Advances in

Communications, Computing, Networks and Security

Volume 7

Editors

Paul S Dowland

Steven M Furnell

Advances in Communications, Computing, Networks and Security Volume 7

Proceedings of the MSc/MRes Programmes from the School of Computing, Communications and Electronics

2008 - 2009

Editors

Dr Paul S Dowland
Prof Steven M Furnell

School of Computing, Communications & Electronics
University of Plymouth

ISBN: 978-1-84102-283-3

Preface

This book is the seventh in a series presenting research papers arising from MSc/MRes research projects undertaken by students of the School of Computing, Communications and Electronics at the University of Plymouth. 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 2008/09 academic year. A total of 31 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: Network Systems Engineering, Robotics, Information Systems Security, Web Technologies and Security, Computing and Interactive Intelligent Systems

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, Communications and Electronics
University of Plymouth, May 2010

About the School of Computing, Communications and Electronics

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

The bulk of the staff in the School are housed in the Portland Square building, a purpose built state of the art building costing over £25million and situated near the centre of the historic city of Plymouth on the University campus. The laboratories are located in the newly refurbished Smeaton Building, and the Clean room for nanotechnology also recently refurbished courtesy of a Wolfson Foundation grant is situated in the nearby Brunel Building. All buildings are a short walk from each other, enabling a close collaboration within our research community.

This School sits alongside two other Schools in the Faculty of Technology, the School of Engineering (the merged School of Civil and Structural Engineering and Department of Mechanical and Marine Engineering), and the School of Mathematics and Statistics. There are research and teaching links across all three schools as well as with the rest of the University. The closest links are with the Faculty of Science, principally the Centre for Computational and Theoretical Neuroscience which started in Computing, and Psychology through Artificial Intelligence and Human Computer Interaction research.

Prof. Steven Furnell
Head of School

Contributing Research Groups

Centre for Information Security 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

Centre for Interactive Intelligent Systems
Head: Professor E Miranda & Professor A Cangelosi
Email: eduardo.miranda@plymouth.ac.uk
Research interests:

1) Natural language interaction and adaptive systems
2) Natural object categorisation
3) Adaptive behaviour and cognition
4) Visualisation
5) Semantic web

http://www.tech.plymouth.ac.uk/Research/computer_science_and_informatics/

Centre for Robotics and Intelligent Systems
Head: Dr G Bugmann
Email: guido.bugmann@plymouth.ac.uk
Research interests:

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

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

Fixed and Mobile Communications
Head: Professor M Tomlinson BSc, PhD, CEng, MIEE
E-mail: mtomlinson@plymouth.ac.uk
Research interests:

1) Satellite communications
2) Wireless communications
3) Broadcasting
4) Watermarking
5) Source coding and data compression

http://www.tech.plymouth.ac.uk/see/research/satcen/sat.htm
http://www.tech.plymouth.ac.uk/see/research/cdma/

Interdisciplinary Centre for Computer Music Research
Head: Professor E Miranda
Email: eduardo.miranda@plymouth.ac.uk
Research interests:

1) Computer-aided music composition
2) New digital musical instruments
3) Sound synthesis and processing
4) Music perception and the brain

http://cmr.soc.plymouth.ac.uk

Signal Processing and Multimedia Communications
Head: Professor E Ifeachor BSc, MSc, PhD, DIC, CEng, MIEE
Research interests:

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

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

Contents

SECTION 1 Network Systems Engineering

SECTION 2 Computer and Information Security & Web Technologies and Security

SECTION 3 Robotics

SECTION 4 Computing, Communications Engineering and Signal Processing & Interactive Intelligent Systems

Section 1

Network Systems Engineering

Accessing the Technical Quality of Media Reports

I.Adogu and A.Phippen

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

Abstract

It is no longer news that newspaper articles and TV broadcasts of science news are laden with errors of various types. Previous study aimed at proving this utilized questionnaire-based approaches which involved sending transcriptions of the news material together with a questionnaire to the sources quoted in the reports in order for them to identify errors. Since the issues investigated are technical in nature, this method is prone to the already recognized weaknesses of questionnaire-based investigations such as difficulty in designing a uniform set of questions that would expose errors, mistrust of results, and low level of response from participants. This publication outlines the framework for assessing technical accuracy which uses a more direct and 'self-contained' analytical approach that would yield precise and manageable results.

Keywords

Technical accuracy, Mass media, Subjective errors, Lack of completeness

1 Introduction

Theories in mass communications and established notions on media effects suggest strong influences of the mass media on the opinions and general knowledge of its audience (Severin and Tankard, 2001). Over the years, the widespread dependence on the media for information has grown from its traditional focus on social issues like politics and business, to the more technical subjects of internet threats and cyber-security. This trend has been sustained by the ubiquity, convenience and historical popularity of newspapers and TV which attract more 'followers' than technical journals and magazines (Noelle-Neuman, [no date] in Curran et al, 1977).

Most of the news about malware outbreaks and evolution of attack methods have been carried by the mass media that now have the *power* to prompt awareness and shape the understanding of its audience about dangers present on the internet. With this power comes the responsibility of ensuring that the information broadcast is accurate and sufficiently detailed to keep the public well informed and protected from such threats. However, sensationalism and propaganda are tools of the journalism trade which often get used in the preparation of stories on this sensitive subject (Lawrence and Grey, 1969 cited in Singletary, 1980). Coupled with a lack of technical background of news writers and their tendency towards brevity, the technical accuracy of resulting news stories is questioned.

This paper constructs two models for measuring the technical accuracy of mass mediated information in print and TV media. Each model deviates from the questionnaire-based approach and examines each story for three categories of errors while testing for completeness, readability and overall accuracy. With the results obtained, it will conclude on the suitability of the mass media as a knowledge source for internet threats and security.

2 Research Methodology

The error identification and analysis framework used in this paper is a hybrid of Charnley's 3-category error classification model (in Wimmer, 2004) and the Error Codification Scheme outlined by Carsten and Illman (2002). This framework would be sufficiently explicit to permit direct application to the data sets (news articles) without the need to contact the news sources.

2.1 Measurable Elements of Technical Accuracy (Print Media)

2.1.1 Errors

The definitions and categorisation of errors used are:

(a) Minor errors (mechanical or typographical) - These include errors in a single word or phrase that do not alter the meaning e.g. spelling errors and print errors.

(b) Objective errors (fact-based errors): These include errors in names, titles, ages, addresses, places, times, dates and statistics.

(c) Subjective errors (errors in meaning): These errors result in a change of scientific meaning and are sub-divided into misleading headlines, wrong impression, omission of relevant information, over- and under-emphasis of a point.

2.1.2 Lack of completeness

This examines how exhaustive the coverage or representation of the subject is. It goes beyond the article to obtain missing facts, details and complimentary story that would have painted a clearer picture of the subject matter. It also identifies omitted parts of the main story that resulted in a parochial or "one-sided" presentation of the subject. It excludes omissions that modify scientific meaning in any way.

2.1.3 Readability

Scientific information news articles that read well would often be understood by the reader because of the smooth flow of words. Usually, readability diminishes as the "jargon content" of a news article increases. Dale and Chall (1949, cited in Dubay, 2004)) define readability as "the sum total of all those elements within a given piece of printed material that affect the success a group of readers have with it. In this definition, success is gauged by the reader's comprehension.

2.1.3.1 Readability indices

In order to adequately represent readability measures, the researcher used three popular indices for each article viz.-

(i) Flesch Reading Ease score (FRE): Fashioned by Rudolf Flesch in 1948 and predicts the reading ease on a scale of 1 to 100. On the scale, the value 30 represents a "very difficult" read and value 70 represents an "easy" read. The formula for the Flesch Reading Ease score is:

$$FRE = 206.835 - (1.015 * ASL) - (84.6 * ASW)$$

ASL = average sentence length given by the number of words divided by the number of sentences, and *ASW* = average number of syllables per word given by the number of syllables divided by the number of words.

Reading Ease Score	**Style Description**	**Estimated Reading Grade**
0 – 29	Very difficult	College graduate
30 – 49	Difficult	13^{th} to 16^{th} Grade
50 – 59	Fairly difficult	10^{th} to 12^{th} Grade
60 – 69	Standard	8^{th} to 9^{th} Grade
70 – 79	Fairly easy	7^{th} Grade
80 – 89	Easy	6^{th} Grade
90 - 100	Very easy	5^{th} Grade

Table 1: The Flesch Reading/ Grade Level Scale

Flesch- Kincaid Grade level (FKG): This offers grade level representation of the Flesch Reading Ease index and it is calculated thus:

$$FKG = (0.4 * ASL) + (12 * ASW) - 15$$

(iii) Gunning's Fog (GF) index: This indicated the number of years of formal education that is required to fully comprehend an article on first reading.

2.1.4 Accuracy Checklist

The technical quality of these media reports would also be evaluated by their compliance with the standard guidelines for basic technical report writing (Colorado State University website, 1997).To aid this; the research included a 10- point

Accuracy checklist against which each report was analyzed for technical compliance. In addition to "Yes" or "No" answers to the following questions, the researcher also included comments explaining the answers.

- Were key facts omitted?
- Were inaccurate facts included?
- Were there any inconsistencies with standard views on a topic?
- Is the report concise?
- Is jargon or technical or specialized terminology effectively decomposed into comprehensible phrases and words?
- Were clichés and hype, or overused and self-laudatory language used in the report?
- Were invidious comparisons and discriminatory language used in the report?
- Were acronyms used effectively?
- Were euphemisms used in the report?
- Were reliable sources of information cited in the report?

Grading was based on the answers provided – where a positive answer to a desirable characteristic attracted a mark and a negative answer to an undesirable characteristic was awarded no mark.

2.2 Measurable Elements of Technical Accuracy (TV News Reports)

Considering the real-time nature of TV news, the researcher decided to sift through the archives of TV websites for popular stories and documentaries related to the research topic. Due to the 'streaming' nature of TV news; competition for air-time from other subjects like politics, business and sports; and storage limitations of online databases, not all news reports are archived on the websites of TV stations. While all the news aired on the TV broadcasts are adequately covered in text-based reports on these websites, a recording of the actual news broadcast (as shown on the television) is not readily available for obvious reasons. Usually, online archives contain particular programs and documentaries that have web versions, and the most popular news stories. It is this content that the researcher searched for stories about internet threats. As a result of the limitations outlined above, the number of reports obtained for the time range specified (i.e. not later than two years) was quite small. Technical accuracy of the news videos was determined by answering the following investigative questions:

- **Up-to-datedness**: How current is the news subject and its discussion? Does it adequately reflect the latest information, issues and ideas?
- **Bias**: Are the details of the story reported from a neutral perspective or are arguments made in favour of a particular viewpoint?
- **Completeness**: Were all aspects of the story covered? Were sufficient facts about the subject communicated?
- **Content Accuracy**: Are the arguments and notions of the story technically accurate?

- **Separation of fact from opinion**: How well were the facts of the story isolated from the opinions of the presenter, interviewees and other personalities in the news report?
- **References**: Were credible and reputable sources cited in the report? Were references given to enable the obtaining of more information on the subject?

2.3 Data Sets

The pool of media reports that would serve as raw material for this project would be sourced from websites of popular newspapers, tabloids and television stations. The online archives of these media were searched in order to extract reports that relate to subject of investigation i.e. internet threats and cyber security**.** Focus would be on recent reports with publication dates of not later than two years. This would help it address current threats and responses to these threats by the public. The media titles to be used include:

(1) Newspapers: *The Guardian, Independent, Times, and Telegraph*
(2) Tabloid newspaper: *The Sun, Daily Mail, Daily Express and Daily Mirror.*
(3) Television stations: *BBC News, CNN, Sky News and Five News*

2.4 Analytical steps

Step 1- Data collection: The key words: 'internet', 'computer'' security' and 'threats' would be input into the search engines of these websites to obtain related stories contained in recent back issues.

Step 2- Identification of errors

- Identification of the internet/ computer security firms, government and non-government agencies, anti- virus providers, etc that were quoted in news reports. Collection of press releases, surveys, reports and 'on- site' technical whitepapers that relate directly to the events (security threats & breaches) that were mentioned in the news reports. This would serve as the news source.
- Critical and comparative study of the media report and its sources.
- Identification of the different errors contained in the reports using the definitions and categorizations introduced in Section 2.2.1. In each error, references would be made to source documents that contain information that adequately corrects the error and presents a clearer point of view.

Step 3: Gauging the completeness of the media report by comparing them with their sources.

Step 4: Measuring the readability of the news articles by subjecting them to the afore-mentioned readability tests. Calculating parameters such as 'average sentence length' and 'average number of syllables per word' becomes very arduous when one considers the large number of words and sentences contained in each article. To efficiently obtain the values for these parameters, a Flesch readability calculator was downloaded from the internet and installed on a personal computer. Each article was

saved as a text file or MS Word file and examined by the software to calculate the FRE score and the FKG level. An online utility was also used for the calculation of the GF index.

Step 5: Applying the Accuracy Check-list according to Section 2.2. Grading was based on the answers provided – where a positive answer to a desirable characteristic attracted a mark and a negative answer to an undesirable characteristic was awarded no mark.

Step 6: Plotting of results on graphs and tables for evaluation and comparison.

3 Key Results and Findings

3.1 What are the most frequent errors in news reports on internet threats and cyber security?

Table 2 shows that subjective errors were the most frequent accounting for two-thirds of all observed errors while objective errors constituted 35.8%. These errors were identified in parts of the reports like the use of technical terms, specialized terminologies, acronyms and other scientific statements/ information. The verification technique is similar to that used in objective errors where the 'questionable' data was compared with identified information-sources. Table 3 shows that the dominant type of subjective error were the omission of information which accounted for 77.4% of occurring subjective errors. Over/ under-emphasis and misleading headlines constituted 12.9% and 6.4% respectively.

Type of Error	Total No. of Occurrences	Valid Percent
Minor	2	3.7
Objective	19	35.8
Subjective	32	60.3

Table 2: Total number of errors in newspapers/ tabloids

Types of Subjective errors	Frequency	Valid Percent
Misleading Headline	2	6.4
Wrong impression	1	3.2
Omission of information	24	77.4
Over- and Under- emphasis	4	12.9

Table 3: Frequency of subjective errors

On an average; newspapers contained more subjective errors than tabloids as shown in Figure 1 below. The highest number of subjective errors for a single news article occurred in the *Guardian* and subjective errors also constituted 80% of all observed errors for that newspaper. More than half of the errors in *The Independent* and 80% in *The Sun* were subjective in nature. 100% of all the errors encountered in the *Telegraph* were subjective errors while *Times*, *Daily Mirror* and *Daily Mail* showed relatively low levels for this error type.

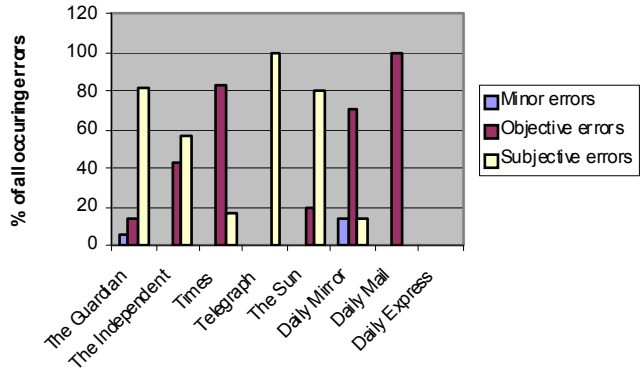


Figure 1: Frequency of error types per newspaper/ tabloid

The analysis shows that subjective errors were mostly as a result of omission of information arising from incomplete definition or lack of definition of technical terms and phrases. It is quite clear that, while the newspapers and tabloids correctly use the technical terms in question, they often fail to add definitions or explanations for such terms. The term that lacks proper definition in newspapers like the *Telegraph* and *Independent* is 'Phishing'. Other terms with shortage of explanation included 'spam', 'pharming', 'trojans' and 'spyware'. These terms may be regarded as fairly simple and commonly used in the web community, however, it should be considered that many internet users, especially those on the 'home front' are not very versed in internet terminologies and might misinterpret them or mistaken one for the other.. In cases where brief explanations followed the use of such terms, the information was more comprehensive and illuminated.

Broadcast	BBC#1	BBC#2	CNN#1	CNN#2	Five News#1	Five News#2	Sky News#1
Complete?	**No**	**No**	**No**	**No**	**No**	**No**	**Yes**

Table 3: Completeness of TV reports

Except the Sky news report, the other TV reports were incomplete and failed to give a full account of the subject under discussion. The issue of incompleteness is clearly the main deficiency in 6 of the 7 reports examined.

It was reasoned that the main cause of the problem of lack of/ partial definitions were word-count limitations imposed on writers of scientific stories. This strictly defines the amount of text they can put down in an article and aims to ensure that only very essential information is included in a report. These force writers to use technical terms without adding sufficient definitions thus, the meaning, significance and implication of some terms go hidden. Also, brevity of reports, which allows aired TV news bulletins to fit restricted time slots on a TV station's broadcast schedule, could also cause a lack of completion. This summarization measures could lead to lack of full awareness about internet threats and web security issues. The sub-set of under-/ over-emphasis can also be related to a lack of proper definition and explanations.

3.2 Do these errors sufficiently distort the understanding or knowledge gained from the report?

Together, the occurring minor, objective and subjective errors weren't enough to significantly alter the meaning so as to cause misinformation. This is because the essential and most important information, such as the loopholes in social networking sites and the warnings about phishing e-mails, *ultimately* get conveyed to the readers. The errors occur in sections that provide further technical information or additional information (like statistics) which serve to emphasize an already stated subject. The errors affected the technical quality of the articles more than it corrupted the information derived

3.3 Does the mass media constitute an accurate source of information about internet threats and cyber security?

The issues of internet threats and cyber-security are mostly dynamic and require not only up-to-date, but also detailed discussion in order to sufficiently raise awareness. Since newspapers and tabloids deal with the' general' news, such elaborate discussions would not be carried out at the expense of other types of news like politics and sports. At the moment, the mass media mostly alert or notify the public about internet threats – throwing in a lot of statistics and quoting experts who would highlight the gravity of these threats. Further information about these threats that would assist the public in countering this threat is still lacking. More technically accurate and complete explanations of internet risks and security could be obtained through the websites, publications and e-newsletters/ reports of internet security agencies, security solution vendors and government websites.

The verdict: mass media merely serve a notification function and do not adequately inform the general public about internet threats.

4 References

'Assuring Quality of Public Relations Messages' (1997) [Online] Colorado State University website. Available from:1 [Accessed 23 April 2008]

Carsten, L. D. and Illman, D. L. (2002) 'Perceptions of Accuracy in Science Writing'. IEEE Transactions on Professional Communication, 45(3): 153 -158. [Online] Available from: http://ieeexplore.ieee.org/iel5/47/22133/01029955.pdf [Accessed 1 June 2008]

Curran, J., Gurevitch, M. and Woollacott, J. (1977) 'Mass Communication and Society', London: Edward Arnold.

Dubay, W. (2004) 'The Principles of Readability' [Online] Available from: www.impact-information.com/impactinfo/readability02.pdf [Accessed 20 October 2008]

Severin, W. and Tankard, J. (2001) 'Communication Theories: Origins, Methods, and Uses in the Mass Media', 5th Edition, New York: Longman.

Singletary, M. (1980) 'Accuracy in News Reporting: A Review of the Research' [Online] ANPA News Research Report, No. 25. Available from: http://eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/32/9e/5b.pdf [Accessed 17 July 2008]

Wimmer, T. (2004) 'Correct This! A Content Analysis of 2003 Errors Posted by the New York Times' [Online] AEJMC Conference Papers. Available from: http://list.msu.edu/cgi-bin/wa?A2=ind0411c&L=aejmc&D=0&P=24903 [Accessed 17 July2008]

Evaluating Identity Theft Awareness Online Resources

Z.AlHammad and A.Phippen

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

Abstract

Identity theft is one of the fast growing crimes. Thieves of identities aim to use other identity for many purposes like gain benefits or escape from arresting. Many of organizations aim to educate end-users about identity theft through online resources. The problem of website's information is not always trusted. This paper aims to develop an evaluation methodology for identity theft awareness online resources. Fifty websites were collected from popular search engines (google.com and ask.com) and evaluated by the selective developed criteria. The current state of identity theft awareness websites is pretty good. However, more than one-third of evaluated websites did not have information from qualified resources. The weakness points of the evaluated websites were the authority, accuracy and currency fields. In this project, suggestions to improve these fields by referring the information to trusted resources and update the websites frequently.

Keywords

Identity theft, awareness online resources, evaluation criteria

1 Introduction

Nowadays, end-users are facing many information security issues. Personal information is useful to complete many current crimes. One of information risks is identity theft. Identity frauds may use victim's personal information to gain benefits.

Identity theft is a fast growing crime which includes using anyone identity information wrongly. Credit card frauds are examples of Identity theft. Many end-users do not know about these crimes which make them ease hunt for offenders. Educating end-users about identity theft is a considerable topic for many of official organizations.

Official organizations, experts, and non-professional interested writers try to educate people about security awareness. End users awareness is one way to reduce the frauds success. Some organizations worked to educated people about information security through awareness courses (Bishop, 2000). In addition, many publishers aim to educate people through their websites. However, the website's information quality is not guaranteed because there is no monitoring for the published information quality. To be able to use the website's information as trustable resources, the quality of these websites should be examined.

2 Literature Review

2.1 Identity theft

Identity theft is a crime which someone uses wrongly another person identity to get economic benefits or frauds (USD of Justice, 2009). According to the Home Office, ID fraud costs the Britain economy more than £1.3 billion yearly and more than 53,000 victims in 2001 in the UK only (Porter, 2004).

There was no one definitive definition for identity theft until 1998 when Congress passed the Identity Theft Assumption and Deterrence Act (the Identity Theft Act; U.S. Public Law 105-318) (Newman and McNally , 2005). This act identifies offenders as anyone who

"…knowingly transfers or uses, without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

US Department of Justice list some ways used by thieves to get victim's identities information (USD of Justice, 2009). One way called "shoulder surfing" this depends on collecting your information by listening to telephone call or looking on identity card without permission. Collecting identity information could be found in garbage bank's balance report or copies of checks which called "dumpster diving". Also, the internet could be a source for thieves to steal the identities. Phishing messages and spyware may lead to identity theft (Furnell, 2005).

2.2 Information Security Awareness

Internet is an open source for gathering information because it is easy to access and available for most of people. The quality for online resources is not guaranteed and no monitoring for information published in the internet. Lack of security awareness is a major problem for most of beginner internet users (Furnell et al., 2008). Internet threats are increasing these days and they consider the end-user as easy prey (Furnell, 2005).

Many security awareness interested researchers studied educate end-users ways. Brodie, C (2009) suggest some methods to train employees in security: First way is classroom-style training where lecturers can interact directly with audience. Also, Helpful hints which may appear when the users login or as remainders. Visual aids will help for improve end-users security awareness through security posters. The Final way mentioned is security awareness websites which can train more than organization employees.

2.3 Evaluation of online resources

Researchers designed more than one methodology to evaluate online resources. Smith, Alastair (1996) published a bibliography that contains many evaluation's

criteria which used for evaluate internet information resource (Smith, 1996). This bibliography is modified in June, 2009. For example, Susan's criteria have five evaluative criteria: authority, accuracy, objectivity, currency and coverage (Beck, 1997). Lida L. Larsen, who works in University of Maryland, design criteria has seven primary evaluative fields: scope, authority and bias, accuracy, timeliness, permanence, value added features and presentation (Larsen, 1996). Many other criteria were designed and tested by educational organizations. In this project, some of these published criteria were reviewed to develop selective evaluation criteria.

3 Research Methodology

3.1 Criteria Design

The first step in the project was developing criteria for evaluating online resources. Two criteria developed for this purpose. The first one (initial appraisal) was developed to rate the searched websites according to website's type which is an indicator for bias, coverage and availability of references which is an indicator for accuracy of the website. The rate scale was designed from one to five: rate one given to web pages that provide the minimum of evaluated fields. The rate five is given for excellent online resources. The first six pages of both search engines (google.com and ask.com) were evaluated by these criteria. Table 1 shows the description of "Initial appraisal" criteria rating scheme.

Rate	Type	Coverage	References
Rate-1 very poor	Educational	Very low	Not considered
Rate-1 very poor	Commercial	Low	Not considered
Rate-2 poor	Educational	Low	Not considered
Rate-2 poor	Commercial	Medium	Not considered
Rate-3 good	Educational	Medium	Not considered
Rate-3 good	Commercial	High	Not considered
Rate-4 very good	Educational	High	No
Rate-4 very good	Official	Medium	Yes
Rate-5 excellent	Educational	High	Yes
Rate-5 excellent	Official	High	Yes

Table 1"Initial Appraisal" criteria's description.

The second criteria will evaluate the searched website in detail. "Content analysis" criteria will evaluate seven fields in each searched web page: Authority, Accuracy,

Objectivity, Coverage, Currency, Purpose, and Presentation. Each field have couple questions to make the evaluating more accurately. Each question will be answered by numbered scale depending on its accomplishing of the required issue. Table 2 shows the description of "Content Analysis" criteria. For example, the authority field were measured by four questions: Is the author name written, is he/she qualification written, is there any further information about the author and is the website published by qualified organization. Each question of these four questions worth two points which mean the authority field total mark is eight. All fields will be evaluated in each website. The total marks for all fields will be calculated to find the website's quality.

1. Authority	2. Accuracy	3. Objectivity
Author name? Author qualifications? Further information about the author? Qualified publisher?	References Qualified information resource?	Author's motivation Advertising on the site
4. Coverage	**5. Currency**	**6. Purpose**
What is the ID theft? How can it happen? How can we protect our ID? Additional helpful organizations?	Publishing Date Last update Date	Intended audience Effectively of the site
7. Presentation		
Colours Design		

Table 2 "Content Analysis" criteria's description

3.2 Data Collection and Analysis

The data will be gathered from two search engines (google.com and ask.com). The keywords used in the search were, identity theft prevention. The first criteria will evaluate the first six pages. End-users usually did not go further than this number in their researches. The second criteria will evaluate fifty websites from both search engines.

Google is the most popular search engine. It approaches 70 percent of U.S. searches in June 2008 (Hitwise, 2008). Ask.com is one of famous search engines. Hitwise.com announced that ask.com received 4.17 percent of U.S. Searches in June 2008 (Hitwise, 2008). In spite of Google is most popular search engines according to many hits' counters sources, using Google does not mean better results will be gained. When the first criteria were applied in the first six pages in google.com and ask.com, the same websites were found in different order. The noticeable point that the total websites were found in Google.com is greater than Ask.com but most of additional Google.com websites are commercial websites. The number of excellent and very good websites in both search engines was equal.

The choosing of google.com and ask.com was decided to see how the results will be affected by using different popularity rank search engines. In this project, before choosing ask.com, Yahoo.com and Msn.com were examined. The same websites in the first pages were given. The choosing of ask.com in this project was decided to discuss in the project's results there is not big different in excellent websites when using google.com or ask.com to search in the same keywords. In this project, the most popular search engines provide the same results with minor changes in commercial websites.

Google was the first search engine used with the websites given a number from 1 to 25 in order of their appearance on the search engine. Ask.com was used second and any repeating websites / pages will be ignored. They were given a number of 26 to 50, in order of precedence.

4 Results and Discussion

4.1 Analysing of "Initial Appraisal" criteria results

First, the "Initial Appraisal" criteria results can show the percentage of different rated websites in overall six pages that evaluated. The both search engines provide almost the same results.

Figure 1 shows the average of websites rate's percentages. This figure presents the big different between high qualified information's websites and low qualified websites. Rates 5 and 4 which is excellent and very good website are just around 27% which is low percentage in overall evaluation. Rate 2 and 1 which mean poor and very poor websites represent around 51%. These results illustrate the shortage of excellent security awareness online resource in identity theft topic.

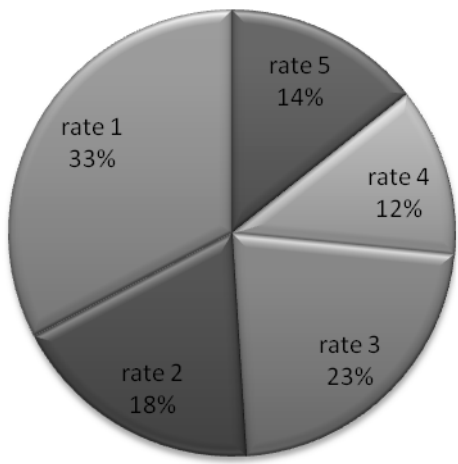


Figure 1: Websites rate's percentages

Also, it was a noticeable point that three of the excellent websites was found in page number four in Ask.com search's results and two of excellent websites was found in page five in Google.com search results. These results show the need to search in later pages in search engines because of the probability of finding excellent resources.

4.2 Analysing of "Content Analysis" criteria results

Second, the analyses of "Content Analysis" criteria's results were discussed. The criteria evaluate fifty selected websites from both search engines (google.com and ask.com), twenty five from each of them. The selected websites are different rated websites.

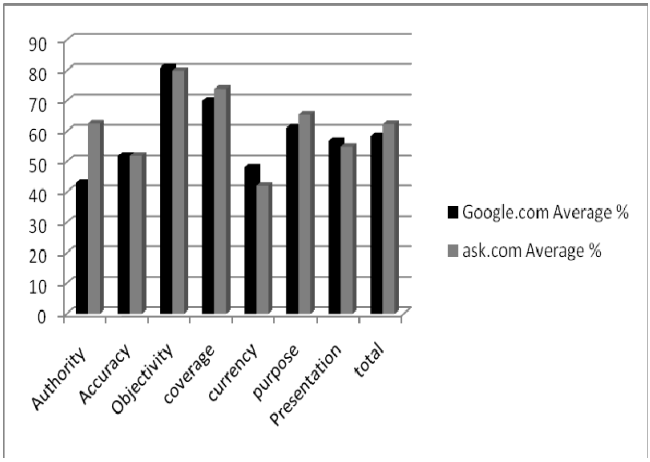


Figure 2: The percentage of "Content Analysis" criteria fields' results

Figure 2 presents the percentage of each evaluated field according to selective evaluated pages from Google.com and Ask.com search's results. The figure shows a sufficient percentage in objectivity, coverage, purpose and presentation fields. However, it demonstrates main weaknesses in authority, accuracy and currency.

Also, the average of total marks for the fifty evaluated websites is around 60%. This average is acceptable. However, the identity theft awareness field need more work to give the maximum efficiency for end-users.

5 Conclusion and future work

Identity theft is one of the fast growing crimes. One of the ways to educate end-users about it this crime is online resources. In this project, these awareness websites were evaluated by developed criteria. The results of this evaluation lead to define the weakness fields in these websites which are authority, accuracy and currency.

The educational website's designer should consider the sources of the information that posted. If the published website owned by qualified author or organization, the authority information must be added to give information accuracy evidence. When

the author is not qualified, the information should be collected from qualified sources and reference should be added in the website. Also, the currency is critical in active topic's websites. The website should be updated frequently to keep the end-users aware about latest news and techniques in the field.

The end-users should critically choose the reliable websites. Users should avoid commercial purpose's websites or author's bias writing. Many websites offering 'information' were really engaged in nothing more than a sales pitch to sell their products under the guise of providing information. Users should look for websites with qualified resources before gathering information. Some of websites collect information from unqualified resources like forums or commercial resources. Also, currency is very important in crime's awareness websites because new thieves techniques are usually appears frequently.

The general state is pretty good and if the users are aware about information quality which mean takes information from qualified resources, they will get useful information. Users should look after the first page if they looking for useful information. Users should find the useful resources from search engine's pages and use another search engine when needed.

As a suggestion for future work, creating a survey of end-users awareness about identity theft will be helpful. The result of the suggested survey will help to find what end-users know about this crime and what end-users are looking to know about the topic. They will help to provide suggestions for modify identity theft educational online resource.

6 References

Beck, S. (1997), "Evaluation Criteria (from The Good, The Bad, and The Ugly: or, Why It's a Good Idea to Evaluate Web Sources.)". Available: http://lib.nmsu.edu/instruction/evalcrit.html Last accessed [21 August 2009].

Bishop, M (2000), "Education in Information Security," IEEE Concurrency, vol. 8, no. 4, pp. 4-8, doi:10.1109/4434.895087

Brodie, C. (2009), "The Importance of Security Awareness Training". SANS Institute.

Furnell, S. (2005), "Internet threats to end-users: Hunting easy prey". Network security, 2005, 5-9.

Furnell, S., Tsaganidi, V. & Phippen, A. (2008), "Security beliefs and barriers for novice Internet users". Computers & security, 27, 235-240.

Hitwise Pty. Ltd (2008), "Google Approaches 70 Percent of U.S. Searches in June 2008", Available from: http://www.hitwise.com/press-center/hitwiseHS2004/us-google-70-percent-of-searches.php. Last accessed [24 August 2009].

Larsen, L. (1996), "Information Literacy: the Web is not an Encyclopedia" University of Maryland, College Park. Available: http://www.oit.umd.edu/units/web/literacy/. Last accessed [22 August 2009].

Newman, G. and McNally, M. (2005), "Identity theft literature review". Available http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf. Last accessed [24 August 2009].

Porter, D. (2004) Identity fraud: The stealth threat to UK plc. Computer fraud and security, 2004, 4-6.

Smith, A. (1996), "Evaluation of information sources". Available: http://www.vuw.ac.nz/staff/alastair_smith/EVALN/EVALN.HTM. Last accessed [2 February 2009].

USD of Justice. (2009), “Identity Theft and Identity Fraud”. Available: http://www.usdoj.gov/criminal/fraud/websites/idtheft.html. Last accessed [2 February 2009].

Internet User's Awareness and Understanding of Spyware and Anti-Spyware

M.Alshamrani and S.M.Furnell

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

Abstract

Spyware represents one of the main Internet threats. It can secretly compromise and control the devices and the personal data of the individual user or the organization without their knowledge. This research paper examines the level of awareness for Internet users about Spyware threats and Anti-spyware protection services. An online survey was designed and published, with 225 respondents with different backgrounds and experience participating. From the analysed results, the study found that there is a significant lack of awareness amongst Internet users about Spyware threats and Anti-spyware protection services, while the number of Spyware attacks has increased. A quarter of participants had no idea about Spyware threats at all. At least 40% have been attacked by Spyware, and 32% of the respondents do not understand how to use Anti-spyware or the protection system in their PCs. The research found that the lack of training was the main reason for the lack of awareness about Spyware threats and Anti-spyware protection services. Only 31% of the respondents had attended a course or training session about computer security. The trained participants in general are the most aware and protected group of respondents regarding to Spyware threats. However, the study showed that the training sessions are not focusing on or giving sufficient information about Spyware and Anti-spyware. Only 25% of the aware participants received some information about Spyware and Anti-spyware from the training sessions they received from their organizations.

Keywords

Spyware, Anti-spyware, Software, Spyware Training, Information Security

1 Introduction

Spyware represents one of the most significant security threats for individual users and organizational networks. Spyware is a software program which can compromise the covert and the overt of the confidential and non-confidential information from the Internet users' PCs and/or networks (Dinev and Hu, 2007). These programs have the ability to hide in the background on victim's systems or move through the Internet or local networks. Other types of spyware are remotely controlled and directed by its creator commands (Thomson *et al.,* 2006). Spyware can efficiently attack Internet user's privacy by data collecting, system controlling, and/or actions reporting of victims PCs and networks (Cordes, 2005).

While Internet user's awareness of the general Internet threats has been increased over the years, they are still not doing enough to protect themselves, often due to a

false sense of security. An increased number of online attacks have been reported since 1998, which caused huge financial losses estimated to hundreds of millions American dollars in the U.S. which infected companies, organisations, and some governmental agencies, where the worldwide estimated losses were much more (Cavusoglu et al., 2004).

Internet users are targeted by a number of threats that intent to get an unauthorized access to their private and critical data or trying to compromise their system privacy where their systems are often not well protected. Awareness is defined as the extent to which a target population is conscious of an innovation and formulates a general perception of what it entails (Schmidt et al, 2008). Moreover, the number of users of this technology had been increased, which give the above research result an important part for Internet security resolving and improvement.

At the present time, the Internet is joining users from many communities and with different knowledge, experience, background, gender, and ages. These factors have direct effects on the Internet user's attitudes, behaviour, awareness, and reactions against Information security (Furnell, 2008; Dinev and Hu, 2007). The importance of information security and the related awareness of Internet users are the major motivation of this research study. In order to accomplish this, researchers need to have a comprehensive understanding about how Internet user's awareness of Spyware and Anti-spyware have been measured and what level of awareness they have. This study contributes by including some basic aspects about Spyware awareness that have not been investigated yet. The main aims and objectives of this research paper are to demonstrate the actual level of user awareness of spyware and Anti-spyware. This will help to improve the security level against spyware threats by giving the interested security researches and providers a clear realization of Internet user's awareness and practices. In addition, this paper aims to prove the reality of spyware threats in terms of knowledge and practical actions depending on some stated results of some previous research studies.

2 Background

The gradually increasing studies and articles about spyware and the information security awareness are reflecting the massive and the widely distributed threats that spyware could cause. In terms of examining Internet users' spyware awareness, while there is only a limited amount of academic research and other reports, some relevant research has been done.

In the investigation of Internet consumers' awareness about spyware, Zhang (2005) found that the general comprehension and understanding about security, confidentiality, and Spyware are lacking. Moreover, the privacy attacks are not sufficiently noticed by the users, with respondents having limited knowledge about using Spyware removal tools. This research was one of the earliest studies examining Internet users' awareness and its direct relation with spyware threats. Later, Poston et al. (2005) stated that general PC users are aware about security threats in general. However, they are not prompted to react with protecting their systems by using anti-spyware protection system. Schmidt and Arnett (2005) reported that 94% of PC users

know about Spyware threats, while 61% had discovered incidences of spyware infection in their systems.

Freeman and Urbaczewski (2005) provided considerations of the damaging effects of spyware and investigated why people hate Spyware. In addition, the study reported that users' privacy and service performance are very important concerns. Furthermore, the report mentions that Internet users presume that governments and IT industries are responsible about controlling and defending them from spyware threats. In addition, the results showed that most of the respondents felt that they are not having to be responsible about protecting themselves. However, there are different points of views about the awareness and who is really responsible, where users, vendors, governments, organizations, or industries are all have to share within this mission.

Awad, and Fitzgerald (2005) investigated the Internet users' negative thoughts about Internet security. They showed four illusory behaviours were appreciably related to the this feeling: the variable nature of PC system settings, slowing and crashing of the system, installing un-approval protection system, and spyware downloads.

Kucera et al. (2005) reported about the presence of spyware in many of the popular freeware and shareware that may download from Internet websites. Once it downloaded, it has been found that this software has the ability to gather various forms of victims' personal information.

Meanwhile, Lee and Kozar (2005) identified 3 types of factors that had significant impacts upon Internet users' adoption of anti-spyware protection. Firstly, they determined two user attitude factors; namely users' compatible morals and relative advantages of anti-spyware usages. Secondly, they determined two social influence factors; namely the visibility and image of Spyware threats. Finally, they stated two behavioural control factors; computing capacity and the ability to test/try the protection product.

Dinev and Hu (2007) studied the main factors that effect users' actions against spyware threats. They concluded with four main determination factors driven from their research study results: Users' awareness of spyware, and the perceiving of the usefulness, the controllability, and the simplicity of use.

Another important result related directly with the research area, Jaeger and Clarke (2006) formed a survey that examined the level of awareness and understanding of home PC users to spyware threats. They found that the majority of home users understand about spyware. However, they found a lack of understanding of the needed protection system to securing their PCs against spyware threats. The survey showed that about 20% of 205 respondents are not using any Anti-spyware system. In addition, the research found that respondents are considering spyware as a "High/Some Threat" where 72% of the respondents had changed their browsing habits and accessing behaviour due to pervious expert, infections, and media/news articles.

A research study by Sipior and Ward (2008) investigated the perceptions of users related to considerations of trust, privacy, and legal protection in using application software that containing embedded spyware. The study reveals further results about the direct influences of the overall trust of a software vendor according to the examination of trustworthiness. The research stated three important factors that affect the software vendor trustworthiness; multi-dimensional construct, reveals trustworthiness-integrity, and trustworthiness-ability. The research results are providing software vendors and regulatory agencies of governments a useful guidance and recommendations in indicating the related concerns of Spyware.

3 Methodology

In order to accomplish the research aims, there are different methods that can be taken on. For instance, the research can interview a group of Internet users, monitoring their practices, and recording their information. However, these methods might not be very effective for the research approach. The personal interview by the researcher with the respondents is very difficult, as it is time consuming and requires a lot of effort to reach the targeted participants in different countries, locations, and with different backgrounds. In addition, it provides limited numbers of respondents for monitoring their practices and recording their feedback. The online survey uses an anonymous way of collecting the data, which encourages the respondents to participate in the survey and give more truthful answers. Nevertheless, the study needs to investigate Internet users who are involved with the research topic which needs to find respondents who are using the Internet service. Thus, the best method that helps to reach different users in different places is by conducting a survey and publishing it by using the online survey.

Such a survey is a cost effective method as it does not require printed papers to be distributed with to target respondents. It can also provide the researcher qualitative, quantitative, and very productive analysis approaches. It helps the researcher to display, retrieve, represent, and modify the collected data of the survey.

The main objectives of this survey were to investigate the Internet user' consciousness and understanding about spyware threats and anti-spyware services. In addition, the research investigated aspects of respondents' wider practices around Internet usage and information security.

4 Results

The group of participants (totalling 225 respondents) gave high reliability to the results of the online survey (See Figure 1, 2 and 3). The participants been invited through the invitation emails and the educational portal of the University of Plymouth. A notable finding is the lack of attendance for computer security training sessions (See Figure 4). Also, the security topics of the attended training sessions or courses were very general in terms of informative and practical contents. Some of the trained participants are still suffering from different Internet attacks, as well as unawareness of the important threats and security tools. The survey showed that the trained participants in general are the most aware and protected group of respondents

regarding to spyware threats. However, the study showed that the training sessions are not focusing or giving sufficient information about spyware and anti-spyware. Only 25% of the aware participants received some information about spyware from the training sessions they received from their organizations.

