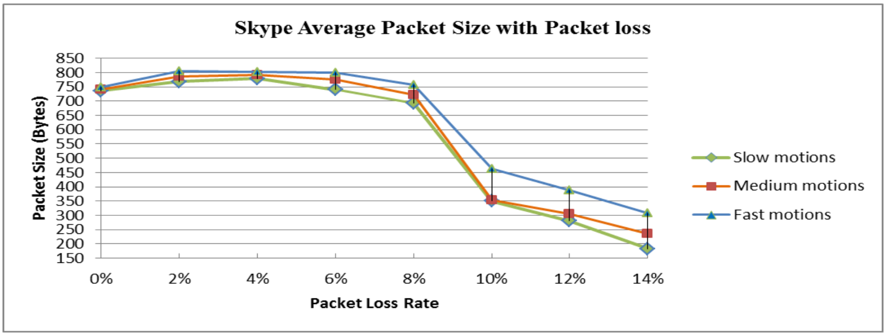


Figure 4: Skype average packet size with different packet loss levels

It is evident that Skype followed two behaviours in order to adapt its packet size toward different packet loss rates. First, when the rate of packet loss was ≤ 8%, Skype's packet sizes increase slightly as the minor rate of packet loss increased. This can be interpreted as a result of employing FEC algorithm by Skype to combat the packet loss. Second, when the level of packet loss was larger than 8%, Skype's packet size dropped dramatically. This indicates that Skype becomes more conservative when it detected that the network condition became very bad. Consequently, Skype only sends out required data at a low rate. These behaviours were observed for the different video calls with different motion speed which used in this experiment.

In summary, Skype adapts to the packet loss using two behaviours. First, when the packet loss is ≤ 8%, Skype behave normally and counter the loss by employing the FEC algorithm. Second, Skype performs in a conservative manner when the packet loss is larger than 8% and it significantly reduces its packet sizes. Skype uses these behaviours for fast, medium and slow clips.

4.3 Skype video call performance when sharing bandwidth with TCP traffic

In an actual network, Skype video calls would not propagate alone; different traffic would share the bandwidth. It is known that the majority of Internet traffic is transferred by the TCP protocol (Jiang and Dovrolis, 2005), which uses a congestion control mechanism to control the load applied on the network. However, since Skype transfers its traffic over UDP protocol (Bonfiglio et al., 2009), it lacks the sense of having a congestion control mechanism at the transport layer. Thus, it is vital that the applications that rely on UDP protocol for their transmissions should be TCP-friendly in order to maintain Internet stability (Floyd and Fall, 1999). Skype copes with this issue by placing its built-in rate control mechanism at the application layer (Xinggong et al., 2012).

Several studies have been conducted to identify whether or not Skype is TCP-friendly (Boyaci et al., 2009), (De Cicco et al., 2011) and (Xinggong et al., 2012).

However, contrary results were achieved in these studies. Boyaci et al. (Boyaci et al., 2009) stated that TCP traffic is more aggressive than Skype when they share the bandwidth, while De Cicco et al. (De Cicco et al., 2011) concluded that Skype behaved more aggressively than TCP traffic. However, Xinggong et al. (Xinggong et al., 2012) stated that Skype is TCP-friendly.
Thus, we aimed to investigate how Skype competes with TCP traffic based on HTTP protocol and how this traffic affects Skype's performance.
In this scenario, we use a network emulator to configure the bandwidth to 1,000 Kbps. In order to generate HTTP traffic, a 12 MB file was uploaded in the middle of a Skype video call to Media Fire, which is a cloud storage service website.

The measured results demonstrate that, in the absence of any other traffic, the sending rate of all video calls utilised the bulk of bandwidth. Once the HTTP traffic was introduced, Skype's sending rate adapted to the existence of HTTP traffic by reducing its transmission rate by approximately 50%, leaving the remaining bandwidth for HTTP traffic. After the HTTP traffic was stopped, Skype resumed its sending rate to utilise the majority of the available bandwidth. This was noticed for all video calls with different speed motions. The following graph shows the Skype sending rate performance of fast video calls in the presence of TCP traffic, based on HTTP protocol.

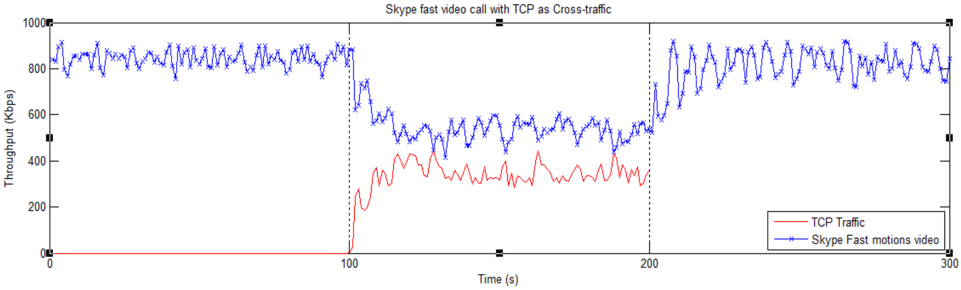


Figure 5: Skype sending rate with TCP traffic based on HTTP protocol

It was mentioned previously in the related work that there has been controversy as to whether or not Skype is TCP-friendly. We found that Skype shared the bandwidth with other TCP traffic in a fair manner, regardless of the video call speed motions. Thus, we agree with Xinggong et al. (Xinggong et al., 2012), and concur that Skype is indeed TCP-friendly.

In conclusion, Skype utilises the bulk of bandwidth in absence of other traffic. When it shares bandwidth with TCP traffic, it does so fairly; thus, it can indeed be considered TCP-friendly.

4.4 Investigating the end-user acceptable quality for Skype video calls

We also investigated the end-user acceptable quality for Skype video calls under different packet loss conditions. This is of central importance in evaluating the extent to which Skype can maintain an acceptable level of quality under different levels of packet loss. This was done by carrying out several actual Skype video calls with various people during which different packet loss rates were introduced by the network emulator.

Once the packet loss level was introduced, the end user was asked whether he/she would tolerate the video call quality or not. We considered that the end user would not tolerate the video call quality if he/she dropped the call, if the call continued with audio only or if the end user declared that he/she could not continue the call.

We found that the drop ratio among end users increased relative to the level of packet loss increase.

We observed that the majority of end users were unable to tolerate the Skype video quality when packet loss rate was 10%, and they asked to disconnect the call. This feeling was more obvious when the rate of packet loss was more than 10%. The following graph shows the cumulative distribution (CDF) of the dropping ratio versus different packet loss rates.

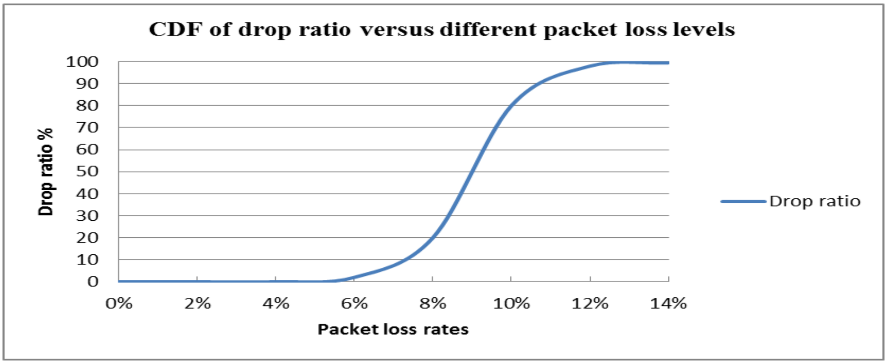


Figure 6: CDF of drop ratio versus different packet loss levels

In conclusion, we examined the end-user acceptance quality for Skype video calls under different packet loss conditions. We found that the drop ratio among end users increased proportionally as the level of packet loss increased. Therefore, it could be said that the end user would tolerate the quality of a Skype video call until the level of loss reached 8%. After this level of packet loss, Skype video call quality was determined to be unacceptable.

5 Conclusion and future work

In this paper, we look at Skype performance under different network conditions. Through extensive measurement, we have illustrated that Skype responsiveness for fast video motion is more effective and it is robust toward minor loss. When network conditions become very bad, Skype tends to reduce its sending rate significantly. In addition, our results reveal that Skype is TCP-friendly. Moreover, we found that end users will tolerate the quality of a Skype video call up to an 8% level of loss. After this level, Skype video call quality was not tolerated and was unacceptable.

For future work, we will extend our outlook to include high-speed connection and then study Skype's performance under this system. Skype performance of multi-users video conferencing is also in the plans for future research.

6 References

Bonfiglio, D., Mellia, M., Meo, M., Ritacca, N. & Rossi, D. (2008) Published. Tracking Down Skype Traffic. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 13-18 April 2008 2008. 261-265.

Bonfiglio, D., Mellia, M., Meo, M. & Rossi, D. (2009). Detailed Analysis of Skype Traffic. Multimedia, IEEE Transactions on, 11, 117-127.

Boyaci, O., Forte, A. G. & Schulzrinne, H. (2009) Published. Performance of Video-Chat Applications under Congestion. Multimedia, 2009. ISM '09. 11th IEEE International Symposium on, 14-16 Dec. 2009 2009. 213-218.

Chen, K.-T., Huang, C.-Y., Huang, P. & Lei, C.-L. (2006). Quantifying Skype user satisfaction. SIGCOMM Comput. Commun. Rev., 36, 399-410.

De Cicco, L., Mascolo, S. & Palmisano, V. (2011). Skype Video congestion control: An experimental investigation. Computer Networks, 55, 558-571.

Floyd, S. & Fall, K. (1999). Promoting the use of end-to-end congestion control in the Internet. IEEE/ACM Trans. Netw., 7, 458-472.

Guha, S., Daswani, N. & Jain, R. (2006). An Experimental Study of the Skype Peer-to-Peer VoIP System. The 5th International Workshop on Peer-to-Peer Systems. Santa Barbara, CA, United States.

Jiang, H. & Dovrolis, C. (2005). Why is the internet traffic bursty in short time scales? SIGMETRICS Perform. Eval. Rev., 33, 241-252.

Manycam. (2012). ManyCam,The best free live studio & webcam effects software [Online]. Available: http://www.manycam.com/ [Accessed 20/05 2012].

Microsoft.Resarch.Asia. (2010). Network Emulator for Windows Toolkit (NEWT) [Online]. Microsoft Resarch Asia. Available: http://blogs.msdn.com/b/lkruger. [Accessed 18/05 2012].

Te-Yuan, H., Kuan-Ta, C. & Huang, P. (2009) Published. Tuning Skype's Redundancy Control Algorithm for User Satisfaction. INFOCOM 2009, IEEE, 19-25 April 2009 2009. 1179-1187.

Xinggong, Z., Yang, X., Hao, H., Liu, Y., Zongming, G. & Yao, W. (2012) Published. Profiling Skype video calls: Rate control and video quality. INFOCOM, 2012 Proceedings IEEE, 25-30 March 2012 2012. 621-629.

Performance Analysis of Voice Call using Skype

L. Liu and L. Sun

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

Abstract

The purpose of this paper is to investigate the performance of voice calls using the current version of Skype. Hence the testbed, consisting of three PCs and one router, was designed for the QoS experiments and QoE experiments about the point-to-point Skype voice calls. In the experiments, the ITU-T P.50 sample voices called "British English" were used to replace the real time conversation. The QoS experiments aimed to find out the congestion control algorithm of how Skype adjust payload size, interarrival time and throughput under different packet loss rates. The QoE experiments investigated the changes of performances of Skype voice calls under different packet loss rates through MOS measured by PESQ and subjective tests. The results showed that Skype may apply the category congestion control algorithm to recover the quality of Skype voice calls under different packet loss rates. The performances of Skype voice calls would degrade and become discontinuous with the packet loss rate increasing.

Keywords

Skype voice call, QoS, QoE, P2P, PESQ, MOS, Congestion Control Algorithm.

1 Introduction

Recently, more and more people use VoIP telephony in which voice calls are established via Internet network. VoIP telephony not only can reduce the cost of voice calls for users, but also can provide new services such as conference video and voice calls. There are many VoIP applications such as Skype, Google Talk and Yahoo Messenger (Sat and Wah, 2007). the most popular application is Skype which applies peer-to-peer technology and has more than 500 million users (Skype, 2012a). According to the official Skype website, the number of users who login on Skype at peak time has exceeded 30 million (Skype, 2012a). Furthermore Skype can provide service with best quality than other VoIP applications under most situations (Boyaci et al., 2009, W. Chiang, 2006).

The current version of Skype uses a new and advanced SILK codec to encode voice stream, in which Skype can adjust bit rate and sampling rate in wide ranges (Skype, 2012b, Goudarzi et al., 2011). The SILK codec supports four operating modes: Narrowband (NB), Mediumband (MB), Wideband (WB) and Super Wideband (SWB). Each operating mode supports different ranges of bit rate and frame time to ensure the quality under different kinds of situations. The ranges of bit rate and sampling rate are shown as Table 1.

Modes	Bit Rate (Kbps)	Sample Rate (kHz)
Narrowband	6-20	8
Mediumband	7-25	8,12
Wideband	8-30	8,12,16
Super Wideband	12-40	8,12,16,24

Table 1: Ranges of bit rate and sample rate for SILK operating modes (Goudarzi et al., 2011, Koen Vos, 2010)

Skype applies forward error correction (FEC) mechanism to recover the lost packets that some packets will piggyback the previous packets based on the redundancy ratio (Wang et al., 2010, Padhye et al., 2000, Te-Yuan et al., 2009, Te-Yuan et al., 2010). The research about congestion control algorithm used in previous versions of Skype shows that Skype always increases payload size, interarrival time and throughput with packet loss rate increasing (Bonfiglio et al., 2008, Te-Yuan et al., 2009, Bonfiglio et al., 2009). However Skype always can provide brilliant voice calls service under the situations of packet loss rate ranging from 0% to 10%. The congestion control algorithm used in the current version of Skype is still unknown. Hence this project has two main objectives: (a) to investigate the congestion control algorithm used in the current version of Skype of how Skype adjusts payload size, interarrival time and throughput under the network situations of different packet loss rates; (b) to find out the performance of how Skype voice calls changes under the network situations of different packet loss rates. This project applies the packet loss rates ranging from 0% to 20%. In order to achieve the two objectives, two types of experiments are designed: Quality of Service (QoS) and Quality of Experiments (QoE) (ITU, 2008a, ITU, 2005). In the QoS experiments, packets are captured by Wireshark and analysed by AWK programs (Wireshark, 2012). In the QoE experiments, Mean Opinion Score (MOS) is used to represent the qualities of Skype voice calls (Kilkki, 2008, Laghari and Connelly, 2012, ITU, 2005). The MOS usually ranges from 1 to 5 standing for the quality from worst to best. Objective measurement models aim to predict MOS which is based on subjective standards such as Perceptual Evaluation of Speech Quality (PESQ) and perceptual evaluation of video quality (PEVQ) (ITU, 2001, ITU, 2008b). This project uses PESQ program to measure objective MOS. Nevertheless the objective MOS measured by PESQ ranges from -0.5 to 4.5 representing the quality from worst to best (ITU, 2001). However the subjective MOS ranging from 1 to 5 is measured by audiences. The conversation is recorded by Audacity for audiences to listen and measure subjective MOS. In the experiments, the ITU-T P.50 sample voices called "British English" are used to replace the real time conversation.

The following section will introduce the design of testbed and experiments. Sections 3 and 4 will present the analysis of QoS results and QoE results, followed by section 5 which draws conclusions and future work.

2 Testbed

Since this project aims to investigate the performance of Skype point-to-point voice calls under the network situations of different packet loss rates, the experiments should establish the Skype point-to-point voice calls under congestion controllable situation whilst avoiding the interferences from the Internet congestion at the same time. Thus the testbed is designed as shown as Figure 1.

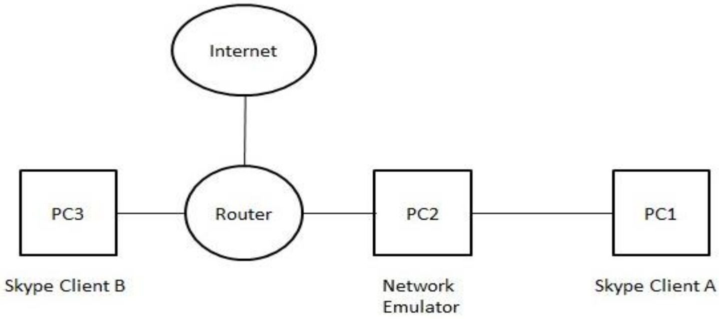


Figure 1: Testbed topology

As shown in Figure 1, the testbed consists of three PCs and one router. PC1 and PC3 are used as Skype clients to establish the Skype voice calls. A Linux operating system is installed on PC2 to create the packet loss for the experiments as network emulator. PC1 and PC3 can connect to Internet through the router. The voice samples are played on PC3 and transmitted to PC1 through the router and PC2 so that the interference from Internet congestion could be avoided. Moreover Audio Virtual Cable is used to transmit voice stream from voice player to Skype on PC3 and from Skype to Audacity on PC1. Since Skype needs a period of time to detect the packet loss in the network, the duration time should be long enough for Skype to react the packet loss. However the audiences prefer to listen to the short conversation. Hence the duration time of QoS experiments and QoE experiments are 12 minutes and 2.5 minutes. Furthermore each sample voice only last about 8 seconds so that the sample voice would be repeat in the experiments. For the QoS experiments, the sample voice is played on PC3 to transmit to PC1 during each Skype voice call. Moreover the packet loss rate increases 2% from 0% to 20% then directly reducing to 0%. The packet loss rate changes every minute. Wireshark is installed on PC1 to capture the packets of Skype voice calls for data analysis. For the QoE experiments, the sample voices also are played on PC3 to transmit to PC1 during the Skype voice calls, but the received voices on PC1 are recorded by

Audacity to measure MOS. Furthermore the packet loss rate is changed every 30 seconds as the consequence from 0%, 8%, 12%, 20% and 0%. Each Skype voice call lasts two and half minutes in the QoE experiments.

3 QoS results analysis

3.1 Average payload size, interarrival time and throughput

QoS experiments aim to investigate the congestion control algorithm of how the current version of Skype adjusts payload size, interarrival time and throughput under different packet loss rates. The results show that the current version of Skype may apply the three different congestion control methods to recover the quality under the packet loss rate from 0% to 20%. The results of average payload size, interarrival time and throughput under different packet loss rates are shown as Figures 2, 3 and 4.

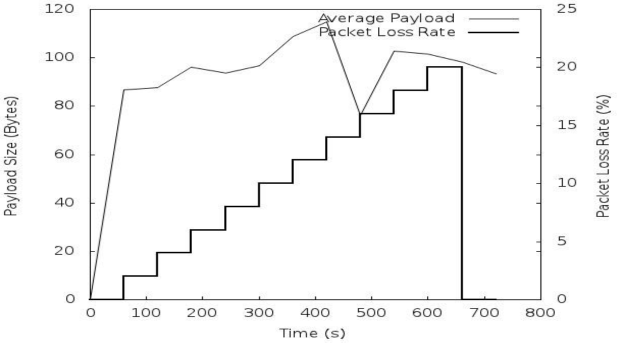


Figure 2: Average payload size under different packet loss rates

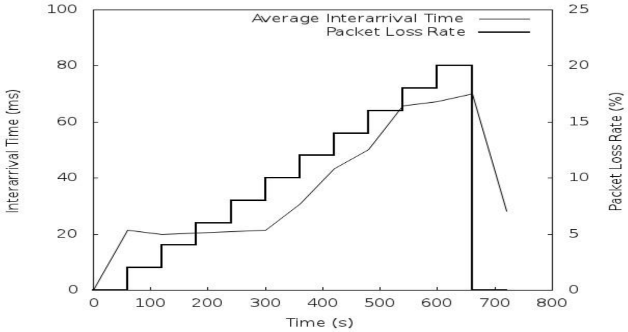


Figure 3: Average interarrival time under different packet loss rates

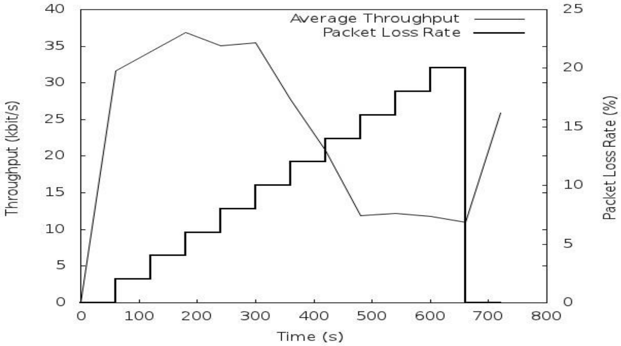


Figure 4: Average throughput under different packet loss rates

Figure 2 showed that Skype increased payload size with packet loss rate increasing until to 14%. When the packet loss rate was 14%, the average payload size became the lowest around 78 Bytes. Then the average payload size increased to about 100 Bytes when the packet loss rate was 16%. When the packet loss rate increased from 16% to 20%, the average payload size slightly reduced. Moreover when the packet loss rate significantly decreased to 0% from 20%, the average payload size decreased to about 90 Bytes which were still higher than the beginning average payload size under the situation of 0% packet loss.

For the average interarrival time, the Figure 3 showed that Skype applied stable interarrival time around 20 ms until the packet loss rate increased to 10%. Skype magnificently enlarged the average interarrival time with the packet loss rate increasing from 10% to 20%. However when the packet loss rate became 0% from 20%, the average interarrival reduced to about 30 ms which still were higher than the beginning average interarrival time under 0% packet loss.

The Figure 4 showed that the average throughput slightly increased with packet loss rate increasing until to 10%. When the packet loss rate increased from 10% to 14%, the average throughput significantly decreased from about 35 Kbit/s to 12 Kbit/s. Then the average throughput was stable around 11 Kbit/s when the packet loss rate increased from 14% to 20%. When the packet loss rate became 0%, the average throughput increased to around 25 Kbit/s which were lower than the beginning.

3.2 Payload size, interarrival time and throughput of each packet

However the average value is too brief to show the congestion control algorithm. Thus the payload size, interarrival time and throughput of each packet in the Skype voice call are shown as Figures 5, 6 and 7.

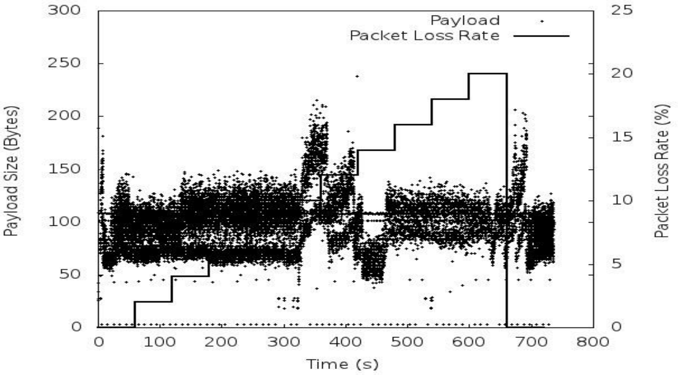


Figure 5: The payload size of each packet under different packet loss rates

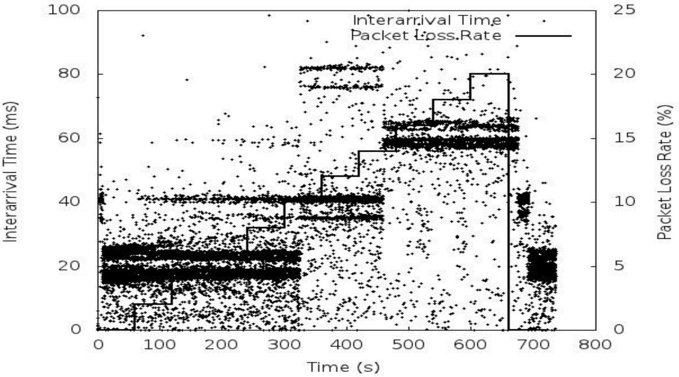


Figure 6: The interarrival time of each packet under different packet loss rates

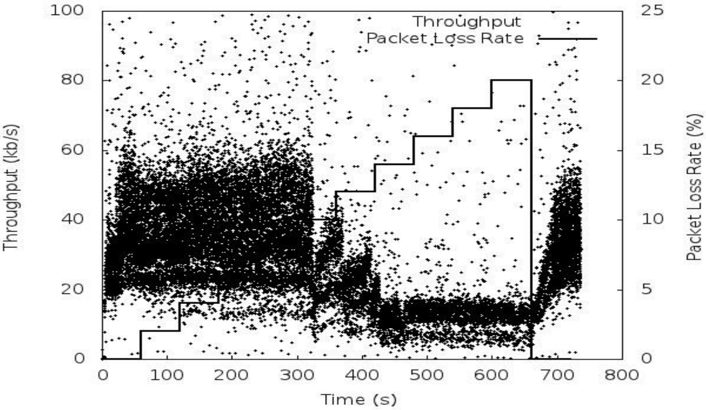


Figure 7: The throughput of each packet under different packet loss rates

As shown in Figures 5, 6 and 7, it was clear that there were three different variation tendencies of payload size, interarrival time and throughput in three period of time. Hence Skype might apply three different congestion control methods to recover the quality of Skype voice call with packet loss rate increasing from 0% to 20%. As shown in Figures 5 and 6, the basic payload size ranged about from 50 Bytes to 140 Bytes and basic interarrival time was about 20 ms. When Skype wants to invoke the FEC mechanism to recover the lost packets, for example to encode 2 frames into 1 packet, the interarrival time would be about 40 ms. Thus more and more packets were sent by the interarrival time about 40 ms with large payload size, when the packet loss rate kept increasing. When the packet loss rate increased to 10%, the interarrival time of most packets were about 40ms and 80ms which meant that most packets were encoded into 2 or 4 frames. Nevertheless the change trend of payload size was abnormal. The trend was similar as the TCP’s congestion window controls algorithm. Because when Skype detected increment of packet loss rate, Skype would send the packets with payload size as half as payload size of previous packets. If the packet loss rate was invariant, Skype would increase the payload size. Nevertheless, when packet loss rate increased to 14%, the interarrival time of most packets were about 60 ms which meant that each packet was encoded into 3 frames. The payload size of most packets ranged from 70 Bytes of 140 Bytes. However the ranges of payload size and interarrival time of most packets kept stable when the packet loss rate increased from 14% to 20%. When Skype detected the packet loss rate becoming higher and higher, Skype not only wants to recover the lost packets, but also Skype tried to recover the situation of network. As shown in Figure 7, when the packet loss rate increased from 0% to 10%, Skype increased throughput to recover the quality. However due to the payload size reduction, the trend of throughput reduction also was similar as the trend of payload size, when packet loss rate increased from 10% to 14%. Then throughput also kept stable when packet loss rate increased from 14% to 20%. However when the packet loss rate reduced directly from 20% to 0%, Skype just adjust smoothly payload size, interarrival time and throughput back to normal situation. If Skype increases throughput immediately, the network might become congestion again.

3.3 Distributions of payload size, interarrival time and throughput

In order to find out the difference between three categories of the category congestion control algorithm, the distributions of payload size, interarrival time and throughput under 0%, 6%, 12% and 20% packet loss are shown as Figure 8, 9, 10, 11, 12 and 13.

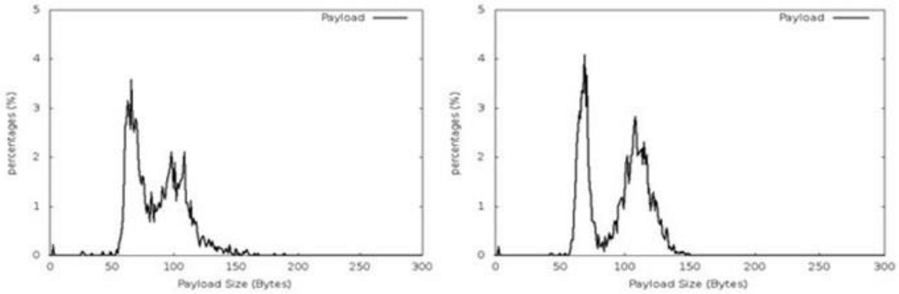


Figure 8: The distributions of payload size under 0% and 6%

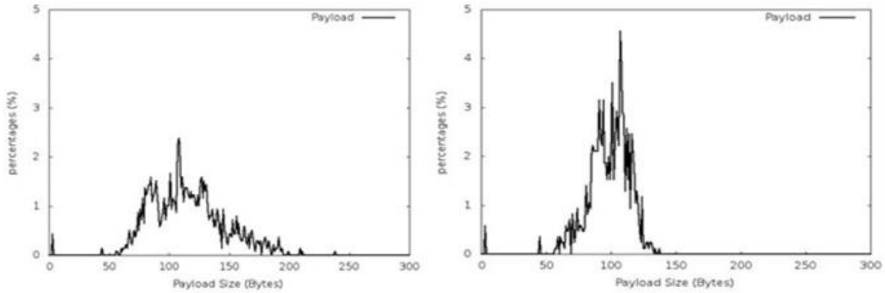


Figure 9: The distributions of payload size under 0%, 6%,12% and 20% packet loss

As shown in Figures 8 and 9, the proportion of large payload size was increasing as the packet loss rate increased. When packet loss rate was 0%, the proportion of packets with payload size around 70 Bytes is obvious higher than the proportion of packets with payload size around 100 Bytes. However when the packet loss rate was reaching to 6%, the proportion of packets with payload size around 100 Bytes was higher than the proportion of the packets under 0% packet loss rate. Furthermore when the packet loss rate increased to 12%, the proportion of packets with payload size around 70 Bytes was significantly less than the proportion of the packets under the network situation of 6% packet loss rate. Finally, when the packet loss rate was 20%, most of packets piggybacked the payload around 100 Bytes. Hence Skype obviously increased the redundancy ratio of FEC mechanism to recover the lost packets with the packet loss rate increasing.

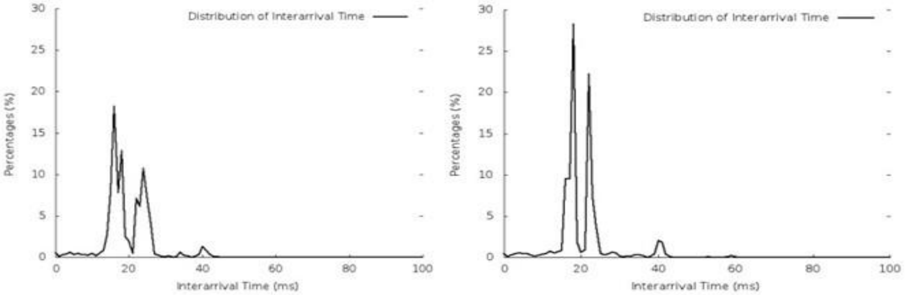


Figure 10: The distributions of interarrival time under 0% and 6% packet loss

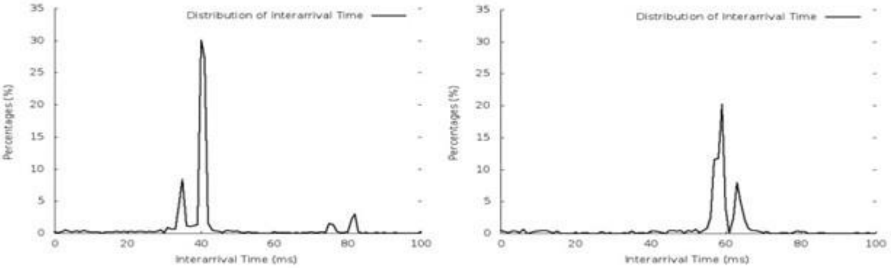


Figure 11: The distributions of interarrival time under 12% and 20% packet loss

As shown in Figure 10 and 11, when packet loss rate was 0%, the interarrival times of most packets were round 16 ms and 25 ms. There were small proportion of packets with the interarrival time around 40 ms. When the packet loss rate increased to 6%, the proportions of packets with interarrival time around 18 ms and 22 ms became about 27% and 23%. Moreover the proportion of the packets with interarrival time around 40 ms slightly increased. Nevertheless, the interarrival times of most packets were around 40 ms when the packet loss rate was 12%. Furthermore there were some packets with interarrival time around 80 ms. When the packet loss rate was 20%, the interarrival times of most packets were around 58 ms and 62 ms.

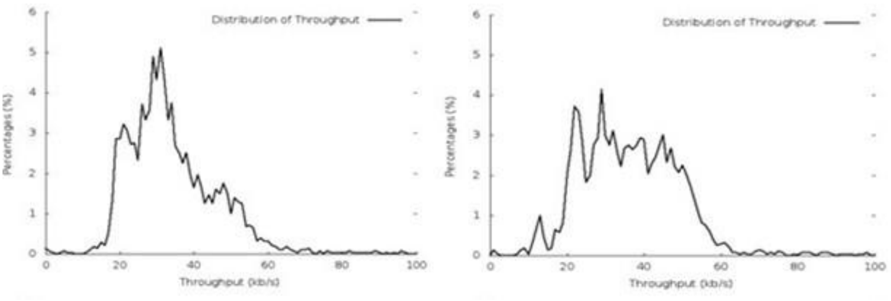


Figure 12: The distributions of throughput under 0%, 6% packet loss

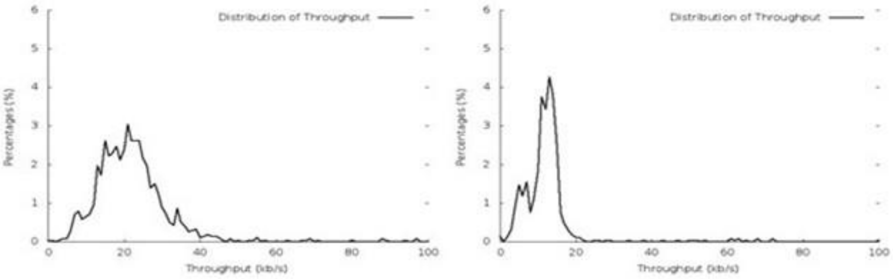


Figure 13: The distributions of throughput under 12% and 20% packet loss

As shown in Figure 12 and 13, the throughput of most packets ranged about from 18 Kbit/s to 60 Kbit/s, when the packet loss rate was 0%. Moreover the proportion of packets with about 33 Kbit/s was about 5% which is the highest proportion among all packets. Nevertheless, the proportion of the packets with about 33 Kbit/s decreased to about 4%, when the packet loss rate was 6%. And the proportion of the packets with throughput ranging from 40 Kbit/s to 60 Kbit/s became higher than the proportion of the packets under the situation of 0% packet loss. When the packet loss rate became 12%, the throughput of most packets just distributed from 8 Kbit/s to 40 Kbit/s which are much lower than the range of distribution of throughput under the situation of 0% and 12% packet loss. However when the packet loss rate was 20%, the throughput of most packets was less than 20 Kbit/s. Furthermore the proportion of packets with 15 Kbit/s was about 4.3% which was the highest proportion among all packets under the situation of 20% packet loss.

4 QoE results analysis

4.1 Objective results analysis

The recorded Skype voice call under each network situation was measured by PESQ application to get MOS (subjective MOS). In order to get average objective MOS, three Skype voice calls were recorded and saved in the experiments. The results are shown as Table 2.

	0s-30s (0%)	30s-60s (8%)	60s-90s (12%)	90s-120s (20%)	120s- 150s (0%)
Voice Call 1	3.863	3.580	3.363	2.150	3.487
Voice Call 2	3.742	2.729	2.438	2.359	3.235
Voice Call 3	3.869	2.701	2.591	2.482	3.219
Average	3.825	3.003	2.797	2.330	3.314

Table 2: The objective MOS of the Skype voice call under each network situation

As shown in Table 2, the average objective MOS of the first 30s of recorded Skype voice calls was about 3.825 which mean that the quality still was almost perfect. Furthermore the differences of objective MOS between the three recorded voice calls are very small. Nevertheless the average objective MOS of the second 30s of record Skype voice calls significantly decreased to 3.003. Hence the quality of the second 30s was worse than the first 30s even though the Skype increased the payload size, interarrival time and throughput to recover the quality. But the quality of the Skype voice call under the situation of 8% packet loss rate still was acceptable. The average objective MOS of the third 30s was 2.797 which were just slight lower than the second 30s. But the quality of the third 30s also was tolerable even Skype apply the second category congestion control algorithm. Thus the second category congestion control algorithm was useful under the stable situation. However the quality of the fourth 30s became intolerable that the MOS was 2.330. All audiences would prefer to stop the call, if they would have a voice call of this kind of quality. When the packet loss rate significantly decreased to 0% from 20%, the average MOS was 3.314. It is clear that the quality of the fifth 30s was lower than the first 30s, even though the packet loss rates were 0% for both Skype voice calls. As mentioned before, when the packet loss rate magnificently reduce from 20% to 0%, Skype would rather switch apply second category congestion control algorithm than adapt the first category congestion control algorithm. Thus the quality of the fifth 30s might be worse than the first 30s. Overall, even Skype adjust the payload size, interarrival time and throughput based on category congestion control algorithm, the quality of Skype voice call still will degrade with the packet loss rate increasing.

4.2 Subjective results analysis

In this subjective test, three testers listened to the recorded Skype voice call and provide the feedback and subjective MOS. One audience only recognised three changes of quality in the recorded Skype voice call. Furthermore when the quality degraded, all audiences felt that the Skype voice call became discontinuous. They all prefer to have a voice call with the quality like the first 30s and the last 30s. The subjective MOS are shown as Table 3.

For the first 30s of the recorded Skype voice call, all audiences gave MOS 5 which means that the quality of first 30s almost was excellent. However when the packet loss increased to 8% in the second 30s, the average subjective MOS was 4.667. Two audiences gave MOS 4.5 to the second 30s, because the two audiences heard a discontinuous voice a few times. But they still thought the quality of the second 30s was almost perfect. Another audience still felt the second 30s was perfect and gave the subjective MOS 5. Nevertheless the average subjective MOS of third 30s was 2.667 which were much lower than the average subjective MOS of the first 30s and the second 30s. Because all audiences thought that the discontinuous voice became frequent in the third 30s but they still could understand the contents and accept the quality. For the fourth 30s, all audiences thought the quality of recorded Skype voice call was unacceptable, because the discontinuous voice became annoying and much more frequent than previous recorded voices. Thus the average subjective MOS of the fourth 30s was 1.167. However when the packet loss rate directly reduced from 20% to 0%, all audiences felt that the quality was recovered immediately and became perfect. Thus all audiences gave the subjective MOS 5 to the fifth 30s. Depending on the average subjective MOS for each 30s, it is obvious that the qualities of the first 30s and the fifth 30s were the best among five 30s recorded Skype voice calls for the three audiences. The quality of the recorded Skype voice call under the situation of 20% packet loss was unacceptable for all audiences.

	0s-30s (0%)	30s-60s (8%)	60s-90s (12%)	90s-120s (20%)	120s- 150s (0%)
Audience 1	5	4.5	2.5	1.5	5
Audience 2	5	5	2.5	1	5
Audience 3	5	4.5	3	1	5
Average	5	4.667	2.667	1.167	5

Table 3: The subjective MOS of the Skype voice call under each network situation

4.3 Correlation coefficients of objective MOS and subjective MOS

As shown in Table 4, the change trend of average objective MOS and subjective MOS under different packet loss rates are different.