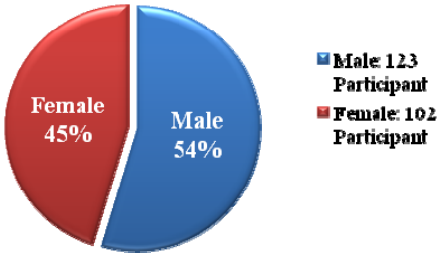


Figure 1: Gender balance of respondents (n=225)

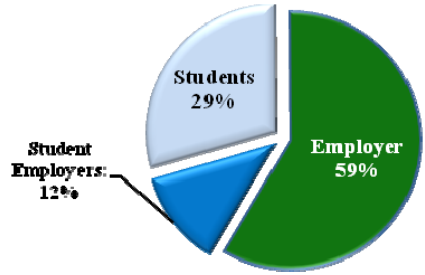


Figure 2: Current employment and/or student status

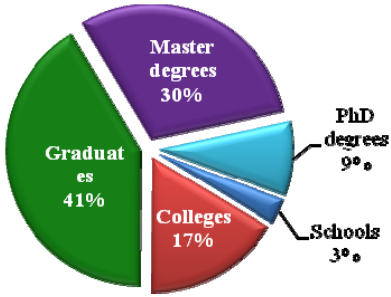


Figure 3: Level of education

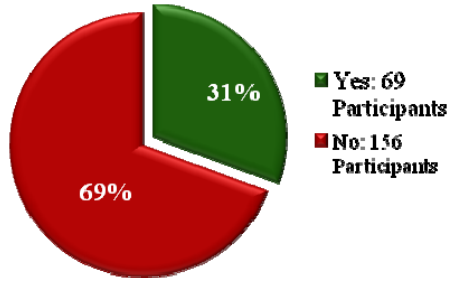


Figure 4: Attendance for any computer security course or training session

The findings have shown that the number of Internet attacks is significant (see Figure 5) and the level of awareness of the average Internet user is still a concern. However, the majority of the Internet users have shown real interest in attending training sessions and receiving instructions about Internet security in general and spyware in particular. Some organizations are providing their users effective protection tools but the training and awareness side is still poor and very limited.

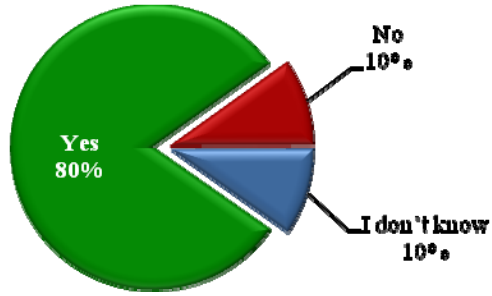


Figure 5: Experience of being attacked through the Internet

The research investigations showed that at least 2 from every 5 respondents have been attacked by spyware (see Figure 6), which represents a high number of attacks. In terms of awareness, 72% of the participants mentioned they knew about spyware threats and malicious activities while 28% of them did not. This result shows that for every four participants, there is at least one participant that had no idea about spyware at all (see Figure 7).

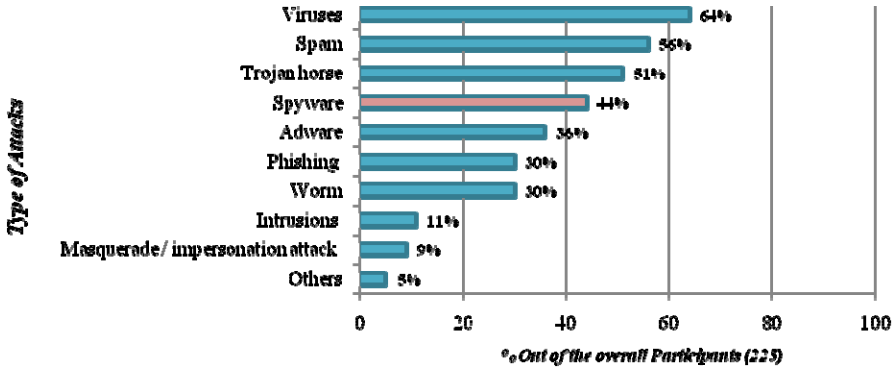


Figure 6: The type of attack that participants had experienced

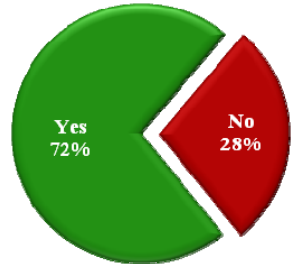


Figure 7: Knowledge about the malicious activities and threats of spyware

Regarding the participants' considerations of protecting, preventing, and cleaning their computer from spyware, the vast majority (79%) mentioned it is a very important issue (see Figure 8). While 18% of the respondents are feeling that spyware is representing a low or middle importance security issue. Further analysis revealed that most of those 18% did not attend any computer security course or training session while the majority of them had been attacked at least one time through the Internet.

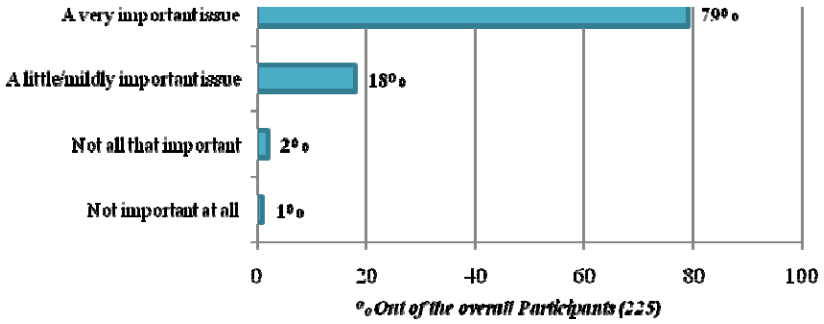


Figure 8: Importants of protecting, preventing and cleaning their PCs from spyware

The majority of Internet users depend on their antivirus systems for protecting themselves against spyware threats, whereas (68%) indicated that they are using specific anti-spyware (see Figure 9). It would seem from the results that a large proportion of these users cannot differentiate between viruses and spyware and between anti-virus and anti-spyware..

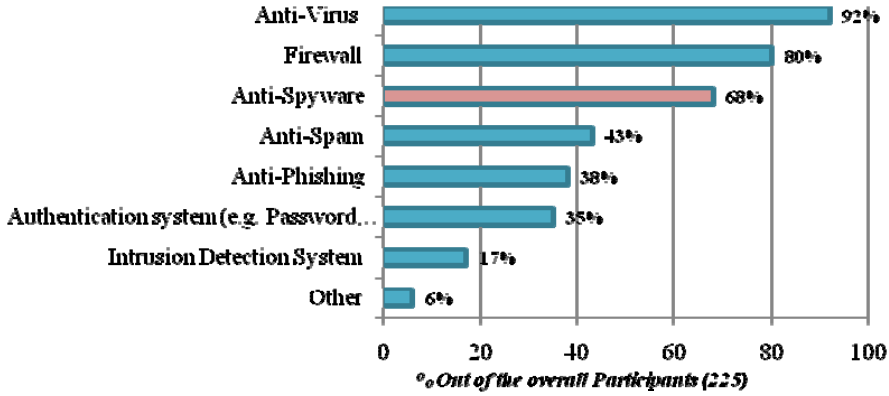


Figure 9: The protection that participants are using for their PCs

5 Conclusion

The findings of this research study provide some useful further information for this area of security interest. The increased number of spyware attacks and the lack of

user awareness about the threats and related protection were the main findings of the research study. Users' awareness in these areas is still very poor and they need to take more efficient steps to enhance their knowledge. The main cause was the lack of efficient training. The trained participants in general are the most aware and protected group of respondents regarding spyware threats. Nonetheless, the investigations still showed that some of the training sessions had not included any sufficient information about spyware threats and protection. Also, the educational courses of computer security had shown some derelictions for its awareness mission about computer and Internet security in general, and spyware threats and Anti-spyware awareness in particular. The Internet users' investigations had shown a good level of acceptance to know about the common Internet threats and the usages of the protection software by attending training sessions or by receiving information on the topic.

The organizations showed a good level of interest of supporting its staff and members with the protection tools and services. However, the training efforts are not sufficient and need to provide more effective training for their group of users. This training should give the attendant information about the common security threats. The training should also give practical advice for using the protection software, such as the ways of updating it, fixing and modifying the protection settings, use of the self-support options, etc.

The protection software usability and price were amongst the main barriers that prevented some of the Internet users from adopting them, while other users are using freeware and unlicensed products. Most of the licensed products that individuals use are related to organizations that provide them with the licensed protection services. The vendors need to offer a more efficient, usable, and informative awareness system about spyware and other common threats. Including such awareness-raising within the protection software will give users more ability to improve their awareness about spyware threats and anti-spyware protection services corresponding to the level of protection that they receive.

6 References

Awad, N.F. and Fitzgerald, K. (2005). "The Deceptive Behaviors that Offend Us Most about Spyware" *Communications of the ACM*, 48(8): 55-60.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). "A model for evaluating IT security investments". Communications of the ACM, 47(7).

Poston, R., Stafford, T.F., Hennington, A. 2005. "Spyware: A View from the (Online) Street" *Communications of the ACM*, 48(8): 96-99.

Cordes, C.S,. (2005) "Monsters in the Closet: Spyware Awareness and Prevention". EDUCAUSE Quarterly Magazine, Volume 28, Number 2, 2005.

Davis, F.D. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 13(3): 319-340.

Delio, M. (2004). "Spyware on my machine? So what?" Wired News, December 06, 2004.

Dinev, and Hu, Qing. (2007) “The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies”. Journal of the Associaton for Information Systems (JAIS),Volume 8, Article 2, pp. 386-408, July 2007.

Freeman, L.A. and Urbaczewski, A. (2005). “Why Do People Hate Spyware?”. Communications of the ACM. August 2005/Vol. **48**(8): 50-53 .

Furnell, S., Gennattou, M. and Dowland, P. (2002). ”*A prototype tool for information security awareness and training*”. Logistics Information Management. Vol.15 No.5/6 pp.352.

Furnell. S, Tsaganidi, V. and Phippen, A. (2008). “Security beliefs and barriers for novice Internet users", *Computers & Security* **27**(7-8): 235-240.

Hu, Q. and T. Dinev, (2005). “Is Spyware an Internet Nuisance or Public Menace?” *Communications of the ACM*, 48(8): 61-66.

Jaeger, M. and Clarke, N. (2006).” The Awareness and Perception of Spyware amongst Home PC Computer Users”. SCISSEC

Lee, Y. and Kozar, K.A. 2005. “Investigating Factors Affecting the Adoption of Anti-Spyware Systems,” *Communications of the ACM*, 48(8): 72-77.

Mazliza, O. and Rodziah, L. (2006). "Women in computer science: no shortage here!" Commun. ACM 49(3): 111-114.

Schmidt, M.B. and Arnett, K.P. (2005). “Spyware: A Little Knowledge is a Wonderful Thing” Communications of the ACM, 48(8): 67-70.

Schmidt, MB.; Johnston, A.C., Arnett, K.P., Chen, J.Q. and Li, S. (2008). “A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness” September 03, 2008, IGI Global Magazine for IT professionals.

Sipior, J.C. and Ward, B. (2008) “User perceptions of software with embedded spyware” Journal of Enterprise Information Management, Vol.21, No.1, pp: 13-23.

Thomson, K. Von Solms, R. Louw, L. (2006). ” Cultivating an organizational information security culture”. Computer Fraud & Security. Vol. 2006, Issue 10,Pages 7-11.

Zhang, X. (2005). “What Do Consumers Really Know about Spyware?” Communications of the ACM, 48(8): 44-48.

Analysis of Structure and Performance of Turbo Codes over Additive White Gaussian Noise Channels: Practical Design and Implementation

A.Anglin-Jaffe and M.A.Ambroze

Fixed and Mobile Communications, University of Plymouth, Plymouth, UK
e-mail: M.Ambroze@plymouth.ac.uk

Abstract

This paper is concerned with the design and effectiveness of a family of error correction codes known as Turbo codes. Turbo codes are correction codes used to eliminate errors from communications networks. This family of code has error performance levels approaching the theoretical limit outlined by Shannon (1948). These codes are applied in the practical setting of error correction in deep space communication. This paper reviews the current literature associated with turbo coding, then outlines and evaluates a practical design scheme for a turbo code. Modifications to the code to provide better error performance are described and the results generated are discussed.

Keywords

Error Correcting Code, Convolutional Code, Turbo Code, S Interleaver

1 Introduction

In 1948, Claude Shannon (1948) proved that by properly encoding information, any errors caused by channel noise could be reduced to an arbitrarily small value, virtually eliminating the problem of noise as long as the rate of information was less than the capacity of the channel. This was the foundation of the field of Information Theory, and laid the groundwork for perfect communication over imperfect channels. However, Shannon's work was all theoretical. He gave no indication of the actual code that would provide these values. Since that time, researchers have been working towards providing codes that begin to approach this "Shannon limit" (Dolinar and Divsalar 1995; Berrou et al 1993). These codes have evolved from relatively simple algebraic codes, up to the most current limit approaching codes. These codes approach Shannon's limit, even at very high levels of noise interference (Vucetic et al. 2007).

The purpose of this paper is to evaluate turbo codes, one of the near capacity achieving types of code. Practical programming techniques are used to create a convolutional coding scheme in addition to a Turbo coding scheme and these methods are compared. Modifications to the Turbo code are described, which involve both changing the style of the interleaver and changing the component codes. An analysis follows as to how these changes affect the codes' performance.

2 Turbo Codes

In the early 1990's Berrou, Glavieux and Thitimajshima (1993) presented a paper on a new line of codes that produced error rates closer to the Shannon limit than ever before, with far less complexity than the codes being produced at the time. These "turbo codes" have an interesting encoder structure consisting of the parallel concatenation of two convolutional codes separated by an interleaver. This interleaver rearranges the data before it enters the second convolutional encoder. After transmission, the information is decoded by two separate iterative decoders using a-posteriori probability (APP) decoding, with an interleaver and a disinterleaver between them (Berrou et al. 1993). This process cycles with the "confidence" level of the system increasing with each circuit. This is known as belief propagation. This circular motion resembles the feedback system of a turbine engine, hence the name "turbo code".

It is pertinent to consider the advantages and disadvantages of the turbo code design. The encoder is simple and performs much better than a convolutional code with a similar decoding complexity (Costello Jr. and Forney 2007), and as stated previously, the code closely approaches the Shannon limit. However, one of the major disadvantages of turbo codes is the presence of an "error floor", where the performance of the code levels off for bit error rates (BER) below 10^{-5}. This is because turbo codes have relatively small minimum distances between code words, so the likelihood of confusing one codeword for another creates a limiting factor in the correction process (Costello Jr. and Forney 2007). This error floor can be lowered by improving the interleaver design (Vucetic et al. 2007), but not eliminated.

3 Research Methods

The aim of this research project, more than simply bringing a theoretical discussion of the advantages and disadvantages in turbo coding, was to construct a practical framework under which turbo codes operate, in order to examine real world results. Therefore data was generated that could validate or repudiate the arguments set forth previously. A test environment was designed which mimicked the channel structure set forth in Shannon's paper. It consisted of: an encoder; a channel which the encoded signals pass through; and a decoder to process received signals. The testing area had the capacity to function both as a convolutional encoder and a turbo encoder. It was one of the aims of this project to compare the functionality of these two types of encoding technique. The effects of a change in interleaver design on the coding efficiency of a turbo code was also studied, in addition to the effects of changing the memory length of its constituent codes.

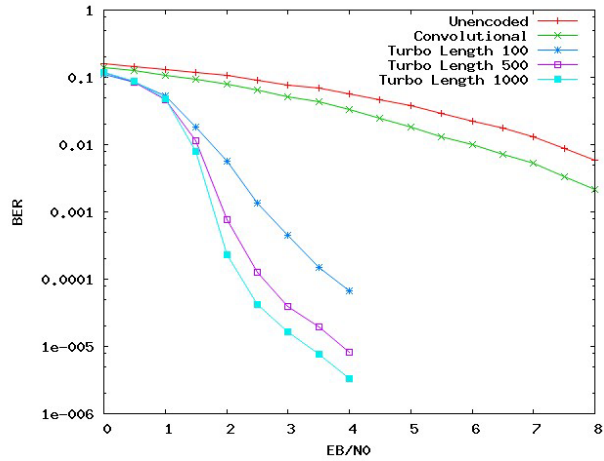


Figure 1: Bit Error Rates for Turbo Codes of Various Lengths Compared to Convolutional Codes and Unencoded Data

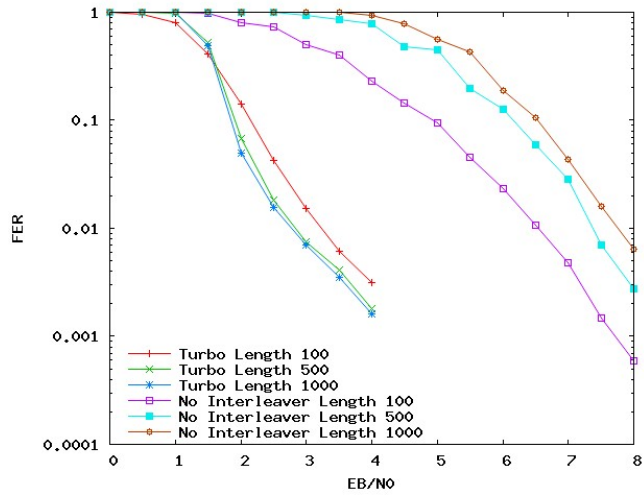


Figure 2: Frame Error Rates for Turbo Codes of Various Block Lengths and Code with No interleaving

4 Results and Analysis

Coding in the real world cannot yet hope to achieve Shannon limit levels of error correction. Each code behaves differently depending on circumstance, and as a result, there is a need to track many parameters to decide the best code to use for specific situations (Lin and Costello 2004).

The in graph in Figure 1 demonstrates the bit error rates for a number of different possible coding situations. The graph illustrates the relationship between turbo codes

and their constituent convolutional code. It also includes a baseline measurement. This measurement was collected by tracking the received values on the decoder side, and then evaluating their bit likelihood based on a simple positive or negative check. In this test, The turbo code significantly outperformed the convolutional code at low signal to noise ratios. Both codes outperform a simple positive or negative likelihood measurement, so it is clear that encoding the signals has an effect on signal reception.

However, the comparision between Convolutional codes and Turbo codes is uneven because Turbo codes transmit data at a rate of 1/3. This means an extra parity bit is sent in comparison to the convolutional codes. However, this can be corrected for by tracking data from a turbo code with no interleaver and no iterative process. This generates a 1/3 rate convolutional code. The previous data was generated to analyse bits in error. The frames (or blocks) in error were also evaluated. A frame is considered to be in error if a single bit in the processed block is in error. The comparison in Figure 2 shows turbo codes in comparison to their equivalent 1/3 rate convolutional codes (codes with no interleaver).

In addition to generating fewer bit errors, the turbo codes were more likely to transmit frames without error than equivalent rate codes. The coding gain here was very large, with a gain of 3-5 dBs even for very low amounts of frames in error. In addition the turbo code frame error rates improved with block length. The block length 500 code had an improvement of almost one full dB at rates below 10^{-2} in comparison to lengths of 100. In contrast, the non interleaved code had improved rates for smaller block lengths.

Changes in the turbo code affect code performance characteristics. Research suggests that modification of the interleaver can improve results in the “error floor” (Costello and Forney 2007; Vucetic et al. 2007). Dolinar and Divsalar (1995) set forth parameters for the creation of a pseudo-random interleaver which eliminates some of the problems of low weight encodings being transferred between the two component codes. Within this test environment a pseudo-random interleaver was created and programmed to function in the same place as the random interleaver. The resulting data is shown in Figure 3.

Both codes operated in a similar fashion for low signal to noise ratios. However, in the higher ranges of E_b/N_0, the pseudo-random code outperformed its random counterpart. However, in some cases, as in the block length 1000, it only slightly improved performance. The reason the interleaver design was specifically affecting the error floor area was because this floor represents the relatively small Hamming distances (the amount that two near codewords differ) between component codes being transferred to one another. With a random interleaver, at least some bit matchings were likely to be within a close range of one another. The S-random interleaver was supposed to correct for this, but in some cases the random interleaver did not have these performance problems, and therefore behaved as well as an S-random interleaver would.

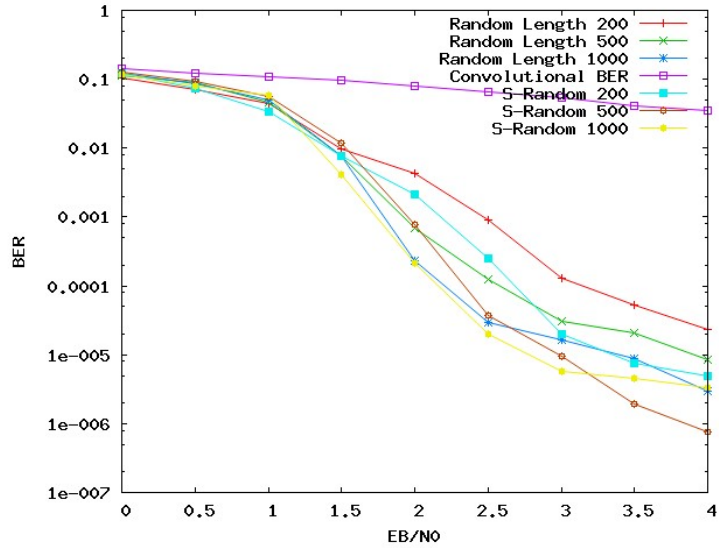


Figure 3: Bit Error Rates for Turbo Codes of Different Block Lengths and Varied Interleaving

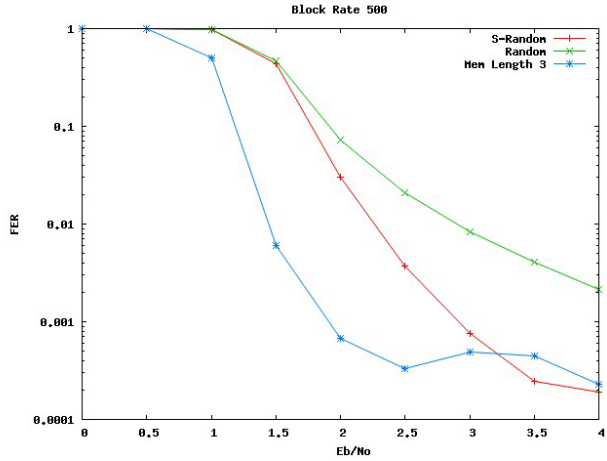


Figure 4: Frame Error Rate for Block Length 500 Turbo Codes with Random

A further significant element of turbo code construction is the design of the constituent code (Lin and Costello 2004). Initially, the experiment had employed a memory length 2 systematic recursive code. In the second stage this code was changed to a memory length 3 code, to evaluate if this produced an improvement. The code was also systematic and recursive, and had the octal notation of (15,13). It was one of the aims of this project to evaluate this code with the presence of both random and S-random interleavers as discussed above. The graph in Figure 4

evaluates the memory length 3 code with random interleaving, in comparison to the memory length 2 code with both the random interleaver and S-random interleaver.

From this chart it can be seen that the increased memory length did tend to improve the code performance. Even without the presence of a spread interleaver such as the S-random interleaver, it outperformed memory length 2 codes with the more advanced interleaver. The coding gain for these longer memory codes ranged from 0.5 dB to almost 1 full dB up to an E_b/N_0 of 2.5 dBs. After this point, the memory length 3 encoder performs poorly. This might be explained by the encoder encountering its error floor. The "waterfall" area for the memory length 3 encoder is much steeper than its counterpart memory length 2 codes. This means it reached error rates of less than 10^{-3} at 2 dBs. As can be seen by the S-random encoder, the memory length 2 encoder does not appear to slow its progress until it approaches the range of 3.5 dBs and greater. Another explanation for the performance of the memory length 3 code after 2.5 dBs may relate to programming difficulties. It is possible that somewhere in coded environment an overflow error occurred. As the memory length 3 code which was run in this experiment required such a large number of iterations, it is possible that there were too many iterations and a bit flip occurred to reset the frame numbers back to 0.

When the component code design change was combined with the interleaving design changes, the combination resulted in slightly better code performance, as well as a slightly lowered error floor. The longer length codes continued to outperform the shorter ones, giving extremely good bit and frame error rates at low SNRs. These codes had BERs of below 10^{-5} at signal rates of 1.5 dBs which is similar to results generated by other researchers (Dolinar and Divsalar 1995; Andrews et al. 2007). However, after 1.5 dBs the slope of the curve changes, as the turbo code entered its error floor area.

The performance of the S-random interleaver for low block lengths gave very marginal improvement. This is due to multiple factors. First, the choice of termination for the S-random interleaver created additional bit errors. Secondly, at lower block rates, the S-distance was smaller and thus could not guarantee improved Hamming distances.

4.1 Discussion of Results

The data suggest that at low memory lengths turbo codes significantly outperform their component convolutional codes, especially at low signal to noise ratios. At high memory lengths, convolutional code performance can be brought closer in line with that of the results here, but the decoding complexity is similarly increased (Divsalar and Pollara 1995). If the available signal to noise ratio is high, and the code required is short, it is possible that shorter convolutional codes may match turbo output. If a hard input-output algorithm was chosen, such as Viterbi decoding, their decoding complexity would be less than turbo codes.

The S-random interleaver created was terminated through a simple process, but one which unfortunately did have limitations. After running through all choices, if no possibilities existed outside the S range, the interleaver simply selected an unused bit

which was within the S-range and continued on. This could be responsible for the same type of bit errors that can be found with random interleavers, and also made the last bits in the stream (those most likely to run into seeding problems) less protected than other bits. This meant that the spread interleaver was not operating optimally and thus the results were closer to random interleaver performance.

The memory length 2 code was unfortunately too short for it to convey an effective relationship between its memory and its encodings. If more interleavers were added, and three memory length 2 codes or more were employed, these short codes might prove to be more effective, as demonstrated in Divsalar and Pollara (1995) and Andrews et al. (2007). However, the memory length 3 code performed much better in the presence of a single interleaver. In terms of practical coding in real world systems, the DVB-RCS standard specifies a code of memory length 3, (Douillard et al. 2000) which has a similar representation as the encoder employed in this project. In addition, while it appears that the modification of the code was a more significant change than the introduction of a new interleaving technique, it is more likely that this relates to the poor performance of a memory length 2 code and an already good performance of random interleaving. It is likely that further modification of the internal coding structure would produce less significant gains; however, further study is needed into the subject.

5 Conclusions

The initial hypothesis was that codes with designed interleavers and a longer memory length would outperform the original code with a length 2 memory and random interleaving. This proved to be the case, but not to the expected extent. As mentioned before, the improvement of the interleaver seemed to play less of a role in coding gain than other factors, such as increased block lengths and component code design. However, when taken against the same type of code with no interleaving, the performance gain was significant. Therefore, the interleaver must play an integral role in improving code performance. It must be concluded, then, that the lack of improved performance from designed interleavers can be attributed to design flaws, and thus these codes were not able to show further coding gain.

The aim of this research was to study the design and structure of turbo codes. In terms of the literature a lack of clarity remains as to how these codes manage to perform so well, or how they can be optimized (Andrews et al. 2007). The error floor can be lowered, but its existence still suggests a flaw in the code design. This experiment was carried out to analyse what components of turbo code design contribute to code improvement. It was found that a combination of increased component code memory length, as well as a pseudo-random interleaver, led to much better code performance. In addition, the longer block lengths performed much better than shorter ones, due to an increased length interleaver.

The field of turbo coding is wide-ranging and there are so many pieces of the codes' design that can be modified. This means that the scope for future research is extensive and can be fruitfully explored until the perfect code is found for all situations. Other types of spreading algorithms should be pursued and evaluated for performance. Of the interleaving types currently available, many perform very well

in lowering the error floor, but none have eliminated it completely (Vucetic et al. 2007). Surveying more interleaving techniques should lead to identifying the design flaws in the interleaver. The possibility of designing a “perfect” interleaver is still debatable, but analysis of each separate interleaving technique may result in more patterns for “good” interleaving. For example, analysis of row/column interleaving led to conclusions on random interleaving performance and introduced the concept of “spreading” (Divsalar and Pollara 1995). Other factors are yet to be discovered in relation to interleaver behaviour and thus may lead to further improvements in design.

These codes continue to be effective technologies to ensure that optimal communication is possible on noisy channels. Satellite technology would not be possible without these forms of error correction to overcome the interference levels which deep space environments impose on communications. Until the perfect code is found, these codes will continue to be improved on to ensure error free communication. The MESSENGER spacecraft, Mars Reconnaissance Orbiter, and New Horizons are all currently using turbo codes for the return of their data to earth. Improvement of these codes will mean that images transmitted from space will be able to be sharper and more detailed, and even opens the possibility of sending movies.

6 References

Andrews, K.S., Divsalar, D., Dolinar, S., Hamkins, J., Jones, C.R., and Pollara, F. (2007) “The Development of Turbo and LDPC Codes for Deep-Space Applications.” *Proceedings of the IEEE.* Vol. 95(11), 2142-2156 [Online] Available at: http://ieeexplore.ieee.org/.

Berrou, C.; Glavieux, A.; and Thitimajshima, P., (1993) "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," *Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record, IEEE International Conference on* , Vol.2, no., pp.1064-1070 [Online].

Costello Jr., D. J., and Forney Jr., G.D. (2007) “Channel Coding: The Road to Channel Capacity” *Proceeding of the IEEE.* Vol. 95(6), 1150-1177 [Online] Available at: http://ieeexplore.ieee.org/.

Divsalar, D. and Pollara, E. (1995) “Turbo Codes for Deep-Space Communications”, *JPL TDA Progress Report* 42-120.

Dolinar, S. and Divsalar, D. (1995) “Weight Distributions for Turbo Codes Using Random and Nonrandom Permutations”, *JPL TDA Progress Report* 42-122.

Douillard, C., Jezequel, M., Berrou, C., Brengarth, N., Tousch, J., and Pham, N., (2000) "The Turbo Code Standard for DVB-RCS", 2nd International Symposium on Turbo Codes and Related Topics", Brest, France.

Lin, S., and Costello, Jr., D.J. (2004) *Error Control Coding: Fundamentals and Applications 2nd Ed.* Upper Saddle River: Pearson Prentice Hall.

Shannon, C.E. (1948) “A Mathematical Theory of Communication” *Bell Syst. Tech. J.,* Vol 27 pp. 379-423 and 623-656.

Vucetic, B., Li, Y., Perez, L.C., and Jiang, F. (2007) “Recent Advances in Turbo Code Design and Theory” *Proceedings of the IEEE.* Vol. 95(6), 1323-1344 [Online] Available at: http://ieeexplore.ieee.org/.

Watermarking using Side Information

A.Antony and M.A.Ambroze

Fixed and Mobile Communications, University of Plymouth, Plymouth, UK
e-mail: M.Ambroze@plymouth.ac.uk

Abstract

Digital Watermarking was developed so as to prevent the illegal use of the digital media. The extreme significance of it started when cybercrimes started to multiply. To a large extend watermarking was capable of preventing such misuse. However with the rise of threats to the watermarking, there was an acute requirement of some technological improvements so as to sustain the fact of securing digital data within the communication systems. The approach to solve this problem was by modifying the existing watermarking schemes corresponding to the levels of security and robustness. The main aim of this paper is to develop a watermarking scheme which has the properties of robustness to attacks and at the same time providing considerable amount of security. For this a research was conducted for attaining this objective and the results publicized that watermarking in the frequency domain can attain this criterion when compared with the schemes of watermarking in the spatial domain. So, a watermarking scheme, in discrete cosine transform (DCT) was experimented for this purpose on the frequency domain. This scheme was supposed to undergo geometric distortions like rotation and cropping. Finally the results revealed that this was really substantial in most of the cases to that of the schemes in the spatial domain like LSB watermarking mainly.

Keywords

Watermarking, Discrete cosine transform, LSB, Robustness, Security

1 Introduction

The very first discussion about the watermarking was made in the year 1979, as a unique method for the production of machine detachable patterns and signs to recognise anti-fraud and anti-counterfeiting activities (Szepanski, 1979). Though this was not been adopted for any real life applications, after around nine years a study was published where an identification code was embedded on an audio signal and this was the very first time that the phenomena of digital watermarking was brought into applying on it (Bani and Bartolini, 2004). From there on there had been tremendrous outbreak of the papers. The growing numbers of papers had been increasing exponentially since 1990 (Cox *et al.,* 2002). This implies that plenty of applications related to the digital watermarking was been wide spread.

Normally in a watermarking process a watermark is added to a cover object to form up a watermarked image. The sender and the receiver share a secret key in order to make this communication secure. However, Steganaography can be classified based on two types they can be either fragile or robust. Fragile schemes of watermarking are easily destroyed if any variation happens to the watermark inside. But, the robust

watermarking schemes are capable of resisting this (Cummins *et. al*., 2004). Based on accruing this specifically the detection mechanism must be efficient.

In this paper, the research was concerned in analysing on the steganographic watermarking using the informed detectors. Normally, detectors used are of two types they can be Informed or Blind. Informed detectors are the ones in which the watermarking information is known to the sender and the receiver (Al-Houshi, 2007). So the only work that is involved with the receiver is that it has to compare with the original cover image, when it is supposed to check for the presence of the secret. Hence, the factor of complexity involved is much less.

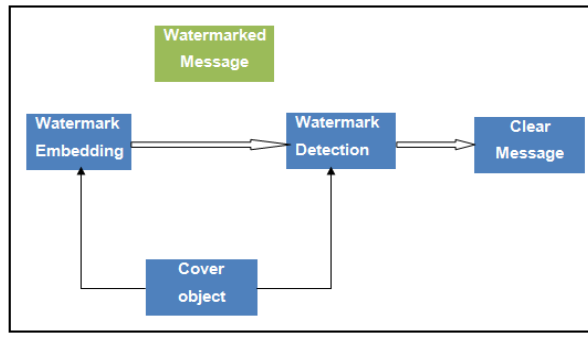


Figure 1: Watermarking using Informed Detctors

In the research we conducted, we where expected to find out a method that could considerly have robustness and security at the same point. The investigation started by analysing on the Least Significant Bit hiding method in the Spatial Domain.

Considering the LSB coding, it is also known as bitpalne coding. In this it basically tries to encode secret information by substituting the secret information on the insignificant parts of the cover. The receiver can extract it easily if he is aware of the secret and knows the positions where exactly it is embedded. Here only very minor modifications are made and it is all upon the assumption that it wont be noticed by the a passive attacker. Our research handled on Bitmap files as, there won't be many losses involved and hence data can be easily manipulated and recovered.

Now analysing of the LSB substitution, it is used on one bit on a very minimum case and that is expected to be distributed over the cover when it is embedded. Which means there will be change in *Ci* (cover image) due to message, *Mi* (*Mi* is either 1 or 0). However this becomes slightly efficient when it uses more bits when swapped with the cover and the secret. Finally in the process of extraction, the LSB of the selected cover elements are extracted and lined up to form the secret. In the process of decoding, the receiver must be capable of knowing how many elements are to be used in the embedding process. In a very simple case what really happens is that the sender would be using all the cover elements to make the substitution starting from the first element. As the secret is having really less number of bits than the l(c) (length of the cover), the embedding process gets over long before the end process of the cover. So, there are possibilities of some cover elements getting unchanged. Now

this is going to be a serious issue creating security problems. To overcome the above mentioned issue it is enough to make the length of the cover and the secret to be the same, i.e., l(c) = l(m)

Now when this is done there will be changes in the number of elements for transmission. When this happens there will be a suspicion in the mind of the attacker and may make him think that some secret is getting exchanged since there is a slightly high variation in the bandwidth consumption.

Hence, another sophisticated approach is the use of psedorandom number generator for spreading the secret message. If both the sender and receiver share a key *k*, used to generate numbers, it will be much efficient to a certain level reducing the level of getting attacked (Katzenbeisser and Petitcolas, 2000).

Now the limitation still existing is the impartment of attacks over this kind of technique. LSB watermarking is not at all resistant to any kind of attacks. Hence there is no phenomenon of robustness involved in them with very less amount of security. So, the research had to take up some other measure so as to improve the above facts.

As this was analysed the research had to turn up towards some other watermarking scheme which could hold attacks. Analysing deeply it was found that the Frequency domain techniques can hold attacks much effectively. Hence a watermarking scheme in the frequency domain was formulated namely the Discrete Cosine Transform.

2 Testing Methodology

Watermarking in the Discrete Cosine Transform is one of the popular hiding technique which works in the frequency domain. In this the relative size of the coefficients is taken into picture. As per the concept we can take two or more of these coefficients. However in this research it has taken up just taken up two coefficients. Again the research is considering a system which makes use of digital covers. This is quite similar to the proposal by Zhao and Koch (Zhao and Koch, 1995).

The investigation is taken into account of a cover communication where a secret is shared in the form of an image between a sender and a receiver. For this in the sending part, we are splitting the cover image into blocks of 8 X 8 pixel and each of these blocks encodes exactly one secret bit every time. Again, in the embedding part we will be selecting a particular block and this will be considered to be in of the same nature. For example if the embedding starts with the selection of a sequence b_i which is used to code the message bits then we can then calculate the discrete cosine transform of the blocks easily using the formulae ,B_i =DCT { b_i }.

Now as per the concept the sending part and the receiving part is supposed to agree in the location of the 2 particular coefficient values in DCT which is to be used for the purpose of embedding. If we are taking up those coefficients to be (u1, v1) and (u2, v2) there are many criteria that these coefficients must satisfy. They must correspond to the cosine functions and must be with the middle frequencies. Doing

this ensures that the information or the secret is contained in the significant parts of the image or the cover. Again the intension behind this is that the secret wont be destroyed by the compression taking up. Hence to maintain robustness to the newly formulated system, it is essential to select the DCT coefficients with equal quantization values.

As per the algorithm, every time a block satisfies the condition B_i (u1, v1) > B_i (u2, v2) it is "1", otherwise it holds the value "0". In the process of encoding, the two coefficients are been swapped if the relative sizes of those two coefficients is much less when compared to the bit to be encoded. By doing this it can affect the relative sizes of the coefficients and during compression the algorithm here make use of a condition and add on some random values for both of the coefficients such that |B_i (u1, v1) - B_i (u2, v2)| > x for every x >0. Here x in this case is assumed to be the gain, higher the value of x corresponds to higher amount of the robustness in the compression. Then the sending part will take the inverse DCT to convert it from the frequency to the space domain. In the decoding section the image is DCT transformed initially. Then making a comparison over each block, i.e., searching for the two coefficients over every block the secret can be restored. If the value of 'x' and the coefficients are selected properly then there will be robustness in the image obtained. The detailed algorithm of implementation of both encoding and decoding is mentioned below.

But the most notable drawback of this system so far analysed is that it wont discard any of the blocks where the relation of the DCT coefficients are not satisfied. In such a case there will be considerable damage in the image (Johnson and Katzenbeisser, 2000).Now the theories say that there is pretty large amount of robustness involved in this using the substitution method. Now the question is how we can measure it. It can be done by implementing attacks over this watermarking scheme.

The DCT watermarking can be done making use of the logic above, now the robustness of that can be calculated, by making some geometric distortions on them. Analysing the fact that small geometric distortions can create distortion to the secret message and prevent in the detection of the watermark (Lin *et. al.,* 2001), the marked cover is been experimented by rotate and crop.

For the purpose of this initially, we did the watermarking in the DCT domain and studied the variations that happened. Analysing them attack where implemented on them. We took a 512 X 512 standard grayscale image of lena as the cover and a black and white secret image as the secret. The framework used was matlab R2007a.

3 Results and Discussions

Results obtained in the case of the normal DCT watermarking was not that different from any of the spatial domain schemes. The usage of informed detectors, vanished the problem of receiving adequate robustness in the subjected methodology. However, there was variations in the secret and the cover when they where subjected to the rotate and crop. Although the cover didn't have considerable amount of variations apart from the normal problem of loosing the luminance coefficients, the

variations in the secret was dramatically, increased when rotated for higher angles and cropped with different coefficients.

3.1 Rotating the cover

Sl No:	Angle in (Degree)	Rotating Clockwise	Rotating Anti-Clockwise
1	0.012		
2	0.05		
3	0.1		
4	0.5		
5	1		
6	5		

Table 1: Secret image modifications with rotation of cover

In rotation the watermarked image is subjected to rotate over an angle. As told earlier in the background, the watermarked file is created by randomly swapping pixel coefficients. Now when rotation is done what specifically happens is that, there involves a "cyclical shift" in the coefficient values which was used in watermarked by swapping (Lin *et al.,* 2001). This fully corresponds to the unequal displacement of the secret image in this case. Now, retrieval of the secret image is really hard at the time being as the coefficients swapped are fully out of order when considered with the initial arrangement. Although if it is the case, if the watermark or the secret image is tried to recover at this point, it is sure to have errors on it. In simple words, it can be assumed that the watermark is expected to be fully degraded. Now the question at this point is how the research did managed to get some visible part of the secret image with very slight errors. This is because, before detection of the secret image it is subjected to be "resized" to the normal size of 512 X 512. This proves that robustness is less when rotation is done but, the watermark can be extracted with minor errors considerably on very small or finer angles. Experimenting on larger angles is reveals that there is no part of the secret that could be retrieved. This is because there is a maximum limit to which recovery of the image can be made with the point of rotation. From around 500 executions made these results were analysed. Again another point to be discussed is why degradation is more in the case of anti-clockwise rotation when compared to the clockwise rotation. This is because rotation is combatable more in one direction alone and not in the other direction (Lin *et al.,* 2001).

3.2 Cropping the cover

In the initial observations of the outcomes on the survival of watermark, it is understood that when the coefficients are given as input with minor variations from the standard size of the image, then the watermark survives.

Sl no:	Pixel Coefficients (used for cropping in the Rect function)				Secret Image Recovered after Cropping
	X_{min}	Y_{min}	Width	Height	
1	1	1	510	510	
2	2	2	508	508	
3	3	3	511	511	
4	250	250	500	500	
5	500	500	500	500	
6	512	512	512	512	
7	64	250	500	500	

Table 2: Secret Image modifications with cropping

As per the results, only in case 1 shown in table 2, this is the only point that a watermark has survived reasonably well. The explanation to this is generally that the pixel coefficients randomly used in the DCT watermarking in the frequency domain is not disturbed much. The watermark survived just because the randomly distributed pixel coefficients used in DCT is almost in the center of every block. As long as this is not disturbed there would not be any other considerable variation. In all situations the degaradation is more. While cropping, a function called the 'rect' in matlab was used to take pixel positions as the input. Now, the notable point is that, depending on the values given as input there will be variations in the cover and the watermarked image. In case 7, it is observed that the cover image is been scaled, although the watermark is completely degraded. If the cropping of the image is not symmetric when considered on both rows and columns, then there will be scaling of the image to a "canonical size" with an associated "translational shift" (Lin *et al.,* 2001). This is the reason for scaling of the image, when cropping was performed at this point as the geometric attack.