	0s-30s (0%)	30s-60s (8%)	60s-90s (12%)	90s-120s (20%)	120s- 150s (0%)
Average Objective MOS	3.825	3.003	2.797	2.330	3.314
Average Subjective MOS	5	4.667	2.667	1.167	5

Table 4 : The average objective MOS and subjective MOS

Depending on the objective MOS measured by PESQ application, the quality of Skype voice call would obviously degrade with the packet loss rate increasing. However the subjective MOS provided by the audiences showed that the quality would slightly degrade with the packet loss rate increasing from 0% to 8%. There was an obvious reduction of the quality when the packet loss rate became 12%. But the quality of the recorded Skype voice call under the situation of 12% packet loss was acceptable for the audiences. When the packet loss rate reached 20%, the quality became unacceptable for the audience who thought that the frequent discontinuous voice was so annoying. Nevertheless there are some interesting differences between objective MOS results and subjective MOS results. For the first 30s and the second 30s, the audiences gave higher MOS than the PESQ application. But the PESQ application measured the higher MOS than the audiences for the third 30s and fourth

30s. The reason might be the audiences found it hard to notice the degradation of the voice accurately as the PESQ application. Thus when the packet loss rates were low, the audiences felt that the quality of the recorded Skype voice calls almost were perfect. But when the discontinuous voice became obvious and frequent with the packet loss rate increasing, the audiences would think that the voice was so uncomfortable and unacceptable. Thus users would feel much more annoyed than the PESQ application for the frequent discontinuous voice. When the audiences listened to the fifth 30s, they all felt that the quality of recorded Skype voice call were perfect as the first 30s. However the PESQ application could recognise that the quality of the fifth 30s was smoothly upgraded from worst to best. Overall the qualities of Skype voice calls will degrade with the packet loss rate increasing. But the quality of Skype voice calls is acceptable for the users until the packet loss rate beyond 12%.

5 Conclusions and future work

Skype may apply the category congestion algorithm to recover the quality of Skype voice calls under different packet loss rates. The category congestion control algorithm includes three categories based on the packet loss rates from 0% to 20%. The thresholds of three categories are 10% and 14%. The first category might range packet loss rates from 0% to 10%. From packet loss rate 10% to 14%, Skype would adopt the congestion control algorithm as similar as TCP’s congestion window control algorithm. The third category congestion control algorithm would be invoked when the packet loss rate is from 14% to 20%. However the performance of Skype voice calls will become discontinuous with the packet loss rate increasing. The objective MOS measured by PESQ showed that the performance will smoothly degrade with the packet loss rate increasing. Nevertheless the subjective MOS measured by audiences showed that the performances of Skype voice calls under packet loss rate 0% and 8% are almost same and brilliant. When the packet loss rate was 12%, the discontinuous voices became obvious. The performance of Skype voice call was unacceptable when the packet loss rate was 20%. Overall the category congestion control algorithm could effectively recover the quality of Skype voice calls under the packet loss rate from 0% to 14%.

Due to time constraint, some aspects of research about the performance of Skype voice calls such as the impacts of delay and bandwidth. The future work will focus on the performance of Skype voice calls under different delay and bandwidth. Furthermore the conference Skype voice calls also will be investigated in the future.

6 References

BONFIGLIO, D., MELLIA, M., MEO, M., RITACCA, N. & ROSSI, D. Year. Tracking Down Skype Traffic. *In:* INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 13-18 April 2008 2008. 261-265.

BONFIGLIO, D., MELLIA, M., MEO, M. & ROSSI, D. 2009. Detailed Analysis of Skype Traffic. *Multimedia, IEEE Transactions on,* 11**,** 117-127.

BOYACI, O., FORTE, A. G. & SCHULZRINNE, H. Year. Performance of Video-Chat Applications under Congestion. *In:* Multimedia, 2009. ISM '09. 11th IEEE International Symposium on, 14-16 Dec. 2009 2009. 213-218.

GOUDARZI, M., SUN, L. & IFEACHOR, E. Year. Modelling Speech Quality for NB and WB SILK Codec for VoIP Applications. *In:* Next Generation Mobile Applications, Services and Technologies (NGMAST), 2011 5th International Conference on, 14-16 Sept. 2011 2011. 42-47.

ITU. 2001. *P.862 : Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs* [Online]. Available: http://www.itu.int/rec/T-REC-P.862/en [Accessed 10/08/2012].

ITU. 2005. *[50] Definition of Quality of Experience (QoE)* [Online]. Available: http://www.itu.int/md/T05-FG.IPTV-IL-0050/en [Accessed 15/06/2012].

ITU. 2008a. *E.800 : Terms and definitions related to quality of service and network performance including dependability* [Online]. Available: http://www.itu.int/rec/T-REC-E.800-200809-I/en [Accessed 16/05/2012].

ITU. 2008b. *P.910 : Subjective video quality assessment methods for multimedia applications* [Online]. Available: http://www.itu.int/rec/T-REC-P.910-200804-I/en [Accessed 16/06/2012].

KILKKI, K. 2008. Quality of Experience in Communications Ecosystem. *Journal of Universal Computer Science,* 14**,** 615-624.

KOEN VOS, S. J., AND KARSTEN SOERENSEN. 2010. *SILK Speech Codec, draft-vos-silk-02* [Online]. Available: http://tools.ietf.org/html/draft-vos-silk-02 [Accessed 16/05/2012].

LAGHARI, K. U. R. & CONNELLY, K. 2012. Toward total quality of experience: A QoE model in a communication ecosystem. *Communications Magazine, IEEE,* 50**,** 58-65.

PADHYE, C., CHRISTENSEN, K. J. & MORENO, W. Year. A new adaptive FEC loss control algorithm for voice over IP applications. *In:* Performance, Computing, and Communications Conference, 2000. IPCCC '00. Conference Proceeding of the IEEE International, Feb 2000 2000. 307-313.

SAT, B. & WAH, B. W. Year. Evaluation of Conversational Voice Communication Quality of the Skype, Google-Talk, Windows Live, and Yahoo Messenger Voip Systems. *In:* Multimedia Signal Processing, 2007. MMSP 2007. IEEE 9th Workshop on, 1-3 Oct. 2007 2007. 135-138.

SKYPE. 2012a. *Free Skype internet calls and cheap calls to phones online - Skype* [Online]. Available: http://www.skype.com/intl/en-gb/home [Accessed 10/01/2012].

SKYPE. 2012b. *SILK* [Online]. Available: http://developer.skype.com/silk [Accessed 10/01/2012].

TE-YUAN, H., HUANG, P., KUAN-TA, C. & PO-JUNG, W. 2010. Could Skype be more satisfying? a QoE-centric study of the FEC mechanism in an internet-scale VoIP system. *Network, IEEE,* 24**,** 42-48.

TE-YUAN, H., KUAN-TA, C. & HUANG, P. Year. Tuning Skype's Redundancy Control Algorithm for User Satisfaction. *In:* INFOCOM 2009, IEEE, 19-25 April 2009 2009. 1179-1187.

W. CHIANG, W. X. A. C. C. 2006. A Performance Study of VoIP Application: MSN vs Skype. *MUTLICOMM.*

WANG, L., WU, M., WEI, L. & LI, M. Year. An Adaptive Forward Error Control Method for Voice Communication. *In:* Networking and Digital Society (ICNDS), 2010 2nd International Conference on, 30-31 May 2010 2010. 186-189.

WIRESHARK. 2012. *Wireshark - Go deep.* [Online]. Available: http://www.wireshark.org/about.html [Accessed 09/06/2012].

AI-Based TCP Performance Modelling

K. Mahmoud and B.V. Ghita

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

Abstract

Different mathematical models exist for modelling TCP algorithms and interrelations between TCP and network parameters. In this research, two artificial neural network models were developed to model TCP performance of both lossless and lossy traffic flows. A mathematical base line was defined for accuracy comparison in terms of regression and MSE of estimated throughput. The presence of idle time in TCP flows was investigated and accounted for in the models, in addition to the consideration of non-standard flows and statistical outliers. Neural models developed had outperformed the mathematical modelling of TCP throughput along all stages of this research. Finally, it was suggested to revise the available mathematical model to take idle time into consideration.

Keywords

TCP Performance, Throughput, History-based Modelling, Neural Networks, Idle Time, Slow Start, Bulk TCP Transfer, Robust AI-Based Modelling

1 Introduction

The importance of TCP performance is due its 90% representation of the Internet traffic and hence its reflection on the overall performance of IP networks (Shah et al., 2007). The need to provide realistic performance modelling of the TCP throughput and find relationships between network conditions and this throughput is essential. Traditional mathematical models do not provide accuracy as expected despite their complexity, especially for short-lived TCP connections (Ghita and Furnell, 2008).

This paper adopts an AI-based approach using neural networks in MATLAB to model TCP throughput (i.e. transmission time) for both lossless and lossy TCP connections, comparing results obtained with mathematical modelling and results from previous research. During the modelling, various TCP parameters are investigated in terms of their effect and relationship to the actual throughput. Conclusions are made on whether mathematical models and TCP algorithm may be revised and modified based on these observations

2 Previous Research

A research was made by He et al. (2007) to develop a model for predicting the TCP throughput for bulk TCP transfers in particular. As a testbed, their research made use of an architecture of 50-60 nodes distributed in universities, research labs and ISPs in the US, Europe and Asia. In their research, they have initially strengthened on the difference between performance estimation evaluated during TCP transfer, and performance prediction which is acquired using probing prior to the actual transfer of data. He et al. (2007) have classified the models used to evaluate the performance of TCP for TCP transfers into two classifications; formula-based or mathematical models, and history-based models, each approach having its own advantages and drawbacks.

2.1 Mathematical TCP Models

Formula-based models depend on mathematical expressions to evaluate the expected TCP throughput from the TCP parameters. A mathematical model was proposed by Cardwell et al. (2000) describing each stage of a TCP connection: slow start, segment loss, congestion avoidance and delayed acknowledgement. This model was considered as a reference and baseline in this research in order to evaluate the performance results obtained from the AI-based model.

$$E[T] = E[T_{SS}] + E[T_{loss}] + E[T_{ca}] + E[T_{delack}]$$

2.2 History-Based Models

History-based models mainly depend on the previous knowledge acquired from historical TCP transfers. The models use adaptive learning in order to form relationships between observed path characteristics and the resulted TCP throughput of each transfer. Accordingly, history-based models are independent of the TCP implementation used at the server and the receiver ends. As per (He et al., 2007), the prediction accuracy of their history-based model gave better accuracy with a RMSRE less than 0.4 for 90% of the traces.

Another research was made by Mirza et al. (2010) in which they adopted a machine learning approach to predict TCP throughput. They have used Support Vector Regression (SVR). The measurements used in their models were the available bandwidth on the congested link, the queuing at the bottleneck node, and the loss rate. They have used both passive and active path measurements. For the passive measurements, parameters (available bandwidth, queuing, and loss rate) were obtained from pre-captured TCP flows, and for active measurements the same parameters were obtained from the active monitoring cards. Their results obtained from their experiments indicated that for bulk TCP transfer, the predicted TCP throughput was within 10% of the actual value 87% of the time.

A research approach for estimating TCP performance using neural networks was adopted by (Ghita et al., 2008). They have used both synthetic and real network traffic. In their research they have divided their training data sets into lossless and lossy flows. The results obtained from the neural model have revealed significant improvement with nearly a ten-fold improvement of the relative error, while that was not the case for traffic with segment losses.

3 Methodology and Model Design

Three sources of captured traffic were used for training and validating during modelling: traffic collected from Brescia University, Plymouth University, and MAWI Research Group. Figure 1 demonstrates the process diagram for this research. Backpropagation feed forward neural networks were considered for the modelling process. Backpropagation, or propagation of error, is a supervised learning method, implementing the Delta rule to update the weights of the networks to reach convergence (Freeman and Skapura, 1991).

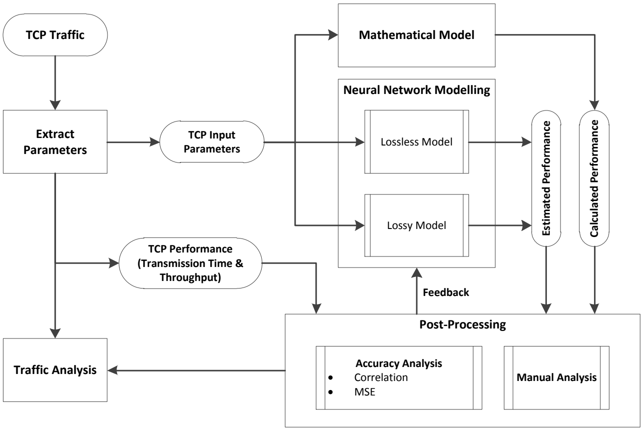


Figure 1: Process diagram of research stages.

Two separate neural models were developed for both lossless and lossy TCP traffic. Six input variables were fed to the lossless model: the actual data sent, the average RTT, the average and maximum segment size, the maximum congestion window, and the initial sender window size. The same were used for the lossy model in addition to the loss rate as evaluated by the count of triple duplicate ACK, and the average retransmission time. For both models, the actual transmission time was considered as the target during training, while the output being the estimated transmission time estimated by the models.

From the statistical analysis performed at early stages of the research, the existence of prolonged periods of idle time within the lifespan of TCP connection compared the average RTT and total transmission time, as show in Figure 2. Hence, further pre-processing and filtering was applied based on the maximum idle time values, and neural model performance was re-evaluated after this exclusion in samples, while comparing them to Cardwell’s mathematical model.

The effect of excluding statistical outliers (i.e. 2nd and 98th percentile) of all TCP variables used was investigated. Additionally, TCP flows with non-standard conditions according to the following conditions were excluded and investigated:

1. RST packets sent in either direction.
2. More than a single SYN/FIN sequence exchanged in each direction.
3. Data packets in the reverse direction.

4. Non-HTTP traffic.
5. Flows with small average MSS (less than 1400 bytes).

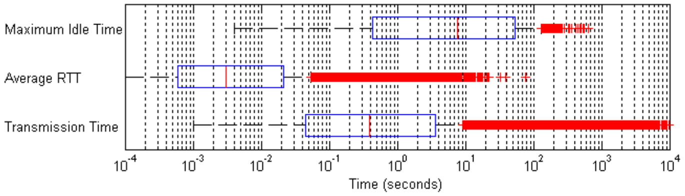


Figure 2: Box-and-whisker diagrams of TCP time parameters (Plymouth University Traffic

4 Results and Analysis

The following sections demonstrate all results obtained from both the mathematical and neural network models developed in MATLAB, for lossless and lossy traffic.

4.1 Lossless Dataset

When considering all valid flows, the regression value obtained from the mathematical model was 0.3216, and from the neural model was 0.7680. As shown in Figure 3, the distribution of scattered actual and estimated transmission time for the mathematical model shows a relatively small subset of samples following the ideal fit line (Y=T), while the majority of scattered samples are well distributed below this line with high residual values, which indicates no account for any possible additional time (idle time) within the lifespan of the connection. On the other hand, the neural model seems to be accounting for this possible additional time and provided an evenly distributed scattering above and below the ideal fit line (Y=T). The MSE of performance estimation was 11.8910 and 1.8253 for the mathematical and neural model respectively, which are considered relatively high.

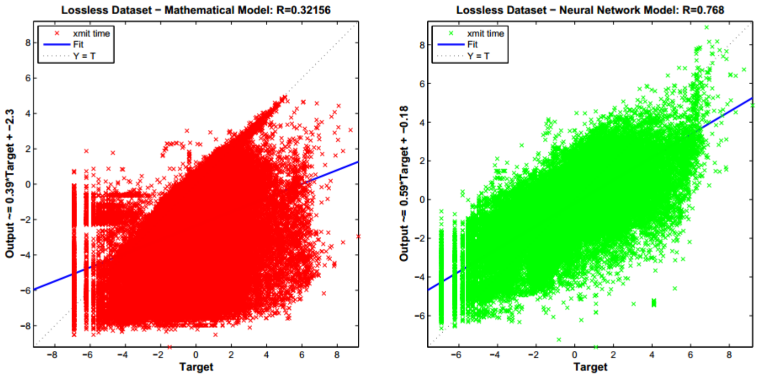


Figure 3 Regression obtained for lossless connections for the combined dataset using both mathematical and neural network model.

Gradually excluding flows with high idle time improved estimation accuracy, as demonstrated in Table 1. The regression and MSE results obtained when filtering connections with maximum idle time less than twice the average RTT were 0.9892 and 0.0229 respectively for the neural network model and 0.9067 and 0.2220 respectively for the mathematical model. The regression analysis for both models is shown in Figure 4. The uniform scattering of estimated transmission time by both model along the idle fitting line(Y=T) had clearly improved. The CDF for absolute relative error is show in Figure 5. At these near ideal conditions, the neural network model is still providing better accuracy performance.

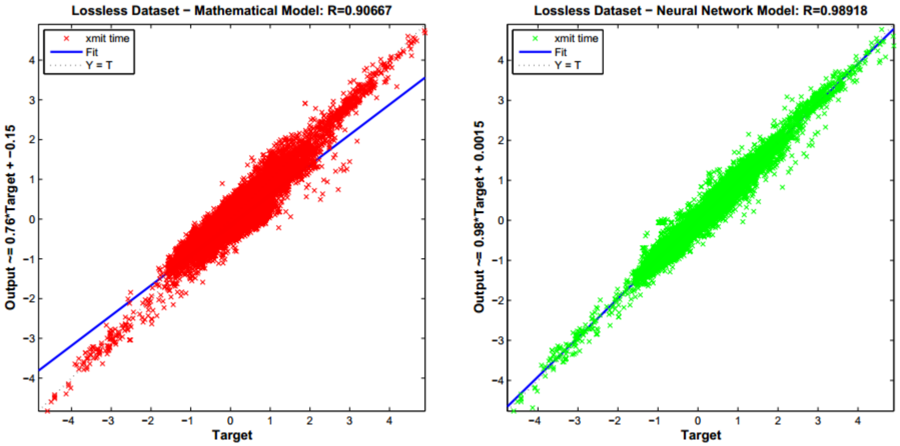


Figure 4: Regression obtained for lossless connections for the combined dataset using both mathematical and neural network model, after filtering connections with maximum idle time larger than twice the average RTT.

Maximum Idle Time to Average RTT Ratio	Number of Samples	Neural Network Model		Mathematical Model	
		MSE	regression	MSE	regression
2	19458	0.0229	0.9892	0.2220	0.9067
6	27342	0.0699	0.9759	0.2945	0.9200
10	30913	0.1108	0.9649	0.4286	0.9019
14	33338	0.1588	0.9510	0.5629	0.8857
18	35627	0.1675	0.9496	0.6982	0.8717
22	37840	0.1995	0.9409	0.8549	0.8574
26	39487	0.2181	0.9363	0.9684	0.8468
30	40848	0.2421	0.9299	1.0821	0.8371

Table 1: Results obtained by gradually excluding flows with relatively high idle time, compared to average RTT for each flow.

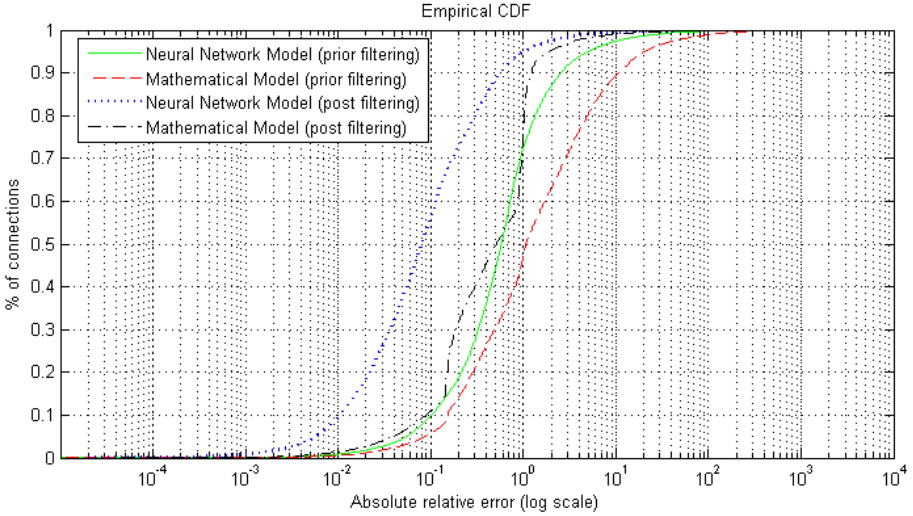


Figure 5: CDF of absolute relative error for lossless connections for the combined dataset, after filtering connections with maximum idle time larger than twice the average RTT.

Filtering statistical outliers and non-standard connections improved performance even more. MSE measure of the neural model decreased from 0.0646 to 0.0325 (50.31%), and regression increased from 0.9778 to 0.9881 (101.05%). While for the mathematical model, MSE decreased from 0.2945 to 0.0921 (31.27%), and regression improved from 0.9200 to 0.9707 (105.51%). The filtering criterion with the most positive effect was to exclude non-HTTP flows. Regression analysis is shown in Figure 6, and the CDF of absolute relative errors in Figure 7.

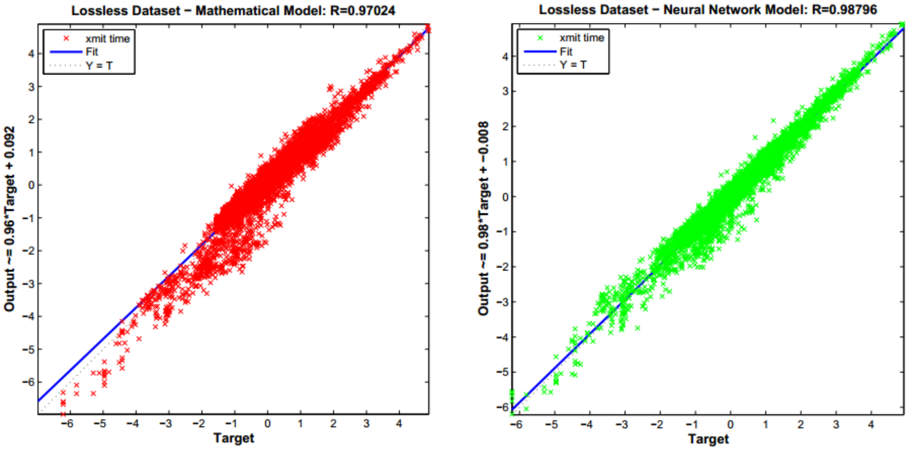


Figure 6: Regression obtained for lossless connections for the combined dataset using both mathematical and neural network model, post filtering non-standard TCP connections.

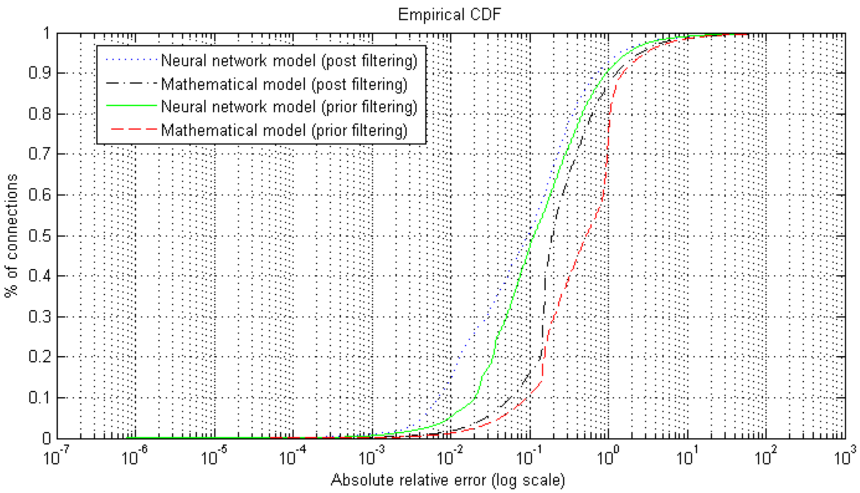


Figure 7: CDF of absolute relative error for lossless connections for the combined dataset, prior and post filtering non-standard TCP connections.

4.2 Lossy Dataset

For the lossy subset, filtering all sorts of outliers and idle time has improved the MSE of the neural model from 0.0371 to 0.0301 (81.13%), and slightly increased the regression from 0.9857 to 0.9863 (100.06%). As for the mathematical model, MSE decreased from 0.5990 to 0.5381 (89.83%). At this stage of filtering, the variation and inconsistency in performance was observed due to the reduced number of training samples to only 3341 TCP flows, which may have led to over-fitting the model.

4.3 Results from Plymouth University Dataset

The results obtained using the dataset from Plymouth University under same testing conditions are summarised in Table 2.

Filtering Criteria	Number of Samples	Neural Network Model		Mathematical Model	
		MSE	Regression	MSE	Regression
All Valid lossless flows	100000	3.3045	0.7722	19.5918	0.3408
Excluding high idle times and non-standard flows	100000	0.5102	0.8697	0.9951	0.7428
All valid lossy flows	57299	1.3533	0.8697	12.2968	0.5886
Excluding high idle times and non-standard flows	1913	0.1066	0.9828	0.7173	0.9419

Table 2: Summary of results obtained using the dataset from Plymouth University

5 Conclusions and Future Research

At all stages of modelling and testing, the neural models have provided better accuracy in estimating TCP throughput with respect to the mathematical model.

The observation made to the estimation of transmission time as resulted from the neural model and how the model in way anticipated for the idle time periods in TCP connections suggests the modification of available mathematical models to possibly include an additional average additional time to the total transmission time. This average could result from a function of average RTT, loss rate and congestion window. The application of such modified model could be implemented and evaluated in a simulated environment such as (NS2) to study the effect on congestion window when resuming data transfer after an idle time period. In this research, only the maximum idle time as calculated by tcptrace was considered. Although this value may give a good representation of total idle time, specially using AI-based methods, more research can be done to modify the output from tcptrace to iteratively evaluate the total idle time during the complete lifetime of a TCP connection, and consider this value as input at neural network modelling stages. This is expected to provide better estimation accuracy.

It was found difficult to identify TCP algorithm for manual analysis and traces investigation. A proposed approach is to identify the implemented TCP congestion algorithm used in captured TCP traffic in order to investigate how each implementation deals with the presence of idle time, and how congestion window is modified after the occurrence of an idle time period. Hence, a comparison could be done between different TCP congestion implementations and evaluate how each implementation performs in finding the ideal congestion window after an idle time, which should result in faster transmission after these idle time periods.

6 References

Cardwell, N., Savage, S. and Anderson, T. (2000), Modeling tcp latency, pp. 1742–1751.

Freeman, J. A. and Skapura, D. M. (1991), Neural networks: algorithms, applications, and programming techniques, Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA.

Ghita, B. and Furnell, S. (2008), ‘Neural network estimation of tcp performance’, International Conference on Communication Theory, Reliability, and Quality of Service 0, 53–58.

He, Q., Dovrolis, C. and Ammar, M. (2007), ‘On the predictability of large transfer tcp throughput’, Comput. Netw. 51(14), 3959–3977.

Mirza, M., Sommers, J., Barford, P. and Zhu, X. (2010), ‘A machine learning approach to tcp throughput prediction’, IEEE/ACM Trans. Netw. 18(4), 1026–1039.

Shah, S., Rehman, A., Khan, A. and Shah, M. (2007), Tcp throughput estimation: A new neural networks model, in ‘Emerging Technologies, 2007. ICET 2007. International Conference on’, pp. 94 –98.

Routing Protocol Convergence Comparison using Simulation and Real Equipment

D. Sankar and D. Lancaster

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

Abstract

Routing protocol is one of the significant factor in determining the quality of IP communication. RIP, EIGRP and OSPF are the dominant interior gateway routing protocols. Factors that discriminate different routing protocols are convergence duration, ability to select the best path among the different routes and the amount of routing traffic generated. The convergence time is one of the key factors which determines performance of the dynamic routing protocol. The primary objective of this paper was to deliver an in depth understanding of Interior Gateway Routing Protocols (RIP, EIGRP and OSPF) and compare the convergence duration of different routing protocol. We also analyse how convergence duration affect the quality of realtime application using OPNET simulation tool and real equipment.

Keywords

Routing Protocols, Convergence Duration, RIP, EIGRP, OSPF, OPNET.

1 Introduction

Routing is selecting the best path from a source to a given destination. It can be done by means of routing protocols that are based on various routing algorithms (Kurose and Ross 2010). Routing protocols are broadly classifieds as “Interior Gateway Routing Protocols and Exterior Gateway Routing Protocols”(Ivener and Lorenz 2004). Most popular interior gateway routing protocols are RIP, EIGRP and OSPF. They are used for routing within an autonomous system (Ayub, Jan et al. 2011). Factors that discriminate different routing protocols are their swiftness to adapt to the changes in the network called the convergence, capability to select the optimal path among the different routes and the amount of routing traffic generated (Thorenoor 2010).

This research is a comparative study of convergence duration of different routing protocol and how it affects the quality in realtime application. We make this study by designing similar scenarios and implement it both in simulation and real equipment with realtime application.

Our Research questions are follows:

I. Analyse how quickly RIP, EIGRP and OSPF adapt to network changes.

II. How network convergence affects realtime application performance. Convergence Duration is the time it takes by a group of routers in a network to come to an agreement on which links are up/down, on which links are faster and which are the best path to every destination. Performance of the realtime application can bemeasured using the performance metrics like end to end delay, jitter and the amount of traffic lost during re-convergence.

In the first phase of our research we design a network model in OPNET and create three same scenarios with RIP, EIGRP and OSPF respectively. In all three scenarios we observe the network convergence behaviour and analyse how it will affect the packet loss and quality of realtime application. Second Phase of our project includes the design of a network model using real equipment and configure with RIP, EIGRP and OSPF. In all three scenarios we observe the network convergence behaviour and analyse how it will affect the packet loss and round trip time.

"Optimised Network Engineering Tool (OPNET)" will be used to measure and analyse the performance of routing protocol in simulation. In the real equipment experiment we used Cisco routers to configure the network topology.

2 Routing Protocol Overview

Routing protocol are classified into following groups based on their characteristics: Static routes are administratively defined routes and will not change until the administrator override it (Ivener and Lorenz 2004). A routing protocol is said to be dynamic routing protocol, when it follows predefined rules defined by the routing algorithm, exchange routing information, and selects the optimal path based on the routing algorithm it uses. Classful routing protocols does not incorporate the subnet mask details along with the routing updates so the subnet mask should be same throughout the entire network. In Classless routing, routing updates includes the subnet mask details and it support VLSM. Distance vector routing protocols are centred with the distance and vector/direction of the destination. Link-State routing protocols offer a greater scalability and quick convergence compared to distance vector routing protocol.

2.1 Routing Information Protocol (RIP)

RIP is one among the first distance vector routing protocols designed and is still popular because of its simplicity and extensive support. Important characteristic of RIP is that it uses hope count as the metric for the best path selection. The route with hope count greater than 15 is considered as unreachable. RIP sends its routing table to all of its neighbours as a broadcast every 30 seconds. The Data part of the RIP routing protocol is encapsulated into a UDP segment and the source and destination port is set to 520. RIP uses broadcast address 255.255.255.255 as the destination address (Graziani and Johnson 2008).

2.2 Enhanced Interior Routing Protocol (EIGRP)

“Enhanced Interior Gateway Routing Protocol (EIGRP)” is a Cisco proprietary routing protocol and operate only on cisco routers. Cisco design EIGRP in 1994 and it is a fast converging and extremely scalable routing protocol for medium and large scale computer networks. EIGRP supports classless inter domain routing (CIDR), variable length subnet masking (VLSM) and also legacy protocols like Novell NetWare, Internetwork Packet Exchange (IPX) and AppleTalk. The key feature of the EIGRP is DUAL. All route calculation in EIGRP is managed by DUAL.Topology table is created by the DUAL finite state machine using the information collected from neighbour routers. From the information available from the topology table DUAL calculates the best route to the destination and makes that path as the successor. DUAL also calculates the feasible successor (second loop free best path) if available. The EIGRP composite metrics consists of Bandwidth, load, reliability and delay. EIGRP keeps information about routes and network topology details in three different tables called neighbour table, topology table and routing table.

2.3 Open Shortest Path First (OSPF)

“Open Shortest Path First (OSPF)” is a link-state routing protocol. It uses SPF (Shortest Path First) algorithm to calculate the best path to a destination in a network. OSPF is a widely preferred non-proprietary routing protocol because of its significant scalability. OSPF keeps information about all the networks in its topology table. OSPF has a hierarchal structure. To run OSPF, the router needs to have a more powerful processor and more memory. OSPF packet header is included in every frame and it contains the source and the destination address. OSPF uses multicast address 224.0.0.5 or 224.0.0.6 as the destination address. To indicate it is an OSPF packet the protocol field is set to 89 (Graziani and Johnson 2008). OSPF rely on 5 distinct types of OSPF LSP’s to distinguish their neighbours and to update the link-state routing informations. It has a hierarchical design. Every router depends on their position in the network have a specific role. Different types of OSPF routers are Internal router, Backbone router, Area border router and AS Boundary routers (Zottmann 2000). OSPF uses cumulative bandwidth from the source interface to the destination interface to calculate the cost. It does support VLSM.

3 Simulation Experiment Setup

In this research, to design the network model we used OPNET Modeler V 17.1.A. To obtain the desired statistics and analyse the RIP, EIGRP and OSPF routing protocol we designed three different scenarios using cisco 3600 router, Ethernet server, Client PC, 100 Base T Ethernet link, 10 Base T Ethernet link.

Experiment testbed is configured on the geographical outline of Europe. We placed each router in London, Amsterdam, Frankfurt, Berlin and Stockholm. An ethernet server is placed in London and the client PC is configured in Stockholm.

An Application Definition is used to generate the application traffics. In this paper we used both video and voice traffic. The video traffic we used is a multimedia video stream of 128x120 pixel video frames and we used video with different frames per second to study the effect of packet loss with different transmission rate. The Audio traffic used is built in PCM quality speech.

The first network scenario is configured with RIP routing protocol. The same model is then duplicated and configured with EIGRP and OSPF. We configured the network topology in such a way that all the routing protocol will select the path London->Amsterdam->Stockholm in the beginning. A link failure is configured between the link London and Amsterdam at 300 sec of the simulation. This will force the router to re-converge to the new path London->Frankfurt->Berlin->Stockholm. The Server is connected to the London router and the client Pc to the stockholm router. Different scenarios are used for Video and Audio traffic.

4 Simulation Result and Discussion

In order to compare three different routing protocols, we measure the following: performance metrics, convergence duration, routing protocols traffic, End-to-End delay in video/voice traffic, and number of packet loss during the re convergence.

Routing Protocol	Initial Convergence (sec)	Re-Convergence (sec)
RIP	11.010	8.66
EIGRP	5.018	0.025
OSPF	10.75	5.01

Table 1 Convergence Duration using simulation

Initial convergence duration of EIGRP is better compared to OSPF and RIP and RIP takes a long time to converge. When a network change occurs EIGRP re-converge in milli seconds where RIP and OSPF takes more time, as shown in table 1.

In order to measure how the convergence duration affect the quality of the real time application we now measure the packet loss, end to end delay and the jitter with different routing protocols.

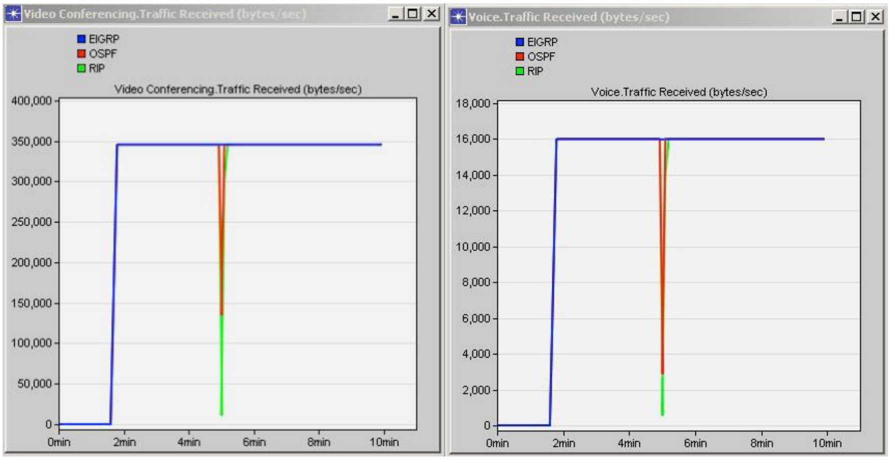


Figure 1: Video and Voice Traffic Sent and received (bytes/sec)

The above figure shows that when the link failure happens the packet loss percentage of RIP becomes high compared to the other two routing protocol. This is because RIP will take more time to re-converge and it may cause the buffer overflow which eventually leads to packet loss. Since the EIGRP re-converge in sub seconds the packet loss percentage is very less compared to OSPF and RIP as we expected.

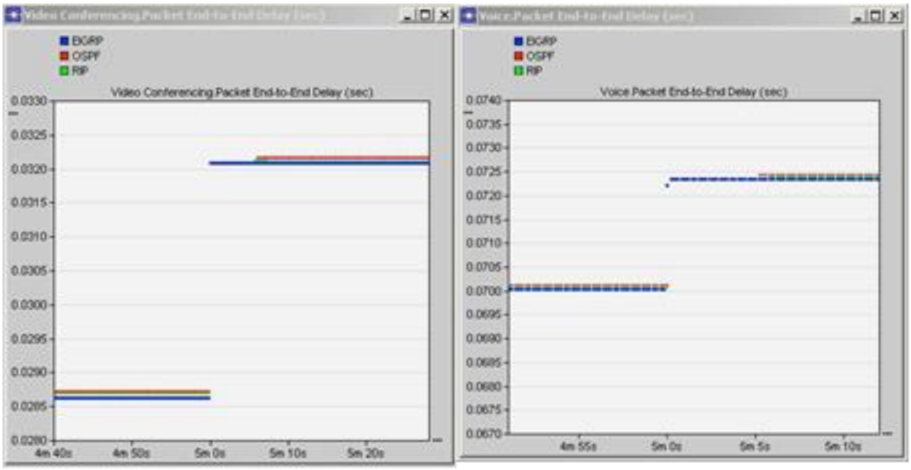


Figure 2: Video and Voice End to End Delay with link fail

End-to-end delay in the EIGRP network is slightly less than the RIP and the OSPF network before and after the link failure.

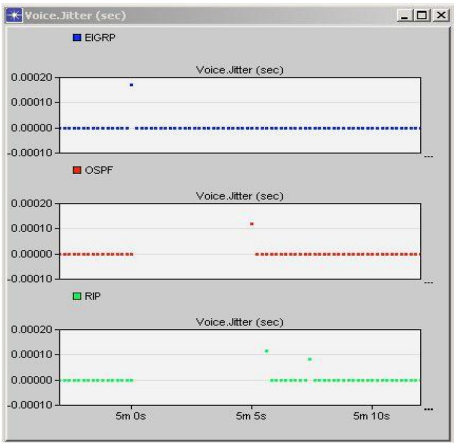


Figure 3: Voice Jitter with Link Failure

The above figure shows the voice jitter when the link failure occurs. When there is no link failure jitter in all the three routing protocol is null. In case of link failure the jitter value of the EIGRP goes to higher than OSPF and RIP.