4 Conclusion and Future Works

The results that we got in the case of rotation and cropping significantly proved that the DCT watermarking had potentially higher resistance in the case of robustness and security, when compared to the spatial domain techniques like the least significant bit hiding. Although the research fundamentally aimed in getting a centum performance on acquiring robustness and security, another prime objective was to

work on the watermarking with side information which was not yet achieved due to the limitation of time and the pace of research. To make this possible, more investigations must be done in the principles of spread spectrum techniques of watermarking and on concepts to improve, for bringing blind detectors to work like informed. Error analysis can be further done on the scheme that we have proposed, if this is done significantly well then, there will be more effectiveness achieved of this proposed model. Investigations even should be done regarding the experimentations of using different cover images including different colour patterns. If attacks are done more than one at a time, is yet again a possible area to be researched into.

5 References

Al-Houshi, (2007), 'Watermarking using Side Information' MSc. Thesis, University of Plymouth

Barni, M., Bartolini, F., (2004), '*Watermarking Systems Engineering: Enabling Digital Assets Security and other applications'.* New York, USA

Cox, I J., Miller, M L., Papathomas TV., (2002) '*Digital Watermarking*' London, UK: Morgan Kaufmann.

Cummins, J., Diskin, P., Lau, S., Parlett, R.,(2004) '*Steganography and Digital Watermarking*' School of Computer science, The University of Birmingham.

Katzenbeissser, S., Petitcolas, F., (2000) '*Information Hiding Techniques for Steganography and Digital Watermarking*' Chapter 3: Survey of Steganographic techniques Page nos: 43-74 Artech House, Boston, London

Lin, C. Y, Wu, M., Bloom J.A., Cox, I. J., Miller, M.L., Lui, Y. M., (2001) '*Rotation, Scale, and Translation Resilient Watermarking for Images*' IEEE Transactions on Image Processing, Vol. 10, No.5

Sepanski, W., (1979) '*A signal theoretic method for creating forgery-proof documents for automatic verification*' Proceedings of Carnahan Conference on Crime Countermeasures (May 16-18, 1979), by John S Jackson Page no: 101-109

Zhao, J., Koch,E., (1995) ' *Embedding Robust labels into images for copyright protection'*, in Proceedings of the International Conference on intellectual property rights for information,knowledge and new technique, Munchen ,Wein: Oldenbourg Verlag, 1995,pp 242-250

Trend Analysis of Snort Alarms

K.Chantawut and B.V.Ghita

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

Abstract

Network intrusions have been active topic for researches for many years. However, in order to gain insight into the nature of the current threat on the Internet is challenging. This paper, addresses this problem by systematically analysing a set of traffic trace collected over three months in front of the firewall at the Internet gateway of the University of Plymouth. The motivation of this study is to quantitatively understand the nature of the current Internet threat which leads to long-term analyses of trends and the recurring patterns of attacks. In the study, fundamental features of intrusions activities was investigated by evaluating the log data along a number of aspects (e.g. daily volume of intrusion attempts, the source and destination of the intrusion attempts and specific type of intrusion attempts, etc.). The result of the study shows both a large quantity and wide variety of intrusion attempts. It also shows that numerous amount of denial of service and ICMP scanning activities can be detected as common threats on the Internet. The patterns of these activities can be found at daily timescale and the on/off patterns exhibit recurrence of correlated behaviours. Furthermore, worms like SLAMMER and Sasser.D still persist on the Internet long after their original release. Deeper investigation reveals that sources of intrusions spread all over the globe. However, a major proportion of intrusions are from China. Also a very small proportion of sources were responsible for a significant portion of intrusion attempts for a given period of time.

Keywords

Trend analysis, Intrusion detection system, Snort, DoS, SLAMMER

1 Introduction

Prevention is normally recognized as the best strategy to protect critical information infrastructure from malicious attacks. Security staffs or network administrators must understand the trend of the threats in order to be able to prevent any catastrophic damage to their networks in advance. The understanding of the trend of the attacks would help organisations to determine the current fitness of their security systems and the budget for improving the system to defense against cyber attacks due to the uncertainty of the occurrence of the attacks.

Even though, currently, there are various tools to help analysing intrusion data, for example, BASE (Basic Analysis of Security Engine), SnortSnarf. These tools provide querying and presenting the intrusion analysis in easy to use graphical mode. However, the tools offer only basic and limited set of analytic options to users. It is not possible to perform in depth statistical analysis using these tools, for instance, to

look for the trends of attacks from specific country or to forecast the trend in the future. This is the initiative why this study was conducted.

Instead, the research has involved obtaining and anonymising the traffic traces coming toward the university as the inputs to the IDS, then extracting and analysing the output of the IDS to gain an understanding of the behaviours of the threats (e.g. the source countries, number of attacks per unique IP, the distribution of attack on the targets) and be able to analyse the nature of some of major threats using normal statistic and time series analysis theories.

2 Related Studies

The trend analysis of network attacks is an important subject in IDS. Many of related studies have been focused in the field of the analysis of Internet intrusion trends. Many of the studies are based on packet level investigation of intrusion logs generated by either firewalls or IDS.

The well known projects existing on the Internet that have been set up to collect large scale attack data from firewall and intrusion detection logs are the SANS Internet Strom Center and Symantec's Deep Sight system.

(Moore, 2004) provides the analysis that gives a better understanding of the nature and the long term trend and recurring patterns of the denial-of-service (DoS) attacks on the Internet. The study concludes that DoS attacks are a common threat for those depending on the Internet.

The study of (Yegneswaran, 2003) investigates fundamental features of intrusions activities by evaluating the log data along a number of dimensions (e.g. daily volume of intrusion attempts, the source and destination of the intrusion attempts and specific type of intrusion attempts, etc.).

The studies of (Jouni, 2009; Kim, 2007; Wu, 2005) focus on finding best-fit forecasting model for the studies of anomaly detection analysis. (Wu, 2005; Jouni, 2009) present various types modeling techniques based on time series analysis for representing the dynamic of intrusion and attack activities including the comparison of the model accuracy.

3 Common Intrusions

3.1 Viruses and Worms

Typically, viruses are attached to excusable files and they need human interaction to infect target hosts. A virus may only exist on a computer and it cannot be spread without a human action, by sharing infecting files or sending e-mails with viruses.

A worm is similar to a virus by its design. However, it has the ability to copy itself from machine to machine through computer networks. A worm takes advantage of known vulnerabilities in software or the operating system. The infected computer

could send out hundreds or thousands of copies of itself. The end result is that the worm uses up computer time and network bandwidth causing service outage.

3.2 Scanning

The purpose of scanning is to collect as much information as possible about target networks or hosts using tools to send probes into targeted systems and listen to the response which is coming back. At the end, if it is successful, attackers will gain information about vulnerabilities and openings (i.e. ports or services or live hosts) of victim's networks.

4 Network based Intrusion Detection System (NIDS)

NIDS monitors the traffic in specific network segment or subnet. NIDS looks for anomalies in the traffic, such as port scanning or denial of service attacks. In order for NIDS to be effective, it has to be located where it can monitor the most traffic that an organization deems critical. Therefore, placement is critical to the success of uncovering of anomalous traffic or behaviour in the monitored area.

There are, typically, two types of detection mechanisms using by NIDS which are **"signatures (or rules) based detection"** and **"anomaly based detection"**. In signature based detection, the NIDS look in bytes codes and expressions to match any known attacks expressions (signatures or rules). When it matches any intrusion, flags an alarm. Signature based detection is useful for detect known threats but it cannot detect new unknown threats or even the variants of already defined attacks.

In anomaly based detection the NIDS first establishes a normal activity model (a baseline) after training the system for specific period of time. Then the NIDS will use the baseline model to detect suspicious events that deviate from normal activity model. If an anomaly is detected, the will flag alerts for an intrusion. The benefit of anomaly detection is that it can detect unknown threats without having to understand the cause of the threats. The main problem for this approach is that it is prone to false alarms.

Snort is the most famous open-source intrusion detection system capable of performing packet logging and analyzing real-time traffic on computer networks.

5 Time Series Analysis

In general, the analysis of a time series will be based on the fact that observations close together in time will be more closely related than observations further apart and values in a series for a given time will be expressed as deriving in some way from past values, rather than from future values.

5.1 Stationary Time Series

In stationary time series, the random variables fluctuate about a fixed mean level, with constant variance over the observational period. This property is a requirement

for time series analysis because there must be a sort of regularity exists in the time series so that the behaviour of the time series can be predicted. Various levels of stationarity exist; however, in a context of univariate time series, the time series must satisfy the assumption of **"weakly stationary",** that the mean is a constant, independent of any time shift.

5.2 Autocorrelation (ACF)

ACF is a statistical measure that captures the correlation between different time shift samples (or lag) of the process. (NIST/SEMATECH, 2006) has summarised the main purposes of ACF into two points. The first purpose is to detect the non-randomness in time series and the other is to identify an appropriate time series model if the data are not random.

5.3 Long Range Dependency (LRD) and Self Similarity (SS)

A stationary process is said to be "Long Range Dependence (LRD)" if it has a high degree of correlation between distantly separated data points, even across large time shifts. Whereas in short range dependence processes, the correlation between values at different times decreases rapidly as the time difference (lag) increases.

"Self Similarity (SS)" is a property of an object whose appearance remains unchanged regardless of scale of which it is viewed. Self similarity detected in the intrusion data could explain certain characteristics and behaviours of a specific intrusion attempt. It is also useful to note that some self-similar processes may exhibit LRD, but not all processes have LRD are self-similar. The degree of SS and LRD can be estimated by the calculation of "Hurst parameter (H)". For a self-similar process with LRD, the value of H will be in the range of $0.5 < H < 1$. As $H \rightarrow 1$, the degree of both self-similar and LRD increases. Any pure random processes would have $H = 0.5$.

6 Examining Snort Alarms

6.1 Data Collection

The data for this study was collected from the Internet gateway of the University of Plymouth network. The collection used a SPAN port of a layer-2 switch located in front of the university's firewall to capture traffic. The reason for this is to ensure that the overall behaviour of Internet attacks on internal network can be studied; otherwise the firewall would filter out most of the attacks before the traffic is captured. The purpose of the study was not to test the efficiency of the university firewall, but to observe the amounts, structure, and evolution in time of the alarms.

Capturing network traffic on high speed network requires very large storage. Therefore, in order to overcome this problem, Snort, running in packet logger mode, was utilised to capture only header parts of the network traffic. The filter was set to capture only the traffic destine to the internal subnet of the University of Plymouth

(UoP) network. The traffic traces were collected from 24/04/2009 to 28/07/2009 period.

Due to user privacy and network security concerns, the destination IP addresses of traces (i.e. the IP addresses within the university) had to be anonymised in prefix-preserving way prior to the analysis, so that the traces would still contain the structure of the subnet. More details on the anonymisation tools used and the associated procedure can be found in (Koukis, 2006; Foukarakis, 2007)

Then the next step was to analyse the released anonymised traces using snort. For this study, Snort (version 2.8.4.1 and VRT Certified Rules released on 21/07/09) was run in off-line mode to detect alerts in the captured traffic traces using signature based detection method. As the large amount of traffic traces were analysed, the unified alert record format was set as the output in the snort.conf because of the small size and the completeness of details contained in the output.

Subsequent to successfully creating the complete unified alerts, Barnyard was used to convert all the unified alert files generated by snort into a single output file in ***csv*** format.

6.2 Distribution of Alerts

There were totally 71 types of alerts, distinguished by unique Snort's signature ID (SID), detected by Snort which contributed the total number of 157747024 alerts. Only 3 types of alerts, which are triggered by Snort Signature IDs (SID) 2003, 2004, 2050 represent almost 95% of all the attacks. It was found that these alarms were all represent the MS-SQL (SLAMMER) worm attacks and generated by the same packets and similar snort rules. Therefore, the duplicated alarms were removed and the distribution of SLAMMER alerts is plotted in Figure 2.

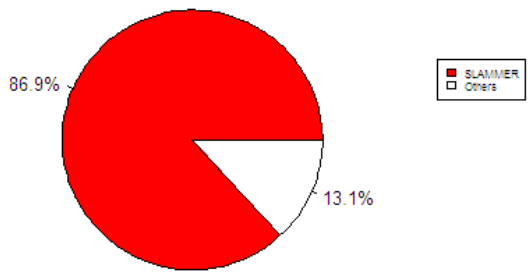


Figure 2: Distribution of SLAMMER attacks

Nevertheless, even the duplicates were removed, the proportion of SLAMMER is still very large (87%) compared to the others. The next figure shows the distribution of other alerts after removing SLAMMER.

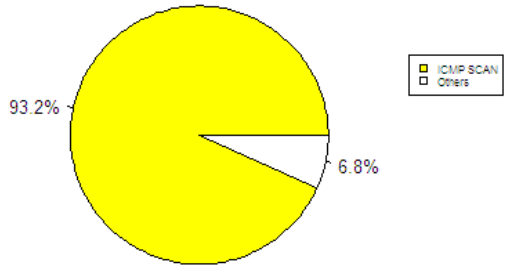


Figure 3: Distribution of ICMP Scanning attacks

After removing SLAMMER, it was found that there were another 3 types of ICMP scanning attacks presented as the majority in the alarms, which were ICMP NMAP PING (SID469), ICMP L3retriver (SID466) and ICMP PING CyberKit (SID463). All these scanning attacks represented 93% of the rest of the alarms.

From the above analysis, it can be said that the majority of intrusion attempts on the Internet were governed by SLAMMER and ICMP scanning attacks. Therefore, the trend analyses were based on SID2003 to study the trend of SLAMMER and SID469 to study the trend of ICMP scanning. The results of the study would represent the trend of the majority of the attacks on the Internet.

6.3 Analysis of SLAMMER

The analysis of SLAMMER attacks showed that the attacks came from all over the World (i.e. 125 countries). However, the majority were from only top five countries which were China, Korea, the United States, Romania and Mexico. China was the main contributor of SLAMMER attacks and all the top attacking hosts were all in this country. The analysis also showed that the majority of SLAMMER attacks on the Internet were governed by only small clusters of hosts each automatically and constantly broadcasting a vast number of the worms and the number of attacks did not necessarily depend on the number of the attacking hosts. Additionally, it was found that the periodic pattern of attacks in every 24 hour might cause by the competition for Internet bandwidth among the SLAMMER sources and the packet drop by SPAN port overloading during peak hours. There was no specific target of the attacks as the number of attacks on each unique IP was normally distributed all over class B of the University of Plymouth's allocated space. The analysis of the time series of number of the attacks per hour showed that the time series was nonstationary, however, strong degree of correlation and periodicity could be spotted from the ACF plot which supported by further analysis on Self Similarity (SS) and Long Range Dependence (LRD) by the calculation of Hurst parameter. The results showed strong degree of SS and LRD exist in the time series.

6.4 Analysis of ICMP NMAP PING

The analysis of ICMP NMAP PING also showed that the attacks came from various part of the World (i.e. 75 countries) and the United Stated was the largest source of the attacks. The results of the analysis showed that ICMP NMAP PING had similar

behaviours to SLAMMER worm attacks in the ways that most of the major attacks seemed to be automatically generated processes, came from a small group of hosts and this type of attack also had a periodic pattern of 24 hours. As a matter of fact, it could be the target discovery part of Sasser.D worm attack as mentioned in (Hideshima, 2006). The daily pattern of attacks was also found. It was spotted that the volume of attacks tended to very active during the peak hours when the most number of targets were active. The targets of ICMP NMAP PING were also as diverse as the targets of SLAMMER. However, it was found that the targets were focused on only 12 IP hosts which received the most number of attacks. The analysis of the time series of number of ICMP NMAP PING per hour showed that the time series was also nonstationary with strong degree of correlation and periodicity. Further analysis on the time series was done to find the degree of Self Similarity (SS) and Long Range Dependence (LRD) by the calculation of Hurst parameter. The results showed strong degree of SS and LRD exist in the time series.

7 Comparison of the results to previous studies

The analysis shows the similar finding as the two prior studies (Moore, 2004; Yegneswaran, 2003) in the way that DoS activities are numerous, a very small collection of sources are responsible for a significant fraction of intrusion attempts and there is a little sign of reduction of such intrusion attempts. This could mean that the behaviour of intrusion attempts on the Internet, especially DoS attacks, has not been changed very much since the earlier studies of the attacks and the situation tends to be going on as common threats on the Internet for very long period of time.

8 Conclusion

The results of the analyses of the can be summarised into the following points:

- Numerous amount of denial of service and ICMP scanning activities could be detected as common threats on the Internet.
- A detection of continuous pattern of ICMP scanning activities could be an indication of a victim discovery phase of another worm (DoS) attack.
- Worms like SLAMMER and Sasser.D still persist on the Internet long after their original release.
- China has now become the largest distributor in injecting attacks onto the Internet.
- A large number of attacks were generated by a small number of attacking hosts.
- DoS and information gathering attacks showed the behaviours of being automatically generated attacks sent by the infected hosts as the daily patterns of these attacks could be detected throughout the observation period.

9 Recommendations

Two recommendations can be made for future study. Firstly, in order to obtained accurate collection of alarm records and, hence, the meaningful analysis results, Snort must be updated and optimised before the analysis begins.

Secondly, to obtain more complete collection of data to be analysed, the problem of packet being dropped before reaching the sensor must be mitigated by implementing a network TAP to capture the flow of traffic to the sensor instead of using SPAN port.

10 References

Hideshima, Y. and Koike, H. (2006). STARMINE : A Visualization System for Cyber Attacks. In Proc. *Asia Pacific Symposium on Information Visualisation (APVIS2006)*, Tokyo, Japan. CRPIT, 60. Misue, K., Sugiyama, K. and Tanaka, J., Eds. ACS. 131-138.

Jouni, V., Herv, D., Ludovic, M., Anssi, L. and Mika, T. (2009) Processing intrusion detection alert aggregates with time series modeling. *Information Fusion,* 10**,** 312-324.

Kim, D., Lee, T., Jung, D., In, P. H. and Lee, H. J. (2007) Cyber Threat Trend Analysis Model Using HMM. *Information Assurance and Security, International Symposium on*, The Third International Symposium on Information Assurance and Security.

Koukis, D., et al., (2006) A Generic Anonymyzation Framework for Network Traffic. *Communications, 2006. ICC '06. ,* 5**,** 2302-2309.

NIST/SEMATECH (2006) e-Handbook of Statistical Methods. The National Institute of Standards and Technology (NIST), http://www.itl.nist.gov/div898/handbook/eda/section3/eda35c.htm (Accessed on 30/06/09).

Wu, Q. and Shao, Z (2005) Network Anomaly Detection Using Time Series Analysis. *Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services.* IEEE Computer Society.

Yegneswaran, V., Barford, P. and Ullrich, J. (2003) Internet intrusions: global characteristics and prevalence. *Proceedings of the 2003 ACM SIGMETRICS international Conference on Measurement and Modeling of Computer Systems.* San Diego, CA, USA, ACM.

Accessing Spyware Awareness and Defences amongst Security Administrators

M.Koliarou and S.M.Furnell

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

Abstract

Spyware threats have become very dangerous in recent years and the extent of the problem is increasing every day. Spyware works sneakily and underground, without giving signs of its presence in order to remain unnoticed, and trying to fool users in order to be installed in their systems. Therefore, to fight the spyware problem, it is very important to ensure awareness amongst end users. Many researchers found that the end users hardly understand security issues. So within organizations, there is a key role for Security Administrators. These have the responsibility for the company's security, therefore is very important to know about all of threats in high extent. This paper shows the results that gathered from a number of interviews amongst companies' Security Administrators about their awareness of spyware threats and their actions regard to security, their opinions, and their thoughts. This research found that the majority know much about spywares and much more about security defences. However, there are some respondents that did not know some features of spyware behvaiour and underestimate the threat and avoid some important actions.

Keywords

Awareness of Spyware, Security Administrators, anti-spyware adoption

1 Introduction

The extent and the power of Information Technology are increasing every day. New attractive facilities are developed on the Internet and encourage people to go online for more and more of their activities. This online world also risks many dangerous consequences. One of the security risks is the spyware threat, which can cause serious problems to both home users and to companies. The level of threat caused by spyware is sometimes underestimated because the activities often appear as harmless (Hunter, 2004). Some spyware can used for a good and helpful purpose such as to remember the user's preferences in a commercial web site in order to give an effective experience when the user visits again the site. However, it can also steal personal information such as email addresses, credit card numbers and passwords and finally they may slow down the Internet connections, and may lead to system instability and crashes (Cordes, 2005).

In the recent years, the extent of the spyware problem has increased significantly. Consequently, IDC analysts predicted that the market for antispyware products

would grow from $12 million in 2003 to $305 million by 2008 (Furnell S, 2005). It seems that the extent of spyware problem is in high levels.

Spyware threats should not be underestimated and end users should take all the appropriate countermeasures in order to prevent the threat. The required safeguards are anti-spyware products together with end user awareness in order to avoid some risky activities. In order to be taken the appropriate measures by the end users, they have to be aware of those threats and how important is to protect themselves. Because users can install spyware when clicking pop ups, downloading pirate music or videos, and shareware, their knowledge about the threat plays a key role to the extent of the problem. After that, they should also be aware of how the security products are used. According to Microsoft Chief Privacy Strategist Peter Cullen, people are concerned about their online security/privacy, but have little understanding of the threats they face (LeClaire, 2009).

2 Findings of interviewing Security Administrators

This research involved face-to-face interviewing of 20 Security Administrators and IT Managers working for companies in Limassol, Cyprus. Due to the aim of the research the interviews questions addressed two subjects. The first was the participants' awareness about spyware threats and the second was their awareness about related protection. Therefore, the interviews began with questions that refer to general knowledge about spyware threats and then continued with questions that refer to anti-spyware products.

Through the interviews it was intended to establish the Security Administrators' thoughts about spyware threats, whether they find them dangerous and what they think about them when compared with other threats. Therefore, from these thoughts we can estimate the extent of their awareness about spyware threats. Also, when taking into account their actions regarding spyware protection, we can estimate their awareness about spyware defences. To assess and decice if the respondents were aware of something or not, we analyzed whether they said something relative, similar or if they did not mention it at all even though they could have. The results include some possible reasons that maybe explain the participants' answers, but without suggesting that this is a categorical or absolute interpretation.

2.1 Awareness of spyware characteristics

The interview firstly sought to establish what respondents thought about the extent of the spyware danger. Many felt that spyware threats are very dangerous, as answered by half of the respondents. The fact that the danger of a spyware depends on the type of the spyware involved was only mentioned by 6 respondents. They notified that there are types of spyware that are harmless but there are others that may cause a lot of damage and therefore being very dangerous. Furthermore, 4 out of 20 think that spyware threats are not very dangerous. That means that a minority of respondents potentially underestimated the danger of spyware programs.

The second key point was what respondents know of spyware sources, and the ways that it can intrude into the system and the network. The infection by opening a

prohibited email was referred to by 10 respondents. Meanwhile, infection by visiting a malicious website was mentioned by 15 respondents. Further routes, such as downloading files, clicking pop-ups, and insertion of infected media, were all referred to by a minority of respondents (with each identified by 5 persons or fewer).

2.2 Awareness of Spywares' impact

An important possible effect of spyware programs is that they may steal confidential, personal or other kind of information by spying upon the user's actions, and send them to third parties. Surprisingly this effect, which is the main purpose of spyware, was only mentioned by 15 respondents. The lack of awareness of possible spyware effects connected also with the lack of awareness of the spyware risk level. If respondents do not be aware what spyware is able to do, they will also underestimate the spyware's risk level for a company.

Half of the respondents mentioned that another effect of spyware threats is that they slow down the operations of the computer or the network. This answer was referred from more respondents than other more serious spyware effects, such as destroying data, causing system instability and crashes, or damaging the whole system etc. The lack of speed of the operations is arguably a *symptom* that shows the spyware infection rather that a serious spyware effect. The aim of a spyware is not to slow down the operations but it has more serious damages. That shows that the 50% of the respondents, which answered that as an effect. Thus the respondents may be giving undue attention to visible consequences and disruptions rather than to the real and dangerous consequences that a spyware could have.

2.3 Awareness of Spywares' risk level

The participants were asked in a question of the interview to identify the level of risk for spyware compared to other threats. To this question all respondents directly indicated how they rate the spyware's risk level and some of them they also compared the spyware with other threats such as viruses, Trojan horses, and spamming. In the first case, 13 respondents considered that spyware has a high risk level, while the other 7 considered it medium risk. Some respondents compared the spyware threat with other threats that they face in the organization. They said if spyware is more or less dangerous than other threats such as viruses, Trojan horses, and spamming. Some respondents compared spywares with viruses, with 5 respondents considering that the latter are more dangerous. In contrast, 3 respondents think that spywares are more dangerous than viruses. Compared with spamming, 2 respondents said that spam emails are more dangerous, perhaps overlooking that spyware can be used by spammers in order to steal email addresses or other information that help them to send spam emails. Therefore, spyware's power plays very important role to the spamming threat.

2.4 Security Administrators confidence

Due to their education or training and most important due to their experience, it was expected that respondents would feel confident about their skills on spyware threats, because they are not just an ordinary end user. However, none of them suggested that

they were ‘very confident’, and only a quarter indicated that they felt confident and knew a lot about spyware,. The most common response, from 9 respondents, was to suggest that they felt quite confident or fair. Unfortunately, 5 respondents did not feel confident about their skills and knowledge about spyware threats. These respondents may need to search more about that threat in order to be more aware about it, since their position rather obliges them to have knowledge and skills about all of threats in order to be able to protect the company from them.

2.5 Promoting spyware awareness to the end users

It is recognised that end-user awareness about spyware threat plays an important role in the prevention of spyware since the threats coming from the Internet. So, probably the company’s protection is depends also to the behaviour and the awareness of its employees. Therefore, it was expected to find that Security Administrators do whatever it takes in order to promote awareness to the employees. The majority of the respondents (70%) said that they inform their employees about the threats and they also guide them to their actions in order to avoid any infection. However, 2 out respondents claimed to wait until they spotted a threat in the company and then alert users or the owner of the infected computer to be more careful. Unfortunately, even worse, 4 respondents claimed not to inform the users at all about the spyware threats and how they can protect themselves and the company agsinst them.

2.6 Use of anti-spyware technologies

Most Security Administrators prefer to use one product for all the computers, but 8 indicated that they used several products to different computers because they think that having several sets of computers protected by different anti-spyware products is better protection.

One of the questions that refer to spyware detection and the way of protection that each IT Manager choose, was how often they scan the computers with the anti-virus or anti-spyware products. Most of respondents prefer to schedule the scanning to be done automatically rather than to do it manually. Everyone schedules the frequency of the automatic scan and setting the system. Nine respondents schedule a daily scan, while 2 do it twice a week, 7 schedule the scanning once a week, and finally 2 only perform a scan once a month.

When asked about the effectiveness of the anti-spyware products that they use, all respondents said that they found them effective, but none product can be 100% effective because threats every day are updated. Security Administrators do not expect the anti- spyware product to detect all of the threats, so they do not expect more from that they already get about that product, therefore they feel satisfied with what they can get.

The respondents were also asked if they trusted the protection from the anti-spyware products. Here, while 6 indicated that they trusted them, a further 8 indicated that they trusted them but not completely, as the products are able to find only the known threats and not the new ones, and new threats are emerging every day. Also, they trust them more for the prevention and less for the cleaning. They need to search for

other tools in order to clean some spyware. By contrast, 6 respondents said that they did not trust them, but had no choice but to use them.

2.7 Security Administrators Actions for cleaning Spyware infections

All respondents said that firstly they wait for their products to remove the threats automatically. If their products cannot remove the threat, Security Administrators have to do some actions to clean the system from the spywares. In those cases, a quarter of the respondents are trying to find and remove the threat manually from the registries. Meanwhile 8 respondents preferred to research on the Internet to find how the spyware can be removed. They search for patches for their existing products or other tools that they can use in order to remove the threat manually. For 6 respondents, the manually cleaning of spyware is time consuming. Therefore, they prefer to re-format the infected computer. Some indicated an order of preference to their approaches, trying first to remove spyware manually, but then formatting the computer if it still remained.

2.8 Following News and Developments about Spyware Technology

Another important action that Security Administrators can do to improve their awareness about spyware threats is to follow related news and developments. Since the participants are Security Administrators and are responsible for the company's security, it was expected that they are following news about security threat included spywares. Nine respondents answered that they follow news and do the appropriate steps in order to be fully informed by following news frequently. A further 3 suggested that they followed news and developments but not to a satisfactory level. The remaining respondents admitted that they did not try to remain informed about spyware threats and technology.

3 Conclusions

The research as a whole was very informative due to the fact that the participants were Security Administrators or IT Managers for medium or large organizations (i.e. real-world professionals facing practical security issues). In general, respondents are aware of the spyware threat as a dangerous Internet risk and having also in their minds the other threats they trying for the better protection of the company. The majority of the respondents are aware that the spyware threats are spying the users' actions and can steal very important information. They are also aware of the risk level for the company. While, the majority showed that they are aware of the problem and feel quite confident to deal with it, it seems that there are some that still underestimate the threat. This finding is significant given that respondents are Security Administrators or IT Managers.

The findings in relation to the Security Administrators' actions about protection provide rather more relief, since that they are aware of what they have to do. Each company has its own plan about protection according to the company's needs and to the number of its computers, servers and employees. Differently from the protection policy and the network topology of each company, the point that this research referred was the use of anti-spyware programs. The research found that every

respondent used anti-spyware products, even though many do not trust them completely or find them 100% effective.

Overall, this research with the methodology of interviews finds interesting results that show the extent of Security Administrators' awareness of spyware threats and their protection actions. Indeed, while other researcher have found that end users may not know much about spyware, it is fortunate that Security Administrators generally appear to have a high extent of awareness of the threat and can protect their company's safety acccordingly.

4 References

Cordes, C. S, "Monsters in the closet: Spyware awareness and prevention", *Educause Quarterly*, 2005, Number 2, pages 53-56, online on http://net.educause.edu/ir/library/pdf/EQM0526.pdf

Furnell, S, "Internet threats to end-users: Hunting easy prey", *Network Security*, Vol. 2005, Issue 7, July 2005, Pages 5-9

Hunter, P, "New threats this year", *Computer Fraud and Security*, Vol. 2004, Issue 11, Nov 2004, Pages 12-13

LeClaire, J, "Data Privacy Day Seeks to Raise Awareness", CIO TODAY, January 28, 2009, http://www.cio-today.com/story.xhtml?story-id=64370

Usability of Security Mechanism

J.Ofomata and N.L.Clarke

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

Abstract

In spite of the available sophisticated security mechanisms to safeguard computer systems and work stations, the rate of computer crime and abuse is still on the increase simply because most computer users find it difficult to effectively implement the available security mechanisms. Consequently, users' inability to secure their system resulted to loss of funds, reputation and other sensitive data. However, this study aims at investigating the problems experienced by end-users which impede their effective implementation of security mechanism, for this purpose, a survey was designed and published online at the CISNR web site for a period of one and half month. The analytical review of the result generated by 231 respondents highlighted many usability weaknesses and based on these identified usability problems, some useful recommendations were suggested to nip these usability problems on board.

Keywords

Security, Usability, Security Mechanisms, Human–computer interaction and Computer interface.

1 Introduction

The purpose of this paper is to draw the attention of the general public on the need to develop usability methods and metrics for information security controls that will tackle usability issues. The need for information security necessitated a revolution in IT security industry that lead to the development of powerful security mechanisms that have the capability of combating various forms of computer crime, most unfortunately, users find it difficult to understand and implement these available security techniques to tackle the problem of attack and other lingering security issues that threatens the confidentiality, availability and integrity of information. Despite the level of publicity and awareness on usability of security mechanisms, the implementation of security applications is still poor, "Generally, security usability is poor" (Microsoft Security Ecology Report, 2008).

Most computer security packages are made up of security features that are presented for computer users to configure and install on their systems for the purpose of safeguarding computer users against intrusion and unauthorised access to their private network or database. Due to the problems posed by unclear functionality of some features in Human Computer Interaction, end-users are often confused at situation where they must take security related decisions.

However, the manner in which security interface features are designed and presented for users' implementation usually play a major role in influencing the users' action either by properly guiding them or complicating the process, such that users cannot actually use the security that they desire. This paper presents the results of a survey of 231 end-users in order to determine their weaknesses in implementing security to safeguard their systems. The study revealed some significant areas of usability difficulty and pointed out the need for a better designed computer interface and more considered approach to present security functionality in order to give computer users a realistic chance of safeguarding their systems.

2 Consequences of poor security implementation

The social and commercial benefits of online activities brought by the advancement of the internet leaves behind some costs associated with them since the internet has proven to have a big influence on criminal activity, as well as legitimate activity. For instance, about 830,000 businesses in the UK suffered an online/computer related security incident in 2007/08, (UK Cybercrime Report, 2008). The study carried out by Symantec indicated that out of 2249 new threats identified during the first 6 months in 2006, 86% were aimed at home users (Symantec, 2006). The personal and confidential nature of the financial data held in E-Banking service therefore inflicts fear into the mind of end-users because of the existing balance between security and usability of security features.

It was estimated that there were about 255,800 cases on online financial fraud in 2007 and with approximately 2.8 billion visitors annually, social networking websites offer a whole new dimension to potential online harassment, (Stefan Fanfinski, 2008). Despite the existence of sophisticated mechanisms like anti-spam software and email filters, the success rate of phishing crimes continues to escalate (Laurie Werner, 2008). A total of 2870 phishing sites were experienced in March 2005, and since then there has been 28% increment of the above figure on the monthly bases, meanwhile as result of phishing and online attack, USA consumers lost an estimated $500 million in 2005. It was also specified that the number of crime-ware-spreading sites infecting PCs with password-stealing codes reached an all time high of 31,173 in December 2008, (APWG, 2008).

3 Security Usability Study

A survey was published online at the CISNR web site of the University of Plymouth between mid July and September 2009 and a total number of 231 participants (126 male and 105 female) responded from over 40 countries across the world. Some of the countries include; Nigeria, USA. UK, Ghana, Germany, Saudi Arabia, Brazil, Pakistan India etc. The major challenge encountered during the course of this research work is problem getting the attention of the respondents who would actively participate in the survey. After the online publication of the survey it was noted that quite few number of respondents were recorded. This triggered the promotion of the survey link to the end-user community via email, telephone call, and postings to Internet forums that is likely to be visited by end-users. The link to the survey was also published on the International Students Advisory Service (ISAS) of the University of Plymouth.

At the surface level the responses overall suggested a high level of general IT experience and usage because above 50% of the respondents see themselves as intermittent users while 20% see themselves as experts. In terms of academic qualification, over 75% indicated to have either a Bachelor or Master's Degree. Almost all age brackets from under 20 and above 60 were represented but 80% of the respondents fall in between the age brackets of 20 and 39. A more in dept investigation into what the respondents claimed to know, proved that they lack most basic IT experience and usage. At the beginning of the security interface configuration section, users were asked if they know how to configure security interfaces, as seen in figure 1, 61% claimed to have a perfect understanding of interface configuration, 23% said they have some ideas while 16% owned up of not having any idea on interface configuration.

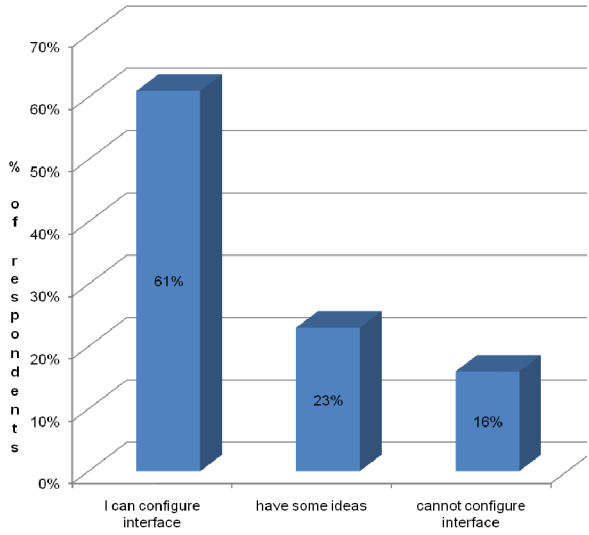


Figure 1: user's ability to configure interfaces

Subsequent test questions presented the images of firewall configuration interfaces to investigate their perception of the features. As seen in the figure 2, 48% of the respondents could not understand most of the features, while 11% did not understand them clearly.

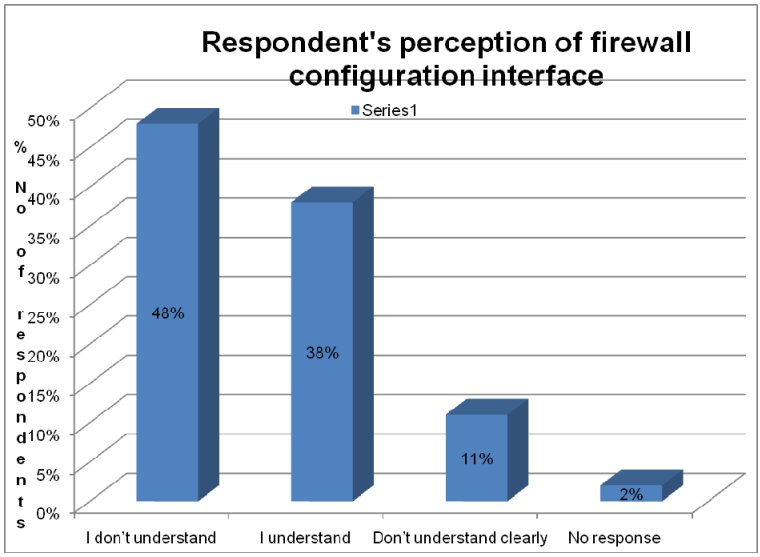


Figure 2: user's perception of interface configuration

However, interfaces are indispensable to human computer interaction because computer users can only be exposed to technology through the user interfaces. The average computer user's perceptions and understanding of certain technology is based on his experience with computer interfaces (Johnston et al., 2003). Therefore if security interface or related features within security software are poorly designed, even the most accomplished users will find it difficult to implement. The interface therefore needs to ensure that the user is guided so as to minimise the potential for the user to be vulnerable to attack. Human Computer Interaction is concerned with how the design of interfaces could be improved to make sure that they are understandable, usable and user friendly

Users were also probed on the frequency with which they update their security mechanisms; it was seen in figure 3 that 27 % carry out update on their security mechanisms at their convenient time, 25% do that on monthly basis while 23% update their mechanisms weekly.

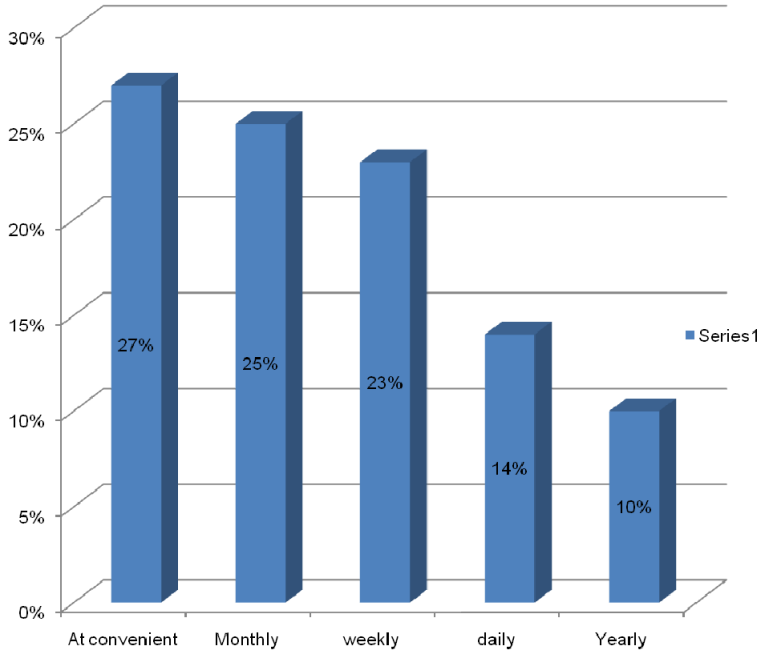


Figure 3: Respondent's frequency of security mechanism update

This really highlighted users' level of usability weakness because security systems need to be updated many times on the daily basis. However, updating security software very frequent will reduce the success rate of a skilled attacker. A skilled attacker has an 80% success rate of doing his exploit if a response is to be carried in 10 hours and 95% success rate if a response is to be issued in 20 hours. Then if an update is done in 30 hours the attacker has 100% of succeeding in his activities but when the response is instant, the attacker is left with almost 0% of succeeding in his malicious exploit (Cohen, 1999). This illustration describes the need for a real-time response and frequent update of security mechanisms in other to minimise the success rate of online attack.

Coming to good selection and usage of password and PIN in authentication processes as shown in figures 4 & 5 , 54% of the respondents use password of 6-8 character length while 18% choose their password to be between 4 and 5 character lengths, also 61% reuse the same password on multiple systems.

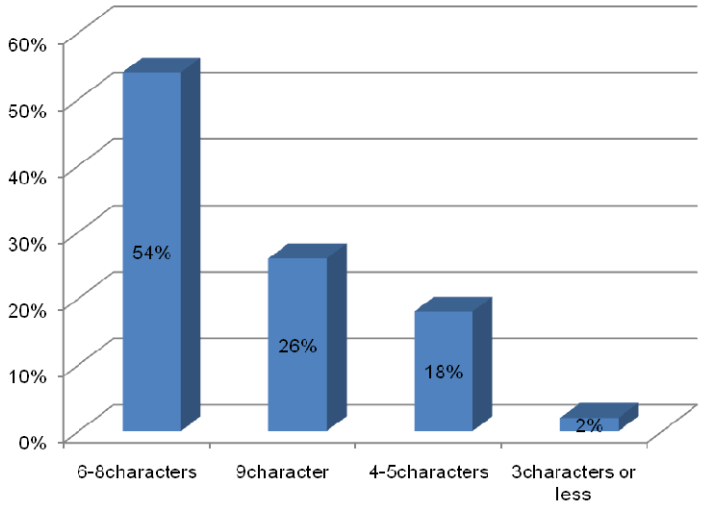


Figure 4: character length of respondents password

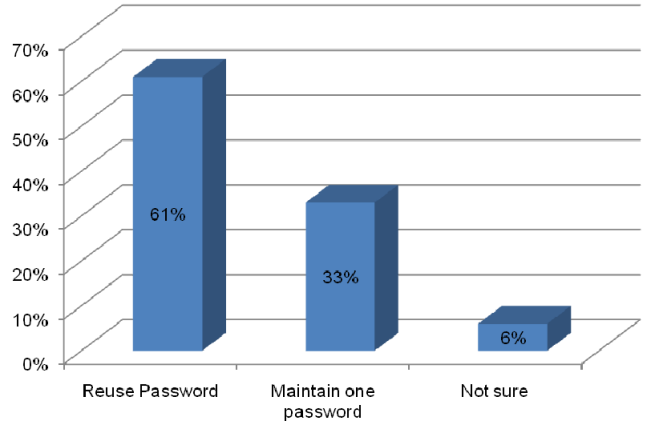


Figure 5: Ability to maintain one passwordon only one authentication process

It was seen from the survey result that end-users share their password with relatives and friends; also the character length of respondent's passwords in most cases are less than 9. However, for the purpose of maintaining good security in authentication processes, Passwords should not be written down let alone sharing with people, they should be strongly selected by ensuring that they are not too short, dictionary words and personal data that is mixed with numbers and special characters. This will foil the password cracker's ability of doing a simple look-up and apply brute-force technique or even apply password cracking tools. The more the password length, the more permutation the attacking tool is forced to try if the attacker must succeed.