5 Real Equipment Experimental Setup

In order to investigate the performance of different routing protocols, we set up a experimental topology as shown in the figure 5. In this experiment we used five cisco 2811 routers connected using the serial link and the two clients are connected to the router R1 and R3 using 100 Base T Ethernet link respectively.

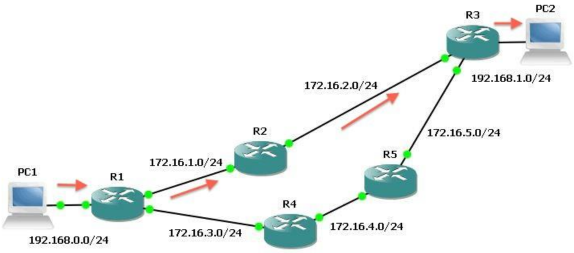


Figure 4: Experiment Testbed

To analyse how the routing protocol behave to a sudden network change, we fail the link between router 1 and 2 using the shutdown command in the respective interface. It is not easy to measure the convergence duration in the real equipment so we generate UDP packets using a network packet generator and send from client 1 to client 2 at different transmission rate and at client 2 we capture all the packets received using Wireshark. Using the amount of packet lost and transmission speed we measure the convergence duration.

6 Result and Discussion

Initially we measure the convergence duration using the ICMP packets and the result shows that RIP, EIGRP and OSPF took 14, 3 and 6 second respectively to converge. In order to calculate more accurate convergence duration we conduct the following experiment. Using the packet generating software (Ostinato packet generator) we created dummy UDP packets with the source address as PC1 address and destination as PC2 address. The packets are sent from the PC1 to PC2 with different transfer speed (05 pkt/sec, 10 pkt/sec, 15 pkt/sec, 20 pkt/sec, 25 pkt/sec and 30 pkt/sec) and calculate the number of packet lost every time. In every experiment ten seconds after transmission is started, we fail the link between routers R1 and R2. All the packets received by PC2 are captured using the Wireshark. The captured packets are analysed and the number of packet lost during the re-convergence of the routing protocol is measured and calculated the convergence duration.

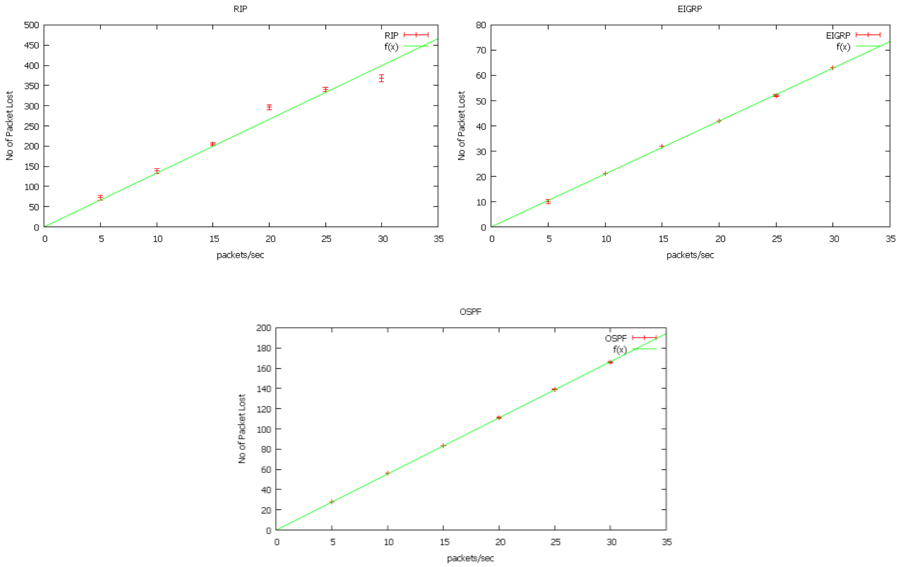


Figure 5: RIP, EIGRP and OSPF Packet Loss

The measured results show that the number of packets lost will increase linearly as we increase the number of packets transmitted. For every transmission rate we repeated the experiment for six times, and calculated the standard deviation and plotted in the graph (shown in figure 5). The time it takes to re-converge this topology is the aggregate of the time taken to detect the link failure of a valid forwarding path and the time it takes to update routing tables and related CEF tables with the new routing details. The measured convergence duration in the real equipment is shown in table below.

Routing Protocol	Re-Convergence (sec)
RIP	13.66
EIGRP	2.12
OSPF	6

Table 2: Convergence Duration using real equipment

The average RTT of an IP packet for different routing protocols is measured using the ICMP packets. The time difference between the request and the reply will give us the RTT.

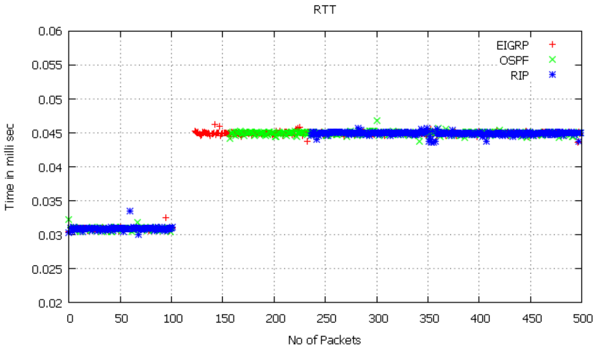


Figure 7: Round-trip Time

The experimental result shows that the average round trip time of the packets in the network using OSPF protocol is slightly less than the network with EIGRP and RIP routing protocol. The scale of difference in RTT is in micro seconds, which in-fact does not have significant impact on application performance. This small variation is possibly because the hello packets that are sent by the OSPF are smaller than EIGRP and RIP and this will reduce the overhead in the router and in turn reduce the delay.

7 Conclusion

In this research, first we compare the routing protocols in terms of convergence both using simulation and realtime and we found that the re-convergence time for EIGRP is much quicker than all other routing protocols. Convergence duration of all routing protocol shown in the simulation is lesser than the convergence duration we measured using real equipment. Analysis using the network simulator shows that EIGRP re-converge within milli seconds but in real equipment it took around 2 seconds. This is possibly because simulator will not count the time it takes to identify and detect the link failure of a valid forwarding path. RIP takes long time to converge both in network simulator and in real equipment compared to other protocols. Convergence time of RIP in the real equipment is suffered from a small variation. This may be because RIP routers send triggered update only to the failure interface and depends on the moment the link failure happen router will converge at different time. Also the convergence time will vary depending on the size and design of the network.

Since the time to re-converge the EIGRP network is lesser, both in simulation and real equipment, packet loss in the EIGRP network is very low compared to the other routing protocol. Packet loss is a significant factor in determining the performance of realtime applications. In order to analyse how packet loss vary with different transmission rates, we transfer different traffic with different transmission rate both in simulation and realtime. The result shows that packet loss linearly increases as the transmission speed is increased.

In this thesis, among the different findings the most significant one is the superior convergence of EIGRP compared to RIP and OSPF both using simulation and real equipment.

8 References

Ayub, N., F. Jan, et al. (2011). "Performance Analysis of OSPF and EIGRP Routing Protocols with Respect to the Convergence." European Journal of Scientific Research 61(3):434-447.

Graziani, R. and A. Johnson (2008). Routing Protocols and Concepts, CCNA Exploration Companion Guide, Cisco Press.

Ivener, R. and J. Lorenz (2004). CCNP 1 : advanced routing, companion guide. Indianapolis, Ind., Cisco Press.

Kurose, J. F. and K. W. Ross (2010). Computer networking : a top-down approach. Boston, Addison-Wesley.

Thorenoor, S. G. (2010). Communication Service Provider's Choice between OSPF and IS-IS Dynamic Routing Protocols and Implementation Criteria Using OPNET. 2010

Second International Conference on Computer and Network Technology (ICCNT). Zottmann, H. (2000). "OSPF -- Scalable Autonomous System Routing." from http://www.cellsoft.de/telecom/autonomoussystemrouting.htm.

Application of LDPC Codes to Networks

R. Bijjargi, M.A. Ambroze and B.V. Ghita

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

Abstract

Internet is growing very fast and it's rapid. At present internet is used by everyone for one or the other reason. Data is sent from source to destination in the form of packets. Packets are the small pieces of original data which contains original data along with header information. Each and every packet has header, which contains the information like source and destination address, mac address, etc.

Original data is sent from source to destination over network. But it is no guarantee that data will reach the destination without any errors that is it will not be corrupted. It may be corrupted and may contain some noise in it. Therefore error correcting codes are implemented in case of data transfer to avoid the data corruption.

Error correction codes are applied on data bits. But in the proposed project error correction codes are tried to implement on packet loss. If there i a packet loss then receiver will send a request to source for retransmission. This will lead to a network traffic and congestion over network. Using error correcting codes lost data is recovered by destination without asking for retransmission.

To avoid the retransmission original data is sent with overhead. Size of the overhead is less, definitely less than the lost data size. Data encryption and decryption is performed using Hamming Code to recover the lost data. As huge the Parity Matrix is less overhead will be transferred. Maximum 25% of the lost data can be recovered. To recover lost data buffer should contain all the remaining data along with parity data.

Keywords

Encryption, Decryption, Congestion, Network Traffic, Delay, Packet Loss, Buffer Size, Overhead.

1 Introduction

Invention of the Computer changed the whole world and networking is complemented it in a great way. Networking is started with ARPANET and grown rapidly. J C R Licklider of MIT wrote series of memo discussing about "Galactic Network" concept in the year 1962. In his concept he clearly mentioned that computers are interconnected and anybody from anywhere in the world can access the data which is present in it. It replicated very much about the present Internet (Internet Society,2011). In the beginning data was transferred in network through circuit switching. Later packet switching is introduced and it captured whole market within no time. Compare to the older technique and methods of data transfer, present data transfer rate is much higher. Still research is going on to make it more accurate, better and faster. Error correcting codes have played an important role in the case of data transfer and is contributed by Claude E. Shannon.

Information theory took birth in the year 1948. In this year Claude E. Shannon published his thesis. He is the first person who gave the limits of reliable data transmission over the unreliable channels and provided the solution to achieve the limits. Like Turbo Codes, Low Density Parity Check (LDPC) codes form another class of Shannon Limit. LDPC codes were first discovered by Robert Gallager in the early 1960's in his MIT Ph. D. Dissertation. Low-density parity-check codes are a class of linear codes with sparse parity-check matrix (Lin and Costello,2004).

In case of data transmission over the network entire data is divided into number of packets. Packets contain original data along with source and destination address, that is IP address and MAC address of source and destination. Router chooses the path for each and every packet to travel and path is decided depending on the routing table. As the packets are transmitted through different path, they reach the destination in different time and in different order. In few cases packets may not reach the destination due to congestion, delay, jitter, etc. So in this case destination request the source to resend the packets which are not received. Therefore source will retransmit the lost packets.

In case of packet loss, lost packets are retransmitted by source to destination. Retransmission will increase the network traffic and leads to congestion. My approach is to avoid the retrans- mission in case of packet loss. First of all will develop a code to encrypt and decrypt the data based on Hamming Code and using C programming language. Hamming Codes are used for error correction by the help of parity matrix. C is a procedure oriented high level programming language.

2 Testbed setup for data transfer

As the whole data can not be sent over network at once. First it will be broken into number pieces called packets. Each packet is maximum size of 1500 bytes. This includes header length which contains source and destination IP address, Mac address, flags, etc.

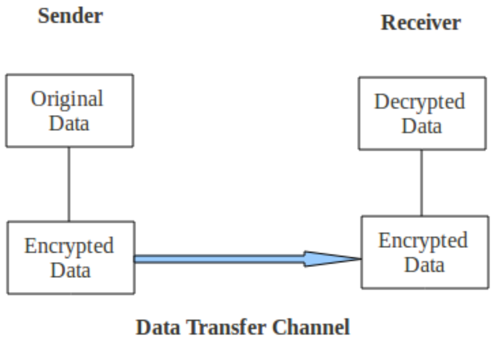


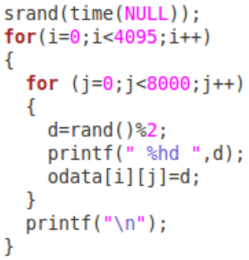
Figure 1: Testbed Setup for Data transfer over network

In the proposed project 1000 bytes of data size is considered excluding header data. Later header part will be added as per the requirement. Figure 1 shows the testbed setup for the data transfer over network.

It is clear from the figure 4.3 that data is encrypted before sending through channel. And it will be decrypted to get the original at the receiver end. Procedure of the data transfer is explained in the following section.

2.1 Procedure

First of all a huge Parity Matrix is generated that is Parity Matrix (12,4095). This Hamming Code is used in both the side that is by sender as well as receiver. The data is encrypted as well as decrypted using the same Parity Matrix (12,4095).



```
srand(time(NULL));
for(i=0;i<4095;i++)
{
  for (j=0;j<8000;j++)
  {
    d=rand()%2;
    printf(" %hd ",d);
    odata[i][j]=d;
  }
  printf("\n");
}
```

Figure 2: Generating Random Data (Kioskea.net, 2011)

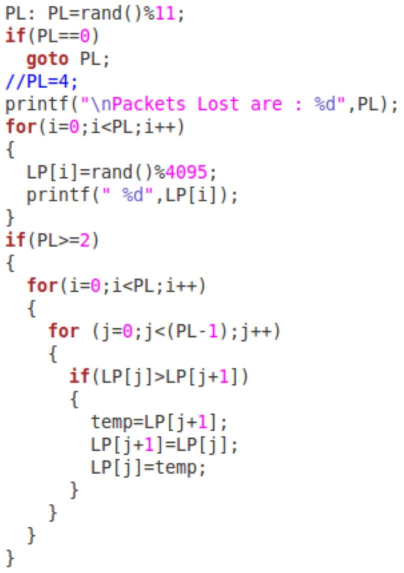
Parity Matrix is generated and saved in a file, this file is kept open and read the data at the time of encryption. The needed data for encryption is generated randomly. To generate random data a code is written. Figure 2 shows the code written for generate random data.

Once the random data is generated, data is encrypted using Parity Matrix. The procedure mentioned in the section 4.3.2 is used to encrypt the data.

Parity Matrix	Data packets	Parity packets	Total No of packets	Recoverable Packets
(3,7)	4	3	7	2
(4,15)	11	4	15	4
(5,31)	26	5	31	8
(6,63)	57	6	63	16
(7,127)	120	7	127	32
(8,255)	247	8	255	64
(9,511)	502	9	511	128
(10,1023)	1013	10	1023	256
(11,2047)	2036	11	2047	512
(12,4095)	4083	12	4095	1024

Table 1: Parity Matrix and Number of packets can be recovered

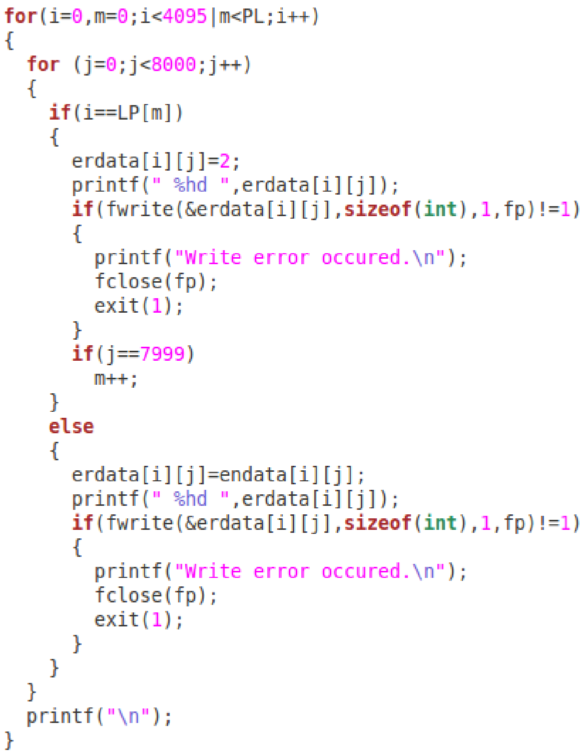
After encryption of data a random number is picked for a packet loss using the function rand(). Each parity matrix can recover a specified number of packets. Table 1 shows the recoverable packets for a particular parity matrix.



```
PL: PL=rand()%11;
if(PL==0)
  goto PL;
//PL=4;
printf("\nPackets Lost are : %d",PL);
for(i=0;i<PL;i++)
{
  LP[i]=rand()%4095;
  printf(" %d",LP[i]);
}
if(PL>=2)
{
  for(i=0;i<PL;i++)
  {
    for (j=0;j<(PL-1);j++)
    {
      if(LP[j]>LP[j+1])
      {
        temp=LP[j+1];
        LP[j+1]=LP[j];
        LP[j]=temp;
      }
    }
  }
}
```

Figure 3: Random Packet Loss and Sorting (Kioskea.net, 2011; Allian, 2011)

A random number is generated using C code for a packet loss. Later those many a random number is chosen between 0 to 4095. After generating all the random number they are sorted using bubble sort. C program for the random number generation for packet loss and sorting them in order is shown in Figure 3



```
for(i=0,m=0;i<4095|m<PL;i++)
{
  for (j=0;j<8000;j++)
  {
    if(i==LP[m])
    {
      erdata[i][j]=2;
      printf(" %hd ",erdata[i][j]);
      if(fwrite(&erdata[i][j],sizeof(int),1,fp)!=1)
      {
        printf("Write error occured.\n");
        fclose(fp);
        exit(1);
      }
      if(j==7999)
        m++;
    }
    else
    {
      erdata[i][j]=endata[i][j];
      printf(" %hd ",erdata[i][j]);
      if(fwrite(&erdata[i][j],sizeof(int),1,fp)!=1)
      {
        printf("Write error occured.\n");
        fclose(fp);
        exit(1);
      }
    }
  }
  printf("\n");
}
```

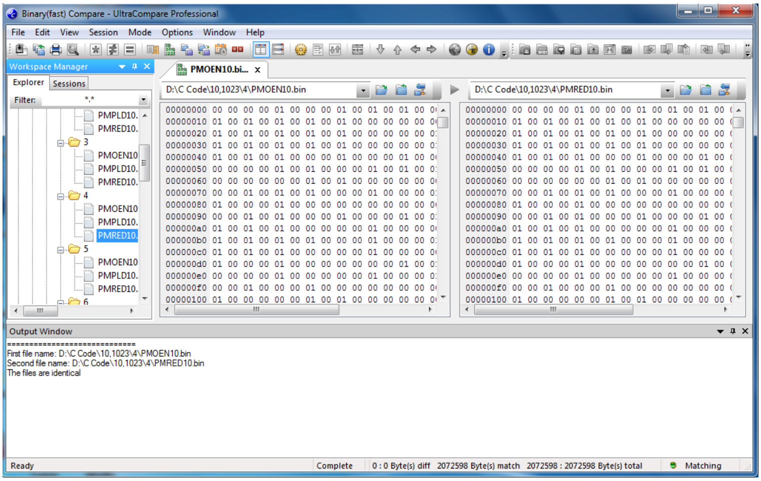
Figure 4: Implementation of Packet Loss through Code

Once all the numbers are set then the packets are loss is performed manually. This is done by using C program. As mentioned earlier packet loss or corrupted data is indicated by '2'. By using for loop lost packets are identified and they are replaced by '2'. The C program for manual packet loss using C code is shown in Figure 4

After performing the packet loss manually lost data is recovered using C code. Here a point is to be considered that a buffer size will be same as total number of packets sent including parity packets. So data is recovered only when all the packets are received. That is minimum required packets to recover the data is 75%. Because maximum data recovered is 25% in case of packet loss. The lost data is not requested for retransmission.

2.2 Results

Original data is huge and it is tedious task to verify the original with recovered data. Therefore a software tool called Ultra Compare Profession is used to compare the data. It will display clearly where the difference, if there is any difference. The result of the comparison is shown in the output window of the software which is present bottom of the window. The comparison result of the recovered data and original data is shown in figure 5



D:\C Code\10,1023\4\PMOEN10.bin

```
00000000 00 00 00 00 01 00 00 00 01 00 01 00 01 00
00000010 01 00 01 00 01 00 01 00 01 00 00 00 00 00
00000020 01 00 01 00 01 00 01 00 01 00 00 00 00 00
00000030 01 00 01 00 01 00 01 00 01 00 00 00 00 00
00000040 01 00 01 00 01 00 00 00 01 00 00 00 01 00
00000050 00 00 00 00 01 00 01 00 00 00 01 00 01 00
00000060 00 00 00 00 00 00 01 00 01 00 00 00 00 00
00000070 00 00 01 00 01 00 01 00 00 00 01 00 00 00
00000080 01 00 00 00 01 00 00 00 00 00 00 00 00 00
00000090 00 00 01 00 01 00 00 00 01 00 00 00 01 00
000000a0 01 00 01 00 01 00 00 00 00 00 01 00 00 00
000000b0 01 00 01 00 01 00 01 00 00 00 01 00 00 00
000000c0 01 00 01 00 01 00 00 00 00 00 01 00 00 00
000000d0 01 00 00 00 01 00 00 00 00 00 00 00 01 00
000000e0 00 00 00 00 01 00 00 00 00 00 01 00 00 00
000000f0 00 00 01 00 00 00 01 00 00 00 00 00 00 00
00000100 01 00 00 00 00 00 01 00 01 00 00 00 00 00
```

D:\C Code\10,1023\4\PMRED10.bin

```
00000000 00 00 00 00 01 00 00 00 01 00 01 00 01 00
00000010 01 00 01 00 01 00 01 00 01 00 00 00 00 00
00000020 01 00 01 00 01 00 01 00 01 00 00 00 00 00
00000030 01 00 01 00 01 00 01 00 01 00 00 00 00 00
00000040 01 00 01 00 01 00 00 00 01 00 00 00 01 00
00000050 00 00 00 00 01 00 01 00 00 00 01 00 01 00
00000060 00 00 00 00 00 00 01 00 01 00 00 00 00 00
00000070 00 00 01 00 01 00 01 00 00 00 01 00 00 00
00000080 01 00 00 00 01 00 00 00 00 00 00 00 00 00
00000090 00 00 01 00 01 00 00 00 01 00 00 00 01 00
000000a0 01 00 01 00 01 00 00 00 00 00 01 00 00 00
000000b0 01 00 01 00 01 00 01 00 00 00 01 00 00 00
000000c0 01 00 01 00 01 00 00 00 00 00 01 00 00 00
000000d0 01 00 00 00 01 00 00 00 00 00 00 00 01 00
000000e0 00 00 00 00 01 00 00 00 00 00 01 00 00 00
000000f0 00 00 01 00 00 00 01 00 00 00 00 00 00 00
00000100 01 00 00 00 00 00 01 00 01 00 00 00 00 00
```

```
==============================
First file name: D:\C Code\10,1023\4\PMOEN10.bin
Second file name: D:\C Code\10,1023\4\PMRED10.bin
The files are identical
```

```
Ready    Complete    0 : 0 Byte(s) diff   2072598 Byte(s) match   2072598 : 2072598 Byte(s) total    ● Matching
```

Figure 5: Data Comparison using Ultra Compare Software

Table 2 shows the total number of packets sent over network. It also includes the overhead and the recoverable data using the over head.

Total No. of Packets	Overhead(%)	Recoverable Data (%)
7	42.86	28.57
15	26.67	26.67
31	16.13	25.81
63	9.52	25.40
127	5.51	25.20
255	3.14	25.10
511	1.76	25.05
1023	0.98	25.02
2047	0.54	25.01
4095	0.29	25.01

Table 2: Total no. of packets, overhead and recoverable data in %

Using the data present in Table 2 a graph is drawn and which is shown in figure 6. From the graph it is clear that the maximum data recovery is 25%. Even though how big / huge parity matrix is used to for encryption and decryption of data. But as the Parity Matrix size is increased the overhead is reduced. Therefore we can use huge parity matrix for data recovery so that it will carry less overhead.

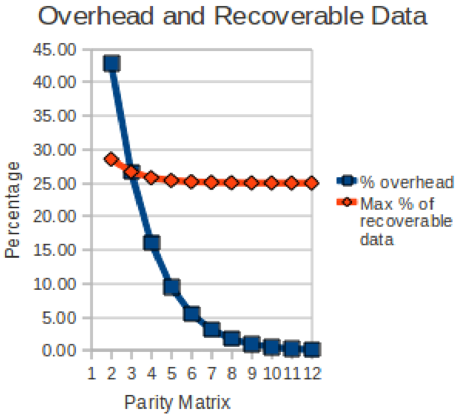


Figure 6: Graph for Overhead and Data Recovery

3 Conclusion

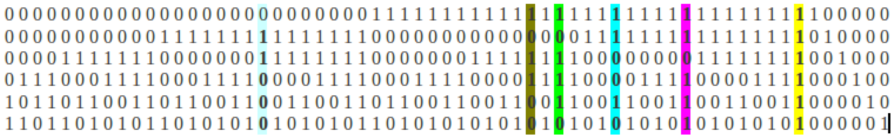
As the internet is growing so fast and almost all the work is done through internet. Message passing, media, entertainment, everything is done through network using computers. Present circumstances everyone want the work done quickly and faster, without any errors. To achieve the same concept error correcting codes should be implemented in the network while data transmission. Even though there are number of error correcting codes are present in market, proposed project tried to implement a error correcting code for packet loss. It is using a very simple and easy code to provide the most accurate answer. So that there should not be any retransmission of data in case of data loss. If this is achieved then surely it will speed up the data transfer rate. Also avoids the congestion and network traffic to some extent by stopping retransmission of lost data.

4 Limitations

As nothing is perfect and all matter have its own limitations. Proposed project also got some limitations. The main limitation is it has to carry some additional data along with original data. This additional data is used to recover the lost data.

The main and important limitation of the proposed project is, it is unable to recover more than

5 packets. Even though a huge Parity Matrix is used for encryption and decryption of data. The problem associated with this is, it is can not recover a lost data because one or the other data is also lost which is used to recover the lost data.



```
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0
0 0 0 0 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 1 0 0 0
0 1 1 1 0 0 0 1 1 1 1 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 0 0
1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 0
1 1 0 1 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0 1
```

Figure 7: Limitation for a Hamming Code

Figure 7 shows that the 6 bits are lost and are highlighted in different colors. When the program try to recover any of the lost bit then one or the other is lost whose value is need to calculate the lost bit value.

5 Future Work

An important problem associated with Hamming Code is that it can not recover more than 5 packets. It is mainly due to random data in matrix that parity matrix. No matter how huge parity matrix is but the problem remains same. To over come this problem different matrix should be generated which will over come this problem.

In the future work a point to be considered to reduce the overhead size as much as possible.

6 References

Allian A., (2011), Sorting Algorithms - Bubble Sort [accessed on 26-09-2011] http://www.cprogramming.com/tutorial/computersciencetheory/sorting1.html

Internet Society (2011), " Brief History of the Internet" [accessed on 18-12-2011] http://www.internetsociety.org/internet/internet-51/history-internet/brief-history- internet

Kioskea.net (2011), Generating random numbers with rand() Share , [accessed on 25-09-2011] http://en.kioskea.net/faq/878-generating-random-numbers-with-rand

Lin S.; Costello, D. J. (2004) 'Low-Density Parity-Check Codes in Error Control Coding, Pearson Education, Inc., USA: 851-947.

Oualline S., (1997), Practical C Programming 3rd Edition, O Reilly & Associates, Inc., CA

Schildt H., (1997), Teach Yourself C ,Third Edition, McGraw-Hill, USA.

Section 4

Robotics

Graphical Interface for Watermarking

R. Amiot and M.A. Ambroze

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

Abstract

An application was coded in C++, using Qt libraries, to run watermarking algorithms and attacks on images. Two algorithms were used: random LSB Insertion, and informed embedding. Four attacks were implemented: cropping, rotation, compression, blur. The output image after embedding can be compared to the cover work with the help of zooming and panning around.

Keywords

Watermarking, GUI, C++, Qt, trellis, informed embedding, convolutional code.

1 Introduction

Digital Watermarking is an important field for a variety of reasons; most of these have to do with protecting content producers. It is mainly applied to security and copyright (Cox & a, 2008). The field is very vast, allowing one, for example, to use the timing of packets over a network to encode information.

This application more specifically implements an algorithm modifying the pixel contents of a cover image, embedding an arbitrary message. The original image is not required to decode the message.

The design goals were to have an efficient interface, allowing to one select an algorithm and parameters, to visually witness the results of embedding on the image or to use various attacks on images.

This application was developed in C++, using Qt technology for the GUI, file IO, image edition and such. Qt was chosen for its versatility and portablity (tested on Windows XP SP3; and Mac Os X 10.5 and 10.6). The executable needs about 20Mb of .frameworks or .dlls to run.

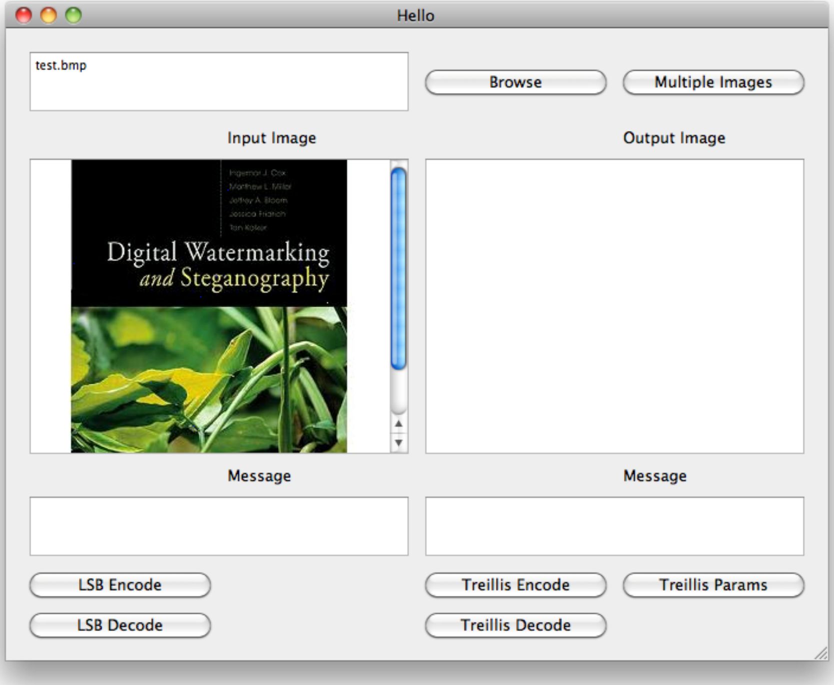
2 UI Features

2.1 Operations on single images

The application can select an image from the user's hard drive with the help of a file dialog. The image is displayed on the left view port.

The user can set parameters, encode a message, or look for one in the image, using either a random LSB insertion algorithm or the Informed Embedding and Coding algorithm from J Cox & al (2004).

Should a message be encoded, the user can compare the output image and the input image: the output is displayed in the viewport to the right. It is possible to zoom and pan around on the images; they will be automatically synchronized. Finally, this window allows access to an important component, the Batch Operations window.

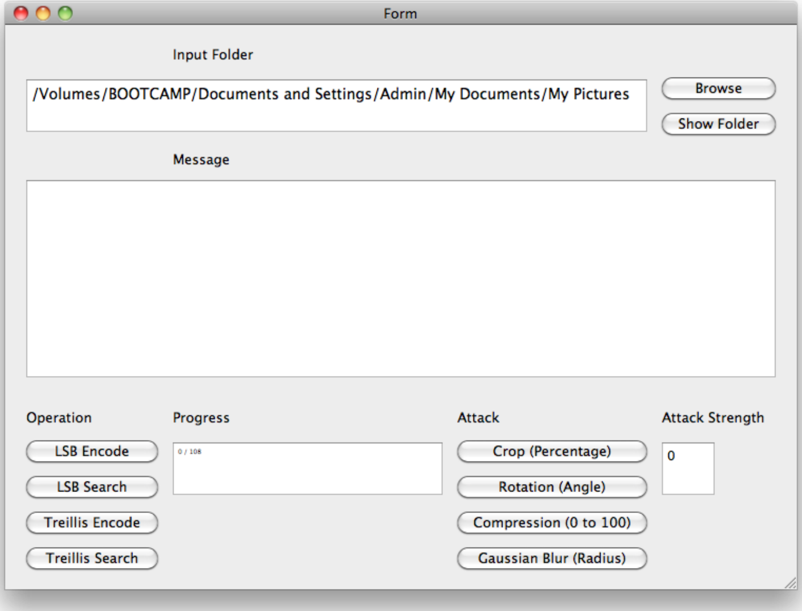


test.bmp

Figure 1: Interface for single images

2.2 Operations on image folders

The application can also work on folders, modifying all images within. It can either embed messages using any of the algorithms, search for a message (this returns the amount of images containing the image for LSB insertion, and the bit error rate for Informed Embedding), or apply an attack: cropping, rotation, compression, gaussian blur. The strength of the attack can be set by the user. There is no image viewport.



Input Folder: /Volumes/BOOTCAMP/Documents and Settings/Admin/My Documents/My Pictures

Progress: 0 / 108

Attack Strength: 0

Figure 2: Interface for whole folders

Given an attack parameter “x”, the image can be

- Cropped vertically and horizontally by x%
- Rotated by x degrees, around the center of the image
- Compressed with a strength x
- Blurred with a radius of x

Modified files, either by embedding or attacks, are saved in a specific subfolder, depending on the modification. The user is kept informed of the progress (eg, “x images done / y total images”).

2.3 Other Considerations

The user is informed of errors, insane parameters, and such by a popup covering the window. This popup closes whenever the user presses any key. File browsing behaviour is different when the operating system changes; it adapts to user habits there, and OS features. For instance, Mac users can get a preview of a selected image by pressing space. This is a very nice Qt feature. The program is CPU bottlenecked.

3 Algorithms

3.1 LSB Insertion

This algorithm randomly accesses pixels and modifies their parity in the blue channel's value according to the bits of the payload message. Decoding accesses the same bits but reads the parities and writes to message bits. This algorithm was modified to have visible effects (the blue channel values can go from 0 ↔ 255) to showcase the input/output comparison. Messages can be of any length, provided the image is large enough.

3.2 Informed Decoding

This algorithm follows what is described in Cox & al, 2004.

- The image's luminance is converted into a frequency representation via 8X8 block DCT.

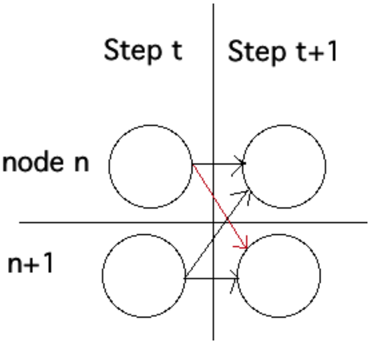


Figure 3: Arcs explanation

- A vector is extracted from the low frequency terms.
- A trellis is built according to user-defined parameters (number of arcs, number of nodes, random seed). This trellis is represented in memory by a set of arcs. Every node is set to have the same number of arcs exiting it than entering it. Arcs do not change over iterations. They have 3 properties: origin node, destination node, and a randomly generated label. In this figure, for the red arc, that would be n, n+1, and (float)rand(). Every arc also encodes either a 0 or a 1.

- A Viterbi decoder (Wesel, 2003) is run and returns the path (set of arcs) that is the most highly correlated with the vector extracted from the image. Correlation is done by comparing bits of the vector term at this step and the label of the arc.

- As each of these arcs encodes a bit, a message can be rebuilt from them.

3.3 Informed Encoding

This works the wau same as informed decoding, except that we only accept paths which encode the desired message. We then have an optimal vector, **g**, which we want to be the most highly correlated with the vector, despite noise.

3.4 Informed Embedding

We consider a “bad vector”, **b**. This vector is the one decoded in the current state of the extracted vector, while adding random noise. The objective is to have **g** decoded instead of many possible **b**s, and the extracted vector is modified toward that objective. Should **g** be more highly correlated than 100 **b** by a certain amount (a user defined target) (every b is slightly different due to noise)**,** the extracted vector is considered acceptable, put back into the image, which is then converted back to pixels and saved. Unfortunately, this part of the algorithm doesn't work in that program: the original paper was not very clear on this step, and no matter the way of interpreting the relevant equations, the modified extracted vector grows less and less correlated with **g** with every update.

4 Conclusions

Despite setup difficulties on Os X, being rather CPU hungry, and some low level quirks, Qt proved ideal for this kind of application: it offered many powerful GUI features, and events, threads, many image operations, easy portability, easy UI layout design. Moreover, it made use of the host OS features.

Algorithm-wise, the coder could not draw results since the final embedding part was not done in time.

Should anyone want to finalize the application, here are some possible suggestions:

- Finalizing the trellis embedding algorithm
- Measuring duration of algorithmic calculations over a batch of images
- Implementing Plots
- Optimization: aside from some light parrallelization on Os X, performance was not considered at all
- Adding a scaling attack.

5 References

Cox, I. J., Miller, M. L., Bloom, J.A., Fridrich, J., Kalker, T., (2008), “Digital Watermarking and Steganography”, second edition, Chapters 1 and 2 Morgan Kaufmann Publishers.

Cox, I.J., Miller, M.L., Doerr, G.J (2004), “Applying Informed Coding and Embedding to Design a Robust, High capacity Watermark”, IEEE Trans. on Image Procesing, 13, 6, 792-807, June 2004.

Wesel, R. D. (2003). “Convolutional Codes”. Encyclopedia of Telecommunications.

Humanoid Robot: Auto-Calibration & Gait Stabilisation

G. Michel and G. Bugmann

Centre for Robotics and Neural Systems, Plymouth University, Plymouth, UK
e-mail: guido.bugmann@plymouth.ac.uk

Abstract

Controlling a biped robot with a high degree of freedom to achieve stable movement patterns is still an open and complex problem. To travel the must quickly between one location to another, the biped must have a robust dynamic gate that is stable under small perturbing external forces. To achieve this goal, a good understanding of the robot used, its tools and performances is needed. This paper will focus on researches and functions made to improve the stabilisation of a gait thanks to feedbacks from accelerometer and gyroscope.

Keywords

Gait, IMU, Time Delay, Feedback

1 Introduction

Humanoid robots have a high potential to support our daily activities in the future, but for the time being they substantially lack in mobility. In order to enhance high-mobility, the humanoid motion should be generated in real time in accordance with the dynamics, but yet no control algorithm has been developed or implemented in a responsive form that allows the above-stated high-mobility. A technical reason is that real time generation needs feedback and a large a lot of computation.

As good as can be a gait, if it does not use any feedback, it is restricted to a close to “perfect” environment, or close. An efficient robot needs to be able to handle variations in his environment, and so to use as much feedback as possible.

Several researches are needed:

- First, measurements of the existing time delays must be made. Indeed, if the delays, whether to execute a command or to get feedback, are too big, it will be quite useless, or impossible, to have any short-term feedback.

- The second important point is to have a good comprehension of “what should happen?” “How should the robot move?” Something defined as “the normal movement”.

- Then, the actual feedback must be understood according to the second point, compared to a basis, in order to find the relation between what the robot detects, and the formulas and ideas developed before, which means know and understand how the robot moves. And also understand the meaning of an unexpected feedback, to know which feedback is linked to which problem.

- Finally the last point is to create algorithms to handle the problems detected, using the comprehension of the feedback and the robot to know what it should do according to its feedback.