Human Computer Interaction as a research discipline is no doubt a well developed area of study with experts who are of the opinion that usability of security mechanism could be significantly enhanced by employing certain interface design criteria in the design of these technologies.

Ben Shneiderman proposed some golden rules for interface design is as follows: the interface must be consistent, enable frequent users to use shortcuts, offer informative feedback, design dialogs to yield closure, offer simple error handling, Permit easy reversal of actions and reduce short term memory load.

However, in spite of the level of usability awareness and volume of academic studies that have been published on the existing relationship between end-users and Human Computer Interaction, user interfaces for security still tend to be clumsy, confusing and non-user friendly.

4 Findings

This study highlighted some of the problems that face end-users while attempting to understand and use related functionality in security software applications. This includes poor perception of security interface features, inability to understand and use security settings and users' lack of awareness of attack method used in social engineering. At the surface level, most respondents actively sort to cover their lack of knowledge, but with in dept exploration of usability issues by some of the designed test questions of the survey, certain usability weaknesses were revealed. Looking at the three major countries that have the highest number respondents, the level of usability and awareness of security were seen to be low in these three major countries, however, respondents from the USA displayed a higher level of usability and security awareness, followed by UK respondents and then Nigeria. On a more general note, the statistics of this result have been correlated with the results of some other related studies that investigated usability problems and there exists some strong similarities among these results. The common characteristic found is that security usability amongst end-users is still poor and as a result, suggestions have been made for security awareness and training sessions to educate computer users on the implementation and usage of specific security interface features. A major problem that hinders users from implementing security is that computer users find it difficult to understand the security features on the interface. The result of this study also pointed out that security interfaces are much relied upon technical terminology which makes interfaces unclear and confusing to users. Interfaces also lack visibility and force uninformed decisions to users, in respect to these, there is need for interface designers to improve on the design of the security interface for the purpose of improving the Human Computer Interaction to ensure effective usability of security mechanisms.

Another usability problem identified by this study is users' improper selection and implementation of password in authentication processes. The obtained result of the survey indicated that passwords are badly selected and implemented. From the result, greater number of the respondents selects their password to be pet names, dictionary words, or even personal data with character length of about 6. It was also seen that end-users share their password with relatives and friends. However, for the purpose of achieving strong security using password, they should be strongly selected by ensuring that they are not too short, dictionary words and personal data, but should be a non-dictionary word that is mixed with numbers and special characters. This will frustrate efforts of the skilled attacker because the more the password length, the more permutation the attacking tool will be forced to try on the password which will

frustrate the attacker's efforts. Also the investigation on users' awareness on phishing techniques illustrates that vast majority of respondents felt that they understood most phishing attack vectors. However, a notable percentage of the participants owed up to have problems in identifying and recognizing phishing sites. This particularly appears very surprising, because phishing threat had been the focus of media attention at the present days due to the escalating level of such attack coupled with the variety of related scams being perpetrated by skilled attackers.

5 Conclusion

This research study explored the existing relationship between computer users and their perception of usability and implementation of software security mechanisms.

The result highlighted some of the problems encounter by computer users while attempting to use security-related functionality within security related software applications.

From the general point of view, this study indicated that large proportion of respondents who claimed to be well knowledgeable regarding the implementation of security could not demonstrate effective security practices. Consequently, user's greater confidence in proper handling and implementation of security systems present a potential risk on its own since it hinders researchers from getting the clear overview of usability difficulties in order to properly device better means of tackling usability problems.

Although majority of the respondents claimed to be experts in the implementation of security systems, the results of this study demonstrated their shallow perception of security usability and lack of awareness of security threats. Considering the question that investigated if users have ever been trained on computer security, it was obvious that quite good numbers of users indicated of never been trained or educated on computer security. However, the major problem that must be addressed is that of awareness and education since users lack deep knowledge regarding their own protection. Also, the use of official and mass media efforts to educate the citizens for awareness creation is seen to be lacking. Consequent upon this, there is a need for more research studies that will look into a more viable model of engagement and awareness promotion amongst the entire populace for an optimised awareness creation on usability of security mechanism.

6 References

Anti-Phishing Working Group, APWG Phishing Archive, http://anti-phishing.org/phishing_archive.htm [Accessed 20 /05/ 09]

Anti-Phishing Working Group, *Phishing Activity Trends Report March 2005*, http://www.antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf [Accessed 15 /05/ 09]

AOL/NCSA online safety study America Online and the National Cyber Security Alliance, December 2005.<http://www staysafeonline.info/pdf/safety_study_2005.pdf>;[Accessed 21 /05/ 09]

Audit Commission. 1990. Survey of Computer Fraud & Abuse, Audit Commission Publications, UK. [Accessed 07 /07/ 09]

Audit Commission. ICT fraud and abuse 2004: an update to yourbusiness@risk. Public section update, Audit Commission; June 2005 [Accessed 15 /02/ 09]

Batya Friedman, David Hurley, Daniel Howe, Edward Felten, Helen Nissenbaum, *Users' Conceptions of Web Security: A Comparative Study.* CHI 2002 Extended abstracts of the Conference on Human Factors in Computing Systems, 2002: p. 746-747[Accessed 12 /07/ 09]

Bidgoli, H. (Ed.), 2006. Handbook of Information Security Wiley, Hoboken, NJ. [Accessed 12 /07/ 09]

Bishop M. Psychological acceptability revisited. In: Cranor, Garfinkel, editors. Security and usability O'Reilly; 2005 p. 1–11 [chapter 1] [Accessed 22 /07/ 09]

Cohen F.B (1999) "Simulating Cyber Attacks, Defences, and Consequences", *The Infosec Technical Baseline studies,* http://all.net/journal/ntb/simulate/simulate.html Date accessed(20/7/09).

Eastin M. Diffusion of e-commerce: an analysis of the adoption of four e-commerce activities. Telematics and Informatics 2002; 19(3):251–67. [Accessed 22 /07/ 09]

Fafinski, S. (2008) *UK Cybercrime Report 2008* Available at: http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf. [Accessed: 6/07/09]

Federal Deposit Insurance Corporation: Division of Supervision and Consumer Protection Technology Supervision Branch: December 14, 2004[Accessed 12 /01/09]

Furnell. S 2007. "Making security usable: Are things improving?" *Computers & Security,* vol. 26, no. 6, pp 434-443. [Accessed 26/01/09]

Furnell, S. and Bolakis, S. 2004. "Helping us to help ourselves: assessing administrators' use of security analysis tools", *Network Security*, February 2004, pp7-12. [Accessed 11 /03/ 09]

Furnell, S, Bryant P and Phippen A. 2007. "Assessing the security perceptions of personal Internet users", *Computers & Security*, vol. 26, no. 5, pp410-417. [Accessed 14/05/09]

Galletta, D. and Lederer, A. (1989). Some Cautions on the Measurement of User Information Satisfaction. *Decision Sciences,* Vol. 20, Issue 3, pp.419-438.

Holzinger, A., 2005 "Usability engineering methods for software developers" *Communications of the ACM* , Vol. 48, Issue 1, pp 71-74

Johnston, J., Eloff, J.H.P. and Labuschagne, L.. 2003. "Security and human computer interfaces", *Computers & Security*, vol. 22, no. 8, pp 675-684. [Accessed 22 /04/ 09]

Lewis, C. and Wharton, C. *Cognitive Walkthroughs Handbook of Human-Computer Interaction, 2nd ed*. M. Helander, Ed. Elsevier, Amsterdam, 1997, 717–732. [Accessed 16/01/09]

National Identity Fraud (2007)" How ID fraud Occurs". [Online] available at: http://www.stop-idfraud.co.uk/How_IDF_Occurs.htm [accessed 16 /02/2009]

Schultz, E.E. et al. (2007) "Research on usability in information security" [Accessed 12 /07/ 09]

Whitten, A. and Tygar, J.D.. 1999. “Why Johnny can’t Encrypt: A usability Evaluation of PGP 5.0”, *Proceedings of the 8th USENIX Security Symposium,* Washington, D.C., USA, August 23–26, pp169-184[Accessed 18 /03/ 09]

Experimental Evaluation of Jitter Buffer Algorithms on Voice over IP Networks

J.P.Ouedraogo, L.Sun and I.H.Mkwawa

Signal Processing and Multimedia Communications,
University of Plymouth, Plymouth, United Kingdom
e-mail: L.Sun@plymouth.ac.uk

Abstract

In Voice over IP (VoIP) applications, speech quality is mainly affected by network impairments such as delay, jitter and packet loss. Jitter buffer algorithms are used to lessen the impact of jitter by delaying the packet playout time. The aim of the paper is to evaluate and enhance the performance of different jitter buffer algorithms over a VoIP testbed based on Gstreamer. Preliminary results show that a combination of an algorithm that reacts more quickly to network variations and an algorithm that reduces the playout delay achieves the best trade-off between playout delay, buffer discarding rate and perceived listening only speech quality.

Keywords

Voice over IP; Jitter buffer algorithm; Gstreamer; Listening only speech quality

1 Introduction

In Voice over Internet Protocol (VoIP), one of the main challenges for applications is to smoothly deliver voice samples despite network impairments such as delay, packet loss and jitter. To deal with those situations, a jitter buffer can be used to achieve a better overall speech quality for the user. Hence, each arriving packet is held in a buffer, and its real playout time is delayed to allow late packets to reach the receiver on time (i.e. before the delayed scheduled time).

Two major approaches can be noticed, fixed jitter buffer which does not adapt through time and adaptive jitter buffer which takes network variations into account. The latter can be divided further into buffer that adjusts at the beginning of talkspurts (Ramjee *et al.* 1994) or during talkspurt (Liang *et al.* 2001). This paper focuses on adaptive jitter buffer, as more algorithms and computations are involved.

In terms of jitter buffer, a trade-off must be found between the delay added by the buffer and the loss due to packets late arrival.

Several papers have been published in relation with the efficiency of Ramjee *et al.* (1994) algorithm, such as Moon *et al.* (1998) and Roccetti *et al.* (2001) but none of them investigates the impact of its algorithm on Gstreamer.

Hence, the aim of this paper is firstly to evaluate the jitter buffer of Gstreamer, and the impact of the fourth algorithm presented in Ramjee *et al.* (1994), and secondly to enhance the efficiency of the latter in terms of playout delay, buffer discarding rate and perceived listening only speech quality.

The remainder of the paper is structured as follows. Section 2 presents the research method and experimental design. Section 3 describes the algorithms used. Section 4 explains the findings and analyses. Section 5 concludes the paper.

2 Research method and experimental design

The jitter buffer algorithms assessment is performed under a range of jitter values between 10ms and 60ms (as suggested by Calyam and Lee, 2005). Nevertheless, the paper only present the significant results obtained at 60ms.

Figure 1 shows the test bed set up and the following explains the main components used in this study. An audio file (ITU-T English female voice sample, 2009) is uploaded onto a VLC server (PC 1) so it can be retrieved on demand. NetEm, a Linux command line network emulator tool, is used to control the jitter under a normal (Gaussian) distribution. It has been configured to operate on incoming traffic at the receiver end, just after the network device. Finally, Gstreamer (including "Gstreamer Bad Plugins" that contains the jitter buffer algorithm), a streaming media application framework (PC 2), retrieves the audio file from the VLC server, using RTSP protocol. Gstreamer has been chosen because it is an open source product, and it is used in UCT IMS Client (Waiting *et al.* 2009), a VoIP client in development. Lame (2009) is used to encode an audio file in MP3, using variable bitrate. MP3 format is widely used as music on hold source files in Asterix IP-PBX (2009).

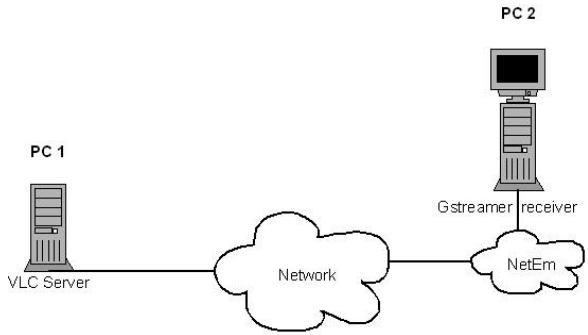


Figure 1: Test bed diagram

The variable bitrate (VBR) algorithm analyses each segment of the file, and reduces its bitrate (thus its size) according to its complexity. Hence, a silence segment will occupied less space than a talkspurt. As a result, algorithms that adapts according to talkspurt and silence can base their calculations on the size of the packet they process.

The length of the ITU-T sample has firstly been elongated from originally 8 to 16 seconds by duplicating the original sample to have enough data to analyse. The audio file was originally in WAV format. As it was not possible with VLC to retrieve the WAV file on demand (only live streaming), the file has been encoded in MP3.

The file retrieved with Gstreamer is stored in MP3, thus it is further encoded in WAV to allow the comparison with the original sample. The re-encoding lessens the audio quality, but the difference is very small: a loss of 2.47% of the quality has been noticed (by comparing two files PESQ score under no network impairment). Thus, this loss of quality is considered as negligible in the scope of this study.

The ITU-T standard P.862 (2001) Perceptual Evaluation of Speech Quality (PESQ) will determine the quality of the degraded audio file. PESQ is an automated tool for the assessment of speech quality, as a human being would perceive it. It is a "full reference" algorithm: it uses a reference test signal, and compares it against a degraded signal. The result is mapped on a scale of 1 to 4.5.

According to Opticom (2008), "the delay between the reference and the test signal is no longer constant". PESQ has then be developed to get over this issue, as algorithms that control the jitter buffer are aimed to change the playout time, i.e. the delay between the original file and the test file. This task is achieved by a "time alignment algorithm" (Opticom, 2008).

A PESQ C language code version defined in ITU-T recommendation P.862 (2001) will be used in this study.

3 Jitter Buffer algorithms

3.1 Implemented algorithms

The paper focuses on adaptive jitter buffer, as fixed cannot adapt to network variations. The notations used to describe the algorithms are explained in Figure 2. For packet i, t_i and p_i are respectively the send time and the playout time, d_i is the mean estimated network delay, v_i is the estimated variation of network delay, and n_i is the actual network delay.

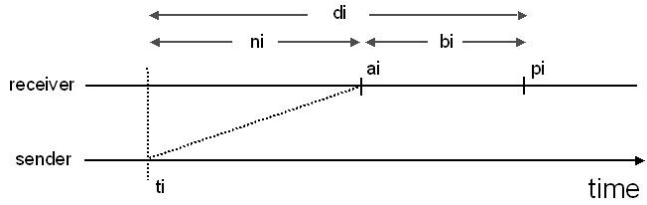


Figure 2 Timing associated with packet *i*

The implemented algorithms are adapted from Ramjee *et al.* (1994). The following one is called Algorithm 0 in this paper, as it is the strict implementation of Ramjee *et al.*'s algorithm. The playout time of the first packet in a talkspurt is computed as:

$$p_i = t_i + \hat{d}_i + \alpha * \hat{v}_i \quad (1)$$

where $\alpha = 4$. $\hat{d}_i$ and $\hat{v}_i$ (running estimates of the mean and variation of network delay, respectively d_i and v_i) are calculated as:

$$\hat{d}_i = \beta * \hat{d}_{i-1} + (1 - \beta) * n_i \text{ and } \hat{v}_i = \beta * \hat{v}_{i-1} + (1 - \beta) * |\hat{d}_i - n_i| \quad (2)$$

where $\beta = 0.875$.

For any further packet that belongs to the same talkspurt, the playout time is computed as:

$$p_j = p_i + t_j - t_i \quad (3)$$

To reduce the large average playout time noticed by Roccetti *et al.* (2001), six algorithms based on Algorithm 0 have been assessed. The computation of p_i for Algorithms 1 to 5 is presented in Table 1. For Algorithms 3 and 5, the weighting factors of $\hat{d}_i$ have been inverted to react more quickly to network fluctuations:

$$\hat{d}_i = (1 - \beta) * \hat{d}_{i-1} + \beta * n_i \quad (4)$$

	Algorithm 1	Algorithm 2	Algorithm 3	Algorithm 4	Algorithm 5
p_i	$t_i + \frac{\hat{d}_i}{2} + 2\hat{v}_i$	$t_i + \frac{\hat{d}_i}{4} + \hat{v}_i$	$t_i + \hat{d}_i + \hat{v}_i$	$t_i + \frac{\hat{d}_i}{6} + \frac{\hat{v}_i}{2}$	$t_i + \frac{\hat{d}_i}{4} + \hat{v}_i$

Table 1 Computation of p_i for Algorithms 1 to 5

The logic behind Algorithms 1, 2 and 4 is to reduce the playout time and investigate to what extent it affects the perceived speech quality. Algorithm 3 investigates the influence of $\hat{d}_i$ when it is set to attach more importance to the latest network delay variation. Finally, Algorithm 5 is a combination of Algorithms 2 and 3, based on their performances (see Section 4).

3.2 Jitter buffer in Gstreamer

"Gstreamer Bad Plugins" (2009) includes a jitter buffer algorithm. It will be compared to six algorithms implemented in the same structure. Gstreamer uses two algorithms adapted from Fober *et al.* (2005). The first one, a parabolic weighting factor algorithm, is applied during the two first seconds (or the 512 first packets). The following one is known as "window low point averaging". The calculation is computed as:

$$New\ skew = \frac{MIN\left[\left(a_j - a_i\right), \left(t_j - t_i\right)\right] + 124 * previous\_skew}{125} \quad (5)$$

Where a_j and a_i are respectively the current packet arrival time and the first packet arrival time; t_j and t_i are respectively the current packet send time and the first packet send time (see Figure 2); MIN is a function that outputs the lowest number of its arguments.

This skew is added to the RTP timestamp, so the final playout time of packet *j* is:

$$p_j = a_i + \left(t_j - t_i\right) + skew \quad (6)$$

4 Jitter buffer performance analysis

As NetEm generates random numbers to emulate jitter, it produces a different trace each time it is used. The mean of observed parameters is computed for each set of traces (four repetitions for Algorithm 0, fifty repetitions for Algorithms 1 to 5, as proposed by Blatnik *et al.* 2006) and presented in Figure 3 and Figure 4. Although Algorithm 0 could be assessed along with Algorithms 1 to 5, its playout time is too large (30% more than Gstreamer original algorithm) so it cannot be considered as a good trade-off between the delay added by the buffer and the loss due to packets late arrival.

Algorithms 1 and 2 PESQ scores are close (respectively 3.04 and 3.07 on average), even if their delay have been divided by respectively 2 and 4. However, it can be noticed that Algorithm 4 (which divided p_i arguments by 6) PESQ score drops significantly (2.73) in comparison with Algorithms 1 and 2. Hence, it could be concluded that Algorithm 4 computation is not optimum in terms of PESQ score. Algorithm 5, which is partly composed of Algorithm 2, has approximately the same PESQ score of the latter (2.99), instead of the worse Algorithm 3 PESQ score (which compose the second part of Algorithm 5).

In terms of buffer discarding rate, Algorithm 5 behaves the same way as Algorithms 2 and 3 (respectively 13.51%, 12.35% and 13.40%), and discards a similar number of packets. Algorithm 1 discards fewer packets (9.20%) but also has the highest average playout delay (far more than the other algorithms).

In addition, the relation between PESQ scores and buffer discarding rates can be analysed by contrasting the two graphics of Figure 3. Algorithms 1, 2 and 4 behaviours were expected: the greater the PESQ score, the lower the buffer discarding rate. Furthermore, Algorithms 2 and 5 have approximately the same PESQ scores and the same buffer discarding rates.

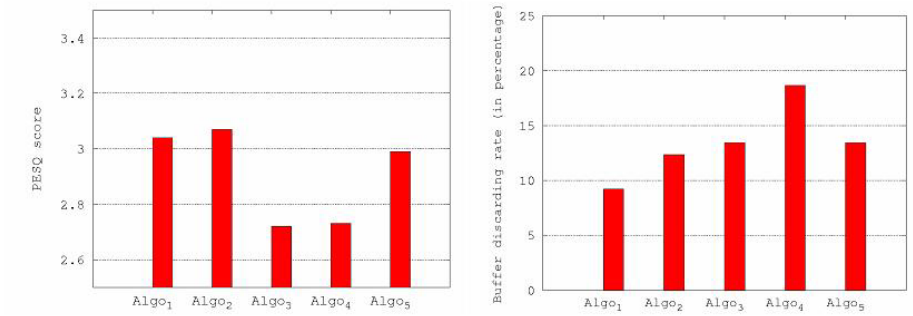


Figure 3 PESQ score and buffer discarding rate (in percentage) for Algorithms 1 to 5

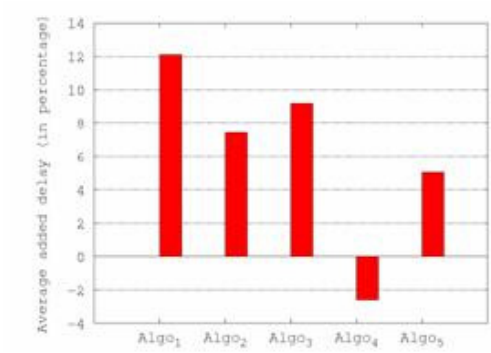


Figure 4 Average added delay (in percentage) for Algorithms 1 to 5

However, an unexpected behaviour can be noticed for Algorithm 3. Indeed, Algorithm 3 buffer discarding rate is almost the same as Algorithms 2 and 5 buffer discarding rate, but Algorithms 2 and 5 PESQ scores are better than Algorithm 3 PESQ score. Algorithms are based on packet sizes to detect talkspurt and silence periods. Hence, some beginnings of talkspurt or silence parts can be misunderstood by the algorithm, if for instance three contiguous packet sizes arrive with the following distribution: $\{x\ ;\ y\ ;\ x\}$ where $\{x\}$ is a packet size that represents a talkspurt and $\{y\}$ is a packet size that represents a silence. In this case, the algorithm will set the second $\{x\}$ as the beginning of a new talkspurt and may change the playout time, especially in the case of Algorithm 3, and the new one can overlap a previous packet that contains a talkspurt. Hence, this could be the explanation of the relation between the PESQ score and the buffer discarding rate noticed above for Algorithm 3. Moreover, the green rectangles in Figure 5 show a lack of several packets at the beginning of the second waveform comparing with the original sample, which confirms this assumption. This behaviour does not happen when a real talkspurt is detected, as highlighted by the red circles in Figure 5, where the new playout time set by the algorithm at the beginning of the talkspurt overlaps the previous silence packets.

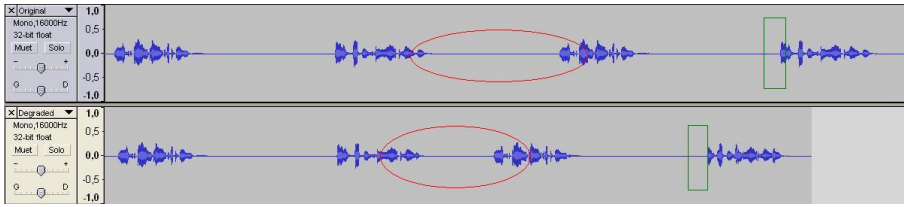


Figure 5 Variable delay (for Algorithm 3)

The original $\hat{d}_i$; d_i (in Algorithm 0) reacts slowly to network fluctuations, as the weight factors are 0.125 for the new n_i, and 0.875 for the previous $\hat{d}_i$. By inverting those weighting factors in Algorithm 3, the "memory" of the algorithm $\hat{d}_{i-1}$ is reduced for the advantage of the latest n_i calculation. Hence, $\hat{d}_i$ will vary more quickly. This behaviour is clearly noticeable in Figure 5, where the red circle on the first sample (the original one) corresponds to the original silence length, whereas the second red circle below corresponds to the degraded silence length.

Finally, Algorithm 5 is a combination of Algorithms 2 and 3. Algorithm 5 has overcome the issue addressed by Algorithm 3: the variable delay between two talkspurts is not as larger as Algorithm 3. Its playout delay is also reduced, compared with Algorithms 1 and 2. In terms of buffer discarding rate, although it drops more packets than Algorithm 1, this percentage can be compared to Algorithm 2 as they have the same p_i calculation. By applying the findings of Algorithm 3 to Algorithm 5, the latter reacts more quickly to network variations.

5 Conclusion and future work

This study pointed out the significance of the trade-off between jitter, buffer discarding rate and perceived quality speech. A test bed composed of two machines, a sender (VLC server) and a client (Gstreamer pipeline) has been set up to study the performance of several jitter buffer algorithms under jitter values from 10ms to 60ms.

It appears that Algorithm 5, which is a combination of an algorithm that reacts more quickly to network variations (Algorithm 3) and an algorithm that reduces the time at which the packet is played at the client side (Algorithm 2) generates the best overall results when it comes to find a good trade-off between jitter, buffer discarding rate and perceived quality speech.

Those findings can be carried out further, and it could be interesting to evaluate the performance of Gstreamer and the modified code in a "real" VoIP environment. Hence, the implementation of the modified Gstreamer code in a VoIP client that can handle a communication in both ways, such as UCT IMS Client (Waiting *et al.* 2009) could be a really attracting project.

6 References

Asterix Web Site (2009) “The Open Source PBX & Telephony paltform”, http://www.asterisk.org/, (Accessed 08 September 2009).

Blatnik, R., Kandus, G., Javornik, T. (2006) *Experimental test-bed for VoIP/VoWLAN voice quality measurements*, Proceedings of the 4th WSEAS International Conference on Electromagnetics, Wireless and Optical Communications, 2006, World Scientific and Engineering Academy and Society, pp5-10, ISSN:1790-5095.

Calyam, P., Lee, C.G. (2005) *Characterizing voice and video traffic behavior over the Internet*, International Symposium on Computer and Information Sciences (ISCIS), Proceedings published by Imperial College Press in a special edition of "Advances in Computer Science and Engineering".

Fober, D., Orlarey, Y. and Letz, S. (2005) *Real Time Clock Skew Estimation over Network Delays*, Laboratoire de recherche en informatique musicale, Grame, France.

GStreamer Web Site (2009), “Bad Plugins 0.10 Plugins Reference Manual”, http://gstreamer.freedesktop.org/data/doc/gstreamer/head/gst-plugins-bad-plugins/html/gst-plugins-bad-plugins-gstrtpjitterbuffer.html, (Accessed 17 February 2009).

ITU-T Web Site (2009), “Test Signals for Telecommunication Systems, Annex B speech files”, http://www.itu.int/net/itu-t/sigdb/genaudio/AudioForm-g.aspx?val=10000501, (Accessed 15 January 2009).

ITU-T Web Site (2001), “ITU-T Recommendation P.862”, http://www.itu.int/rec/T-REC-P.862/, (Accessed 15 January 2009).

Lame documentation Web Site (2009) “Guide to command line options”, http://lame.cvs.sourceforge.net/*checkout*/lame/lame/USAGE, (Accessed 05 May 2009).

Liang, Y., Färber, N. and Girod, B. (2001) *Adaptive playout scheduling using time-scale modification in packet voice communications*, Proceedings of the Acoustics, Speech and Signal Processing, Volume 03, 2001, IEEE Computer Society, pp1445-1448, ISBN: 0-7803-7041-4.

Moon, S.B., Kurose, J. and Towsley, D. (1998) *Packet audio playout delay adjustment: performance bounds and algorithms*, Multimedia Systems, Volume6, Issue 1, Springer-Verlag New York, Inc, pp17-28, ISSN:0942-4962.

Opticom Web Site (2008), “Voice quality testing: PESQ”, http://www.opticom.de/technology/pesq.html, (Accessed 12 March 2009).

Ramjee, R., Kurose, J., Towsley, D. and Schulzrinne, H. (1994) “Adaptive playout mechanism for packetized audio applications in wide-area networks”, *Proceedings of IEEE INFOCOM*, Volume 2, 1994, pp680–688, ISBN: 0-8186-5570-4.

Roccetti, M., Ghini, V., Pau, G., Salomoni, P. and Bonfigli, M.E. (2001) *“Design and Experimental Evaluation of an Adaptive Playout Delay Control Mechanism for Packetized Audio for Use over the Internet”*, *Multimedia Tools and Applications*, Volume 14, Issue 1, 2001, Kluwer Academic Publishers, pp23-53, ISSN:1380-7501.

Waiting, D., Good, R., Spiers, R., Ventura, N. (2009) *The UCT IMS Client*, 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops, TridentCom 2009, pp1-6, ISBN: 978-1-4244-2846-5.

AI-based TCP Performance Modelling

B.Piger and B.V.Ghita

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

Abstract

This project aims to analyse the efficiency of artificial neural networks when modelling the performance of Transmission Control Protocol (TCP). First of all we need to understand what TCP performance depends on. We have therefore researched existing mathematical models. We have chosen to implement the Cardwell (2000) model. By using this model we can retrieve the data transfer time thanks to the timeout, loss rate, round trip time and initial congestion window. We have next built a network features dataset thanks to tcpdump and tcptrace. This set has enabled us to test our mathematical model and to build our artificial neural network. We have chosen to include the result of the mathematical model, the data packet number sent per connection and the average data packet size in the input of the artificial neural network in order to try to improve its efficiency. In order to analyse their performance we have chosen to use the correlation and the average relative error. By analysing our model we have shown the importance of the data. Indeed, we have to choose carefully their type and scope. We have shown also that our implementation of the mathematical model was inefficient. At the same time, we have reached a better accuracy with our artificial neural network model: 86.45% of correlation and 37.4% of average relative error.

Keywords

TCP performance prediction, Artificial neural network model, Mathematical model, Efficiency analysis.

1 Introduction

TCP is one of the core protocols used within networks. Most Internet services are based on this protocol. We can manage more efficiently a network and its services if we know its performance. It is therefore interesting to identify and predict the performance of TCP traffic. We know the performance of this protocol is based on network characteristics such as lost rate and timeout. Existing mathematical model uses some of these network features in order to retrieve the performance of TCP. AI-based modelling is a different approach we can use to determine this performance. Artificial neural network is one of the methods used to create AI-based model. Their implementation will enable us to model the performance of any TCP traffic. By understanding the efficiency of such models we can improve them. This project aims then to analyse the efficiency of artificial neural network when modelling the performance of TPC traffic.

This type of work as already been achieved. We know from a previous research paper (Bogdan and Furnell, 2008) that the creation of such model is possible. This

current paper will suggest a model based on different network features. In order to achieve this aim prior works are necessary. First of all we need to choose which mathematical model we want to implement. Indeed, in addition to many network features, we want to include in the dataset the mathematical model output. Once we have retrieved the dataset we can build an artificial neural network. In practise the first results were bad. We have then decided to filter the dataset. We will then analyse this filtering.

A background part will describe how we have retrieved the dataset and both mathematical and artificial neural network models we have implemented. The second part will present the traffic performance before the filtering. The third part will present the analysis of the filtering process. The last part will show the influence of the filtering on each network feature.

2 Background

This background part will introduce the mathematical model we have chosen and the dataset we will use. Then we will describe how we construct our artificial neural network.

2.1 Mathematical model

We will describe here three mathematical models used to estimate TCP performance.

The first formula comes from Bellcore Labs (Ott et al., 1996). The paper studies the stationary behaviour of the congestion window within an ideal TCP congestion avoidance. Ideal congestion avoidance is defined by independent loss, equal equity to occur and no timeout reached. In order to model this specific behaviour they use Selective Acknowledgments (SACKs).

The second model (Padhye et al., 1998) was developed to determine the steady state throughput thanks to the packet loss rate and the round trip time. This model extends the previous model and takes in consideration the influence of the timeout. Nevertheless it cannot model connection with no loss.

The last model (Cardwell et al., 2000) extends the second model. This time the data transfer time is estimate thanks to the round trip time, packet loss, timeout and initial congestion window. This model can handle connection with no loss. It is design to model short-lived connection.

From these three models we will chose the last one. Indeed, this model takes in consideration more network features and seems to be the most efficient. It uses and extend the two others. In addition, this model suit short-lived connections. This type of connection is likely to happen nowadays. For all these reason we have implemented a C program to retrieve the data transfer time.

2.2 Network Features

Now we know that the mathematical model we have chosen use the round trip time (RTT), timeout, packet loss and initial congestion window, we use them all to build our artificial neural network. In order to help it we will also include the average packet size and the average packet number per connection. In addition to these six network features the input part of our data will be also composed by the result of the mathematical model. The output use in our dataset will be the data transfer time.

In order to construct this dataset we have used tcpdump and tcptrace. Indeed we have captured a trace with tcpdump from the University of Plymouth network. This trace gathers the information of all the connection to the Internet. We specified to capture only TCP packets to ease to subsequent use. Once we have this trace we use tcptrace to retrieve the seven network features we wanted.

2.3 Artificial neural network

From the dataset we can start to train and test our artificial neural network. Our dataset will be split in two parts: 90% to make the training set and 10% to create the testing set. In order to build this model we use Stuttgart Neural Network Simulator (SNNS). We have then decided to use a very basic neural network configuration: one input layer, one hidden layer and one output layer. On the input layer we have to fit seven data types, we have then seven neurones. On the hidden layer we have four neurones. On the output layer we have just one neurone representing the data transfer time. Figure 1 shows us this initial neural network configuration.

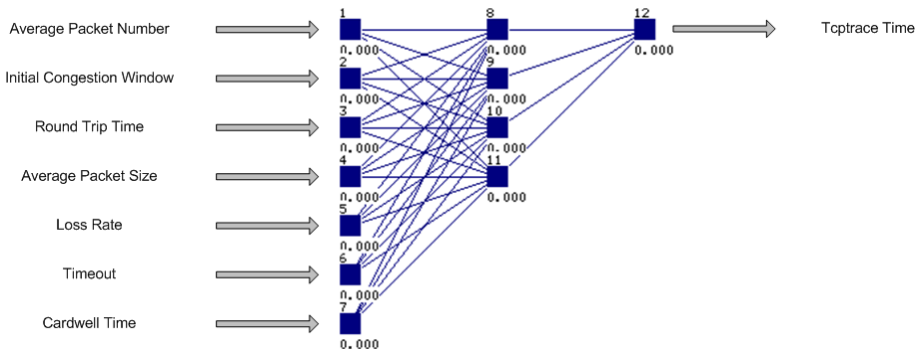


Figure 1: Initial Network Configuration (7-4-1)

Concerning the learning process, we have used the standard Backpropagation function with a learning rate at 0.3 and a desired error at 0.001. We have also chosen to run the creation process with 500 cycles.

In order to evaluate the efficiency of our models we will use the correlation and the average relative error. The correlation give us the relation between the estimated data transfer time and the real one. The relative error gives us the precision of the model between those same two values.

3 Traffic Performance

This part will present the performance of the traffic we have captured. This traffic is characterised by the seven network features plus the output of the Cardwell (2000) model. The performance analysed is the distribution of each data composing the traffic.

The scope the number of data packet sent per connection is 2 to 9,100. A single packet can transport 1380 bytes of information. The corresponding scope of the amount of data transported start from 2.69 kilobytes to finish at 11.97 megabytes. These values can happen in practice. Nevertheless the value of the 99th percentile is 383 packets. There is then a presence of extremum values over this point.

The initial congestion size is ranged from 2 to 13 segments. This scope can exist in real life. Nevertheless 89% of the connections possess an initial window of 2 segments. This configuration is the basic configuration of TCP. Furthermore 99% of our data are below or equal to 5 segments. Therefore a connection with 13 segments is very rare.

The round trip time is ranged from 0 to 99,812 milliseconds. A round trip time of zero millisecond cannot exist in practice. That means the transmission of the data within the whole network takes no time. Furthermore, 96% of the data are between 10 and 1,000 millisecond. These values are more likely to be good. For example, a round trip time between London and Sydney is roughly 330 milliseconds. The values over 1,000 milliseconds need then to be removed.

The average packet size is ranged from 136 to 1,379 bytes. The value of the 5th percentile is 585 bytes. The main part of the connection has then an average data packet size between 585 and 1,379 bytes. The maximum value is reached for 2% of the connections. The maximum amount of data a packet can transport is 1,380 bytes. As the last packet finishes the transmission, its size is very unlikely to be exactly equal to 1,380 bytes. That is why an average size of 1379 bytes happens many times.

The loss rate is ranged from 0 to 0.5. The value of the 99th percentile is 0.058824. Furthermore only 5% of the connections possess a loss. The main part of the losses is included between 0.01 and 0.1. This performance is good and possible. For the loss rate a filtering by the top can be done.

A timeout can by set up by the network administrator. It is generally ranged between 1 and 5 seconds. In the trace, the timeout is ranged from 0 to 191,867 milliseconds. The value of the 99th percentile is 3,894 milliseconds. Furthermore only 9% of the connections reach a timeout. This performance is then normal despite of maximum values which we need to filter.

The data transfer time calculated with the Cardwell (2000) model is ranged from 0 to 429,135 milliseconds. First of all, a transmission time of zero millisecond is not possible in reality. A connection cannot transfer data in nil time. Such values do not have to be taken under consideration. A value of 429 seconds can potentially happen in practise, but this phenomenon is still very rare. 98% of the connections are ranged

between 10 and 10,000 milliseconds. The values not in this scope may need to be filtered.

The data transfer time retrieved from tcptrace is ranged from 0 to 1,719,515 milliseconds. Here again the value of zero millisecond need to be removed. 3% of the connections possess a zero millisecond data transfer time. That is very strange and let us thinks of a weakness in tcptrace. The maximum value is also possible but very rare. 94% of the connections are ranged between 10 and 100,000 milliseconds. The values not in this scope may need to be filtered. By comparing this data transfer time with the Cardwell data transfer time, we can see that they have almost the same distribution. Nevertheless the scale is not the same at all.

4 Dataset Filtering

This part will present the filtering process. In order to see its impact on the artificial neural network model efficiency, we will also present its initial and new performance.

4.1 Initial Performance

First of all we will describe the initial efficiency of both mathematical and artificial neural network models. Table 1 presents these results.

Model	Correlation	Relative Error
Mathematical model	0.3221	2.5661
Artificial neural network model	0.1978	30.4014

Table 1: Initial Performance

We can see in this table that both models possess very low correlation. The mathematical model has power of the neural network one. Figure 2 illustrates the performance of the artificial neural network. The red dots represent the response of our model. The x-axis is the real data transfer time and the y-axis is the estimated one. The green line represent a correlation of 1, its function is y=x.

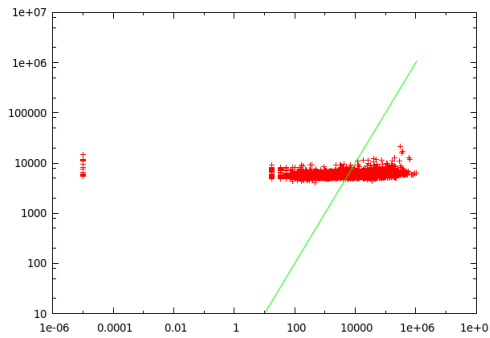


Figure 2: First efficiency

In this figure we can see that our response is ranged between 4,000 and 20,000 milliseconds while the real scope is 0.00001 to 1,000,000 milliseconds. Furthermore our response is far to follow the green line. We can then not estimate the whole range. That the result of a bad correlation. As our response is quite excessive we need to pay attention to our maximum values. Moreover a data transfer time that low is suspicious. We then need to take care of the minimum values as well.

4.2 Filtering Process

To filter our data we start to cut from maximum values. Once we obtain an interesting response we cut from the minimum values.

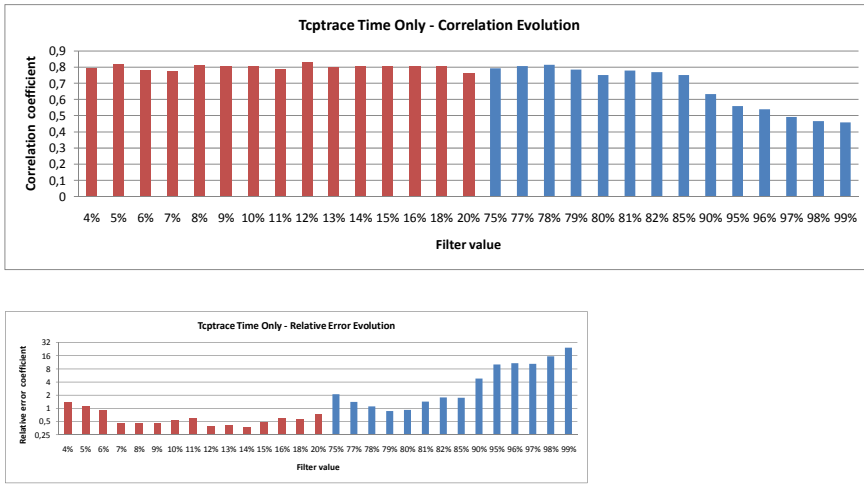


Figure 3: Filtering process

We can see that the efficiency is increasing when filtering from the top. By cutting just one percent we obtain already a correlation more than twice better at 47.79%. This correlation keeps increasing until it reaches a limit over 80%. The best correlation is 81.6% and it is reached at 78% of filtering. We can see also the effect of the filtering on the relative error. It is decreasing until it becomes lower than 1 for 79% and 80% of filtering. After this point the relative error is increasing we are then ignoring relevant information. At this point we will then keep the filtering at 79% as it possesses the lowest relative error with 0.86. The corresponding correlation is 78.55% which is nearly four times better than the initial one.

By filtering from the minimum values we can see that the correlation is not improved in a significant way. Nevertheless the precision is becoming lower. It even becomes lower than 0.5 for many values. The best value is 0.38 and it is found when we filter at 12%. The corresponding correlation is also the best: 82.88%.

4.3 New performance

After the filtering process we have retrieve the efficiency of our both models. Table 2 resumes these new results.