2 The Bioloid Humanoid Robot

This robot used is a Bioloid humanoid robot based on the Robotis Bioloid Kit It is equipped with 20 servomotor controlled by a CM-700 controller. It also owns a camera in his head allowing it to use a vision system, which is developed on a beagle-board placed on the front of the robot. The servomotors enable the robot to a high degree a freedom, 20 degree for the 20 motors. The main sensor used on this project on the robot is the Inertial Measurement Unit (IMU) block. It includes a 3- axis accelerometer and a 2-axis gyroscope.

The Gait used by the robot is a dynamically stable gait. This mean that it has a repetitive motion that remains unchanged over a given time of observation or task, and also that the oscillation motion of the legs has to be inherently stable and resistant to small surface defects and changes in surface.

In order to create this stable gait, a fictive grid has been created, parallel to the leg and having the same angle than the hip, to define the positions of the feet. According to those positions, an inverted kinematic model of the legs of the robot is created by approximating the robot legs as a two link system for ease of computation. The accessible plane of operation for each leg is segmented into the grid, and the joint angles are pre-computed for each of these points and saved in a lookup table.

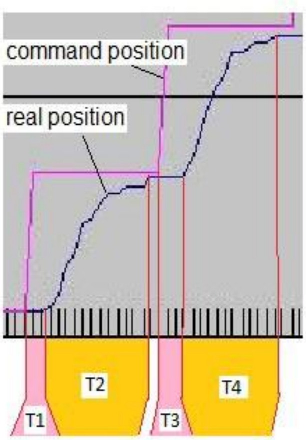
3 Time’s delay

As good as can be a gait, if it does not use any feedback, it is restricted to a “perfect” environment, or close. An efficient robot needs to be able to handle variation in his environment, and so to use as much feedback as possible. To use feedback on a robot, several researches are needed.

First measurements must be done to check the possibility to use feedbacks, did by an examination of the times delay. Knowing the time delay inside the robot allows us a better comprehension of the robot and mainly provide us information on how improve the gate and if it is improvable.

The time delays we are interested in are the delay needed by the robot to start moving a servomotor after have sent a command. And the delay of the feedback returned according to the reality.

Two methods can be used to measure the time delay on the bioloid humanoid robot; using the internal clock of the robot, accurate according to the robot’s frequency, the second one measure it thanks to external electronic systems, so accurate according to those systems.



The first method, using the internal clock of the robot, sends a command to a servomotor every X ticks and reads at each tick the position of this servo. This command is a distance to reach and a speed, the feedback from the servo will show after how many ticks the servo start moving, and how many ticks are needed to reach the distance sent. This will give the sum of all delays, but to know just one of them we need to know the other one, which is impossible just by using the clock.

On the figure, T1 and T3 are the delay we are looking for, the time lost to start moving the servo after a command has been sent. T2 and T4 are the delays to reach the position asked by the controller.

Therefore more tests are needed using electronic sensors. The idea is to use the robot’s LEDs, combined with a light sensor, to calculate the feedback delays. E.g. a LED is turned on when a command is sent and when the motor start moving, reading the difference on an oscilloscope.

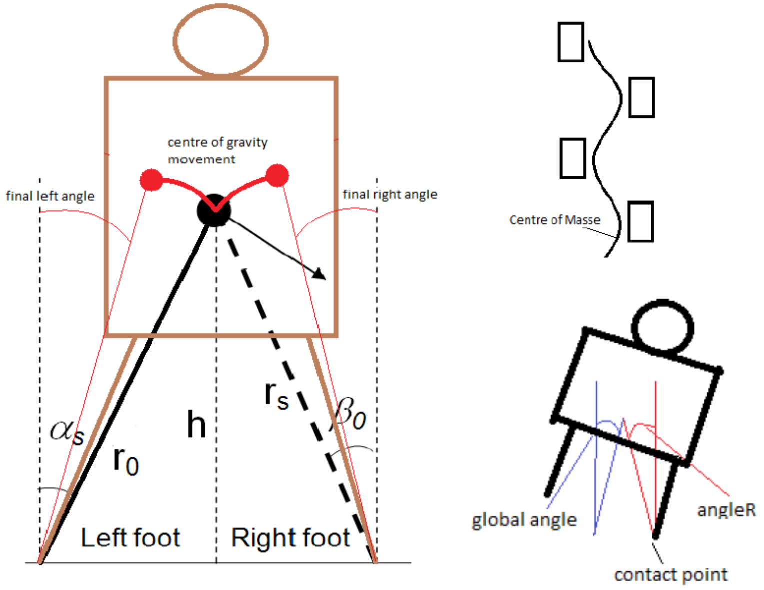
The results from these experiments are variable when using electronics devices or not accurate when using the clock of the robot. However, the results are :

- The time to get feedback from the servomotors is less than 5ms.
- The time to get feedback from the IMU is less than 1ms.
- The time to start moving a servomotor (T1) is less than 32ms.
- The total time delay during the gait (T1 + T2) is about 50ms.

4 Movement of the robot

The basics principles of this robot gait have been developed by Dr. Guido Bugmann to a better comprehension of the current gait. The principle is “a weight shift to one foot to enable the other one to move”. Most concepts are based on the theory of the inverted pendulum, so the robot is considered as being on only one leg with a constant centre of gravity with a distance “r” from the ground.

Formulas were developed to know the current sideways angles of the robot at any moment of the gait. These equation allow us to make a graphic of the theoretical lateral position of the robot, knowing its parameters like weight, size, camber.



global angle(t) = starting contact angle – | contact angle (t) |

Figure 1: Position of the robot

Two angle can be used to know the lateral position of the robot. Those two angles must not be confounded, knowing all accelerations returned from the IMU are according to the global angle while the angular speeds returned are according to the contact points. (see figure 2)

To understand the results from the IMU, which returns accelerations and angular velocity, a new formula has been developed. The accelerations from the IMU are the sum of all accelerations applied on the IMU, thus the accelerations applied on the robot.

$$\boxed{a_{sideways} = a_Y = a_{gravity} + a_{linear} + a_{impact}}$$

$a_{gravity} = g.\sin(\alpha)$ is the acceleration created by the gravity.

$$a_{linear} = \mathrm{r} \, . \, \ddot{\alpha}$$

is the own acceleration of the robot created by the movement, it is an angular acceleration, need to be transform in a linear acceleration: multiply by 2πR/360.

$$a_{impact}$$

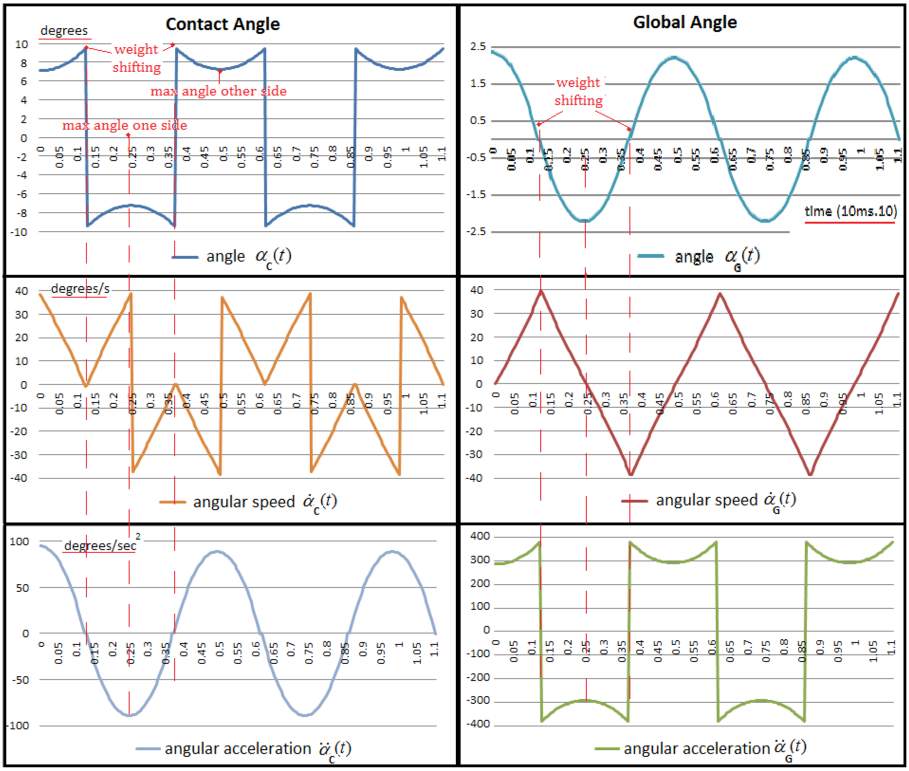
is the acceleration created by the impact of a leg on the floor, else equal to 0.

Using this equation, it is possible to calculate the angle when the impact acceleration is 0.

$$\sin(\alpha) = \frac{a_Y - (2.\pi.\frac{r^2}{360}).\ddot{\alpha}}{g}$$

The angular acceleration $\ddot{\alpha}$ can be calculated by derivating the angular speed return by the IMU, knowing the roll returned is according to the contact angle and this formula is about the global angle.

Therefore we are theoretically able to estimate the angle of the robot in real time using some assumptions (like a constant r) . In reality, due to the time delay and the integration, the angle returned has some delay.



$$\alpha_c(t) = C_1 \exp(pt) + C_2 \exp(-pt)$$

$$\dot{\alpha}_G(t) = pC_1 \exp(pt) - pC_2 \exp(-pt)$$

$$\ddot{\alpha}_G(t) = p^2 C_1 \exp(pt) + p^2 C_2 \exp(-pt)$$

$$p = \sqrt{\frac{g}{r}} \text{ in units of } \frac{1}{\text{sec}}$$

$$C_1 = \frac{p\alpha_0 - w_0}{2p}; \; C_2 = \frac{p\alpha_0 + w_0}{2p}$$

$$\alpha(t=0) = \alpha_0 \quad \text{and} \quad \dot{\alpha}(t=0) = \omega_0$$

$$\alpha_G(t) = 9.46 - |\alpha_c(t)|$$

$$\dot{\alpha}_c(t) = \max \dot{\alpha}_G(t) - |\dot{\alpha}_G(t)|$$

$$\ddot{\alpha}_c(t) = \max \ddot{\alpha}_G(t) - |\ddot{\alpha}_G(t)|$$

$$r = 0.2433 \text{ m}$$

$$\omega_0 = 0$$

$$\alpha_{c0} = 7.1$$

$$\alpha_{G0} = 9.46 - 7.1$$

Figure 2: Theoretical lateral angle, angular speed and acceleration of the robot for its contact and global angle

5 Implemented functions on the robot

5.1 Auto-calibration

The auto calibration created on the robot uses two feedback accelerations from the IMU and feedbacks from six servos, this auto-calibration will enable the robot to start with a vertical position whatever the ground surface.

The first goal of this auto-calibration is to avoid loss of time to calibrate a robot before using it. The auto- calibration developed here allows the user to not having to calibrate the six motors of each leg used for forward movement, neither than having to calibrate the tilt of the robot. The only calibration needed is on the three remaining servomotors of each leg managing the roll and the yaw of the hips and the feet flatness.

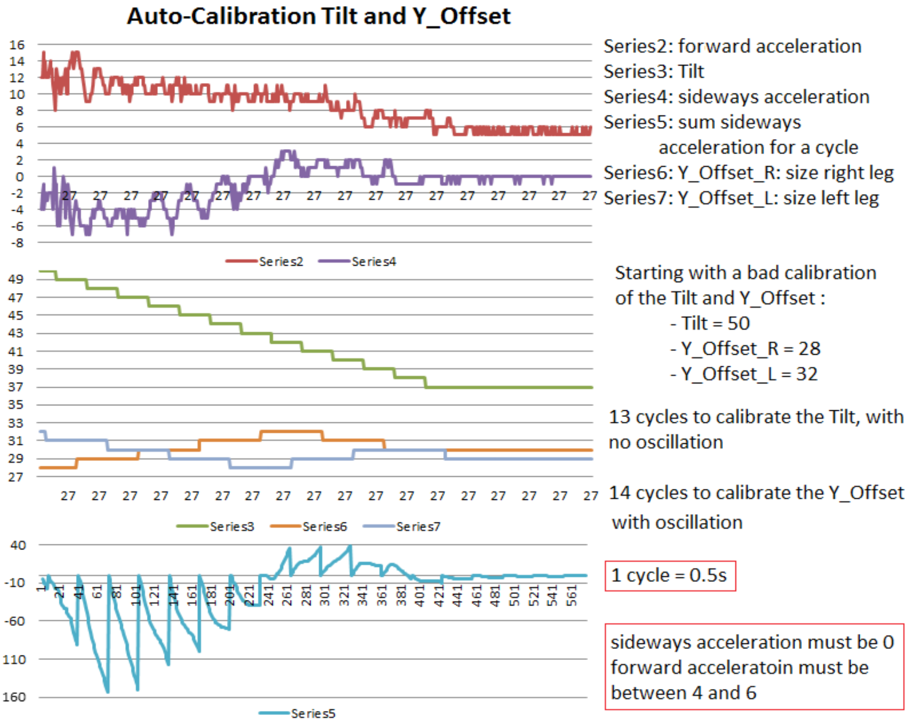
The second goal is to help the robot handling floor variations, by calibrating itself according to the floor it will deal with. The auto-calibration implemented have three part:

Y_Offset Auto-Calibration: Thanks to the sideways acceleration, the robot manage the sideways floor differences, like a slope or something under its foot, by calibrating the size of its legs (Y_Offset of the leg).

Tilt Auto-Calibration: The forward acceleration calibrates the tilt of the robot, to keep the robot close to a vertical forward position

Servomotors Auto-Calibration: Those both calibrations are completed by one made on the 3 servomotors of each legs used to walk forward, performed thanks to their own feedbacks. An offset value is added to the servomotor position if its returned position is different than its set position.

Example of a auto-calibration of the Tilt and the Y_Offset of the legs. The robot started with a bad calibration: too much tilt and not the same size of its legs. The forward acceleration value equalizes slowly to 5, the code using the value 4 and 6 to compare to the acceleration, to have the required tilt. The sideways acceleration tends slowly to 0.



Series2: forward acceleration
Series3: Tilt
Series4: sideways acceleration
Series5: sum sideways acceleration for a cycle
Series6: Y_Offset_R: size right leg
Series7: Y_Offset_L: size left leg

Starting with a bad calibration of the Tilt and Y_Offset :
- Tilt = 50
- Y_Offset_R = 28
- Y_Offset_L = 32

13 cycles to calibrate the Tilt, with no oscillation

14 cycles to calibrate the Y_Offset with oscillation

1 cycle = 0.5s

sideways acceleration must be 0
forward acceleratoin must be between 4 and 6

Figure 3: Example Auto-calibration Tilt and Y_Offset

5.2 Stabilisation

The stabilisation have several objectives, one is slow calibration of the robot according to the variations of the ground, e.g. a slope. The main objective is to allow the robot to handle a prompt variation on its usual movement, e.g. working on something unexpected on the floor, or receive a slight hit.

There are three type of stabilisation, according to their frequency. The first one, called “slow” on this project, is done on one entire cycle, with a frequency equal to the one of the cycle: 2Hz. For example using the average value of an acceleration during a cycle.

Then there is the “Quick” or “Punctual” stabilisation, which is effected twice per cycle on the project, usually looking for what happens at one tick of the cycle, so the frequency is 4Hz.

The best possible stabilisation should look at each ticks of the cycle, with a frequency equal to the one of the gait, 64Hz. This “high frequency” stabilisation has not been implemented mostly due to a lack of knowledge about the results.

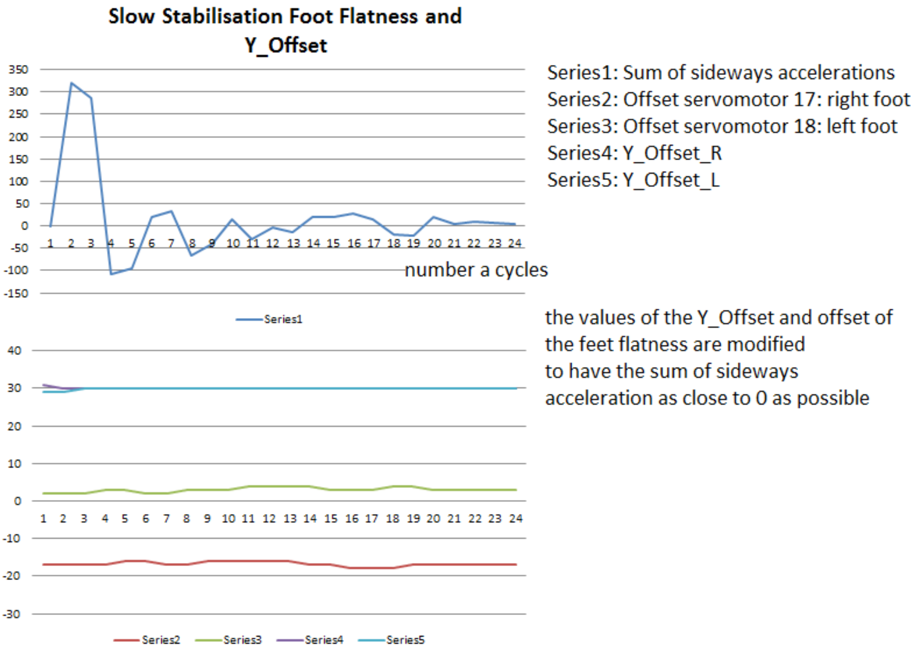
5.2.1 SlowStabilisation

The slow calibration functions are remaining functions, which means when they modify a value, this value will not change unless being modified again by a stabilization function. Three functions have been created:

Foot Flatness and Y_Offset Slow Stabilisation: This function modifies the flatness of the feet or size of the legs (Y_Offset) according to the sum of the lateral acceleration on a cycle, which should be equal to 0.

Hip Slow Stabilisation: Spread or narrow the legs according to the maximal and minimal value of the lateral acceleration during a cycle, which is when the feet hit the ground. These value should be inversely proportionate.

Tilt Slow Stabilisation: Modifes the Tilt value according to the average of the longitudinal acceleration.



Series1: Sum of sideways accelerations
Series2: Offset servomotor 17: right foot
Series3: Offset servomotor 18: left foot
Series4: Y_Offset_R
Series5: Y_Offset_L

the values of the Y_Offset and offset of the feet flatness are modified to have the sum of sideways acceleration as close to 0 as possible

Figure 4: Example Foot Flatness and Y_Offset Slow Stabilisation

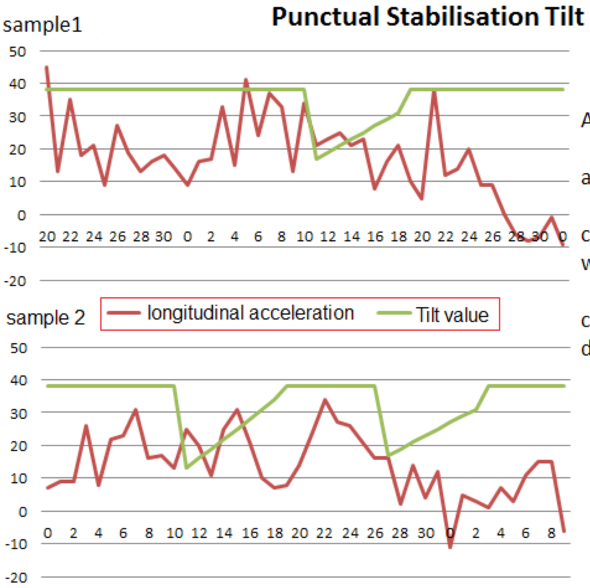
5.2.2 QuickStabilisation

Even if it is possible to have a perfect calibrated robot, with a perfect floor (with no slope), no one can predict to have a perfect cleaned ground. Small dirt on the ground can easily make the robot falling down, and something can hit the robot, like others robots. To manage these potential problems, the robot needs to have a good quick stabilization. Three functions have been implemented here, all according to the longitudinal acceleration:

Feet Quick Stabilisation: Modifies the longitudinal position and angle of a foot according to the acceleration returned by the IMU when the robot has a vertical position, if this acceleration is bigger than expected, the foot will be positioned further than usually with some angle (by rising the tip of the foot).