Model	Correlation	Relative Error
Mathematical model	0.1308	1.1890
Artificial neural network model	0.8288	0.3847

Table 2: New Performance

At the end of the filtering process we have then increased the performance of the artificial neural network. Nevertheless the mathematical has not been improved in the same way. The correlation has become very low. However, the relative error becomes twice better. Figure 4 illustrates the efficiency of our new artificial neural network model.

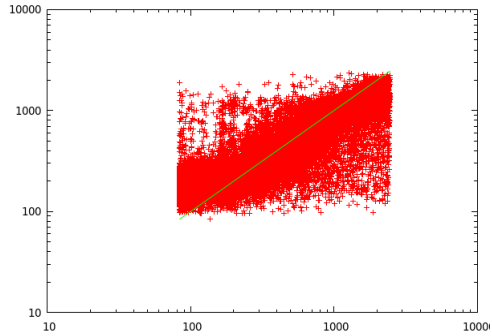


Figure 4: New efficiency

We can see here the scope taken by our response corresponds to the real one. Moreover, the general behaviour is closer to the optimum efficiency. That the effect of a better correlation. The enhancement of the relative error determines how close to the green line our response is. We can see that we need still need to improve it.

5 New Traffic Performance

After the filtering process, the distribution of all the data has changed. This part will describe the new distribution of each data.

The data packet number sent per connection is now ranged from 2 to 1,666 packets. The value of the 99th was 383 packets. After filtering the dataset, this range keeps more than 99% of its initial distribution. Moreover the scope from 2 to 100 packets represents now 99% of the data against 97% before the filtering process.

The initial congestion window size scope remains the same as before the filtering process. Furthermore, its distribution is almost the same.

The round trip time is now ranged from 0 to 42,148 milliseconds. Here again the new scope keeps 99% of the original distribution. 97% of the data represent now the scope 10 to 500 milliseconds, before it was representing the scope 10 to 1,000 milliseconds.

The average segment size is now ranged from 206 to 1,379 bytes. The previous minimum was 136. The value of the first percentile was 140 bytes, it is now 512 bytes. This data has then been filtered by the minimum.

The minimum loss rate has not been changed. Nevertheless, the connections having a loss represent now 2% against 5% before. The maximum was 0.5, it is now 0.33. The main scope is still from 0.01 to 0.1.

The minimum timeout has not been changed. Nevertheless, the connections reaching a timeout represent now 4% against 9% originally. The maximum was 191,867, it is now 4,899 milliseconds.

The minimum Cardwell data transfer time is still zero milliseconds. Its maximum falls from 429 seconds to 156,349 milliseconds. 99% of the original distribution has been kept. The tcptrace time is now ranged from 84 to 2,456 milliseconds. This scope represents 95% of the scope of the Cardwell time. This filtering process has then the right effect on our data.

6 Conclusion

In this current paper we have shown the performance of an artificial neural network when modelling TCP traffic. The characteristic we were targeting was the data transfer time. After optimising the artificial neural network, we have obtained a performance of 86.45% of correlation and 0.374 of relative error. This paper has also shown the importance of the scope of data we use. When mastering the data and the artificial neural network we can improve this performance. We can then use this technique to model other network protocols.

7 References

Cardwell, N., Savage, S. and Anderson, T. (2000). Modeling TCP latency [Online]. Department of Computer Science and Engineering, University of Washington. [Accessed the 24th of February 2009] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.1513

Ghita, B.V. and Furnell, S. (2008). Neural network estimation of TCP performance, Proceedings of the 2008 International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2008), Bucharest, Romania, 29 June – 5 July, pp53-58

Ott, T.J., Kemperman, J.H.B. and Mathis, M. (1996). The stationary behaviour of ideal TCP congestion avoidance [Online]. [Accessed the 24th February 2009] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.50.9373

Padhye, J., Firoiu, V., Towsley , D. and Kurose, J. (1998). Modeling TCP throughput a simple model and its empirical validation [Online]. University of Massachusetts. [Accessed the 24th February 2009] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.34.7826

Combined Data Compression and Error Correction

A.Sasikumar and M.A.Ambroze

Fixed and Mobile Communications, University of Plymouth, Plymouth, UK
e-mail: M.Ambroze@plymouth.ac.uk

Abstract

The basic intention behind the project is to understand and familiarize with the concepts of data compression using LZW and encoding, error correction using Hamming codes. After achieving the desired results by creating algorithm for compression and error correction, gives a clear idea how it works on a text file. For a detailed analysis of compression, did study on comparing the rate of compression of WinZip and WinRAR.

Keywords

Data Compression – Lzw; Error Correction- Hamming Code

1 Introduction

In the field of information the quality of service of any data depends mainly on 1) the transferring data speed and 2) the rate of error (Shannon, 1949). The data transmission rate through a medium depends on a) the bandwidth of the channel and b) the size of the data. For the purpose of improving the rate of transmission, any of the above two parameters must be altered; and in most of the cases uses the second method decrease the size of information by compressing it. Due to compression there are mainly two advantages it reduces the time of transmission, and also shrink the storage space. And in the second part error, the chance of occurring error when the data is pass through a channel is more because of the effect of noise in that field. Due to those error factors the quality of the data will be compromised. So error correction is an important part in the field of data transfer. Hence in the field communication, both compression and error correction are two non-evitable factors. So the combination of both can able to transfer the data at high speed without so much of errors.

1.1 Aim and Objectives

The main aims of this project are; 1) to study the concepts of data compression and error correction in the field of communication. 2) Investigate the best combination of compression and error correction that gives lustiness to errors and attaining a diminution to the size of the data that to be transmitted.

The main objectives in the project are; a) Understanding the concept of compression, decompression, encoding and error correction b) Choosing proper method for data compression and error correction. c) Creating algorithm using

selected techniques. d) On the basis of those algorithms, find out the results, analyse it and draw graphs for it.

The programming part of the project is mainly split into three parts a) Data compression and decompression b) Encoding and error correction c) Combined data compression and error correction.

2 Background

2.1 Data Compression

The data compression technique starts in the year 1948 with Claude E.Shannon by his paper 'A Mathematical Theory of communication'. Shannon mainly explains about two types of compression lossless and lossy compression. Lossy compression is also known as rate distortion theory. Rate distortion theory and lossless data compression theory are jointly known as 'source coding theory' (Shannon, 1949). There are different methods are available for data compression and in that LZW was choose as the technique for this project. LZW is an advanced form of LZ78 created by Terry Welch in the year 1984. LZW is work on the basis of the dictionary. In LZW it creates its own dictionary on the basis of the input text, and these dictionary words were used for representing redundant data in the text. And at the decompression part it adds the redundant data on the basis of the dictionary that created at the time of compression (Welch, 1984).

2.2 Error Correction

Error correction is the technique that is used of correcting the errors that occurred while transferring the data through a channel. So these error correction coding provides a required level of exactness; as similar as that of the actual data. Accuracy of system can also attain by increasing the signal strength per unit of data, but the main advantage of using error correction to data is the accuracy can be achieved without any change in power (Prakash, 2006). There are different techniques available for error correction and hamming code is one among them. In the field of telecommunication hamming code is considered to be a linear error correcting code. The hamming codes were invented by Richard Hamming in the year 1950. These codes can able to detect two bits of errors and can correct single-bit error. A reliable form of communication can be achieved when hamming distance (hamming distance is defined as the bits position (error) difference between two files of same length) among the transmitted bit pattern and received bit is equal to or less than one, which means burst error is not occurred at the medium of transmission. But in demarcation, the simple parity code is not able to correct errors can only to detect the odd sequence of errors (Hamming, 1950).

3 WinSip WinRAR Comparison Study

The compression study then led me to study and compare different aspects compression tools like WinZip 12 and WinRAR 3.70.

Both WinZip and WinRAR are used for compression but there are lot of differences in their properties. And some of their properties are explained below.

The given below are some of the difference between WINZIP and WINRAR. When go through different aspects about WinZip and WinRAR, found that the compression ratio of WinRAR is slightly more than WinZip; so for proving that fact, compress different files using WinZip and WinRAR and find out their respective rate of compression. And those studies and its results are explained in this part.

3.1 Differences between WinZip and WinRAR

	WinZip	WinRAR
Multi OS Support	Only for Windows	Windows,Linux, Mac, DOS, OS/2
Compress Formats	ZIP	RAR, ZIP
Method Used	Deflate method(combination of LZ77 and Huffman coding)	LZ and Prediction by Partial Matching (PPM)
Dictionary Size	Default	Can Set Dictionary Size
Profile For Compression	Not Applicable	Create Our Own Profile For Compression
Extraction	ZIP,RAR,TAR,JAR,BZIP2,UUE,Z,CAB	RAR,ZIP,TAR,JAR.BZIP2,UUE,Z,CAB,ARJ,ACE,LZH,GZIP,7-ZIP,ISO.

Table 1: Difference between WinZip and WinRAR (WinRAR, 2009)

For this study; compressed around fifty to sixty different size files in default settings of both WinZip and WinRAR and compare their respective ratios, and found that the WinRAR compress a file more than that of WinZip. So for a deep analysis of the performance of WinZip and WinRAR, try to compress different format of file like .txt file, .jpg file, .bmp file, .wmv file and .mp3 files; and find out their respective rate of compression. And their respective graphs were plotted and those results are explained below.

3.2 Text File (.txt File)

In this section, using WinZip and WinRAR compress different text files of variable size, the below graph drawn on some of the files sizes and their compression ratios that did for the study, more than fifty files of different sizes were compressed and determine the compression ratios and compare their respective ratios of WinZip and WinRAR, and their result shows that the compression ratio was slightly more for WinRAR than WinZip and the ratio goes on increasing with the file size.

The following graph plot, file size on X axis and compression ratio on Y axis and the graph shows that the difference in compression ratio increases with the increase in file size. And also it shows; the files that were compressed more in WinRAR than WinZip, and their respective ratio was goes on increasing with the file size.

3.2.1 File Size vs Compression Ratio for Text Files

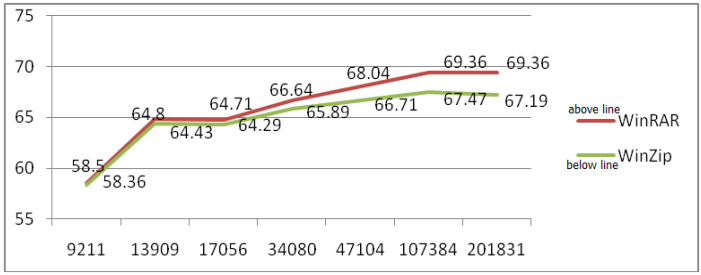


Figure 1: WinZip vs WinRAR for .txt files

3.2.2 Result

WinRAR compress text files more than that of WinZip.

3.3 Image (.JPG File)

In image compression, when compress different size of images; their result shows that the compression for images were more in WinZip than in WinRAR. But the difference is not as much as that in text files compression, even though their differences in size were almost as thousand bytes for both type of compression. The compression ratios for these .jpg images were very less, because these .jpg files were already compressed ones.

In the below graph, original file sizes in KBs on X axis and compressed file sizes in KBs on Y axis. And the graph shows that the WinZip has less number of bytes when compared to WinRAR, which means the compression is more in WinZip than in WinRAR.

3.3.1 Original File Size vs Compressed File Size (in KB)

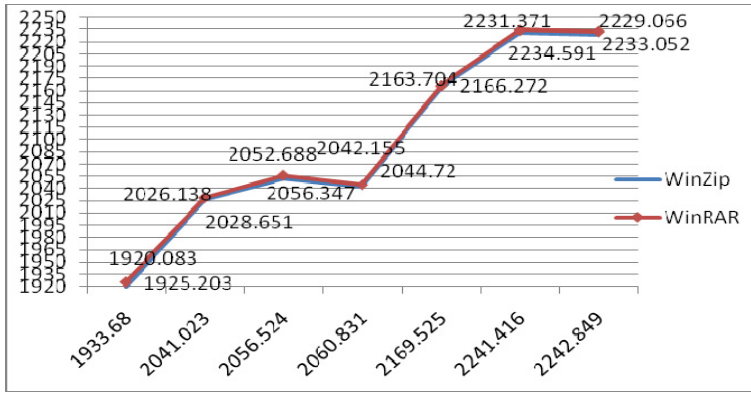


Figure 2: WinZip Vs WinRAR for .jpg files

3.3.2 Result

In compression for images (.jpg) WinZip compress more than WinRAR. In the above graph; it is not clearly shows that but we can found the truth by checking the file sizes of each compression. Even though it is only few bytes when compared to the original size, still more than thousand bytes difference were there between two.

3.4 Image Compression (.bmp File)

In WinZip, WinRAR compression study, next study was done on .bmp images, because in .jpg image files were already compressed ones so it was not clear about the idea of compression. For that different size .bmp images were downloaded from different website and did compression with both WinZip and WinRAR. In graph shown below, image sizes on X axis and compression ratios on Y axis, and when comparing their respective ratios shows that the compression ratio is more in WinRAR compared to WinZip.

3.4.1 WinZip vs WinRAR for .bmp IMAGES

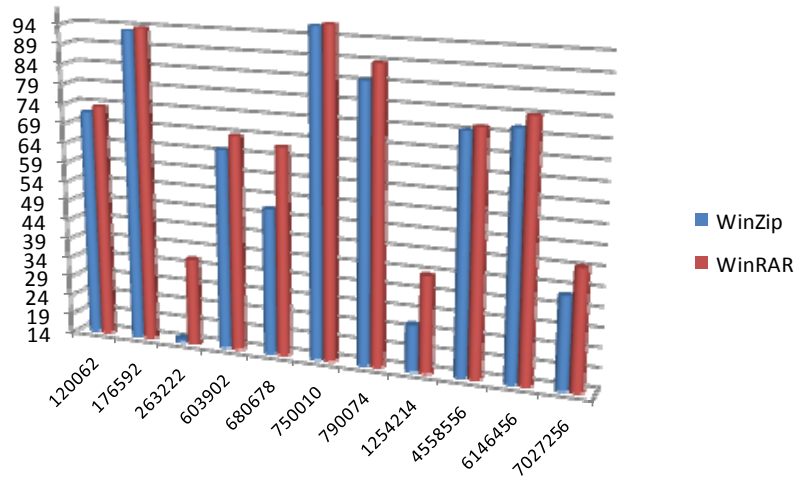


Figure 3: WinZip Vs WinRAR for .bmp files

3.4.2 Result

After comparing different .bmp images of variable size, the respective results shows compression rate is more for WinRAR than WinZip.

3.5 MP3 and Video

The next study of compression was on video and mp3 files, when compared different files of both of variable sizes; the compression ratios got in a varying mode, means in some mp3 and video files WinZip compress more than WinRAR and in some vice

versa. So it could not able to conclude which one is better for these mp3 and video files.

3.6 Conclusion FOR WinZip WinRAR Study

These studies were done on the basis of compression result of few files (around fifty files); but in some cases the result may vary because of the structure and content of the file. So the above results were written in a generalised way, so it means in some cases it may happen vice versa too.

4 Combined Compression and Error Correction

4.1 Result and Analysis

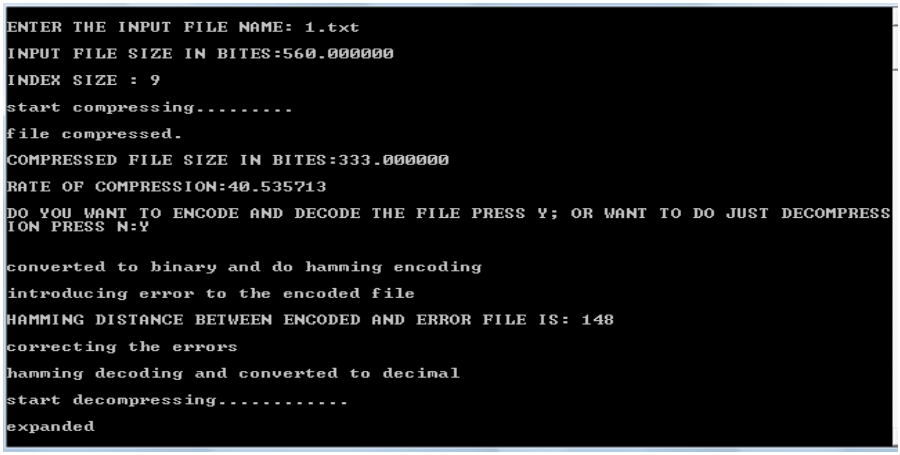


Figure 4: Result of the program

The main outputs of the program are 1) the size of the input file: which shows the number of bytes in the input for compression 2) the size of the output file: which shows the number of bytes in the compressed file 3) rate of compression: which indicate the rate at which it compress the input file 4) index size: it represent the bit size for compression 5) hamming distance: it shows the number of bit position difference between encoded file and error file (or number of errors) and these represent the main output of the program, and when compiling the program respective compressed, encode, error, correct, decode, decompress file were created which represent the output of each step. Here below shows different graph for the algorithm.

The below graph shows file size verses compression ratio of a normal text file. Graph shows that the compression ratio reach up to 25.6%. This means it compresses that particular file up to 25% of its original size.

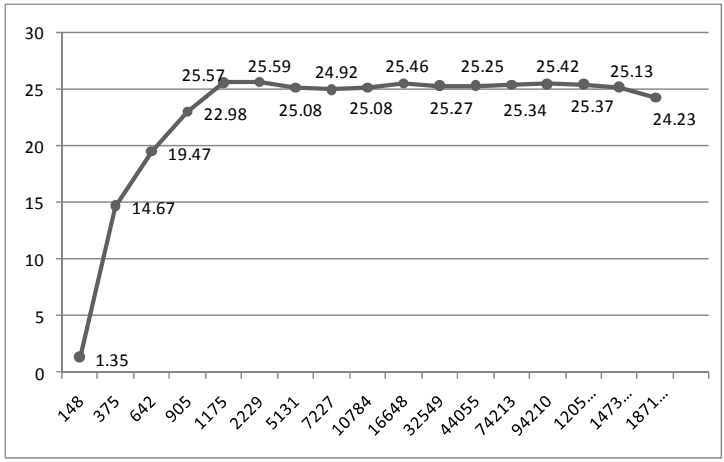


Figure 5: Graph for file size vs compression ratio

In the below graph; plotted with file size on X axis verses compression ratio for files of more repeated text on Y axis and the result shows the compression ratio reaches up to 85%. So by comparing the first graph and the below graph we can state that the rate compression of a file using LZW is depends on the content of the file (repeating sentences, words and symbols).

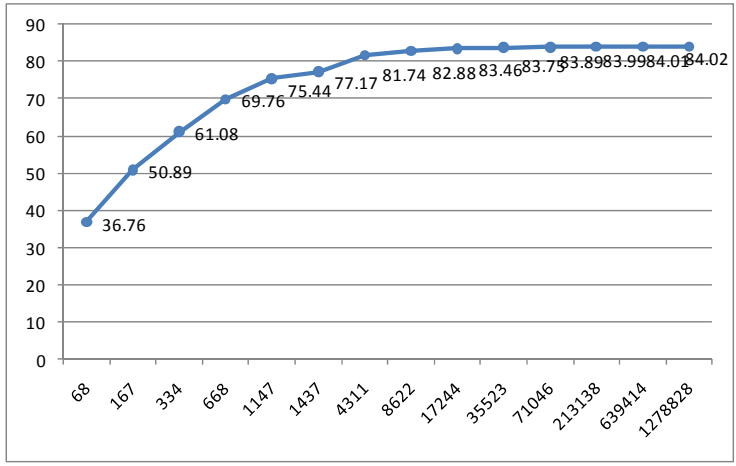


Figure 6: Graph for repeated text vs compression ratio

In next graph it shows about how compression rate changes with index size. Here graph was plotted compression rate verses size of the file. For a same file it compress with different index sizes and the result shows that for a small files when it compress the file with index size 9 shows maximum compression rate and then it decreases for the other index sizes. But considering a large file, the case was different the compression rate increases with increase in index size, i.e. minimum compression

rate when index size 9 and for every other index sizes it shows an increment in compression rate.

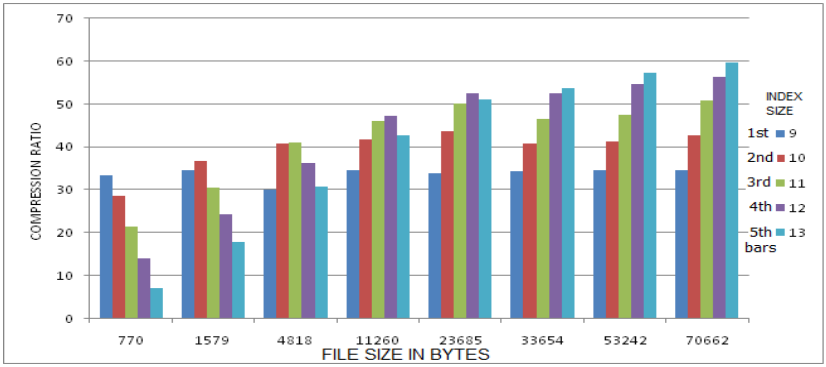


Figure 7: Graph for file size vs rate of compression for variable Index size

5 Conclusion and Future Work

The important aspects of this project is to familiarise with the concepts of data compression and error correction, after detailed study of two, give a clear cut idea about how it operates in the field of communication system. Since there are different techniques available for both the methods; so it is very difficult to say that which combinations produce the best result. Within a limited period of time; tries to find out the best and easy way to implement methods for compression and error correction technologies. Both LZW and Hamming code developed using C algorithm, and the results were achieved, but still the result not accomplished in a desired way, even though these result gave a good idea about how these technique works on a text file. The main concepts of LZW are; it compresses a text according to the content of the file and the rate of compression changes concordant with index size; these two factors were practically proved using with the help of algorithm and their respective graph were plotted, those graph were give a clear idea about these two concept of LZW compression. Another thing achieved by this project was about, how the encoding and error correction process done by using hamming code (11, 7). Next goal achieved was the understanding of effect of error in a compressed and encoded data, for those studies some files were compressed manually and program vice then introduce some errors to the file by deleting some bits from it and do the decompression and the effect of error for both compressed and encoded file are so desolating one. So error correcting is a significant factor in the field of communication.

So as mentioned early both compression and error correction are two non-evitable factors in the field of information theory. Proper compression technique helps the data to be transmitted in a faster manner and also reduce the storage space; the error correction technique assists the data to be retrieve accurately as possible as the original data that sent by the transmitter. So if both these technologies implement properly, i.e. the best combination of both give a great result to the field of communication. Compression and error correction technologies have a lot of

alteration over past few years, and still researches are going on these technologies. And it is very difficult to predict which combination of both gives a perfect result, because these technologies changes day by day. So we can hope in near future the best combination of both will find and help to transfer data more than twice or thrice faster and accurately as compared to today's technology.

6 References

Dipperstein, M. (2008), "Lempel-Ziv-Welch (LZW) Encoding Discussion and Implementation", http://michael.dipperstein.com/lzw/index.html#strings (Accessed 20 August 2009)

Hamming, R.W. (1950), "Error Detection and Error Correction Codes", Bell Systems Tech. Journal, Vol. 29, pp 147-160

Nelson, M. (1989), "LZW Data Compression", http://marknelson.us/1989/10/01/lzw-data-compression/ (Accessed 20 August 2009)

Prakash, A., Singh, A. K., and Tiwari, M. (2006), "Digital Principles and Switching Theory", New Age International (p) ltd, India, ISBN-10 : 812242306X

Shannon, C. E. (1949), "A mathematical theory of communications", University of Illinois Press.

Welch, T.A. (1984), "A Technique for High Performance Data Compression", IEEE Computer, Vol. 17, No. 6, pp. 8-19.

WinRAR Web Site (2009),"WinRAR 3.70 vs. WinZip 11.1 comparison", http://www.win-rar.com/winzipcomparison.html (Accessed 20 August 2009)

Assessing the Risks of Plymouth's Presence on Social Networks- A Case Study of Bebo

O.Shodiya and A.Phippen

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

Abstract

This research paper considers the sorts of risks associated with the posting of personal information on social networking sites, using Plymouths presence on the social networking site Bebo as a case study. It also considers the data that users provide, that makes them more vulnerable to these risks. The paper then concludes that there is a low level of awareness of internet protection amongst the Plymouth community on Bebo, and user education is needed in order to mitigate against the risks that Bebo users in Plymouth expose themselves to when they post their personal information online.

Keywords

Risk, Social Networking, Bebo, Personal Information, Plymouth.

1 Introduction

Social networks play a crucial role in our everyday lives, as most of us have integrated social networking sites into our everyday living, as we see them as a way to network with people and connect to friends. In today's world there are so many social networking sites, with most of them continuing to see an increase in their user base, in a recent report posted on the social networking site Facebook, it stated it just crossed the 90 million user mark (Facebook website, 2008). Social networks has described by Boyd et al (2007) are "*web based services that allowed individuals to (1) construct a public or semi public profile within a bounded system (2) articulate a list of other users with whom they share a connection (3) view and traverse their list of connections and those held by others within the system"* (Boyd et al, 2007).

Despite the benefits provided by the social networking sites there have been growing concerns about the safety of personal information provided on these sites. Personal information comprises of information such as our names, date of birth, e-mail address, residential address, workplaces and photos and they usually serve as identification information. In a recent report published in the BBC, the child exploitation and online exploitation centre said it was concerned about the posting of personal information by children on social networking sites, as one in twelve children met up with someone encountered first online (BBC website, 2006). The various concerns raised about the safety of personal information on social networks have brought about the need for the assessment of the risks associated with the

posting of personal information on social networking sites using Plymouths presence on Bebo as a case study.

2 Previous Study

Research carried out by Sameer Hinduja and Justin Patchin in the area of "*personal information of adolescents on the internet, a case study of my space"* showed that youths are posting and identifying personal information, but not to the extent to which they are supposed to. They based their conclusions on a online survey they carried out on the SNS Myspace which revealed that 81.25% of adolescents profile pages viewed revealed their current cities, 38.4% provided their first names, 27.8% provided their school names, 14.5 provided their birth date, 8.8 provided their full names, 4.2% provided their IM names, 1.1% provided their e mail address, and 0.3% provided their phone numbers. The research was designed to extract data that will determine the validity of the media's claims about whether My Space deserved all of the antagonistic attention and stain it had received from many adults in administrative capacities. The research also wanted to confirm if the numbers support the high volume of reports received. As such, the researchers embarked on an inclusive content analysis of representative sample of pages of my space profiles. The researchers as a measure of caution, in order for the research to be representative, made sure that profiles to be studied had to have a balanced and random chance of being selected for analysis from the entire collection of My Space pages. This they accomplished using a random number generator, as each profile page created on the SNS my space is uniquely assigned a numeric identifier within the site upon its creation. The research further investigated the possibility of cyber bullying and online contact by sexual predators in SNS, and its results revealed that the possibility of been contacted online by sexual predators online is extremely low, but there are possibilities that children could be bullied online (Hinduja et al, 2008).

3 Research Methodology

This research in arriving at its result, used a combination of quantitative methods which include that adopted in researches carried out by Sophos, and Hinduja et al, 2008. Sophos in its Facebook ID probe study created a fake Facebook profile page called "Fraudi Staur" (Sophos website, 2007) and used this profile to send out friend requests to random profiles on face book. "Fraudi Staur" (Sophos website, 2007) was a green plastic frog profile on face book that gave out less information about itself (Sophos website, 2007). In order for the research to find and determine the number of people in the Plymouth network on Bebo, a domain specific search for the hometown Plymouth was conducted using the following parameters (Age – Null, Sex- Male and Female, Relationship Status – Any, Hometown –Plymouth). Then in order for this research to carry out a balanced comprehensive content analysis of the profile pages of people in the Plymouth network, it used a random number generator similar to that used in the research carried out by Hinduja et al, 2008, to determine the profile pages to be viewed. This made it possible for the profile pages to have a balanced chance of been selected among profile pages of people in the Plymouth.

An excel data sheet was then designed to collect the data provided on 200 profile pages of people in the Plymouth network. Due to the fact that the profile pages were

sampled randomly, the Bebo pages that were identified could have been that of a child or an adult, although Bebo does not allow the ages of those less than 16 to be displayed on their profile pages. Additionally data could not be extracted from some profile pages, as a result of them restricting access to their profile pages; Bebo provides its users with the ability to enable privacy settings. The research then looked at all publicly accessible information on the Bebo profile pages identified and this information included the basic profile information provided by the users and comments left by friends. Most of the information was found on the basic profile pages of the users. Additional information was also discovered on the comment portions of the profile pages. Then in order for this research to further investigate the attitudes of the Plymouth community to divulging sensitive information such as identity data on the social networking site Bebo, a fake profile page was created to see the possibility of obtaining sensitive information from users. The fake profile pages then sent out friend requests to 50 users identified from the earlier data collection phase.

4 Results

A domain specific search for people in Plymouth turned up a figure of 25,169, this value represents those who put up Plymouth as their hometown, as there are some others who would have specified United Kingdom as their hometown, but this research would ignore such as we are only interested in those who set Plymouth as their hometown. Among the profile pages selected by the random number generator for content analysis, were some profiles which enabled privacy settings, thus these profiles could not be viewed unless you are a friend. This finding indicates that some users might be aware of the risks of posting personal information online as this information could compromised, thus in this regard they have enabled privacy settings as a safeguard. Additionally, some profile page searched for, returned errors and this might be attributed to their accounts been inactive or been deleted.183 of the profile pages people had an age displayed on their basic profile pages, which represents of the profile pages sampled. Among the 200 people sampled, 74 of them could be termed minors (less than 18 years old).This finding shows that there are good numbers of minors that use the social networking site Bebo, thus there might be a possibility of cyber bullying or cyber stalking occurring to this class of users.

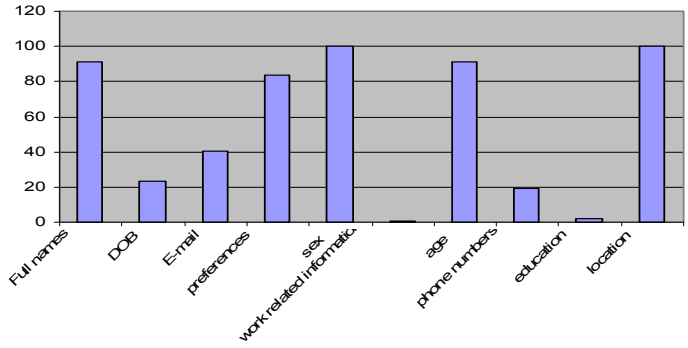


Figure 1: Information posted by people on the Plymouth network on Bebo (%)

46 of the users put up their dates of birth on their profile pages, although we noted earlier that Bebo does not allow ages less than 16 to be displayed on profile pages. The putting of sensitive data such as date of birth which is used in identification of persons, on this profile pages can be due to the insensitivity of the owners of this profiles to internet protection, or the fact that they are not aware of the risks of posting sensitive personal information on social networks. Among the 200 profile pages 182 provided their full names on their profile page, The posting of full names in combination with dates of birth on social networking sites has been identified as a major source for online identity theft in the past, and it will be a source for identity thieves obtaining information about potential targets in the years to come. 168 of the profile pages analyzed provided preferences on the profile pages and this information is also usually used by computer users as password to their systems, as they see them as easy to remember secrets for which they can not forget. The provision of preferences on these profile pages can be said to be no harm to the owners of these profiles until this information is used to compromise items such as their E- mail accounts. All of the profile pages sampled provided the sex of the owners of the profile page, this is so because the SNS Bebo requires users to provide their sex before joining the sites. The display of sex on the profile page of users on the SNS Bebo is a default, which users cannot control, thus they are bounded by this default setting. Among the profile pages sampled, 172 provided their photos on their profile pages and this can be attributed to the interactivity of the web technologies that are used by SNS which enable users to make statements about themselves in form of photos. The posting of personal information such as photos is no risk to users of the Plymouth community on Bebo, but if this photos are used in combination with other data such as date of birth, full names, sex then it maybe a potential risk to the users who posted this information, as this information can be used to make clone passports of the users. In all the profile pages analyzed 81 users had their E- mail address or chat IM displayed on their profile pages and of this number are 26 minors (less than 18). The posting of this information is of no harm to the posters of such information, until the information is either used to stalk or bully the person who posts the information. Among the 200 profile pages analyzed, 183 provided their ages on their profile pages, as this might be attributed to the focus group that Bebo attracts. Adolescents tend to provide their ages on their profile pages so as to show they are young and can be networked. The posting of the users age is not a source for concern until this information is used by some someone such as a cyber stalker or online predators to identify potential target that they are going to stalk. In all of the profile pages analyzed 4 provided education related information, while another 2 provided work related information. The posting of work or education related information is no requirement when joining Bebo, but an additional feature on these sites. The posting of sensitive data such as work and education related information cannot be explained, as this information can be can be acquired by cyber stalkers or online identity thieves in identifying targets.

The second part of this research which involved an Identity probe turned up mind bugging results. This fake profile page was able obtain response from 18 people, in form of confirmation of friend request, and among the people that confirmed friend request, the fake profile was able to obtain the phone numbers of 5 of them on their profile pages. In other to further investigate the possibility of me obtaining the contact details of the 13 who did not put up their contact detail on their profile pages,

6 of those who accepted friend requests from the fake profile were added to live messenger accounts using the live messenger ID they provided on their profile pages, although not all provided live messenger IDs.

In other to further investigate the possibility of me obtaining the contact details of the 13 who did not put up their contact detail on their profile pages, 6 of those who accepted friend requests from the fake profile were added to live messenger accounts using the live messenger ID they provided on their profile pages, although not all provided live messenger IDs. The purpose of this is to see the possibility of them divulging sensitive information such as their contact details and workplace to me. The results were astonishing as the fake profile was able to get the contact details of 2 of them within a week of meeting online, although 3 others refused to reply to chat messages but they confirmed the friend requests on their live messenger accounts, and one is yet to reply to my friend request on live messenger as of the time of writing this report.

5 Recommendations and conclusion

Social networking sites (SNS) such as Bebo will continue to thrive as long as they continue to adapt themselves to the dynamics of meeting user social needs. The users will also continue to provide personal information on SNS as them see it as an opportunity to network themselves. If users cannot be prevented from providing personal information, it will become imperative to educate users on the attendant risks that go with posting personal information such as Full names, Date of birth and E- mail address on SNS. This measure will go a long way in increasing the level of awareness of internet protection in the Plymouth community, which is our case study. And in light of the above mentioned points this research will also summarize the protection measures that can be taken by users in Plymouth on Bebo to protect themselves against the risks that go with posting personal information on social networking sites which include Cyber stalking, Cyber bullying, and Online identity theft. Additionally the summary of measures will also consider the measures that can also be taken by SNS service providers to protect user information, without undermining the purpose for which SNS where designed for, which is networking.

- Social networking sites should consider investing more money in increasing user education on the potential for harm in posting sensitive personal information online.
- Privacy settings should be enabled by users of social networking sites.
- Read the privacy policy that social networking sites provides its users.
- Parents of Minors should monitor their children when using social networking sites.
- Users should limit the amount of personal information they post on social networking sites.
- Users should avoid the temptation of adding strangers to their list of buddies or friends.
- Users should avoid posting information which can be described as revealing.

- Users should make use of covert channels of communication in reaching out to friends rather than using social networks.
- Social networking sites should consider investing more money in increasing user education on the potential for harm in posting sensitive personal information online.

6 References

BBC website, 2006. "*Child online safety card unveiled*". (BBC.co.uk). Available at http://news.bbc.co.uk/1/hi/technology/5238992.stm [accessed 11th May, 2008]

D Boyd et al, 2007. Social networking sites: Definition, History and scholarship. Journal of computer mediated communication. Page (210-230) Available at http://www.blackwell-synergy.com/doi/pdf/10.1111/j.1083-6101.2007.00393.x Social Network Sites: Definition, History, and Scholarship [accessed 21 April 2008]

ENISA (European network and information security agency) (2007). "*Security issues and recommendations for online social networks"*. Available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf [accessed 2nd June 2008].

Parry, 2008. "*Parrys guide to cyber bullying"*. (Bebo.com). Available at http://www.bebo.com/CyberBullying.jsp [Accessed 23 November, 2008]

Ralph Gross, Alessandro Acquisti. 2005 "*Information Revelation and Privacy in Online Social Networks (The Facebook case)*". (Heinz college.edu) Available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf [Accessed 31st December, 2008

Smith p, Madhavi J, Carvahlo M, Tippet N. "cyber *bullying, its forms, awareness and impact, and the relationship between age and gender in cyber bullying"* (Anti- bullying.org) Available at http://www.anti-bullyingalliance.org.uk/downloads/pdf/cyberbullyingreportfinal230106_000.pdf

Sophos website, 2007. *Sophos facebook probe shows 41% of users happy to reveal all to potential ID thieves.* (Sophos.com). Available at http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html [Accessed 1st January 2008].

Combined Data Compression and Error Correction

S.Sudhan and M.A.Ambroze

Fixed and Mobile Communications, University of Plymouth, Plymouth, UK
e-mail: M.Ambroze@plymouth.ac.uk

Abstract

The primary objective of the project is to familiarize with the concepts of data compression and error correction. The project intends to analyze the impact of data compression on error propagation. As the data is compressed more, error propagation through the transmission channel increases. When this data is decoded, it will bear no resemblance to the original data being transmitted. To reduce error propagation, it is necessary that the data is not compressed to a great extent. Another main aspect which the project intends to investigate is the best combination of compression and error correction that is likely to make data being transmitted to be sufficiently compressed and also less prone to errors.

Keywords

Data compression, Error Correction, LZW, LDPC.

1 Introduction

In the field of information theory, data compression and error correction are two coding subsystems, which though theoretically diverse seem to be codependent on each other. Source coding is the process of removal of redundant information from the input sequence where as error correction introduces redundant information as a means to safeguard data from error introduced due to error correction. Error correction can hence be considered as a necessary evil. It negates the very purpose of compression by increasing the size of compressed data. But if completely ignored can cause serious errors particularly in the case of text data. The level of correction depends on various factors like type of data being compressed, the level of compression required and also on the accuracy of the received data. Even though these two techniques are integral part of information theory, their diverseness requires them to be studied separately for better understanding. Initial part of this literature review will be dealing with data compression.

The project intends to investigate very important aspects which have a direct bearing on how degree of compression and integrity of data being transmitted are affected. The main purpose of such an undertaking is to identify factors that affect compression and error correction in addition to understanding the core concept about its working.

The project will follow a straight forward approach.

- Detailed research on various coding techniques used for data compression and error correction.
- Select one coding algorithm each for data compression and error correction.
- Divide the project into 3 parts
    1. Data compression: This part will deal with data compression alone. Using the selected coding algorithm various text sources will be compressed, transmitted (error introduced randomly) and decompressed. Degree of compression will be observed. By analyzing the results, the impact of data compression on error propagation can be investigated. The actual implementation of the algorithm would require the development of software using C language programming.
    2. Error correction: This part of the project will deal with error correction. Using the selected coding algorithm, the uncompressed text source will be coded (redundancy introduced), transmitted (error introduced) and finally decoded. The process is repeated by varying the number of redundancy bits introduced during coding. The extent of error correction achieved in each case will be observed.
    3. Combined data compression and error correction: The proposed digital communication system will be implemented and simulated by means of software developed for this purpose. The input text source will be compressed to varying degree. In addition to this the degree of error correction will also be varied. Detailed analysis of the simulation results will help in arriving at a proper conclusion regarding the best combination of data compression and error correction.

The report will begin off by delving in to the background of the two coding subsystems which as mentioned earlier are integral part of information theory. Thereafter the report goes on describe the research methodology that was undertaken to achieve the proposed objectives. This section also includes some results that were achieved during the course of trying to gain better understanding about the subject. Results of the simulation obtained by running the program was then analysed and presented towards the end of the report.

2 Overview of Data Compression and Error Correction:

Data Compression: One of the earliest forms of text compression was MOS code, which was invented in 1838. This was one of the simplest form using short codes for most often repeated letters. But the actual birth date of information theory is considered to be 1948. It was then that Claude E. Shannon published his epoch making paper on limitations of trustworthy data transmission over untrustworthy channels and also proposed various methods to achieve these limits. The paper also included the concept of information theory. It was actually the first known work to have established bounds for maximum amount of information that could be transmitted over an untrustworthy channel. The very foundation of data compression

was laid by Shannon and Robert Fano. They together introduced a method of compressing data making use of probabilities of blocks.

This work was later overshadowed by a more efficient coding system – Huffman coding. Huffman coding (1952) is similar to Shannon coding. It can perform compression by reducing redundancy in coding of symbols. It was found to be one of the most efficient fixed length coding methods going around. Or so it was, until the emergence of arithmetic coding which made the idea of replacing input symbol with a specific code obsolete. Instead, it introduced a new and innovative idea of replacing stream of input symbol with a single floating point number. But the main drawback of this method was that a long and complex information required more bits.

More recently dictionary based compression algorithm have become popular. This technique is entirely different from various other compression techniques that were available at the time of its introduction. These coding algorithms encode variable length strings of symbols as single tokens. The token will then form an index to a phrase dictionary. In case the tokens are smaller compared to index phrase, the tokens will replace the phrase. In this way compression is achieved.

In 1979, Abraham Lempel and Jacob Ziv took a different approach to symbol coding. They assigned code words to source words that were repeating or to patterns in a text. This approach was different from the usual approach to assigning code words to symbols in advance. Such was the success of this method of compression that it is still the basis of modern lossless data compression.

In 1984, Terry Welch improved the Lempel-Ziv method, which was known as LZ78 and renamed the method as LZW. This algorithm is now being used by commercial compression software such as PKZIP and by mainframe image formats GIF and some versions of TIFF. (Wolframscience, 2002)

Error Correction: Performance levels that are achieved in case of coded communication system are clearly stated in popular theorems proposed by Claude Shannon, who can well be considered as the father of information theory. He, in 1948, laid the foundations of information theory in a paper entitled “A Mathematical theory Of Communication”. These theorems not only define the limits on efficiency that can be achieved with information theory but also the importance of coding in achieving these limits. The paper published by Shannon in 1948 formulated statistical evaluation of various problems faced in communication, based on earlier works of Hartley, Weiner, Rice, and Kotel’nikov. Shannon’s work contradicted earlier notion that noise places a limit on accuracy that can be achieved in communication. Shannon showed that various communication channel characteristics such as noise level signal power and bandwidth determines a very important parameter called channel capacity represented by C. the channel capacity actually sets an upper limit on the rate at which information transmission is reliably transmitted and received through the channel. Shannon’s work proved beyond doubt that probability of error in the information being transmitted can be made very low by use of long coded transmission signals if the transmission rate of the information is less than the channel capacity C. this shows that noise places limit only on the

information transmission rate and not on the accuracy of the delivered information. (Michelson and Levesque, 1985)

3 Proposed System:

Information source: The information source in this case is a text source. The text will be read manually.

Data Compression (Source coding): Ideally it is preferable to represent source information by the smallest number of bits possible to make the digital communication system efficient. This is done by removing as much redundancy as possible from the source before transmission. This process of compression is also known as source coding.

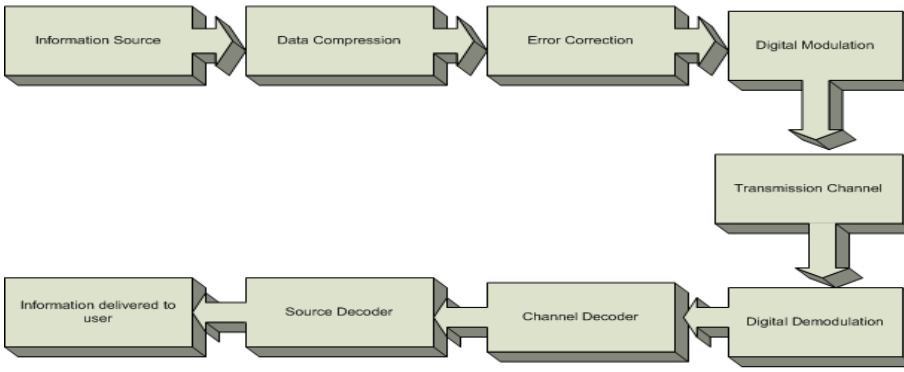


Figure 1: Proposed Digital Communication System

Error Correction (Channel encoder): The encoder receives information bits at the rate R_s and adds redundant bits producing encoded data having a higher rate of R_c. While encoding with a block code, the encoder accepts information in blocks of k bits size and for each k bits it will generate a block of b bits. Typically $n \geq k$. (Michelson and Levesque, 1985)

Digital Modulator: The purpose of the digital modulator is to match the encoder output with that of the transmission channel.

Transmission Channel: Transmission channel is the terminology used to include all the operations that are required to prepare data for transmission in physical channel, the transmission medium and reception operations necessary to bring the received signal upto the point of demodulation. Transmission channel is mainly responsible for introduction of errors in the data being transmitted. Hence during the implementation of the system, introduction of error will occur in this part of the digital communication system.

Digital Demodulation: Demodulation provides an interface between the transmission channel and the function that makes an estimation of the data being

transmitted to the user. The demodulator processes the received data and produces a set of numbers representing an estimate of transmitted symbol. (Michelson and Levesque, 1985)

Channel Decoder: The decoder performs the conversion of demodulator output into symbol decisions that reproduce the actual data being transmitted as accurately as possible. (Michelson and Levesque, 1985)

Source Decoder: The sequence of symbols coming out of channel decoder is received by the source decoder and it then tries to reproduce the original information contained in the original data being transmitted.

4 Research

The project required the entire digital communication system to be simulated by writing appropriate codes in C language. Before the actual programming was undertaken it was necessary to do extensive research on both data compression and error correction. Extensive research was done on both data compression and error correction. From the invention of MOS code in 1838, to actual birth of information theory in 1948 inspired by Claude E. Shanon through to the modern era of commercial compression softwares such as PKZIP and highly efficient error codes such as turbo codes were extensively researched and understood.

The next major objective or rather a dilemma which had to be overcome before starting the project was to decide on the compression technology to be implemented in the project. Of the many compression techniques available, LZW method was chosen. It is not the best encoding algorithm available but for the purpose of the project (which is mainly to study the best combination of compression and error correction), LZW appeared to be lucrative due to its ease of implementation. Having decided on LZW as the means for data compression, an in depth study was done to better understand the LZW technology. The future implementation would require quite an extensive knowledge about the working of LZW technique. After going through coding and decoding algorithm, many examples of LZW coding and decoding were done to familiarize with the process and gain a thorough knowledge.

As the project involves studying the effects of compression and correction in real time transmission it is highly imperative that effect of error propagation not be overlooked. For viewing the effects of error propagation during compression/decompression process, some of the bits of the code were randomly changed and then decompressed. The effects were found to be quite impressive. The change of a single bit produced a rather faulty data after decompression, which bore no resemblance with the actual data being compressed.

The most important part of the project i.e. implementation of the proposed digital communication system involved programming in C language to simulate the entire operation of compression, noise, error correction and decompression. As mentioned earlier of the many compression techniques available LZW was chosen. The LZW algorithm is easy to understand but implementation is not that easy some of the

implementation issues faced while developing the coding for LZW are listed in the commencing section.

4.1 Implementation issues of LZW:

4.1.1 Size of Code Word

Main thing that needs to be settled during the implementation phase of LZW is deciding the size of code word that needs to be used. Some of the things that need to be taken into consideration when deciding on the size of the codeword being used are:

- Code words generally need to be bigger than a length 1 string of the string being encoded.
- Each and every encoded string requires a code word for representing them.
- Code words which are bigger size generally imply that there are more entries in the dictionary. (Dipperstein, 2008).

4.1.2 String representation in the Dictionary

The dictionary in the Lempel-Ziv-Welch algorithm has a unique way of associating strings with code words. Even though code words are of limited length, the LZW algorithm does not enforce a limit on the string length that is encoded.

Strings of arbitrary length are represented by a null terminated array. There may be cases when there may be a large number of strings which may amount to thousands of bytes in length. With the increase in the machines memory size, the memory requirements of the null terminated strings become negligible. (Dipperstein, 2008).

4.1.3 Dictionary Layout

Deciding the dictionary layout affects locating and inserting strings. The strings are stored in the dictionary as a codeword prefix and a byte suffix.

In the beginning, the dictionary has only one entry for a character string. As the process of encoding proceeds, the strings contained in the dictionary expand. There is however an upper limit on the number of strings that can be accommodated in a dictionary. It depends on the size of the code word. If the code words are n bits long, there can be up to 2^n unique code words. (Dipperstein, 2008)

4.1.4 Memory complexities:

The advantage of using 14 or 15 bit long codes is that it gives better compression ratios for large files as they have larger string table to be utilized during it operation. It does however affect the performance drastically for smaller files. On the other hand compression of long files cause the compression ratio to degrade gradually as more of the file is read in. The reason for this is quite obvious. As the string table is of finite size, on adding more strings to the table, it becomes full and no further

strings can be added to it. String table can only function properly for the part of the file that was read in when the table was built. Remainder of the file has different features and hence requires a different string table.

5 Results and Discussion

The input parameters that are required are:

- Input file
- Index size
- Error correction encoding enable or disable
- If encoding enabled: matrix size and noise level

The output parameters are:

- Original file size
- Compressed file size
- Compression ratio
- BER
- PeR

In the commencing section we will be seeing how each of these parameters is related to each other by performing actual compression-error correction process by running the program. The results are plotted in graphs and the results analyzed.

5.1.1 Compression and Decompression Only:

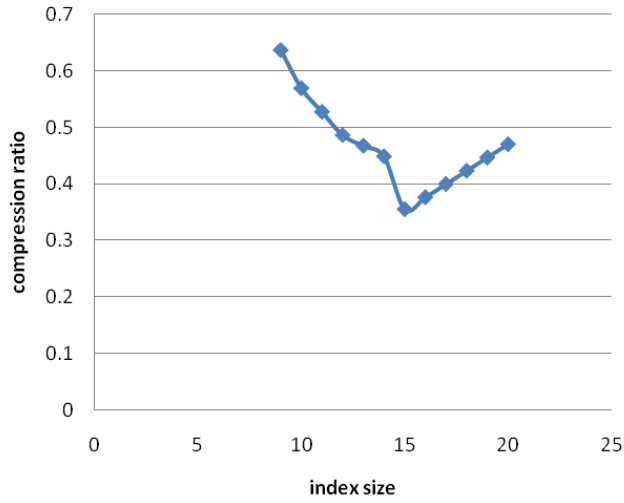


Figure 2: Compression ratio vs index size

- Variation of compression ratio with index size: The level of compression varies with the size of codeword being used. The source data was compressed to varying degrees by altering the index size. This helps us to arrive at the best compression for the source data. The source data used in this case was a file named 1.txt. The file size was about 188.7 KB. The index size was varied from 9-20. The results were plotted with index size on the x-axis and the compression ratio on the y-axis.

  From the graph it becomes clear that the compression ratio decreases with increase in the index size. The compression ratio decreases almost linearly with index size. The best compression occurs at the index size of 15. Beyond that, the compression goes on increasing. Thus, in order to achieve the best compression, the index size selected should be 15. In reality, this shift in behavior from linear decrease to linear increase of compression ratio with index size is due to the wastage of space caused due to use of large code words (above 15) hence the best compression for the file 1.txt occurs when index size of 15 is used.

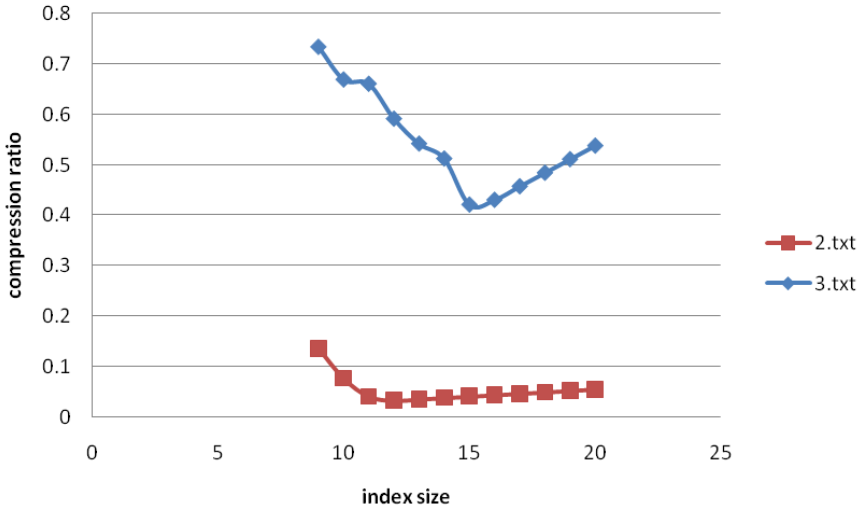


Figure 3: Compression Ratios for different text files

- Compression of different types of text files: Different text files were selected, both of similar size (189 kB) but having different contents. The two files selected were 2.txt and 3.txt. The file 2.txt has more repetition of words than the contents of 3.txt. Hence as a consequence, the file 2.txt is compressed more than the file 3.txt.

  For the text file 2.txt the best compression was achieved at index size of 12 and for 3.txt the best compression was achieved at index size of 15. This is because the dictionary size in the case of 2.txt is much smaller than 3.txt. So if large code words are used there will be wastage of space. This is the

reason why compression occurs at smaller index size for 2.txt as compared with 3.txt which has larger dictionary with more words.

- File Size v.s. Compression ratio:

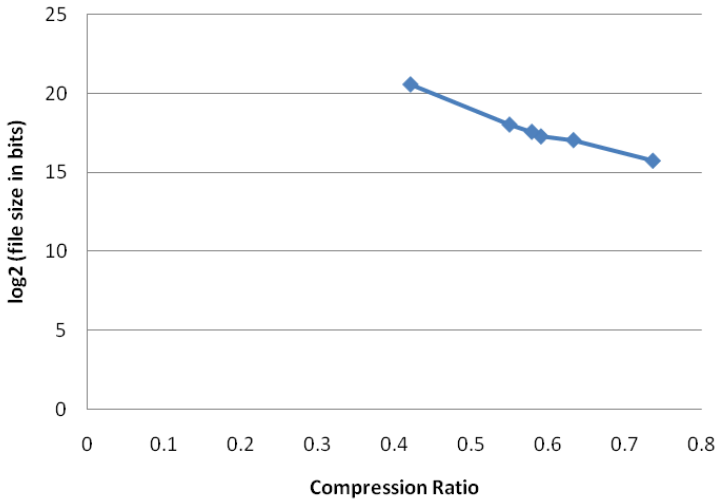


Figure 4: File size vs Compression Ratio

The graph shows the variation of compression ratio when files of different sizes are used. The graph was plotted using files of sizes ranging from 6 kB to 192 kB. The codeword length or the index size was set at 15 which was neither too small nor too big a value. The file sizes were converted to bits and expressed in terms of $\log_2$. On plotting the graph it was found that compression ratio varies inversely with file size i.e. higher the file size, lower was the compression ratio. This means that file of lager sizes were compressed more in comparison with smaller files.

Limitations: Analysis on Error Correction was not possible as LDPC was not properly implemented. Code for LDPC was taken from Ioremap (Ioremap, 2009). Due to compatibility issue with the self developed LZW program, the results obtained for BER and PeR were not consistent.

6 Conclusion

The project was undertaken mainly to familiarise with the basic concepts of compression and error correction, in the process investigating how various parameters has a direct bearing on the efficient transmission of compressed data. Detailed analysis couldn't be carried out due to time constraints as majority of the allotted time was spent on developing the coding. However, most of the objectives were achieved and the results were analysed. The best compression for the file under consideration was found out by trial and it was found to be dependent on the size of the code word. Too large a codeword affects the compression as space is

unnecessarily wasted while too small a codeword doesn't help in realising compression to the full extent. Other results obtained were how different files of same size having different contents get compressed to different levels. Finally the variation of compression ratio with size of the file being compressed was also plotted and conclusion was drawn that for a particular codeword length, better compression can be achieved for larger files.

As already mentioned there are a lot of techniques available for compression as well as error correction. Each of these techniques has undergone a lot of modifications over the years. Still researches are being done on each of these coding techniques as there is still a huge scope for improvement. New, improved and efficient coding techniques are being sought out by researchers in the field of information theory. When compression and error correction are considered separately, the advancements made in each are tremendous. But, as mentioned at the start, these two coding subsystems are inseparable in real world communication system. There is always a trade off between accuracy and the compression. The best combination of compression and error correction hasn't been established yet. Several studies are being conducted to realize this. Eventually, the best combination would depend on the level of accuracy required.

7 References

Dipperstein, M. (2008) "Lempel-Ziv-Welch (LZW) Encoding Discussion and Implementation". Accessed: 10/01/09[Online]. Available at: http://michael.dipperstein.com/lzw/index.html#strings

Gallager, R. G. 1978. "Variations on a Theme by Huffman". *IEEE Trans. Inform. Theory 24*, 6 (Nov.), 668-674.

Michelson, A.M. & Levesque, A.H. (1985) "Error Control Techniques for Digital Communication", John Wiley & Sons, Inc.

University of Birmingham. (2008) "A Brief History of Data Compression" Accessed: 10/06/08[Online]. Available at: http://www.eee.bham.ac.uk/WoolleySI/All7/intro_3.htm

Welch, T.A. (1984) "A Technique for High Performance Data Compression", IEEE Computer, Vol. 17, No. 6, pp. 8-19.

William, R.N. (1990) "Adaptive Data Compression" Kluwer Academic Publishers, London

Wolframscience. (2002) "Some Historical Notes" Accessed: 10/06/08 [Online]. Available at: http://www.wolframscience.com/reference/notes/1069b

Ziv, J. & Lempel, A. (1977). A universal algorithm for sequential data compression. IEEE Transactions on Information Theory, 23(3):337–343.

Ziv, J. & Lempel, A. (1978). Compression of individual sequences via variable-rate coding. IEEE Transactions on Information Theory, 24(5):530–536.

8-bit Embedded Web Server using Intel 8051

F.Tharakan and P.Davey

School of Computing, Communications and Electronics,
University of Plymouth, Plymouth, UK

Abstract

This paper is intended to propose a design concept to implement Embedded Web Server that makes use of some particular features of TCP/IP protocol suite using an 8-bit Microcontroller and an Ethernet LAN Controller. The proposed web server will be a small replica of one of the 1000's of web servers that spread over the internet. This Embedded Web Server will be stored with a small web page, so that whenever a client connects to this web server, can retrieve the page stored in the web server by using protocols like HTTP, TCP, UDP, IP etc. The paper will give a brief idea about how an Embedded Web Server can be built with an old 8-bit Intel 8051 Microprocessor and an Ethernet LAN Controller (CS8900A). It will also give description about how to communicate with CS8900A and also gives a brief idea about how 8051 can be programmed to work as an Embedded Web Server.

Keywords

Embedded System, Chip, Web Page, micro controller, Ethernet controller

1 Introduction

The emergence of Microprocessor to the world of electronics was stared in early1970's. It started with 4bit microprocessors and now microprocessors with 64bits are also available. The main purpose of using microprocessors is to give some intelligence like, human interaction, machine control etc to specific machines and appliances. Later, engineers started to increase the functionality of a microprocessor by adding RAM, ROM, timers, UART, Ports and other common peripherals (Ayala, 2005). There is a common misunderstanding among the people that the term microprocessor is only associated with a Personal Computer (PC) or a laptop. Even though this is an important application of microprocessor, most of the people use microprocessor indirectly for many other applications. For example, a luxury car used today may have about 50 microprocessors to control different functions such as, windscreen wiper, automatic gear changing system, braking system, airbag, electric windows, air conditioning, headlights etc (Heath, 1997).

It has been recently predicted that 95% of the internet connected devices on 2010 will be embedded devices, not computers. This shows the importance of developing embedded system in this modern scientific era. This project 'Embedded Web Server' is such a kind of device that can act as a web server, which is connected to the internet. (Beyond logic, 2006). A device that is capable of accepting HTTP request from clients and serving them HTTP responses together with some data contents is known as web server. In simple words, a device (mostly a computer) that can deliver

web pages is defined as a web server. Each web server will be having an IP address and most probably a domain name. The embedded web server is a web server that works on an embedded environment (PC Magazine, 2008). This report is prepared based on recent developments occurring in the field of embedded internet technology.

2 Embedded Ethernet Basics

TCP/IP is the most commonly used terms in networking. It is said to be the basic communication language (protocol) of the internet. For the smooth working of the system the protocols are made into different layers. Protocols in each layer will communicate to the layer above or below it. So if a host wants to send any information, the information is passed from top layer to bottom layer. The information is then passed to the destination host. The bottom layer of the destination host receives this packet and is passed to the top layer. As the information is passed from a top layer to bottom layer, the information is encapsulated by adding a protocol specific header to it. When the information is passed from a bottom layer to top layer (in destination host) this protocol specific headers are stripped off. (Eisenreich and Demuth, 2003)

The OSI reference model is an ideal protocol stack which is equipped with 7 layers. The OSI layer reference model is shown below.

OSI Layer Name	Functional Description	Examples
Application (Layer 7)	User interface	Telnet, HTTP
Presentation (Layer 6)	How data is presented Special processing, such as encryption	JPEG, ASCII, EBCDIC
Session (Layer 5)	Keeping data separate from different applications	Operating systems and application access scheduling
Transport (Layer 4)	Reliable or unreliable delivery Multiplexing	TCP, UDP, SPX
Network (Layer 3)	Logical addressing, which routers use for path determination	IP, IPX
Data link (Layer 2)	Combination of bits into bytes, and bytes into frames Access to the media using MAC address Error detection and error recovery	802.3/802.2, HDLC
Physical (Layer 1)	Moving of bits between devices Specification of voltage, wire speed, and cable pin-outs	EIA/TIA-232, V.35

Table 1: OSI layer reference model (Source: - Odem, 2000)

The network protocol stack in a computer network consists of different modules involved with networking. The figure shown below is the Skelton of a network protocol stack.

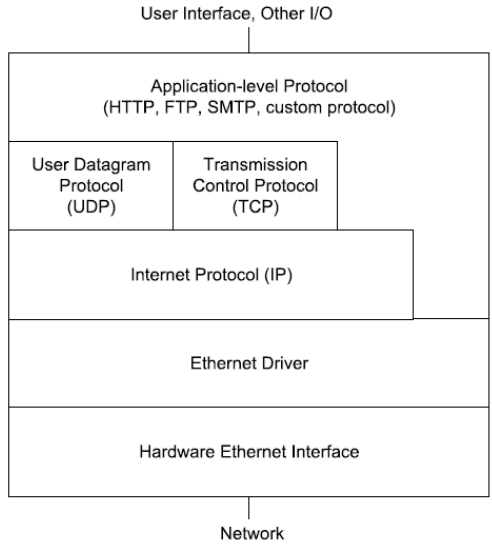


Figure 1: Network Protocol Stack (Source: - Axelson, 2003)

The bottom of the stack is a hardware interface that constitutes the physical layer of the network. The modules in the top of the stack are applications that use the received data for running the application. The middle module constitutes the means of error checking, status and control etc. In transmitting, the frame will travel down the stack from application layer to physical layer that places the frame on the network. This frame travels through the Ethernet cable and when it reaches the receiver, the physical layer of the receiver will receive it and the frame travels up the stack to the application layer. The applications in the application layer use the data in the received frame (Axelson, 2003).

The application level protocol uses the received data and provides the data to transmit on the network. This protocol is attached with a user interface that enables the user to interact with the computer and the network. Through this interface the user can request data from other hosts in the network or deliver data to the other hosts in the network. But in an embedded web server, the user interface will be having limited functionalities like basic configuring, monitoring etc.(Axelson, 2003)

The data like text message, web page, the contents of a web page, files, binary data, program code or any data that a computer want to send or receive from the network. To send these data on the network the application layer must follow certain rules. This will help the application in the receiving host what to do with the received data. These set of rules are called protocols. There are many application level protocols used today such as HTTP(Hyper Text Transfer Protocol) for requesting and sending

web pages, FTP(File Transfer Protocol) for transferring files, SMTP(Simple Mail Transfer Protocol)/POP3(Post Office Protocol) for email (Axelson, 2003).

3 Block Diagram

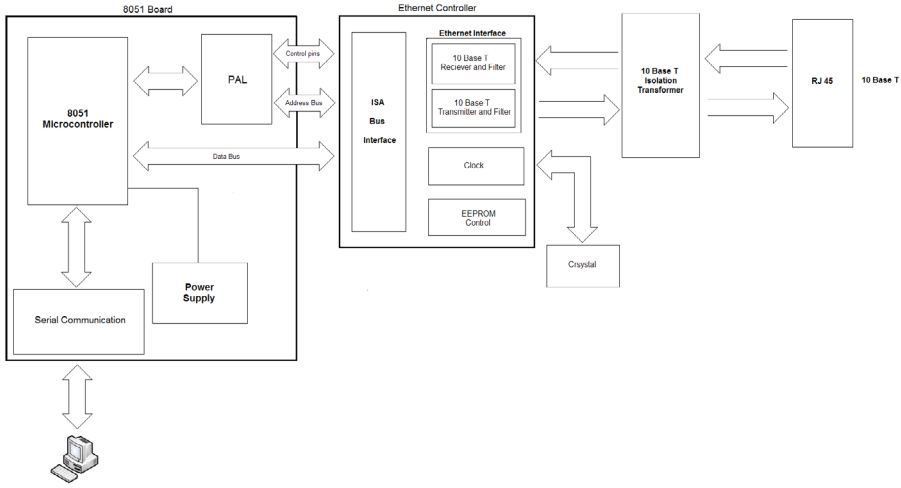


Figure 2: Block Diagram of Designed Embedded Web Server

8051 microcontroller development system is used in this project to get enough space to store the web page. It is mainly used for downloading and storing the program code. The main components in this system are 1) 8 x 32K external ROM which starts at base address 0000h, 2) 8 x 32K external RAM which starts at base address 8000h. 3) A liquid crystal display. 4) A Digital to Analog Converter (DAC). 5) Programmable Array Logic 6) Serial interface.

Microcontroller: - The Intel 8051 microcontroller is one of the most popular general purpose microcontrollers in use today. It is an 8-bit microcontroller which means that most available operations are limited to 8 bits. 8051 chips are used in a wide variety of control systems, telecom applications, and robotics as well as in the automotive industry. The 8051 Microcontroller can be programmed in 8051 Assembly language, C and a number of other high-level languages. Many compilers even have support for compiling C++ for an 8051. (Ayala, 2005)

Programmable Array Logic: - Programmable array logic is a digital device which "has a programmable AND array and a fixed OR array". The PAL is quite simple compared to PLA as PLA involves programming both AND and OR gate inputs. PAL's can be programmed using a wide range of Computer Aided Design programs that are easily available in the market. It accepts inputs like logic equations, truth tables, state graphs or state tables and will automatically generate the required patterns. These program patterns are then downloaded to the PAL IC. In this project

PALCE16V8-25 manufactured by AMD is being used. It is a 20 pin plastic DIP structure, which is made with high speed CMOS technology device (Shobha, 2005).

Serial Interface: - In this project initial configurations of the embedded web server like downloading the program code and debugging are done through a serial interface to the PC. The main mismatch between the 8051 and the PC is the difference in voltage levels. Here IC Max232 is used as a level shifter. 8051 works in TTL logic voltages and serial port of PC (RS232) work in a different voltage level (Sodoityourself, 2008).

Ethernet Controller: - *Ethernet controller* is the most important peripheral in an embedded internet device. The Ethernet connectivity, which is used to access internet, is provided by Ethernet controller. There are many Ethernet controller chip available in the market. The chip used in this project is CS8900A, a 100pin chip which has an on chip RAM, a 10 base T Ethernet interface and a direct ISA interface. The packet page architecture is used to handle the internal registers in this chip. For this very reason it is having good system efficiency compared to other Ethernet controller. The Ethernet controller is connected to an RJ45 Socket via an isolation transformer. (Data sheet)

Isolation Transformer: - Isolation transformer is mainly used to decouple two circuits. It connects two circuits without any physical or electrical contact. In fact it blocks DC and allows AC signals to pass through it. In this project, Valor FL1066 is used as an isolation transformer in between the CS8900A and the RJ45 Socket.

RJ45:- RJ45 is an 8 pined socket mainly used in Ethernet communication and telephony application. It is mainly used in for 10baseT Ethernet Connections. The pin out and pin description of an RJ45 socket is shown below (Nullmodem, 2007).

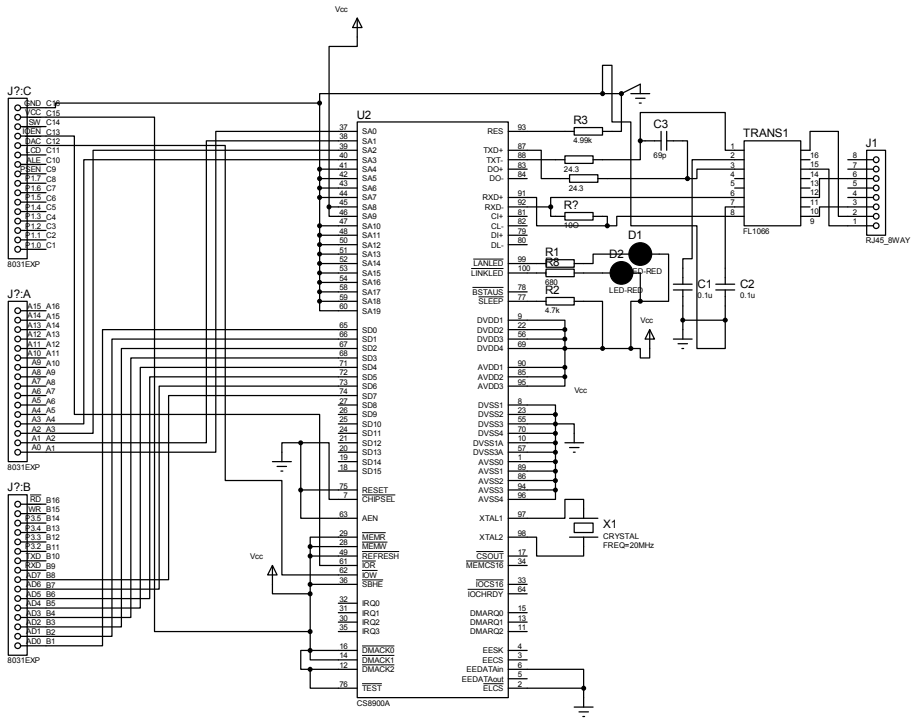


Figure 3: Circuit diagram of the Embedded Web server

4 Interface between Microcontroller and Ethernet Controller

4.1 Hardware Interface

The microcontroller and the CS8900A is interconnected with 8 data lines , 4 address lines and read- write pins. The CS8900A is a16 bit chip. Even though it is capable of 16-bit operations, due to the limitations of 8-bit 8051, we are taking use of only 8 data lines of CS8900A. The data lines SD0-SD7 of CS8900A is connected to the AD0-AD7 of 8051 respectively (Data Sheet).

The default base address of the CS8900A is assigned to be 0300h. In this project we are using the I/O mode operation to access the packet pages in CS8900A. The I/O mode mapping addresses are shown in the table. From the table it is clear that the addresses that we have to access will be in between (base address + 0000h) to (base address + 000Eh). Ie addresses between 0300h and 030Eh. The first 12bit will be a constant. Ie '030' [0000 0011 0000]. This makes clear that from the 16-bit address we have to control only the 4 bits the rest 12 bits remains the same. So the pins SA9 and SA8 need to be connected to Vcc and the rest of the pins are connected to the ground. The controllable 4 address pins SA0-SA3 are connected to the address lines of the 8051 (Data Sheet).

Offset	Type	Description
0000h	Read/Write	Receive/Transmit Data (Port 0)
0002h	Read/Write	Receive/Transmit Data (Port 1)
0004h	Write-only	TxCMD (Transmit Command)
0006h	Write-only	TxLength (Transmit Length)
0008h	Read-only	Interrupt Status Queue
000Ah	Read/Write	PacketPage Pointer
000Ch	Read/Write	PacketPage Data (Port 0)
000Eh	Read/Write	PacketPage Data (Port 1)

Table 2: Packet Page Port Addresses (Source: - Data Sheet)

The !IOR and !IOW pins are used for the read and write operations of the CS8900A in I/O mode operation. To read from the CS8900A the pin !IOR must go low and to write to the CS8900A the pin !IOW must go high. These two pins are connected to the IOEN and DAC pins of the Programmable Array Logic respectively.

4.2 Software Interface

The memory of the CS8900A is structured in a Packet Page Architecture. The 8051 communicates with CS8900A through the packet page registers. The 8051 give instructions to the CS8900A by writing to the Packet page register. During the Transmission and reception process CS8900A itself alters the Packet page registers indicating its change of status. The status of CS8900A can be monitored by 8051 by reading the Packet page registers

A 16-bit data can be wrote to the Packet Page register by first writing the 16bit register address to the packet page pointer port (000Ah) and then writing the 16-bit data to the packet page data port 0(000Ch). A 16-bit data can be read from the Packet Page register by first writing the 16bit register address to the packet page pointer port (000Ah) and then reading the 16-bit data to the packet page data port 0(000Ch). A sample assembly program to read a port is shown below.

```
CS8900A EQU 030AH
ORG 8100H
AGAIN:
READ_WORD:
    MOV DPTR,#CS8900A
    MOVX A,@DPTR      ;
    INC DPTR
    MOVX A,@DPTR      ;
    SJMP AGAIN
    END
```

Program Flow Chart. The flow chart plays a crucial role in the program development. The flow chart of the program code of the embedded web server is shown below.

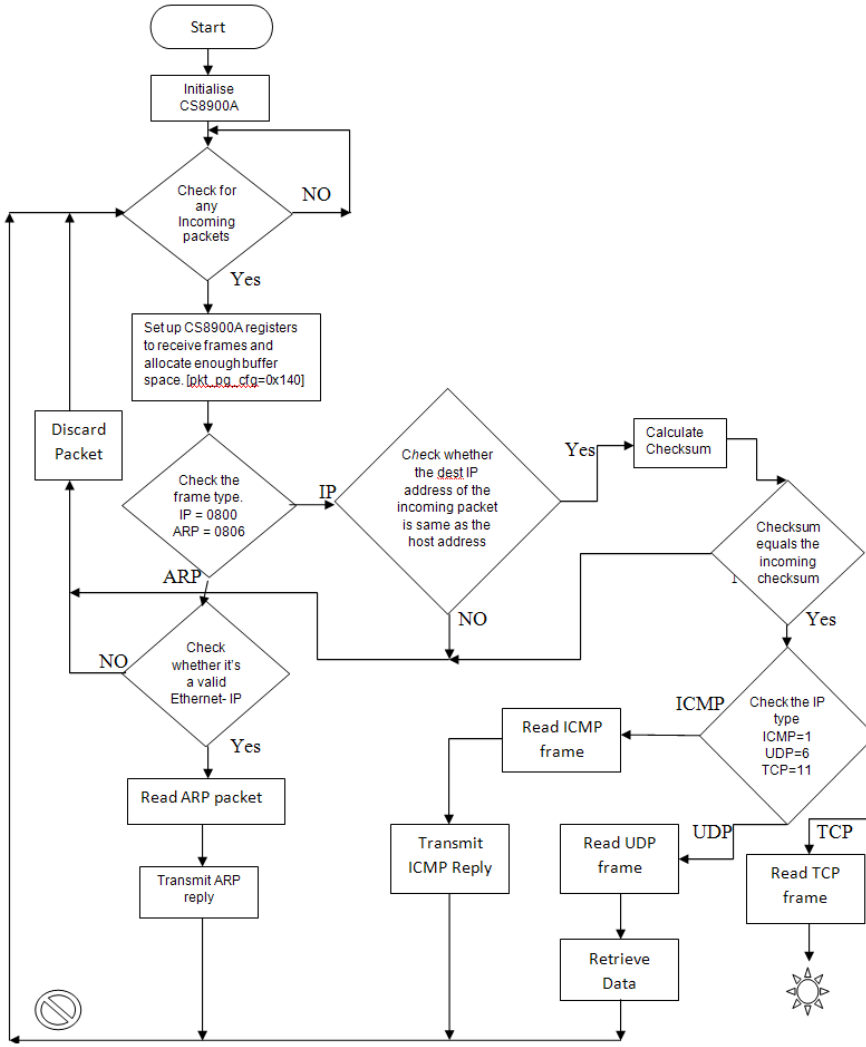


Figure 4: Flow Chart of the Program

The first step is to initialize the chip CS8900A. After initialization the system continuously checks for any incoming packets. If there are any incoming packets waiting, the system will allocate some buffer space and receive the frame. The received frame will be in a normal Ethernet frame format. Then the program checks the frame type. If the frame type is IP (0x0800), the Ethernet header is parsed and is passed to IP processing section. If the frame type is ARP (0x0806) the frame will read the packet (Brady, 2002).

Once if a frame having frame type 0x0800 is received, the frame is declared as a IP frame. The Ethernet header is first stripped off from it and the program checks whether the destination IP address of the incoming packet is same as the host

address. If the program comes out with a negative answer the packet is discarded. If the answer is positive the program will calculate the checksum (Brady, 2002).

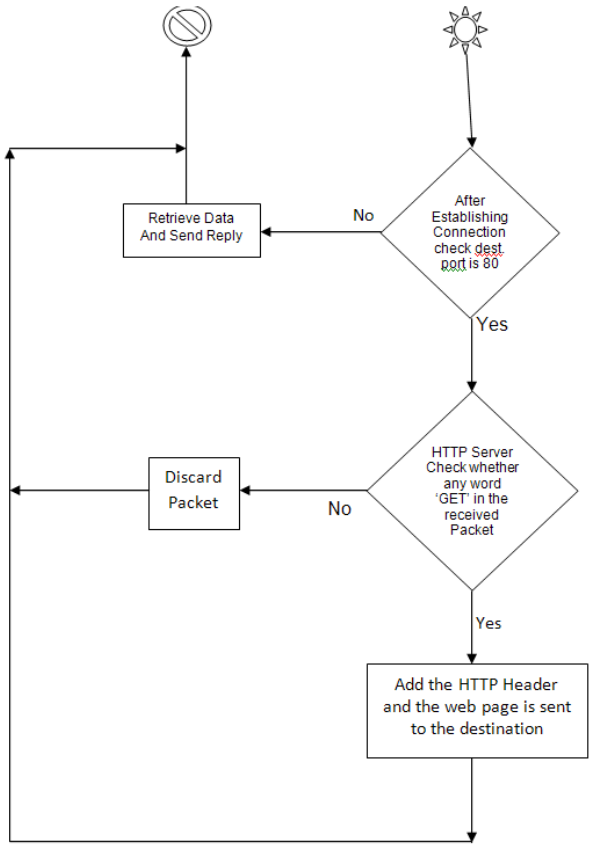


Figure 5: Flow Chart of the Program

The system compares the calculated checksum with the checksum that is encapsulated in the frame. If the checksum doesn't matches the frame is discarded. If the checksum matches the system will checks the IP type of the frame in the type field. The IP type value for ICMP, UDP and TCP are 1,6 and 11 respectively. If the frame is not associated with any of these type values the frame is discarded. If the IP type is ICMP the packet is read and an echo reply is transmitted to the sender of the ICMP frame. If it is a UDP frame the frame is read and data is retrieved (Brady, 2002).

If the received frame is TCP, the system first read the frame and then checks the destination port of the frame. If the destination port is indicated as 80 (HTTP port number) the frame is passed to the HTTP server function. The HTTP server function will checks whether there is any GET word in the HTML header of the received packet. If there is a GET word, the system will send the web page stored in the code memory to the client (Brady, 2002).

5 Results

Writing or reading a Packet Page Pointer is done in two steps. Writing is done by first writing the 16-bit address to the Packet Page Pointer Port(000Ah) and then writing the register value to Packet Page Data Port 0 (000Ch). Similarly reading is done by first writing the 16-bit address to the Packet Page Pointer Port (000Ah) and then reading the 16-bit data from Packet Page Data Port 0 (000Ch). The figure shown below is the screen shot of what I got after running the program (in single step mode) to read the Packet Page Receive Control Register (0104h) from the hardware.

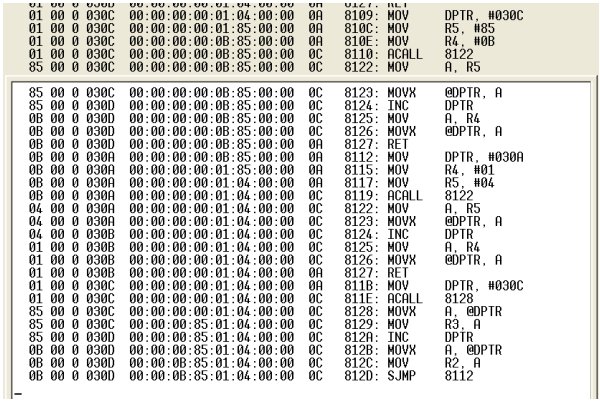


Figure 6: Reading of a Packet Page register

6 Conclusion

Advancements in the field of internet connected Embedded devices are playing a vital role in everyday environments. In the current scenario, workforce is mainly looking forward to integrate the web accessing facility into their handheld devices. The project focuses on proposing a new design concept of an Embedded Web Server that implements a TCP/IP protocol stack for receiving and transmitting Ethernet packets. Embedded web server is a web server that works on an embedded environment. It will be very compact and portable and also it will be capable of delivering a web page according to the client request. In this particular project Intel 8051 will acts as a microcontroller and CS8900A will be the Ethernet Controller. CS8900A is programmed to work in 8-bit Input/output mode. So the internal Packet Page registers of CS8900A can be accessed indirectly using eight 16-bit Ports.

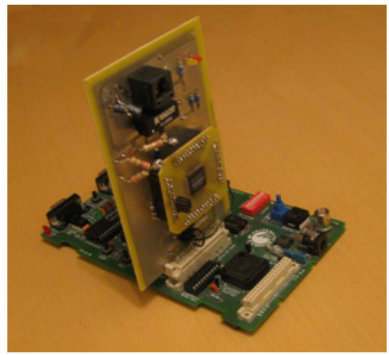


Figure 7: Photo of implemented web server

The microcontroller can communicate with CS8900A by altering these Packet Page Registers. Even though there were a lot of limitations in the designed system, the project proved the fact that the 8051 is flexible to implement even a web server. The photo of implemented embedded web server is shown below. The report concludes hoping that many more engineers will come forward with better design concepts and explanation of how a web server can be designed.

7 References

Axelson.J (2003), *Embedded Ethernet And Internet Complete,* Lake View Research LLC, Madison, ISBN:- 1-931448-01-9

Ayala.K (2005), *The 8051 Microcontroller,* Thomas Delmar Learning, Canada, ISBN-140186158.

Beyond Logic (2006) "IP and Ethernet Interfaces" http://www.beyondlogic.org/etherip/ip.htm (Accessed on 12 - 04 – 08)

Brady. J. (2002), 'Build Your Own 8051 Web Server', *Circuit Cellar* [online], issue 146,Available HTTP :- http://www.circellar.com/library/print/0902/brady/brady.pdf (Accessed on 10 - 05 – 08)

Eisenreich. D. and Demuth. B, (2003), *Designing Embedded Internet Devices* , Newnes, United States of America,ISBN-1878707981

Heath. S, (1997), *Embedded Systems Design,* Newnes-An imprint of Butterworth Heinemann, Oxford, ISBN 0750632372.

Kidd. M. (2002), 'An 8051 based web server' Available at:- http://cegt201.bradley.edu/ projects/proj2002/embedweb/ (Accessed On 15-07-08)

Nullmodem, (2007), "RJ45", Available at:- http://www.nullmodem.com/RJ-45.htm (Accessed on 29-12-2008)

PC Magazine, (2008), "Definition of Web server" http://www.pcmag.com/encyclopedia_term/ 0,2542,t=Web+server&i=54342,00.asp (Accessed on 14 – 04 – 08)

Shobha K.R.(2005), 'Programmable Array Logic' *M S Ramiah Institute of Technology*, Banglore [online], Available at : http://forum.vtu.ac.in/~edusat/PROGRAMMABLE_ ARRAY_LOGIC_VHDL_eNotes.pdf (Accessed on 24-12-2008)

Sodoit yourself, (2008), "Max232 serial level converter" , Available at : - http://sodoityourself.com/max232-serial-level-converter/ (Accessed on 05-06-2008)

Online Security: Strategies for Promoting Home User Awareness

B.Varghese and S.M.Furnell

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

Abstract

In the current world of advanced technology, the Internet has become a part and parcel of our everyday life, but at the same time threats and vulnerabilities are also increasing rapidly. Studies have revealed that home users are among the primary target of attackers, so the need for better awareness and understanding of the security aspects from the home user point of view is the main idea behind this research. Home users need a good understanding of security guidelines in order to achieve maximum security and to investigate the current awareness and practices of the home user, an online survey was conducted which analysed the user awareness about Internet security, their daily practices and their available support resources. A study was also carried on to observe the quality of the existing security guidelines provided by the reliable sources on the Internet. Based on analysis of results from the online survey, and information's gathered from different investigation, we could observe that majority of home users were unaware about threats and vulnerabilities around them and had poor security practices, this may be because of the home users unawareness about reliable security guidance sources. On this ground home user security guidelines where prescribed for secure computing and also strategies for improving the existing promotional activities regarding home user security were prescribed.