Tilt Quick Stabilisation: Twice by cycle, when the robot position is almost vertical, the Tilt value can be modified according to the value of the forward acceleration returned by the IMU. E.g. if the value returned is bigger than expected, the Tilt will be decrease and slowly come back to its normal value.

Speed Quick Stabilisation: As the previous functions, twice per cycle a comparison is made and the speed of the robot will be decrease if the difference is too big, then slowly increase until the normal speed of the robot.



As the feet stabilisation

at PoseNumber = 11 and 27

compare the forward acceleration with its normal value

change the tilt according to the difference for some ticks

Figure 5: Example Tilt Quick Stabilisation

5.3 Conclusionabouttheimplementedfunctions

In conclusion the auto-calibration is good to be used on a "perfect" floor to save calibration's time, but it is still imprecise compared to the potential of a human calibration.

The slow stabilization allow the robot to handle small sideways or forward slopes, but currently it cannot handle a slope which merges both.

The quick stabilisation functions are rather tests than well-thought ideas and need to be improved. However the analyses made on it show some good results for small forward variations and when external forces applied.

6 Conclusion and the Future

The main goals of this paper were to understand what is currently used and what we can use, how it work exactly, whether for the robot movement or the feedback from the IMU. Also to determine what is feasible, thanks to the previous point, and finally to developed stabilisations function on the robot to have a more balanced gait.

For each goal, theories, development and improvement have been done, but no one has been completely reached. The movement of the robot is more discerned than before but still not completely understood. The comprehension of the feedback is rather good; however it remains insufficient even if some interesting theories have been developed according to it. At the end the function developed are inefficient relatively to the expectation at the beginning of the project, due to a lack of time for testing and more development, but still helpful for the gait.

Anyway the method, idea and algorithm developed in this project will be useful even on the new version of the humanoid robot, and the work done here may be considered as first step to a generation of real time stabilisation robots developed at the University of Plymouth.

7 References

Gibbons P., Mason M., Vicente A., Bugmann G. and Culverhouse P., *“Optimization of Dynamic Gait for Bipedal Robots “* Proceding of the 2009 IEEE-RAS Intl. Conf. On Humanoid Robots (Humanoid 2009), Paris (France), December 7-10, 2009, pp 9-14

Tomomichi S., Yoshihiko N., Hirochika I., “*Real Humanoid Motion Generation trough ZMP Manipulation based on Inverted Pendulum Control”* Proceding of the 2002 IEEE International Conference on Robotics & Automation, Washington. DC, May 2002

Toru T., Takashi M. and Takahide Y., “*Real Time Motion Generation an Control for Biped Robot -1st Report: Walking Gait Pattern Generation*”, The 2009 IEEE/RSJ International Conference on Intelligent Robots and Systems, Octobre 11-15, 2009 St. Louis, USA

Wolf J. C., Hall P., Robinson P., Culverhouse P., *“Bioloid based Humanoid Soccer Robot Design”* in the Proc. of the Second Workshop on Humanoid Soccer Robots @ 2007 IEEE-RAS International Conference on Humanoid Robots, Pittsburgh (USA), November 29, 2007.

BugMann G., “Principles of Robot Gait”, School of Computing and Mathematics, ROCO306, University of Plymouth, 2012.

Culverhouse P., “Autonomy and Intelligence – Walking Robot”, School of Computing and Mathematics, AINT509, University of Plymouth, 2012.

A Navigation System for an Unmanned Aerial Vehicle Based on a Kalman Filtering Technique

J. Szostak and R. Sutton

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

Abstract

This paper summarises the research undertaken on a navigation system for an unmanned aerial vehicle base on Kalman filtering techniques. A model glider aircraft, Art-Tech Diamond D-2500, was used to gather experimental data sets, and various on-board sensors data were logged, and later post-processed. The tracking capabilities of the navigation system are demonstrated with MATLAB simulations, where a simplified kinematic model was used to explain various parameters of the Kalman filter. In order to show the full potential of the filtering algorithm, a theoretical discussion on sensor fusion is presented, where the accumulative error of the gyroscope caused by numerical integration is compensated with an accelerometer, thus providing a robust complementary attitude reference system.

Keywords

Navigation system, unmanned aerial vehicle, UAV, Kalman filter, model glider, sensor fusion, inertial measurement unit, accelerometer, gyroscope, magnetometer

1 Introduction

The concept of an unmanned aerial vehicle (UAV) assumes that the aircraft, whether autonomous or semi-autonomous, can perform predefined tasks, e.g. look for casualties in a search and rescue mission. Among many aspects concerning an UAV, a navigations system is particularly important and once developed, a control design can follow. In the example mentioned above, the aim could be to search for any survivals, and when the on-board vision system confirms that the target was found, their coordinates are being transferred, so that a manned vessel could be dispatched and complete the mission. Since the commercially available Global Positioning System (GPS) is prone to limited accuracy readings, and occasional signal losses, an inertial measurement unit (IMU) could be used to provide attitude and heading reference system, and GPS could be used as an additional source or sensor data.

2 Methodology

Art-Tech Diamond D-2500 glider was used as a research platform for the navigation system development. The aircraft was equipped with a GPS receiver providing current coordinates for the aircraft, and an inertial measurement unit (IMU) with triple-axis accelerometer, gyroscope and magnetometer, as well as barometric pressure and temperature sensors controlled by on-board microcontroller was used as attitude and heating reference system. In addition, a 2.4 GHz wireless receiver was used to echo commands sent by the model pilot from the ground via radio transmitter. This configuration allowed both input and output monitoring, and potentially the dynamic model of the model glider could be obtained.

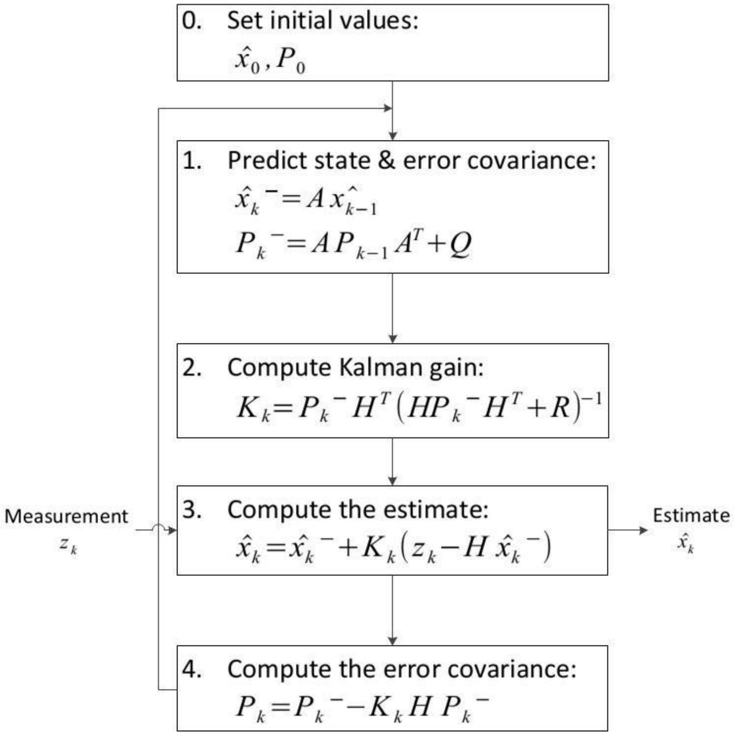

0. Set initial values:
$\hat{x}_0, P_0$
1. Predict state & error covariance:
$\hat{x}_k^- = A\hat{x}_{k-1}$
$P_k^- = AP_{k-1}A^T + Q$
2. Compute Kalman gain:
$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1}$
Measurement
z_k
3. Compute the estimate:
$\hat{x}_k = \hat{x}_k^- + K_k(z_k - H\hat{x}_k^-)$
Estimate
$\hat{x}_k$
4. Compute the error covariance:
$P_k = P_k^- - K_k H P_k^-$

Figure 1: Kalman filter algorithm (Kim, 2011)

It was assumed that the UAV moves only in two-dimensional plane, at the constant height and with a constant speed, therefore four state variables were used, the positions and velocities in each axis. As only the positions were considered for this application, the Kalman system model is presented as follows

$$x\hat{}_{k+1} = Ax_k + w_k$$

$$z_k = Hx_k + v_k$$

$$x_k = \begin{bmatrix} x_k \\ \dot{x}_k \\ y_k \\ \dot{y}_k \end{bmatrix} \quad A = \begin{bmatrix} 1 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Where the error covariance matrices were changed to provide different results

$$Q = q * \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix} \quad R = r * \begin{bmatrix} 10 & 0 \\ 0 & 10 \end{bmatrix}$$

The Kalman filter can be also uses to perform a sensor fusion between two and more sensors, which when selected appropriately can improved their performance. In the theoretical discussion, gyroscope's accumulative error (drift) due to numerical integration was compensated by the accelerometer in order to provide the horizontal attitude system.

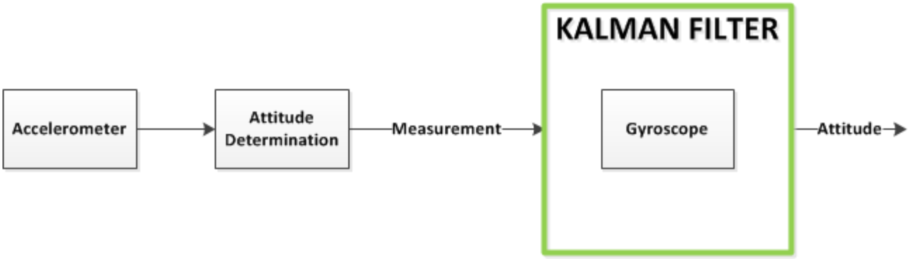


Figure 2: Sensor fusion using Kalman filter

The following system model was used, and quaternion was selected as state variables, therefore the estimation is express by

$$\hat{x_{k+1}} = Ax_k + w_k$$

$$\begin{bmatrix} \dot{q}_1 \\ \dot{q}_2 \\ \dot{q}_3 \\ \dot{q}_4 \end{bmatrix}_{k+1} = \left(I + \Delta t * \frac{1}{2} \begin{bmatrix} 0 & -p & -q & -r \\ p & 0 & r & -q \\ q & -r & 0 & p \\ r & q & -p & 0 \end{bmatrix} \right) \begin{bmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{bmatrix}_k$$

and the measurement transformed into quaternion is described as

$$z_k = Hx_k + v_k$$

$$\begin{bmatrix} q1 \\ g_2 \\ q_3 \\ q_4 \end{bmatrix} = \begin{bmatrix} \cos\frac{\phi}{2}\cos\frac{\theta}{2}\cos\frac{\psi}{2}+\sin\frac{\phi}{2}\sin\frac{\theta}{2}\sin\frac{\psi}{2} \\ \sin\frac{\phi}{2}\cos\frac{\theta}{2}\cos\frac{\psi}{2}-\cos\frac{\phi}{2}\sin\frac{\theta}{2}\sin\frac{\psi}{2} \\ \cos\frac{\phi}{2}\sin\frac{\theta}{2}\cos\frac{\psi}{2}+\sin\frac{\phi}{2}\cos\frac{\theta}{2}\sin\frac{\psi}{2} \\ \cos\frac{\phi}{2}\cos\frac{\theta}{2}\sin\frac{\psi}{2}-\sin\frac{\phi}{2}\sin\frac{\theta}{2}\cos\frac{\psi}{2} \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The H matrix is an identity matrix, as all of the states are desired.

Since the state-space model was analytically derived from the first principles, the Q and R covariance matrices can be expressed as follows:

$$Q = \begin{bmatrix} 0.001 & 0 & 0 & 0 \\ 0 & 0.001 & 0 & 0 \\ 0 & 0 & 0.001 & 0 \\ 0 & 0 & 0 & 0.001 \end{bmatrix} \quad R = \begin{bmatrix} 10 & 0 & 0 & 0 \\ 0 & 10 & 0 & 0 \\ 0 & 0 & 10 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix}$$

Where:

p, q and r and the angular velocities around each axis in the local reference frame g is the gravitational acceleration

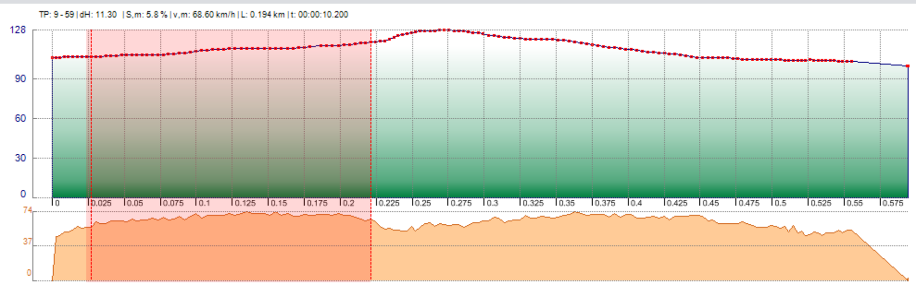
ϕ is the roll angle

θ is the pitch angle

Ψ is the yaw angle

3 Results

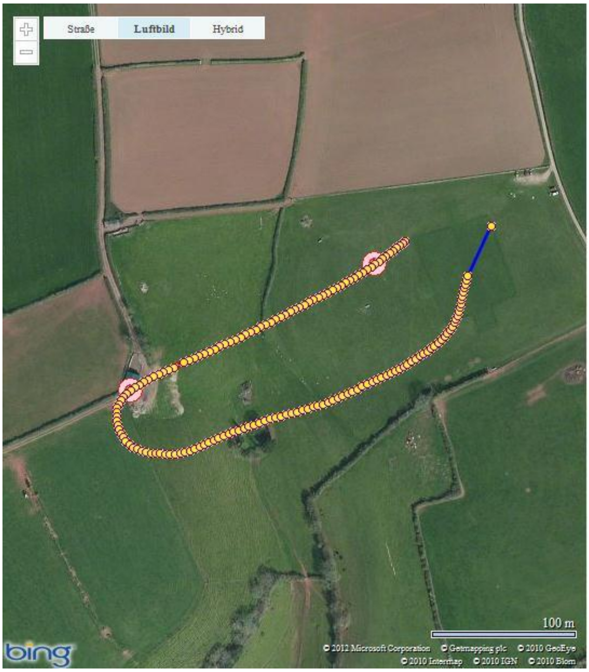
The GPS-Track-Analyse.NET software package (available in German) was used to visualise the GPS data set and helped to select appropriate set of experimental data for the simulation.



TP: 9 - 59 | dH: 11.30 | S,m: 5.8 % | v,m: 68.60 km/h | L: 0.194 km | t: 00:00:10.200

Figure 3: Print screen from the GPS-Track-Analyse.NET

The green colour indicates the height, and pink the velocity. By looking at Figure 3, it can be seen the assumptions made about the vehicle moving in two dimensional plane and with constant velocity are true.



Straße
Luftbild
Hybrid
100 m
bing
© 2012 Microsoft Corporation © Getmapping plc © 2010 GeoEye
© 2010 Intermap © 2010 IGN © 2010 Blom

Figure 4: A map with the flight path marked. Two pink circles show the selected part of the flight in Figure 4.1. Yellow dots show the sampling intervals. Source: bing

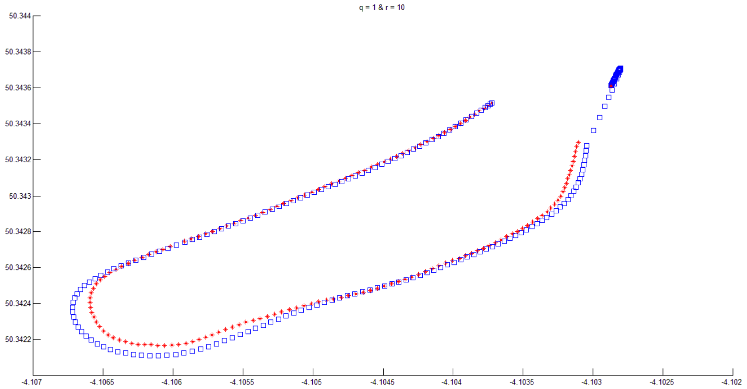


Figure 5: Simulation output of the tracking filter. Red asterisks show the measurement, and blue square the optimum estimation returned by the Kalman Filter, q=1, r=10

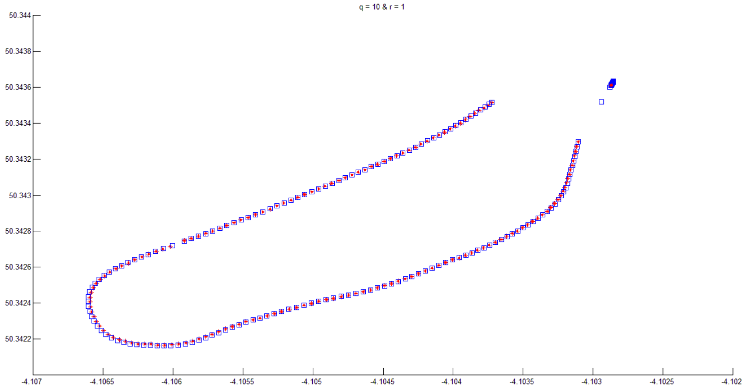


Figure 6: Simulation output of the tracking filter. Red asterisks show the measurement, and blue square the optimum estimation returned by the Kalman Filter, q=10, r=1

4 Discussion and Conclusions

The Kalman filter was used to track coordinates provided by the GPS receiver and the simplified kinematic model considered for the MATLAB simulations. Since the filter's performance is based on the accurate model of the system, and noise distribution, it is seen that further investigation into system identification and sensor modelling is required.

Due to sensor noise provided the electric brushless motor, that powers the model glider, the readings from magnetometers were compromised and the yaw angle could not be calculated correctly. The gyroscope data provided by the IMU were difficult to work with, as a relation between the actual magnitude and digital representation would have to be found, resulting in different H matrix.

5 References

Brown, R. G. and P. Y. C. Hwang (1997). Introduction to Random Signals and Applied Kalman Filtering with MATLAB exercises and solutions. Canada, John Wiley & Sons, Inc.

Juang, J.-N. (1994). Applied System Identification. Upper Saddle River, NJ 07458, Prentice Hall PTR.

Kim, P. (2011). Kalman Filter for Beginners with MATLAB Examples, A-JIN Publishing Company.

Naeem, W., Sutton, R., & Xu, T. (2012). An integrated multi-sensor data fusion algorithm and autopilot implementation in an uninhabited surface craft. Ocean Engineering, 39, 43-52.

Simons, M. (1999). Model Aircraft Aerodynamics. United Kingdom, Special Interest Model Books Ltd.

Sutton, R., Sharma, S., & Xu, T. (2011). Adaptive navigation systems for an unmanned surface vehicle. Proceedings of IMarEST - Part A - Journal of Marine Engineering and Technology, 10(3), 18. IMarEST.

Weia, Q. and F. Jiancheng (23 March 2012). Research on FKF Method Based on an Improved Genetic Algorithm for Multi-sensor Integrated Navigation System. Journal of Navigation 65(3): 495-511

Author Index

Advances in Communications, Computing, Networks and Security

Volume 10

Edited by
Paul S Dowland & Steven M Furnell

This book is the tenth 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 20011/12 academic year. A total of 25 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, Network Systems Engineering, and Robotics.

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 978-1-84102-358-8
90000
9 781841 023588