Keywords

Awareness, Internet, Security, Malware

1 Introduction

There has been a rapid increase in the demand for Internet connectivity recorded in the past years. Home users frequently transact various activities over the Internet that involves personal information. These activities include on-line banking, use of e-health services, community websites and engaging in e-commerce, at the same time the Internet is no more a safe play ground due to the vulnerabilities in these new existing technologies. A large number of home users are totally unaware of their exposure to online security risks. Computer security is important to all users and many software applications are available to protect the online users. Antivirus software's, Anti-spyware's and firewall are commonly used to protect the systems from viruses, malicious codes, information theft and hacking. Home Internet users using broadband connections are more prone to these attacks. On the other hand wireless networks offer home users with many benefits such as flexibility, portability, increased productivity and enables users to access to their organisations

without sitting at a fixed physical point at the same time wireless networks are more and more vulnerable to threats than wired networks. There is ample evidence to show that home users are at risk of attack. Indeed, domestic systems present an environment in which malware can thrive, and the recent success of botnets in the UK presents an example of how easily vulnerable machines can be hijacked for misuse. At the same time, home users who lack security awareness can become easy prey for scammers and identity thieves. This research work examines the strategies for promoting home user awareness on online security.

The threats home users frequently face online include viruses, worms, spam, spyware, phishing and hacking. Any of these attacks may misuse or corrupt the user's information or even see the user himself been attacked. These cyber criminal activities affect the main IT security issues like confidentiality which is the prevention of information disclosure to unauthorised persons, Integrity which tells about the correctness of data and it is prevention of unauthorized modification and availability which means usability and access of data whenever and wherever required. According to UK payments association APACS, the cost of Online banking fraud has increased from £22.6m in 2007 to £52.5m in the year 2008 and the total fraud losses on credit and debit cards in UK amounted to £609m which is a 14% increase from the previous year (BBC, 2009).

In 2007 McAfee and National Cyber Security Alliance conducted a survey of 378 home users in the United States regarding online security and awareness and also conducted a technical scan of their systems. The analysis reveals that the 98% agreed it is important to update the security software and 93% of the participants believed their home computers were safe from malware. However, in reality the technical scans revealed that only 24% of the participants had a protected online environment with an anti-virus protection that had received and update within a week and had an enabled firewall and with the anti-spyware software installed. Other facts revealed by the survey were that 54% of the participants reported they had virus on their system and 44% believed that they had spyware on their machines. Another shocking result was 74% of the participants believed they have received phishing emails. And it was sad to see that 9% of the total participants had been victims of online identity theft and all this has taken place due to the knowledge gap and lack in online security awareness. 64% of the participants revealed they were not able to identify if the website is safe or not before visiting (McAfee / NCSA, 2007).

According to Symantec's Internet security threat report, targeted attacks to home users were around 95%. All these facts lead to understanding more about the home user and this leads to investigate the current state of the home user.

2 Methodology to Study Home User Awareness

The main aspects of the research was to analyse the awareness of home users regarding online security, as the target audience were the online home users, it was decided to do a survey with online questionnaire because through an online survey home users could participate from the home Internet at their convenience. Online survey also had few other merits like, the data can be quickly collected and analysed, the cost considered with the online survey is lower compared to other survey

methods and the results will have accuracy and can be easily be transferred to the spread sheets for statistical analysis.

The survey questionnaire was constructed after the intensive literature study and the format and design of the questionnaire mainly included closed option multiple choice questions to provide results for statistical analysis. There were also a few open-ended questions to further analyse the home users' knowledge and so they could share their experiences.

The questionnaire was divided into four parts and started by collecting some demographic details such as education, age, sex, knowledge level and usage level of the participant to support the analysis and conclusions. This was followed by a security awareness survey, which aimed at identifying whether the user is aware of the security facts and the threats around him while using the Internet. For collecting this information certain questions were used like rating the current Internet scenario whether it is safe or not safe, and depicting the user awareness about malware, firewall and usage of wireless networks. Following this, the next part collected information regarding daily practices of the user while using their computer and checking their awareness in different areas like virus, spyware, usage of firewall, usage of email and backups.. To conclude the survey there were some questions to collect information regarding security promotion and daily commercial practices when using the Internet. These questions were designed to capture information from the home user regarding the promotional activities of online security awareness and the sources from where they gain the information and to know how commercially they are using the Internet. The survey was promoted among the home users through social networking communities and through university students.

3 Findings

The online survey received responses from 259 participants, the majority of whom were in the age group of 18 to 35. A major portion of the participants were academically or technically qualified, and 77% classified themselves as intermediate users, while 16% considered themselves as expert users. Overall, 44% of the participants said that Internet is necessary part of their profession or education.

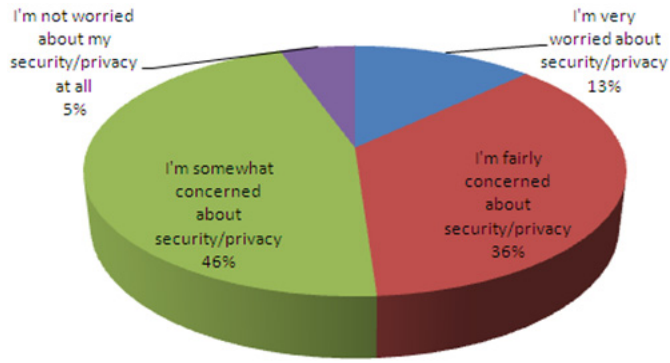


Figure 1: Home User's Concerns about online security & Privacy

From the security awareness investigation we could observe that many of the participants were not sure if the Internet is still a safe place, as shown in Figure 1 below.

When asked if their system was infected with malware 35% of the participants said their systems were not affected and 42% were not sure if their system was affected or not. This actually shows the lack of technical awareness in nearly half of the users and 21% of the participants confidently said their systems were affected with the malware. And 80% of the participants believed that malware would slow down their system performance while 72% of respondents believed it would corrupt or wipe the files in the system. By analysing the user understanding regarding malware, it was possible to see that the user is aware and knows what happens if the system is affected. And in recent years the trend is towards mobile computing and wireless technologies, and when asked with the participants regarding encryption on wireless network 44% did not know about it and just 28% of the participants used encryption on their network.

The next section investigated users daily practices and we could see that around half of the participants update their antivirus daily or weekly and around 20% of the participants did not check or were aware of these updates. 76% believed that antivirus performs regular scan on every file in the system, while 42% of the participant had a misunderstanding that antivirus identifies and prevents hackers. And when the users were asked about spyware, 41% did not know what it is and what it does. Nearly half of the participant's antivirus software also protected spyware, while the rest of the participants were unaware or did not have anti-spyware support. When analysing the participants who did not have anti-spyware, we were able to see that they were victims of some sort of attack. Some of the participants were victims of malware attack and shared there experience, and when analysing these we could analyse that this had happened due to user unawareness and negligence, and once affected it gives big crisis for home user resulting in data loss or even system crash. When the users were asked about how confident they were that their system is free from viruses, 36% replied that their system is okay and 38% believed that they were affectedm, with the rest being unaware of what is happening in their system.

From the responses received it was possible to observe that 74% of participants had firewall installed on the machines. Of these, 38% claimed to have manually checked their firewall configurations, while 61% had not done so. When asked the reason for this behaviour, more than half believed that the default configuration is sufficient to protect them against vulnerabilities.

When the home users were asked about spam mails, 63% indicated that they receive spam regularly, 42% were not interested in using spam filters while 19% were totally unaware what the spam filter is. One of the important reasons for an increase in spam may be that 76% were not interested to report it. This means that the spam providers are getting support from the user itself.

In this world of online insecurity, backups are very important and when, analysed with the responses it was able to observe that 55% do backups while 12% were

ignorant about it. From the participants who did backup we were able to analyse that nearly half of the users did not have a regular practice. Nowadays a good backup culture needs to be developed in the home users so that they will be ready to face any uncertainty.

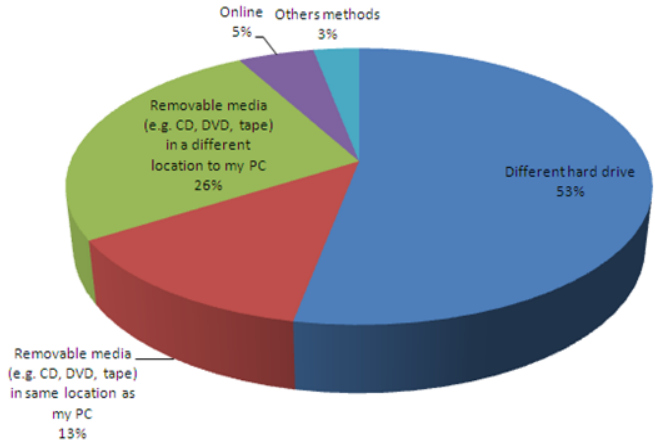


Figure 2: User Data Backup

As Figure 2 shows more than half of the participants preferred different hard drive to have their backup, and it is interesting to see nowadays a small percentage of users willing to have their backup online. When how many of the have successfully restored their back, only 33% of the participants have restored it while 47% of the participants did not have occasion to use their backups.

The reason for the flaw in security is the home user unawareness. When we analyse the resources of home user support as shown in Figure 3, we could analyse that

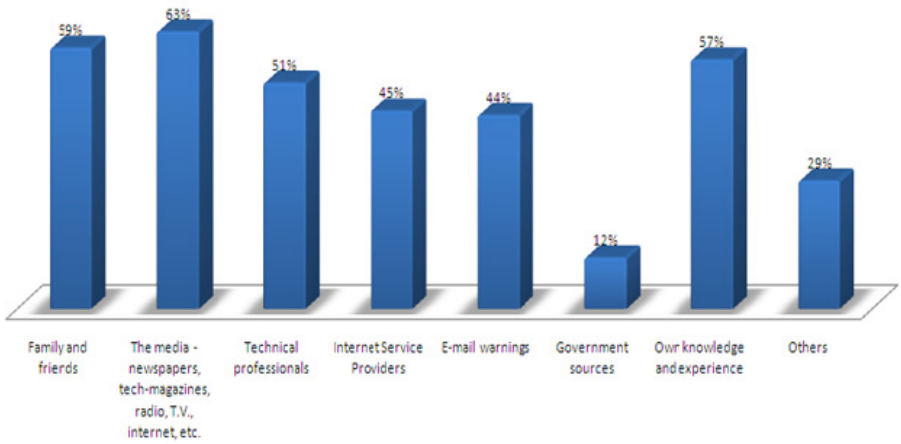


Figure 3: Sources of Technical Support to Home Users

Media like newspapers, tech-magazines, radio, TV and the Internet were the primary sources of knowledge support, followed by the family and the friends circle. The problem is that if the family and friends did not have adequate knowledge or had a misconception it will be passed on the user too, and these wrong practices will then continue. Looking at Figure 3, government sources were clearly the least rated by the user. Governments should take more imitative to promote these security techniques as it safe guard the nation too. Even though government had some of the reliable resources it is not promoted effectively, so that the home users are unaware of it. When user were asked for their common support website these were some of the responses.

"Microsoft, Symantec, Getsafe online"
"help from microsoft, help from google", "security help from google seach results"

Considering the U.K national average of 49.5% of online banking users, we had a response of 59% of the participants who use online banking. This difference may be because we have a greater participation of academically and technically qualified users in our online survey. And to briefly consider the security precautions taken by the user, users password characteristics were analyzed and it was able to see that a major percentage of users and practice good password policy.

4 Discussion

The survey responses provided information regarding how home users think, act and react to the vulnerabilities. While most of the users considered themselves as intermediate or above, half of them were totally unaware and did not know whether there system is affected by malware or not. Moreover, some of the users had incorrect ideas about malware, and at the same time a major portion of the home users were totally unaware of encryption on wireless network, which can lead the intruders to having access on their network. This makes the user extremely vulnerable and can lead to further problems. There are areas where the home user awareness has to be increased like antivirus, anti-spyware and firewall, because in the current scenario even though this software is installed on the user machines, they are generally not enabled or regularly updated to provide good protection to the users.

Many home users assumed that antivirus will prevent them from hackers and online frauds. Many studies say the home users are the target of attackers because hackers capitalize upon their unawareness. Many users did not use proper security applications like anti virus software, ant spyware and firewall and the common problems they faced were corruption of data, change in system settings, decreased system performance, and change in browser settings. Two thirds of the home users did not check the configurations of the firewall and they believed that the default configuration is sufficient to protect them from all these threats. So it is advisable that if the vendors and the developers a good standard of default setting it will be very beneficial for the novice users. As email has made communication easier, it has also enabled that transportation of spam. Nowadays spam levels are increasing day by day and e-crimes are also increasing rapidly, but many users are totally unaware where to report against these activities if they become the victims of it. From our

survey 76% of users replied they are not interested in reporting these complaints. These types of attitudes could be changed only by promoting proper awareness to the home users.

A good backup culture should be developed with the home users so that in case of any data loss the user will be able to retrieve their data. More awareness should be increased with home users so that they do not need to suffer a major loss. The major source of technical support for the home users was the media followed by friends and relatives. If the friend or the relative is not a technical expert, the home users knowledge will be limited which leads to more risk. The home users mostly relied on websites of Microsoft and security vendors for technical advice while the users were totally unaware of the government run websites specifically targeting home users security like Get safe online and IT safe. These may be due to the lack of promotion from the government and other security organizations. Home users are not willing to waste time and effort to find out these sources and expand their knowledge; they just need the things to be done.

5 Conclusion

After a careful study, this research paper has given some important security guidelines and promotion methods of available technical resources to increase the security and awareness among the home users.

Security guidelines included updating the antivirus frequently, and enabling the firewall applications and making sure that it is working fine. Anti-spyware software should be installed and updated regularly and the operating systems needs to be updated frequently with the newly available updates and patches. Users should develop the ability to recognise the genuine and fake websites and take care of their personal credentials. Users should be advised to follow strong password characteristics and should make sure the file and the print sharing should be disabled when not in use. User should be taken more precaution no to open mails of unknown senders and always rely on reliable security sources for help and advice.

Government and other security organization can take more initiatives to promote the security awareness programmes and websites, so that home users can have the full benefit of these resources. More promotional activities can be carried on televisions advertisements, print media, radio advertisements, commercial websites, through mobile communication and by educating from schools.

6 References

BBC, 2009, '*Big jump in online banking fraud'*, http://news.bbc.co.uk/1/hi/business/7952598.stm, [Date Accessed: 08-08-2009]

McAfee / NCSA, 2007, '*McAfee/NCSA Cyber Security Survey'* http://209.85.229.132/search?q=cache:zlc0shdbMFcJ:download.mcafee.com/products/manuals/en-us/McAfeeNCSA_Analysis09-25-07.pdf+mcaffe/ncsa+2007&cd=1&hl=en&ct=clnk&gl=uk, [Date Accessed: 19-08-2009]

Symantec Corporation,2007. "*Symantec Internet Security Threat Report*", http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf [Date Accessed: 26-1-2009]

Voice Quality Assessment for Mobile to SIP Call over Live 3G Network

G.Venkatakrishnan, I-H.Mkwawa and L.Sun

Signal Processing and Multimedia Communications,
University of Plymouth, Plymouth, United Kingdom
e-mail: L.Sun@plymouth.ac.uk

Abstract

The purpose of this paper is to assess the voice quality for mobile to SIP call on the live 3G network and to investigate the effects of codec and packet losses on the perceived speech quality. Asterisk based test platform is used with SIP client on one end and connected to 3G network on the other end to measure the speech quality on the live environment. More than 200 voice recordings are measured in the designed test bed on different codec combinations of GSM-GSM and G711-GSM (codec from SIP to asterisk – codec from asterisk to mobile phone) and results are analysed. Packet losses are introduced in the network to analyze the impact on the speech quality on the live network. The result shown that GSM-GSM codec had more impact on the speech quality with the MOS scores less than 3 whereas the G711-GSM had a fair quality with MOS scores above 3 for most cases. Packet loss is found to have major impact on voice quality and minor impact on call signalling on all the calls established with the duration of 180 seconds or lesser. A formula is derived to predict the MOS values on different packet loss conditions and validation tests on the proposed formula shown good accuracy with the prediction errors range between ±0.3 MOS for most cases. The work should help to better understand the voice quality for new services such as from 3G mobile to SIP call.

Keywords

Speech quality, codec, packet loss, PESQ, MOS, 3G

1 Introduction

Voice transmission is the most important service in mobile, telecommunication and VoIP networks that decide the Quality of Service (QoS) provided to the customer. To provide more effective services, the 3GPP (Third Generation Partnership Project) is producing a technical specifications which is globally applicable for 3G mobile system. The 3GPP group uses the IP technology end-to-end to deliver voice and other multimedia content to mobile handsets. The signalling function and the call control from terminal to network and in between network nodes are fulfilled by SIP (Session Initiation Protocol). This gives more offers to the customers to make calls between 3G phones and SIP phones apart from making calls only between 3G users. The evaluation of the perceived speech quality on such services in the live 3G network becomes an imperative task to the service providers to satisfy their customer's expectation. It is very important to investigate the speech quality and to provide information on the speech quality degradations due to different network impairments on these services. Asterisk based test platform is used with SIP client on

one end and connected to 3G network on the other end to measure the speech quality on the live environment. The different degradation factors that affect the voice quality in the live 3G network are voice codec used in the end-to-end network, network delays, delay variations and packet losses (Nortel, 2003).

In this research paper, we mainly focus on the effects of two different codec in combination in the end-to-end call. The effect of packet loss on the speech quality and call signalling from SIP client to the mobile handset through asterisk server is also analysed and the formula is proposed based on the MOS values obtained during different packet loss size. The rest of the paper is organized as follows: section 2 describes the experimental setup and different scenarios carried out using the test platform. Sections 3 present the experiment results and analysis made on the result. It also explains the proposed formula and model validation test results and prediction error range. Section 4 concludes the paper and suggests some future studies.

2 Experimental Setup and Scenarios

2.1 Test platform architecture:

A speech quality test platform is setup to objectively measure the perceived speech from the SIP phone to the mobile phone. Figure 1 shows the architecture of test bed used to provide the necessary network connectivity to evaluate the speech quality in a 3G mobile network. Four main components of the architecture are SIP client, asterisk server, network emulator and the mobile network connecting mobile phone. Asterisk is an open source hybrid TDM and full featured packet voice PBX system, used as a mediator between 3G mobile networks and the SIP phone IP network to establish live calls. The SIP client and mobile phone are used as two end users where calls are established and the voice quality measurements are evaluated. Network emulator or Netem emulates the properties of wide area network and provides the network emulation functionality for testing protocols. In this research, netem is used to introduce packet loss of different packet loss size inside the network.

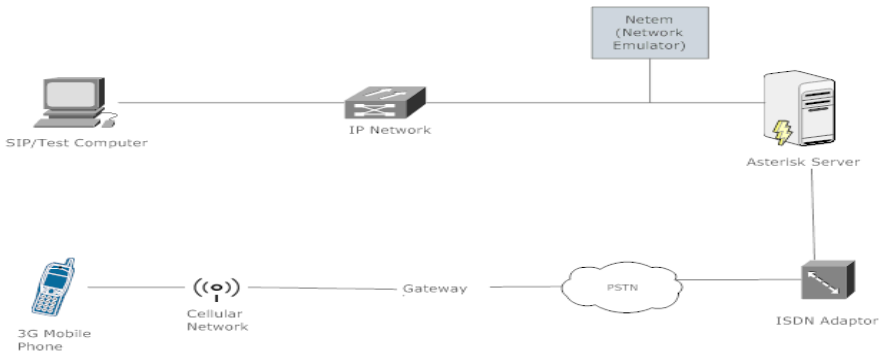


Figure 1: Test platform for speech quality evaluation

Once the test platform is set and the call is established, the speech signals are to be played in the sender end (SIP phone) and recorded in the receiver end (mobile

phone). To perform this play and record operations from SIP phone to the mobile handset, the mobile handset has to be connected to the test computer. This is done by using an electrical cable to replace the air interface such that the audio samples are played and recorded directly through the soundcard instead of hearing the sample from the ear piece and playing the sample from the microphone. It is also important to make sure that the sound card used in the process is of high quality and avoids general distortions caused when using general soundcards such as unwanted noise and gaps. Software used with the soundcard is also tested and found reliable. Loop test is also carried out on the cable that connects the mobile phone with the test computer to make sure that no distortions are introduced by the software or hardware when playing or recording the speech samples. The speech samples used in our experiments are British English reference samples and it satisfies the specifications mentioned in ITU-I P862.3

2.2 Experiment scenario to analyze the impact of codec:

2.2.1 GSM – GSM codec analysis

The calls are made from mobile phone to SIP phone. and the call is transferred from mobile phone to asterisk and asterisk to SIP phone. As it involves two different network, say IP network and the 3G network, two different codec negotiations takes place as shown in the diagram: one between the SIP phone and the asterisk server and the other between the asterisk server and the mobile phone.

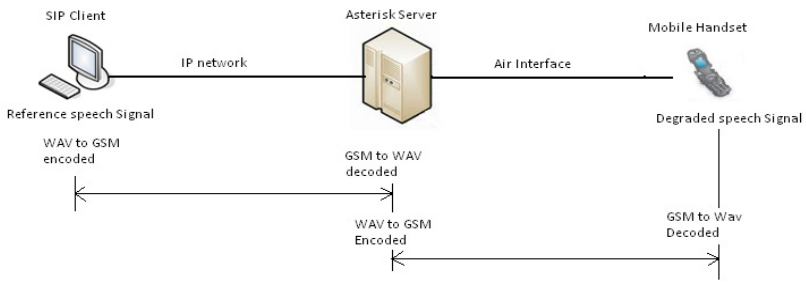


Figure 2: Experiment setup for GSM-GSM codec

In our first experiment, the testing is carried out with GSM codec as shown in the figure 2. However both the codec from SIP client to asterisk and asterisk to mobile handset are same, two different encoding and decoding happened in the process. Session initiation protocol assumes SIP client and asterisk as two user agents and negotiates the codec to compress on SIP client and decompressed on asterisk server. Asterisk server again encodes it using GSM and sends it in the 3G network and decoded in the mobile handset. The result showed that quality of speech signal degraded significantly after sending it through 3G networks. This quality degradation is mainly due to the facts; (i) the voice is encoded to GSM format and decoded to WAV format twice and (ii) the speech samples are carried through 3G network.

2.2.2 G711 – GSM codec analysis

This experiment also follows the same concept as the previous experiment and here we use G711a law codec to encode and decode from SIP client to asterisk instead of GSM codec. G711a also formally known as *Pulse code modulation (PCM) for voice frequencies* is a waveform codec using a sampling rate 8000 sample per second and operates in almost all telephony applications at 64kbps.

2.3 Experiment scenario to analyse the impact of packet loss

In order to investigate the effect of packet loss on the perceived speech quality, the 8 kHz sampled speech signal is processed by the encoder in test computer. Then the parameter based bit stream is sent to the decoder in the asterisk server. Here the asterisk server performs network emulation functionality providing a percentage of packet loss in the network downlink as well as the network uplink. After this loss simulation process, the bit streams are further processed by the 3G network and the degraded speech signal is recorded from the mobile phone. Netem, the network emulator is used to introduce the packet loss size of 5%, 10% and 20% in the IP network and different degraded MOS value measurements are taken.

Initially the speech quality MOS scores resulted in a normal quality of speech signal without having any impact on the emulated packet loss in the network. On further analysis, it is found that the packet loss created on the network using network emulator affected only the network downlink. In our experiment, the voice packets are transferred from SIP to the asterisk server, meaning the packet loss has to be introduced in the network uplink.

3 Experiment Results:

In this chapter, we present and explain the experimental results of the voice quality assessment over 3G networks.

3.1 Codec effects on live 3G network

To evaluate the quality degradation due to the codec combination, we used two different codec combination, GSM – GSM and G711 – GSM (codec from SIP phone to asterisk – Codec from asterisk to mobile phone)

From the experiments made on the GSM-GSM codec, we found that around 87.5% of the MOS scores measured on different speech samples resulted in between 2 and 3 and the remaining 12.5% went below 2 MOS score resulting in bad quality of the perceived voice sample. This is due the fact, that GSM codec has severe impact on the voice quality just by encoding and decoding and it is further reduced, when the encoded voice quality is transmitted through live 3G network.

3.1.1 Comparison of codec effects on live 3G network:

Previous research works on this field shown that, voice quality reduces to 3.55 average MOS score just by encoding and decoding and further reduces to 3.03 average MOS score when transferred through live network. The standard deviation is also found to be in the range of 0.23 and 0.26 (Goudarzi *et al.,* 2008).

	Only GSM encode and decode	**GSM on live network** (Asterisk - Mobile phone)	**GSM - GSM** (SIP - Asterisk - Mobile phone)	**G711 - GSM** (SIP - Asterisk - Mobile phone)
Avg MOS	3.555313	3.034167	2.748	2.959
STDDEV	0.235	0.262414	0.8851	0.8462

Table 1: Statistical summary on the comparison

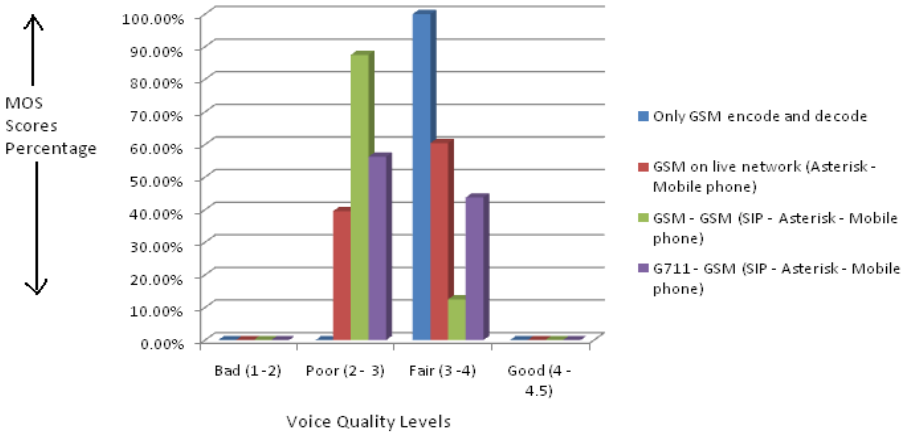


Figure 3: Comparison of PESQ – Only GSM, GSM, GSM-GSM, G711-GSM

The statistical summary in table 1 and the graph in figure 3 gives the comparison of current results with the previous work. In our first experiment case, we have encoded and decoded twice and hence the voice quality degraded more to 2.75. So, in live end-to-end call transfer, it is found that voice quality has severe effect when GSM-GSM codec is used. In the second case using G711-GSM codec, the voice quality is found to be far better than the voice quality of the previous case, having the MOS score of 3 after encoding and decoding twice. The usage of G711 codec instead of GSM codec from SIP client to asterisk increased the average MOS value to 3 from 2.75 (which is the average value of GSM – GSM codec). Another important factor to be noted here is that standard deviation of the MOS scores on codec combination is comparatively high (in the range of 0.85 – 0.89) than the standard deviation of MOS score on the single codec experiments (in the range of 0.23 – 0.26)

3.2 Packet loss effects on live 3G network

3.2.1 Impact of the packet loss on voice quality

Packet losses are introduced with different packet loss sizes, 5%, 10% and 20% and experimented. On each packet loss size, each sample is measure thrice and averaged to get reliable MOS scores. The below mentioned tabular column, table 3 gives the averaged MOS scores on voice quality on different packet loss sizes. It is clear that the MOS value decreases as the packet loss size increases from 5% to 20%

	PESQ MOS Score			
	Loss 0%	**Loss 5%**	**Loss 10%**	**Loss 20%**
Female	2.8	2.3	2	1.6
Male	3.1	2.6	2.3	1.9

Table 3: PESQ MOS scores on different packet loss size on the network

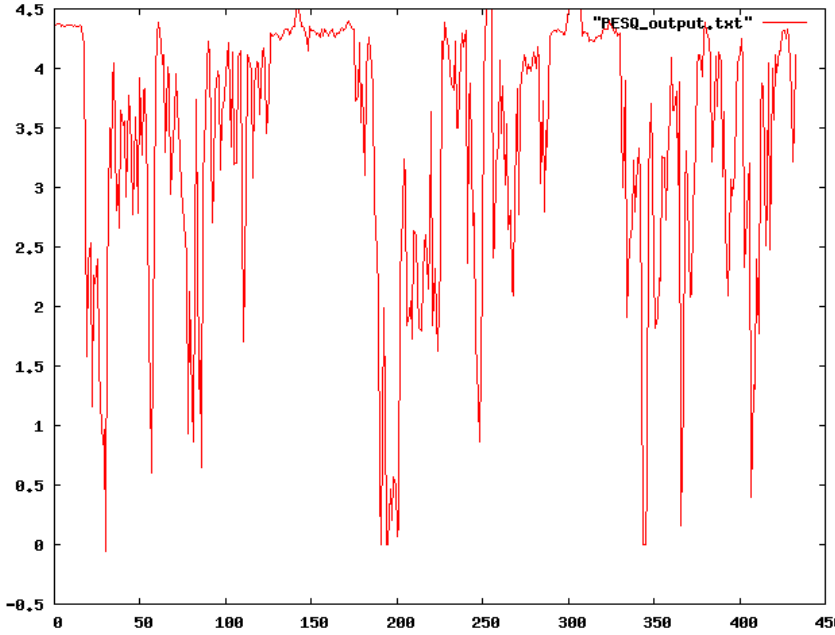


Figure 4: MOS score over number of frames for B_eng_m7.wav

Impact of talk spurt and silence on speech sample: As already mentioned in the previous sections, the speech sample used as a reference signal had three talk spurts separated by silence, is used for quality measurement. The loss at the silence segment had less impact on the perceived speech quality on all codec types and different network condition than the voiced speech segment. Moreover, it is found that the beginning of the voiced segment had more impact than the continuous speech on the perceived speech quality. Figure 5.7 shows the variation of objective MOS value over the number of frames for a speech sample B_eng_m7.wav under

packet loss size of 5%. As it can be seen, two silences in between 3 voice segment in the sample are taken place in the frames 125 -175 and 275-325 and here the PESQ scores are in the maximum of 4.5. Alternatively, the voice quality is decrease to Zero at around 25th frame, after 175th frame and 325th frame (approx) indicating the beginning of talk spurts. The impact is such that the PESQ scores are completely reduced to zero in these parts. Later parts in the talk spurts had more improved scores than the beginning indicating the quality recovery from the beginning. Due to this, the overall voice quality reduced and varied in between the MOS scores of 2.75 and 3. By this analysis, it can be concluded, that the speech samples with more talk spurts will have more impact than the speech sample having less talk spurts.

3.2.2 Impact of the packet loss on signalling part

In the previous section, the voice quality is analyzed and in this section the effect of signalling to establish the call in packet loss conditions are analyzed. To do this, numerous calls are made from mobile phone to SIP phone without any packet losses and then with packet losses. Wireshark, a packet analyzer tool is used to record the signalling of each call and to check the total time taken to establish the call. In our experiment, the call signalling happens between the asterisk server and the sip client. Once the call is initiated from mobile phone, the call is forwarded to the exchange, which in our case is the asterisk server. The asterisk server acts as a user agent and begins the message exchange by sending SIP INVITE message. The INVITE message contains the details of the type of codec supported by the called party. In our case asterisk supports G711a and GSM 06.10 codecs and this information is included in INVITE message. Then the 180 RINGING message sent in response to INVITE from SIP client to asterisk server alerting the ringing in the asterisk server. When the call is accepted in the SIP client, 200 OK response is sent to the asterisk server wherein the SIP client sends the codec information supported by it. In our case SIP is configured to support G711a codec. Asterisk server, in turn, acknowledges with the OK reply to use G711a codec there by establishing a call between SIP client and asterisk server.

In normal case without any packet loss condition, when the call is made between two clients, the calling client will take approximately 101ms to reach the calling client. In this research work, we tried to introduce packet loss of 20% and analysed. Since the packet loss introduced in the network is a random packet lost, some times the calls are established without any packet loss impact in the signalling part. But in many cases, the time taken is increased to 400ms and 1000ms. Signalling part however had the impact of increasing the signalling time to 4-10 times higher than the usual signalling time; the impact is less visible in the overall voice call connection since the time variations are in milliseconds. On all the experiments it is noted that it does not affect the call establishment between two clients. In other words, the call is established and stay connected in all the calls that has carried out for 180 seconds or lesser. From this analysis, it can be concluded that the random packet loss have less effect on signalling part of the call and the effects are visible only on the voice packets that are transferred through the network.

3.2.3 Voice Quality Prediction formula

Totally 16 speech samples are used and more than 200 sample recordings are taken under network condition with different packet loss size, 0%, 5%, 10% and 20%. Three sets of recordings each having sixteen speech samples is taken on all packet loss sizes and the average is calculated from three sets on each packet loss sizes. Figure 5.11 shows the graph plotted on the MOS scores for one sample file with packet loss size in the X-axis and MOS scores on Y axis. On the curve, a second order polynomial line is plotted fitting the original MOS score values and the polynomial equation is derived.

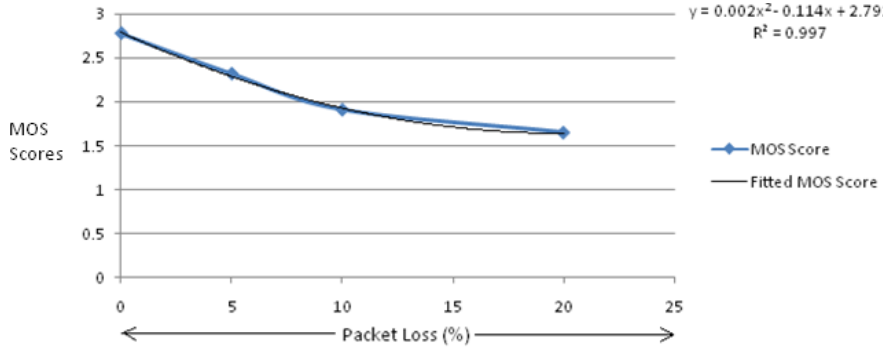


Figure 5 – MOS Score and Fitted MOS score value

The polynomial equation is found to be, $y = 0.002x^2 - 0.114x + 2.791$. Where coefficient a=0.002, b= -0.114 and c = 2.791 ≈ 2.78 which is the actual MOS value. This is the equation derived for one audio sample, *B_eng_f1.wav*.Similarly the co-efficient are calculated for other 15 sample files and the averaged co-efficient are made into an equation to give the prediction formula. The MOS score of any voice quality under x percentage of packet loss is given by the following equation,

$$y = 0.0018x^2 - 0.107x + C$$

Where C is the actual MOS score in the network without any packet loss. To determine the accuracy of the proposed formula in MOS prediction, a set of speech samples are measured for PESQ MOS score and compared with the calculated MOS score. It is found to have good accuracy on the proposed formula with the prediction errors range between ±0.3 MOS for most cases. It can be concluded that MOS can be directly predicted from the formula for the given network condition if the packet loss size and the MOS score without any packet loss is known.

4 Conclusion and Future Works:

This paper assessed the voice quality on live 3G network and effect of codec and the effect of packet losses are analyzed. GSM codec is found to have higher impact on the voice quality just by encoding and decoding the voice sample. When used on

combination, G711-GSM codec is found to have less impact than GSM-GSM codec. On different packet loss size experiments, it can be concluded that the signalling part of the call had less impact on the calls connected for 180 seconds (or lesser) and the call is established between the users all the time and the voice quality had more impacts due to packet loss. After doing more than 200 degraded sample recording, a formula is proposed to measure the MOS scores on different packet loss size, provided the percentage of packet loss on the network and original MOS score of the voice quality in the network.

In our project, both IP network and 3G network are involved and real SIP to 3G call scenario is more complicated. To name a few complexities, packet loss may be bursty instead of random packet losses, transcoding may happen in the call path instead of having two encoding and decoding process in the end-to-end call path, some techniques such as Voice Activity Detection (VAD) may be used. Future works may concentrate on these issues to evaluate more accurate MOS scores on the perceived speech quality.

5 References

Barrett, P.A. and Rix, A.W. (2002) *Applications of speech quality measurement for 3G*. Rix, A.W. (Ed). 3G Mobile Communication Technologies, 2002. Third International Conference on (Conf. Publ. No. 489). pp 250-255.

Goudarzi, Mohammad., Sun, L. and Ifeachor, E. (2008) PESQ and 3SQM measurement of voice quality over live 3G networks, 8th International MESAQIN (Measurement of Speech, Audio and Video Quality in Network) Conference, Prague, June 11, 2009

Nortel Networks. (2003) *Voice over packet An assessment of voice performance on packet networks*. Available online at: www.nortel.com/products/library/collateral/74007.25-09-01.pdf(Accessed: 10/07/09)

Section 2

Computer and Information Security

&

Web Technologies and Security

Information Leakage through Second Hand USB Flash Drives

W.H.Chaerani and N.L.Clarke

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

Abstract

USB flash drives are one of the common removable storages used nowadays. As the capacity increase and the price decrease, the content put on these devices become more valuable and vary than before. These USB keys are not only used to store personal files, but also sensitive information for example password list and CVs. Moreover, it is also not impossible for a person to keep information regarding other people. Additionally, since some company still allow their employees to use USB keys on internal network, it is also not impossible for corporate data to be transferred into these devices. This research try to see whether it is possible to obtain information, particularly sensitive ones from second hand USB keys sold on online auction sites. The keys used on this research were obtained randomly. Using digital forensic software, the keys were imaged and examined to obtain any remaining information that may exist.

Keywords

Information leakage, Second hand USB, Digital forensic, USB flash drive

1 Introduction

The United Kingdom has seen several big cases regarding information leakage due to the loss of storage media such as hard disk, laptop, or USB keys (Kennedy, 2008; Oates, 2008; BBC, 2008; BBC, 2009). The leakage itself was possible since most of those devices were not encrypted, making it possible for unauthorised person to easily access the information kept inside which could cause damage to the owner of the device.

Research regarding to information leakage due to storage media have been conducted annually by University of Glamorgan and University of Edith Cowen since 2005 (Jones, 2005; Jones, 2006; Univesity of Glamorgan, 2007; M2 Communications, Ltd, 2008; Jones, 2009). In all of their researches they could find that the majority of end users, particularly corporate ones, are still unaware of how to properly process their unused storage media so that the devices are clean upon leaving their control. Similar results were obtained from studies conducted by O&O Software (Kehrer, 2005; Kehrer, 2007). From their Data Data Everywhere studies, O&O Software could find that in addition to hard disks, which are the common disposed storage media from organizations, removable storage media such as memory cards and USB keys could also be the source of information leakage.

USB flash drives are one of removable storage media commonly used by people ranging from students to company directors. The device is very easy to use, practical and mobile. As the capacity increases and the price decreases, the value of information it kept become more and more sensitive. Obviously, the consequences might be severe if these keys are lost and fall to the wrong hand.

This research aims to see whether it is possible to obtain any sensitive information from second hand USB keys. Prior to selling their unused USB keys, it is only normal that people 'clean' them first. Some attempts people usually use to clean their USB keys include simply deleting the files, formatting the key, or using appropriate disk cleaning software. The problem is the first two attempts do not always clean the keys thoroughly. Deleting files only clear the path to reconstruct the files. The contents of the files itself still exist until it is overwritten by new files (Bunting, 2006). This remaining information may cause some sensitive information to be leaked without the owner's consent.

2 Methodology

In order to do the research, twenty second hand USB keys were bought randomly from online auction site and were examined forensically to extract any information left on them. The USB keys were picked randomly from different sellers with different range of capacity. In order to maintain the chain of custody, before any investigation can begin, all of the keys were imaged using digital forensic software. All of the investigations are then done on these images. The original keys are kept individually and then labelled along with the packages or envelopes that came with them. This is done so that the original keys will remain unchanged throughout the research. This also helps in maintaining the chain of custody, since the researcher does not know beforehand what kind of information will be found from the key. In case an evidence of a crime is found on the image, the investigation will be stopped and the key along with the packaging will be sent straight to the law enforcement agencies in its original condition.

This research utilised two digital forensic software and two additional file recovery software. The two digital forensic software are Encase 5 and Forensic Tool Kit 1.81.3. However, Encase was the mainly used because Forensic Tool Kit was a trial version and has limitation of number of files that can be investigated. The other two file recovery software was added to obtain more results. Recuva from Piriform was very useful in differentiating between recoverable and unrecoverable files and Zero Assumption Digital Image Recovery was very useful in recovering images. These software are easy to obtain and the use is quite straightforward, making it possible for novice users to utilize them in their own convenient time. Moreover, the last two software mentioned are available for free.

Once the keys were forensically imaged, the software was used to see whether any information was left on the key. Deleted folders were recovered and the unallocated clusters were checked to see remnants of the files. Each file were also analysed to see if it has any security measure applied such as password protection or encryption. Keyword search technique was also used to help in searching specific information. Encase provided templates for keyword search which include email addresses, IP

addresses, web addresses, phone numbers, dates with 4 digits year, and credit card numbers. Basic keywords added in the research were credential keyword such as user, username, uname, password, login, pass, and pwd. Additional keyword can be added in the search based on the findings on each key. For example, if the name of the owner can be found, then the name will be added in the keyword search to find any information related to the owner.

3 Result

A total of 36,136 files could be retrieved from the keys, dominated with documents such as Microsoft Words, spreadsheets, and PDFs. Overall, the information found on the key were ranging from individual to confidential corporate files. Individual information is the kind that relate to a person, either the owner of the key or other person whose data for some reason may reside in the key. This type of information is then divided into personal and private information. Personal information is the type of information that describes the person and the person does not bother to share them, such as names, addresses, and emails. Private information are the type of information that should be kept private and should not be used without the owner's consent, such as bank details, national insurance numbers, date of birth, mother's name, online credentials, etc. The corporate information found during the research includes confidential company reports, client's financial information, meeting notes, internal and external correspondences, etc. Apparently both individual and corporate information could be found on most of the keys.

<table>
<tr><th colspan="2">Category</th><th colspan="2">Number of Keys (out of 20)</th><th colspan="2">Percentage</th></tr>
<tr><td colspan="2">Empty</td><td colspan="2">4</td><td colspan="2">20%</td></tr>
<tr><td colspan="2">Corporate</td><td colspan="2">6</td><td colspan="2">30%</td></tr>
<tr><td rowspan="2">Individual</td><td>Personal</td><td rowspan="2">14</td><td>11</td><td rowspan="2">70%</td><td>55%</td></tr>
<tr><td>Private</td><td>14</td><td>70%</td></tr>
</table>

Table 1: Nature of information found on the keys

After examining the total of twenty keys, the following are found:

3.1 Blank keys

Out of twenty USB keys examined in the research, only four or 20% of the keys were totally blank. The unallocated clusters of these keys were mostly blank with no meaningful information can be obtained.

3.2 Identifiable to previous owners

65% of the keys examined, were identifiable to the previous owner. This means that at least the name of the owner is known. This information obtained from document signatures, CVs, invoices, and correspondences. Additional information found about the owner were ranging from email addresses, contact numbers, addresses, online credentials, personal pictures, bank details and even national insurance numbers. One

of the key even contained medical record and history of the owner. Another key identified to once belong to an insurance company in London and it contains enormous amount of corporate information. The other three keys were not blank and contain information but they were not identifiable to the previous owner.

3.3 Financial Information

15% of the keys examined contain bank details such as account number, sort code, bank name, and bank address. One of the key contains more than 30 bank details belong to companies. The financial information found did not only belong to individuals but also company. In one of the key, reports regarding profit and loss, balance sheet, customer list, invoices, and sales forecast could be recovered. Some of these documents were clearly labelled as 'confidential' or 'for internal use only'.

3.4 Identification Number

40% of the keys examined, contained identification numbers. These IDs can be in the form of passport numbers, national identification numbers, national insurance numbers, driver license number, or license plate number. This information was obtained from documents or scanned pictures. In one case, a document was found and it listed names, addresses, and passport numbers of students in one college.

3.5 Curriculum Vitae

15% of the keys examined contain curriculum vitae of the owner or of the owner's acquaintances. These CVs provide detail of a person starting from names, addresses, contact numbers, and date of births, to passport numbers and national identification numbers. Other information provided includes education and work experience detail. By gathering information from these CVs, impersonator could have enough information about the victim's profile.

3.6 Network Information

One key examined contain full details of the owner's network configuration. This information found from keyword search 'user' and it reveals the network user credentials, the wireless LAN key and phrase, the manual configuration of the network and also the router configuration. By gathering information from the user manual and executables found, the hardware details can also be deduced. Another key examined contain a text file containing a company's VLAN password.

3.7 Medical Information

One key examined contain full medical information of the owner. This information is in the form of medical strip which reveals basically everything one needs to know about the owner's health including what kind of allergy he had, blood transfusion type, main medication, daily medication he had to take, patient number, the doctor's name and contact number, and sickness history. The owner's full health history could also be deduced from the correspondences found on the key.

3.8 Information about other people

Over half of the keys examined contain information about other people. This information include name (or full name), picture, national insurance number, policy insurance number, online account credential, bank detail, and full curriculum vitae where you can get more detailed information such as date of birth, address, contact numbers, address, education history and work experience.

3.9 Corporate Information

20% of the keys examined contain corporate information. This information include company logo, letter or form templates, meeting notes, financial report, list of board of directors along with their contact addresses, contact numbers and date of births. There were also turnover analysis, sales forecasts, signature scans, and companies' bank details. One of the highlight of the research is the last key investigated, which consists of corporate data of an insurance company in London. Around 3000 still intact documents could be recovered from the key and 91% of those files contain sensitive corporate information, not only to the insurance company but also to its partners and clients. It is such a pity that out of these files, only one was password protected, leaving the rest easy to be accessed and analysed. Almost half of the sensitive documents found were explicitly labelled as 'private and confidential' or 'for internal use only'. The rest which were not labelled as 'confidential' also contained sensitive information to the company such as clients' financial reports, bank details, invoices, sales forecast, financial analysis, and board of directors' details. Other than corporate information, the key also contained a collection of personal folders of the staffs. From these folders, a bank detail and signature scan of one of the staff can be obtained. The staff also kept a confidential letter made by his spouse that contained the spouse's sensitive details such as national insurance number, bank details, and holiday dates.

4 Consequences

The richness of information obtained from just recovering files from second hand USB keys was alarming. Moreover, some of the information was simply obtained by recovering files using free file recovery software available online. These software are relatively easy to use and quite straightforward, making it possible for novice users to use and conduct file recovery on these keys. Obviously, the consequences will be severe for the owner (or other people that has their information stored on the keys) if the key ever fall to the wrong hand. Based on the information gathered during the research, it can be deduced that more than half of the keys could cause identity theft if it is loss or stolen. Obviously, this is not the only threat.

Threats	Identity Theft	Fraud	Industrial Espionage	Blackmail	Hacking / Network Intrusion	Robbery
Number of Keys	11	9	2	5	4	1

Table 2: Summary of possible threats to the keys

4.1 Identity theft

The information found on this research were enough to conduct an identity theft which can cost the victim not only money, but life. In extreme case, the owner who kept his medical records on the key may be the victim of medical identity theft, which means it is possible in the future when he need to get blood transfusion, he get injected by the wrong blood type.

4.2 Industrial Espionage

The corporate financial information found on this research was quite recent. Information such as turnover analysis, sales forecasts, and financial reports can be used by competitors in industrial espionage. Not only financial information, documents revealing a company investment strategy could be found and also could be used in industrial espionage which can cause loss in terms of money and reputation.

4.3 Fraud

From a key that contain the owner's request for a web domain, his signature scan could be recovered. This piece of information can be used to falsify document which can lead to fraud. Moreover, company logos, form and letter templates, insurance policy wordings gathered from the key that belong to a company would make a convincing fake document. Even information as simple as scan of license plate number can be used to falsify a stolen car's license plate which could lead to other fraudulent activities.

4.4 Hacking or Network Intrusion

Full network configuration which detailing the W-LAN key and phrase could cause the owner to suffer from network intrusion. Moreover, online credentials such as eBay and PayPal that could be found by recovering encrypted file can be used to access the service without the consent of the owner. Another case is the online credentials found for a company online service. The credential that belongs to one of the staff would make it possible for intruders to login and access the internal resources of the company.

4.5 Blackmail

Illicit material could be found from one of the key, mainly in the form of videos. This might be incriminating to the owner if such information is exposed. Blackmail can also be done to the company whose financial information was kept in one of the key examined.

4.6 Robbery

The financial information found throughout this research was sufficient enough for a criminal to commit theft from the bank account found. In addition, the information

about holiday dates also enables criminals to indicate when the victim will not be home.

5 Reason of Incidents and Preventions

Unfortunately, it seems that most people do not know that simply formatting or deleting files will not clean the devices completely, as the remnants of those files can still be detected and recovered using appropriate software. This lack of knowledge make it possible for someone to buy a second hand USB flash drive for less than £5 and obtain someone else's bank detail instead.

The finding of corporate USB in this research also indicates that there are still companies that do not aware the dangerous risk these tiny devices have. Based on BERR research, 67% of companies do nothing to prevent data from leaving their company premises through removable media such as USB flash drives (BERR, 2008). Another reason is simply ignorance. In accordance to lack of knowledge, people seem to think that it is impossible someone could recover files which are deleted long ago.

In order to prevent this kind of leakage from happening, several preventions can be done:

1. Encrypt all removable storage media
2. Protect devices from unauthorised access by utilising password protection or biometric authentication
3. Use specialised erasure software to clean all storage media that are no longer used.
4. Destroy physically all devices at the end of their lifetime.
5. Companies should have strict rules and guidelines regarding the usage of removable storage media. This rules need to be audited periodically to assess its effectiveness.
6. Government and/or academic communities should give education or public awareness regarding this issue.

6 Conclusion and Future Work

Based on the results found in this research, it can be concluded that it is possible to obtain sensitive information from second hand USB flash drives. It is inevitable that people keep sensitive information on their USB keys. However the problem is when the USB keys are no longer used. Proper erasing method needs to be done in order to erase the content completely and remove any remaining information.

To enlarge the scope of the research, the number of keys should be increased. Thus, more conclusions can be extracted and more variables can be measured. Such as, does the capacity of the key relate to the value of information it keeps, or is there any relation between the origin countries of the keys with the richness of information found.

7 References

BBC, 2008. *More secret files found on train*. [Online] Available at: http://news.bbc.co.uk/1/hi/uk/7455084.stm [Accessed 13 August 2009].

BBC, 2009. *Previous cases of missing data*. [Online] Available at: http://news.bbc.co.uk/1/hi/uk/7449927.stm [Accessed 13 August 2009].

BERR, 2008. *BERR Information Security Breaches Survey*. [Online] Available at: http://www.security-survey.gov.uk [Accessed 15 November 2008].

Bunting, S., 2006. *The Official EnCe: Encase Certified Examiner*. [Online] Available at: http://i.techrepublic.com.com/downloads/home/0782144352_chapter_1.pdf [Accessed 9 April 2009].

Jones, A., 2005. How much information do organizations throw away? *Computer Fraud & Security*, 2005(3), pp.4-9. DOI: 10.1016/S1361-3723(05)70170-6 [Accessed 31 July 2009].

Jones, A., 2006. Cradle to grave - security failure to the very end. *Computer Fraud & Security*, 2006(9), pp.4-8. DOI: 10.1016/S1361-3723(06)70418-3 [Accessed 13 August 2009].

Jones, A., 2009. Lessons not learned on data disposal. *Digital Investigation*, pp.1-5. DOI: 10.1016/j.diin.2009.06.017 [Accessed 15 July 2009].

Kehrer, O., 2005. *Data Data Everywhere 2005*. [Online] O&O Software Available at: http://www.oo-software.com/en/study/study_ddd2005_en.pdf [Accessed 29 May 2009].

Kehrer, O., 2007. *Data Data Everywhere*. [Online] Available at: http://www.oo-software.com/en/docs/ddd2007_en.pdf [Accessed 3 December 2008].

Kennedy, J., 2008. *Another data security breach reported at Bank of Ireland*. [Online] Available at: http://www.siliconrepublic.com/news/article/11718/cio/another-data-security-breach-reported-at-bank-of-ireland [Accessed 13 December 2008].

M2 Communications, Ltd, 2008. *BT: Research Reveals At Least One In Five Second-Hand Mobile Devices Still Contain Sensitive Information; Today's Sophisticated Devices Exacerbating The Problem Of Keeping Sensitive Information Safe*. [Online] Available at: http://www.tmcnet.com/usubmit/2008/09/25/3670481.htm [Accessed 6 February 2009].

Oates, J., 2008. *Million bank details sold on eBay and a few more gone AWOL*. [Online] Available at: http://www.theregister.co.uk/2008/08/26/more_details_lost/ [Accessed 14 July 2009].

Univesity of Glamorgan, 2007. *Discarded Hard Disk Hold Sensitive Data*. [Online] Available at: http://news.glam.ac.uk/news/en/2007/sep/19/discarded-hard-disk-hold-sensitive-data/ [Accessed 6 February 2009].

Web-based Risk Analysis Tool for Home users

M.Jain and N.L.Clarke

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

Abstract

Broadband internet services are widely available in the market with high data transfer rate and attractive low prices. This feature is not only attracting organizations but a large proprtion of residential users have moved towards it. The 'always on' broadband technology comes with potential security threats and unauthorised access to information, resources and systems. The organizations hire security experts or administrators to deal with potential risks but home users have little knowledge to handle such risky situations. Various risk analysis tools, standards and techniques are available to overcome the risk problems but it has been found that these are oriented towards organizations and require expertise. Many websites are available with security risk handling guidelines for home users but they also require certain knowledge and understanding of technical terms. This research has been conducted to develop a web-based risk analysis tool specially for home users. The tool has followed controls and guidleines from ISO17799 information security standard to produce risk scores from individual user responses. The tool has covered features like using simple and accurate risk assessment method along with mitigation guidelines, userfrienliness and easy accessibility. The tool also educates users about security and threat related terminology and offers necessary protection to their systems.

Keywords

Broadband, security threats, risk assessment, home users.

1 Introduction

Majority of the people are changing from narrowband internet connection to high speed broadband connection. This broadband revolution is not only recorded in organizations but there is a large move from dialup to broadband among residential users (Ofcom, 2009). Due to immergence of internet as a part of day to day life, people and businesses cannot imagine life without it (getsafeonline, 2008). Generally people spent their time on the internet shopping, banking, social networking, dating and many otheractivities. The increasing use of broadband internet comes with a down side. As a result a large production and distribution of malicious threats have been detected in 2008 (Symantec, 2008). Online crimes such as malware, spyware, phishing, ID thefts, hacking of data and systems are extremely profitable.

This increase in internet connectivity and online applications are making home users more vulnerable (Furnell et al. 2007) and this has been observerd from the succcess of many online scams and resulting level of threat attacks on home users (Symantec, 2006). The basic requirement in order to protect home based computing is the development of web-based risk analysis tool specially for home computer users. The

tool should provide a simple and accurate risk assessment method with suitable risk mitigation guidelines applicable for individual users.

2 Current attitude towards IT security

More and more of the UK's small and large level organizations are focussing on IT systems and information secuirty. Businesses are changing their secuirty behaviour and taking regular security controls such as data backup, malware protection and encrypt network traffic to avoid any security breaches (BERR, 2008). The CSI computer crime and security survey, 2008 also recorded the average annual loss under $300,000 which shows a break down from the previous year record. The organizations are following security policies, tools and standards to promote security against illegal network access.

Survey results show that many governments and businesses are improving cybersecurity but individual computer users still lack in basic precautions against daily life cyberattacks (Gross, 2008). The home users lack the awareness, time, appropriate resources, security and risk handling skills and lack of standard risk analysis methodology (Furnell et al. 2007). Either they do not know what steps to perfom against malicious codes or they have insufficient information, tools and guidelines to follow. So this research aims to fulfil all security requirements of the home users by developing a web-based risk analysis tool.

3 Risk analysis tools and websites Evaluation

One of the important parts of the research is to analyse different risk assessment methods and their methodology whose output may guide risk analysis tool to follow suitable risk assessment methods applicable to home user environment. The famous risk assessment methods have been included in this analysis. When these methods were reviewed it was found that these are exclusively focused on the information security needs of the organizations and are used for some specific purposes. Some of them are either available at a cost or some are complex to use.

A new project CORAS, provides model-based risk asessement process which do not describe and evaluate risk assessment targets and results (Aagedal et al. 2002). The technical aspects of CORAS are human interaction and is related to organizations and society. From a case study it has been found that some components used during the process were useful and worked well but was time-consuming and required technical backing to perform the application.

The COBIT project addresses good IT security management practices for organizations. This is a very popular framework which provides necessary secuirty policy and good practice of IT controls. The implementation of the tool set consists of all important information such as IT control diagonistic, implementation guide, case studies and FAQs. The down side of this method is that it only suggests 'what' things must be done but does not explain 'how' which is necessary to know in certain things.

The CRAMM risk analysis methodology has been developed to provide a structured computer security management approach for large, small and home offices (Spinaellis et al. 1999). The method was successful and declared as mandatory for the UK governrnent organizations. The problems associated with CRAMM are that it is specifically designed for organizations, it is time-consuming and requires specific knowledge to implement and maintain. A product of ISO17799, COBRA specifically launched for business level security and uses very lengthy questionnaire with high level technical terms (COBRA, 2008). Same as the risk assessment and planning technique, OCTAVE fulfils the organizations' security needs and requires an analysis team to handle its 'plan-implment-monitor-control' methodology (Alberts et al. 2003).

Number of websites are available on the web to help home user computing problems and guide them appropriately. CERT-Home computer security developes and promotes appropriate techniques for different level of computer users to limit cyber attacks, damages and system failures. The home computer security part of the webiste provides certain security controls for the user to follow. Microsoft-Secuirty at home focuses on 3 main points which are protect your computer, protect yourself and protect your family by giving knowledge on security and fraud related terms.

Getsafeonline.org conducts a quiz to test the internet safety bahaviour of the user. It has multiple choice questions and results are displayed using a correct/incorrect option as and when the user answers. It does not concentrate on the individual user's computer security. Whereas Tom-cat provides basic and additional protection guidelines for family and friends computers, information on internet privacy and security programs. Staysafeonline.org asks a questionnaire to the users about the security controls they have on their system but as a result it simply counts the number of users answered particular option. It gives a comparison of different users behaviour towards computer security.

All the above discussed websites are associated with problems. Few of them are complicated, non-userfriendly and require technical knowledge to understand and access their vast data. And most importantly none of them discusses about individual user system's risk level. A risk analysis approach with nature of guaranteed accurate results is required to secure home computing.

4 Risk assessment methodology

The core part of risk analysis tool is risk assessment quiz which follows guidelines and controls associated with ISO17799 international standard. All controls do not map directly to the identification of questions, and considers only the ones which are suitable to home computing environment. The quantitative approach to analyse the risk has been used in the research, in which values are assigned to individual risk types and risk determination formula is used calculate risk as:

Risk level = Impact * Likelihood (Mazareanu, 2007)

Likelihood means probability of risk occurrance in the system and 3 cases of likelihood have been considered for risk analysis tool, as 1.0 for High, 0.5 for

Medium and 0.1 for Low level. The impact is harm or loss which occurs after any successful vulnerability incident, here quantitative impact has been used with 3 values as 100 for High, 50 for Medium and 10 for Low impact. For measurement of risk score, a simple risk model 'Jacobson's Window' has assigned quantitative values of impact and likelihood and it has used to get the accurate risk calculation (Stoneburner et al. 2002).The definition of risk score is also divided into 3 levels, 100 for High, 50 for medium and 10 for Low level risk. The risk assessment quiz has 10 categories, 2 questions in each category and each question with YES/No options. Each question has to be answered and as the user completes the quiz, the result will be shown with according to the category.

Category 1

Question 1 Do you have any anti-virus software insatlled on your computer?

Question 2 Do you regularly update the anti-virus software?

In this category, if a virus, worm or Trojan attack occurs then potential impact can be high (100) and probability of an attack can be high (1.0), medium (0.5) or low (0.1) depends on the user's answer. Here risk calculation will be applied as:

Case1: If answers to both Question1 and 2 are NO, then probability is high (1.0).

Risk level = impact (100) * likelihood (1.0) = 100 (high level)

Case2: If answers to Question1 is YES and Question2 is NO, then probability is medium (0.5).

Risk level = impact (100) * likelihood (0.5) = 50 (medium level)

Case3: If answers to both questions are YES, then probability is low (0.1)

Risk level = impact (100) * likelihood (0.1) = 100 (low level)

Depending on the level of risks, 'Best Practice' part will provide category wise suitable guidelines to follow in order to minimise the level of risk score.

5 Web-based Risk Analysis Tool

The risk analysis tool has used the platform ASP.Net with Visual basic and MS Access as database to include data tables. The application design has focused on user friendliness, consistency and user accessibility. The 'Secure Online Surfing' risk analysis tool consists of five parts which are discussed belo.

Home page: This main page consists of a brief introduction to the tool, so that the user will et an idea about the tool upfront. All five parts are accessible from the top of the home page and is as shown in Figure 1.

Figure 1: Home Page - Web-based Risk Analysis Tool

As discussed earlier, very few home users are familiar with computer security related terminology. To achieve the objective of educating the user on the various terminologies associated with internet security the tool has introduced two sections: 'Beginner's guide' and 'Resources'.

Beginner's guide: This section provides knowledge on malicious threats, freeware and shareware programs, firewall and its different types. This also includes password selection and protection guidelines, information on digital signatures and Microsoft's automatic updates.

Resources: This section of the tool enhances the knowledge of the user by providing additional information on computer security, information security, risk assessment websites and latest news and updates in related field.

Risk Assessment Quiz: This part is a questionnaire of 10 different categories with 2 questions in each category. First of all the quiz section will ask for user identification at login page to be stored in database to show the reference on the result page. This page consists of a brief introduction about number of categories, questions and final result page format.

If the user logins successfully, then only he is allowed to see the question web pages. The question page will look like Figure 2, each question with YES/NO options and user's answers will be stored in database table to calculte risk scores using risk determination function. The web pages consist of validation checks on answering each question and on navigating from one section to another.

Figure 2: Question page - Risk Assessment Quiz

Many users may be sure of the answer to the questions and if they are not, they are provided with a help link such as 'Anti-virus Information-Click here' shown in Figure 3, to help them answer correctly. The tool is suitable for the Windows operating system; similarly help links are provided for windows system. When the user clicks on the link, it will open a web page as shown in Figure 3. The page has some steps with the system's window pictures which the user has to simply follow on his computer system and then he will be able to answer appropriately. The help links are given on selected categories which are most likely to confuse the user. In this way the tool is best suitable from novice users to advanced computer users.

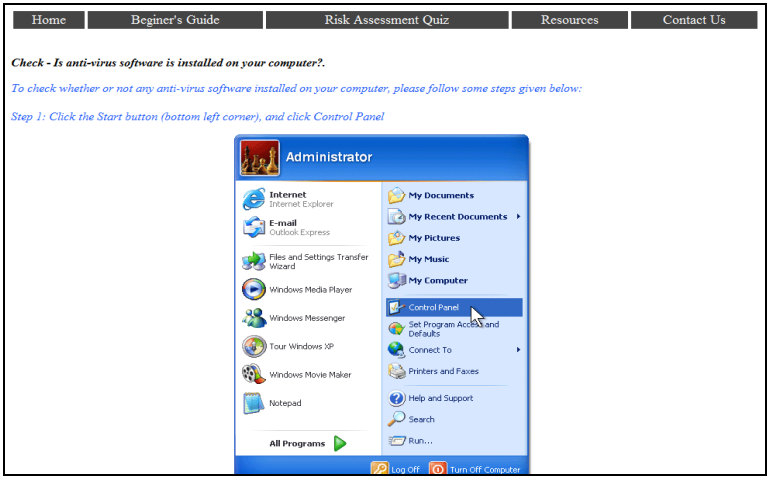


Figure 3: Helping Link Webpage – Category1

The user will be directed to the 'Result page' once he has answered all the questions. This page is divided into two types of views, one a table with user identification and category wise risk scores. The second with the five most important categories are shown in traffic signal system. The result page will look like Figure 4, with risk scores as high level risk (100) – 'Red colour box', medium level risk (50) – 'Orange colour box' and low level risk (10) – 'Green colour box'.

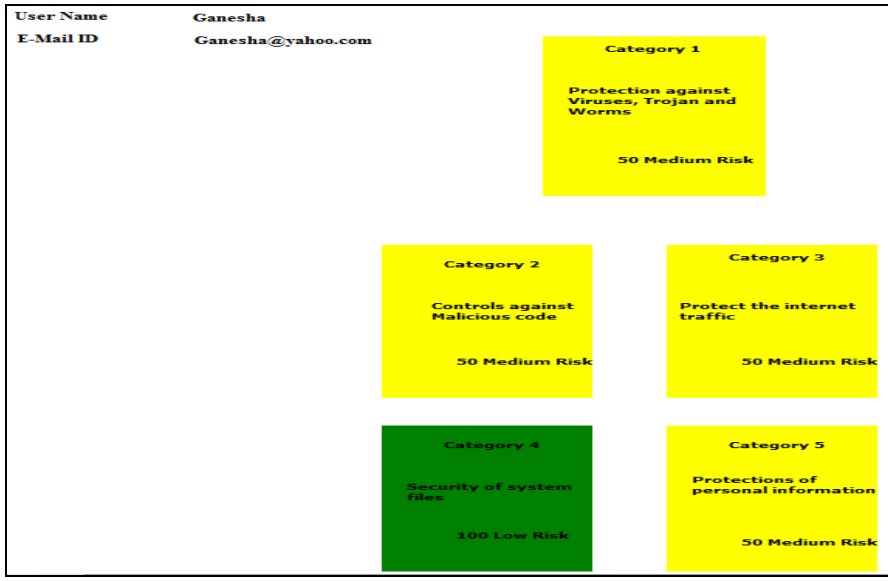


Figure 4: Result page - Traffic Signal System

6 Conclusion

The research revealed that majority of individual users and organizations are adopting broadband services due to its falling prices and unlimited connectivity. The high speed and 'always on' broadband connection comes with various security threats. The discussed survey has resulted that organizations taking care of their information security but the lack of awareness and technical skills of the home users to deal with security threats make them easy targets for hackers. The evaluation of risk analysis tools, methods and websites showed that they are suitable for businesses and organizations, require expertise and available at a cost. The guidelines are sometimes overwhelming and not structured well.

The development of web-based risk analysis tool was proposed to overcome computer security problems of the home users. A risk assessment questionnaire has been constructed by considering ISO17799 controls and guidelines best suited for home computing environment. The questionnaire used a simple and accurate risk assessment method to highlight critical risk areas in the user's system and provides suitable risk mitigation steps based on individual user's responses. The tool is considered to be user-friendly, easy to use and accessible by 20 user's reviews and on comparison with 'getsafeonline.org'. The 'Secure Online Surfing' risk analysis

tool can be launched globally to provide an accurate and trustworthy solution against internet security risks aimed at home users.

7 References

Aagedal, J., Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D. and Stolen, K. (2002), "Model-based Risk Assessment to Improve Enterprise Security", 6th International Enterprise Distributed Object Computing conference. IEEE proceeding.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), "Introduction to OCTAVE Approach", www.cert.org/octave/approach_intro.pdf, (Accessed 24 July 2008)

BERR (2008), "BERR 2008 Information Security Breaches Survey", www.berr.gov.uk/files/file45714.pdf, (Accessed 2 February 2009)

COBRA (2008), "COBRA Knowledge", http://www.riskworld.net/kbases.htm, (Accessed 10 February 2009)

Furnell, S.M., Bryant, P. and Phippen, A.D. (2007), "Assessing the Security perceptions of personal Internet users", Computer & Security, Vol. 26, No. 2006, pp 410-417.

Get safe online (2008), "Get Safe Online Report", http://www.getsafeonline.org/media/GSO_Report_2008.pdf, (Accessed 15 July 2009)

Gross, G. (2008), "Survey: many computer users lack basic security precautions", IDG new services, http://www.pcworld.com/businesscenter/article/151793/survey_many_computer_users_lack_basic_security_precautions.html (Accessed 25 August 2009)

Mazareanu, V.P. (2007), "Risk Management And Analysis: Risk Assessment (Qualitative and Quantitative)", http://www.anale.feaa.uaic.ro/.../06_Mazareanu_V__Risk_management_and_analysis-risk_assessment.pdf, (Accessed 22 August 2009)

Ofcom (2009), "The Communication Market 2009 – 4 Telecoms", http://www.ofcom.org.uk/research/cm/cmr09/cmr09.pdf, (Accessed 12 July 2009)

Spinellis, D., Kokolakis, S. and Gritzalis, S. (1999), "Security requirements, risks and recommendations for small enterprise and home-office environments", Information Management and Computer Security, MCB university press, pp 121-128.

Symantec (2008), "Symantec Global Internet Security Threat Report", http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, (Accessed 12 June 2009)

Improving User Awareness of Social Engineering

M.Newbould and S.M.Furnell

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

Abstract

With online social engineering currently a major problem, it is vital to educate the potential victims of these attacks – everyday Internet users. This paper looks specifically at how a board game was developed and tested to try and educate the user in a more interactive way, with results suggesting that this solution does increase awareness of social engineering with nobody scoring under 55% whilst playing the game, and 86% of users feeling they had improved their knowledge on the subject.

Keywords

Social Engineering, Phishing, Advance Fee Fraud, Spam, Game Development

1 Introduction

This paper summarises a project that was undertaken to improve user awareness of online based social engineering attacks. With this main aim, a range of potential solutions were examined, with research taking place to see what educational solutions already existed. It was found that whilst a lot of literature was available on the Internet, there were fewer solutions that were aimed at users with less technical ability and that involved a higher level of interaction as well as being educational.

It was decided to pursue this path further and ultimately produce a website containing literature and a board game where the user could refer to the website literature when required, thus providing a more interesting way to learn. Rather than aim to produce a finished article which would most likely be rushed in the small development window it was decided that a testable prototype would be produced and with the aid of user feedback, could be developed further at a later date

The focus of the coming sections consists of background information on the topic area and discussion on the game prototype itself, including the reasoning behind the decisions that were made, as well as explaining the defined requirements. The implementation of the solution will follow, as well as how the game was tested on the potential audience and the results that were obtained from this.

2 Background

A social engineering attack in relation to IT is based upon attacking the person rather than hacking them. The attacker uses psychology to typically trick the user into

believing something which will usually result in them handing over money or information that can be used against them. Whilst social engineering attacks did not originate from IT, the frequency of social engineering attacks has increased significantly. With the majority of people now able to access the Internet, a goldmine has developed for attackers with millions of potential victims a single mouse click away.

There are a number of different types of social engineering attacks, and the remainder of this section will give an overview of these attacks, including looking at how they have evolved with new technology.

The most frequent type of social engineering attack is phishing (Microsoft, 2007). This typically involves an email from the attacker imitating an organisation such as banks in an attempt to trick the user into following a link and entering their details. According to research carried out by Gartner (2007), between August 2006 and August 2007 3.6 million users lost money to phishing scams in the US, resulting in a combine loss of $3.2million which shows the scale of the ever increasing problem.

Certain spam can be classed as a social engineering attacks as many offer enticements such as free images, a movie or friendship – provoking intrigue and interest from the user however the attachment is typically a Trojan, Worm or a Virus. The result of this is that a range of things could happen to the users computer such as damage to critical files, a program that steals information such as passwords or a key logger so that a hacker could keep track of everything the victim types on their keyboard.

Another form of social engineering attack is advance fee fraud, also known as the 419 scam which is where the attacker usually exploits human greed or sympathy. When exploiting greed, the attacker suggests to the victim that they will get a large amount of money for sending a small amount of money first, usually explained as a release fee, bribe or legal fee. Other forms of this attack can consist of the attacker imitating a victim of a recent natural disaster – trying to exploit the reader's sympathy. Although most recipients of the emails do not respond there is also a long list of those that do.

The perpetrators of these attacks are highly versatile when it comes to making use of new opportunities. The increase in the popularity of social networking sites has meant that targeted 'spear phishing' attacks are easier to carry out, with attackers making use of information that is freely available on these sites and targeting potential victims specifically via email, including some of the user's personal information to make the attempt look more convincing and authentic.

In August 2009 Sky News reported of attackers hacking users Facebook accounts, imitating the victim and emailing their friends, claiming that they have been the victim of a mugging and requesting some financial aid from their friends. This shows how Web 2.0 websites have opened the gates for perpetrators to move away from the traditional form of social engineering attacks into newer areas that make the attacks more difficult to identify. With attacks such as this rendering email spam filters

useless in protecting the end user, it is not viable for 100% reliance on technical protection measures – therefore education is essential.

3 Board Game Prototype

Once it was decided that an educational game was going to be the main deliverable, a decision had to be made as to what type of game this would be. There were a number of initial considerations regarding this, with early ideas consisting of a role playing game (RPG) where the user takes control of a character and navigates through an area in order to achieve the main goal which would have been centred on answering questions and gaining knowledge. Ultimately, it was decided that with a fairly small development window a more intricate game such as this would pose a greater risk to the project in terms of completing it on time.

Instead, it was decided that a board game would be developed. This was to have accompanying website literature that could be referred to should the user be unable to answer a question. This allowed for an interactive way to learn that was also a much more realistic option given the allotted time frame.

3.1. Required Technologies

The decision was made to develop the solution using an object oriented language, making use of the advantages of developing such a system in an OO language which among other things, allowed for a modular structure to the program, with a reduction in the amount of code needed to update and improve the system. This was seen as essential with the system being a prototype it was plausible for it to be further developed at a later stage. So having a program with clearly defined classes that represent real world objects, each with their own responsibilities, made the system as a whole easier for present and potentially future developers to understand and modify.

When looking at potential ways to develop the solution, it was ultimately decided to use Flash CS3 and therefore Actionscript as the development language of choice. Whilst it was accepted that other IDE's such as Adobe Flex and other languages such as Java would have allowed for a similar implementation, it was felt the advantage of being able to develop and test within the Flash IDE would be beneficial. In addition, there was a lot of learning material in books and online in terms of developing games, whereas literature for other options was less common. This was important as the author was new to web based game development.

A UML approach was chosen for the process of getting the game from the requirements phase, through analysis and design, to a point where it could be confidently implemented. UML helps the software engineer specify, visualize, and document models of software systems, including their structure and design. It consists mainly of a graphical language to represent concepts that are required in the development of an object oriented system (Bennett, 2002).

3.2. Defining the Solution

Having decided on the technologies to be used, it was necessary to define what would be required in the game. It was important that the game was fairly simplistic in terms of how it would be played as the aim of this was to educate users, not to require them to read pages of instructions informing them of how to play the game. A board game ensured that the solution would be easy to understand and therefore maximise time to educate the user whilst still having an interactive interface.

In terms of how the board would be laid out, it was opted for a generic square board, being a prototype it was important to implement a working solution, with aesthetically pleasing additions added at a later stage if time allowed.

The board was to consist of 32 squares with each one to be assigned one of the four categories upon the game starting. The knowledge gained from carrying out background research was used in deciding how to categorize the questions. Time was taken to look at each type of social engineering attack and the most common attacks were used as categories for the game. This encompassed phishing, advance fee fraud and spam, with the fourth and final category labelled ‘other’ which consisted of the less common attacks. Each one of these categories represented a colour on the game board, for example phishing was red and advance fee fraud was yellow. The number of times each colour appears on the board is pre-determined. For example, as phishing was identified as one of the most damaging form of social engineering the red square appears more frequently than the advance fee fraud questions.

In terms of the format of the questions it was decided to use a multiple choice format. This format would provide an effective way to ask the questions and allow easy answer selection compared to asking the user to manually enter the answer which would yield many problems in terms of verifying their answer. A range of other formats were considered but it was felt that there was insufficient time to implement a range of formats and it would instead be included in the testing phase as an option for improvement and therefore ascertain its popularity with the test audience.

A player's score would be tracked throughout the game. This was added to provide an extra level of motivation to the user and thus increase their knowledge and education. This was also used at the testing phase to determine the solutions success and was the first step towards a high score board for the game.

Rather than being a straight forward ‘roll and move forward’ type of game, the option to move back was added. Upon rolling, all squares were to dim, with the available squares staying lit. Whilst this offered nothing other than a minor addition to gameplay, it was felt it was adding something that could be more useful in a later development. For example, if a ‘bonus’ square was added in a future development, the option to move back may allow for the user to get there quicker. This reasoning would also be the same if there were targets to achieve, for example if they were given the task of answering a certain number of phishing questions within a set time.

3.3. Implementing the Solution

As previously stated, Actionscript was used in the Flash CS3 IDE to develop the game and implement the class structure defined by the UML diagrams. The UML analysis and design work carried out meant that the class structure and the communication between them had already been identified and this was vital in getting the solution completed on time.

Actionscript revolves around events when things such as user actions take place. When an event takes place, e.g. clicking on a board square, an event is dispatched by the system and the event listener calls an appropriate function to run. For example, when clicking a square, an event is triggering upon the user click. The event listener was registered in the Game Manager class, which was the main game function, and when the user clicks on a square, the event is triggered by the BoardCollection class and caught by the Game Manager class and the function set to call upon the event trigger is run – in this case the question manager is called. This method was implemented for all game actions, and essentially controlled the game

3.4. Game Flow

The following steps show the general game flow – how the game works from the users' perspective:

1. Upon opening the game the user is greeted with the main menu. From here they can view the instructions and click 'start game' or just click 'start game' without reading viewing the instructions.
2. The user enters their name, selects their piece, and clicks 'submit'.
3. Upon submitting their name and piece, the game begins (see figure 1). The user clicks 'start' to begin the dice animation, upon clicking 'stop' the selector stops.
4. With a number selected, all squares are dimmed, with the two possible movable squares staying lit.
5. Upon choosing a square the user's piece is moved to the chosen location and a question is asked (see figure 2)
6. The user then selects an answer and feedback is immediately provided.
7. Depending on whether the user gets the answer right or wrong, the square deactivates and contains a tick or a cross.
8. Upon answering all questions, or clicking the 'quit' button, the user is given their score and can either close the game completely, or click 'finish' which will take them back to step 1 – the main menu.

3.5. Testing

It was attempted to recruit users who had a varying existing knowledge in the area. Although the solution assumed very little knowledge in the subject area, ideally it would be beneficial to the majority of users and so it was vital to ensure that the test participants represented a range of user ability. A total of 35 requests for user testing were sent, with 21 users subsequently carrying out the test (14 male and 7 female). In

relation to age, 2 were 18 or under, 12 were 19-25, 3 were 26-35, 1 was 36-45 and 3 were aged 45+.

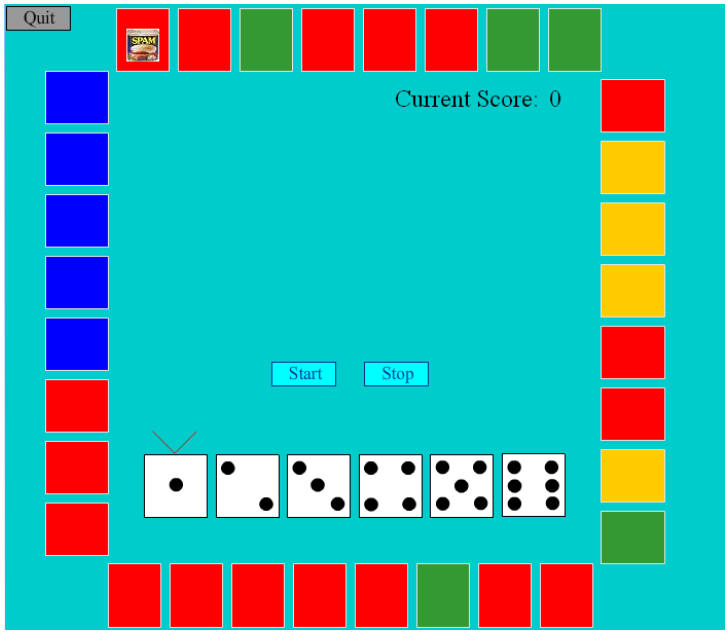


Figure 1: The main game board

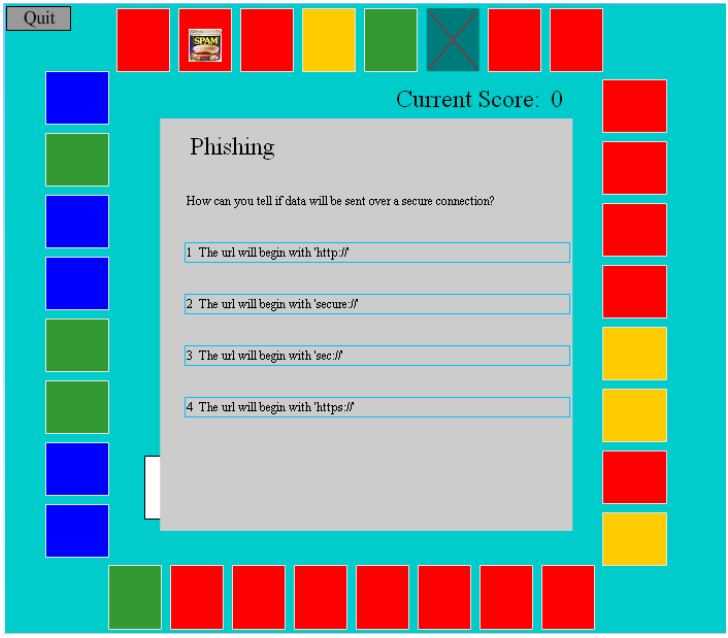


Figure 2: Question Interface

The solution was tested by asking the users three preliminary questions to find the length of time they spend on the Internet every week and their current knowledge in the subject area. They were then asked read through the online material once, and then play through the game whilst referring to the literature if necessary. They then resumed the questionnaire and were asked to provide their score, overall feelings on the game and literature and their recommendations for future development which was vital with this being a prototype.

Figure 3 shows the relation between time spent online and the achieved score. It would be expected that the longer someone spends on the Internet, the better score they would achieve. As seen below this seemed to be generally the case. As the solution is aimed at every day Internet users, the users at the lower end of the Internet usage were not expected to get poor scores as it was ensured that the material was aimed for a range of users. This seems to be shown below, with the lowest score achieved being 450 which is approximately 56% from someone who spends very little time on the Internet

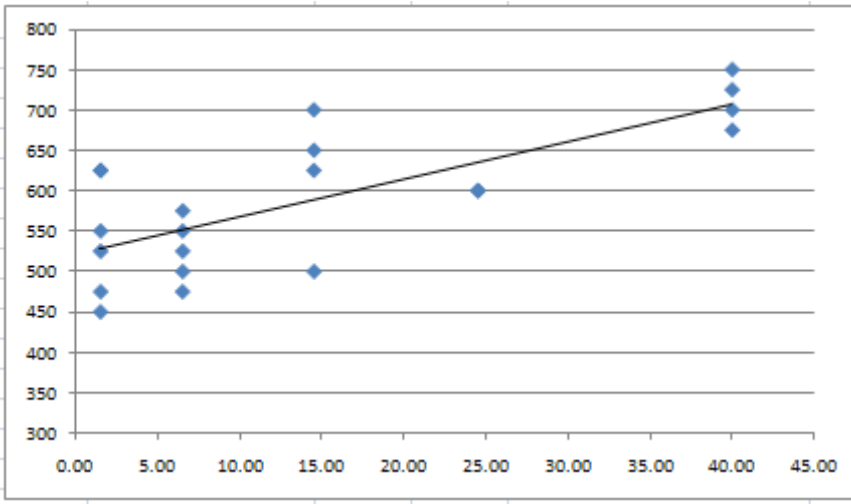


Figure 3: The relationship between time spent on the Internet and score

4 Conclusion and Future Development

The testing results suggested that the project had been a success. The overall aim was to improve user awareness of social engineering and the results detailed in section 3.5 suggest that had in fact happened. In addition to this, 17 out of 21 of the test participants found the level of website literature suitable, with 18 of them satisfied with the question levels in the game. Feedback regarding the questions and literature was very positive. Figure 4 shows the user responses when asked what they would like to see in future developments.

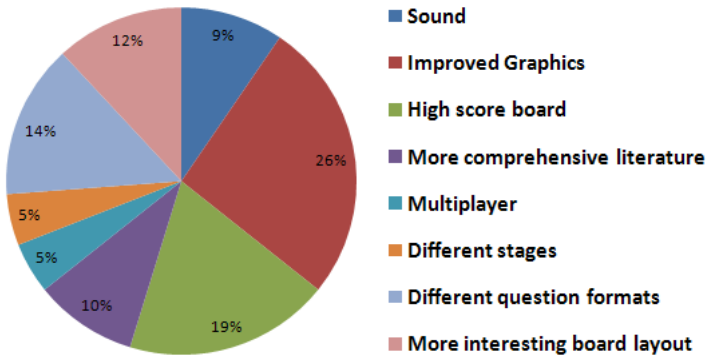


Figure 4: Features desired in future developments

Improved graphics was the most popular option. There is a range of ways this could be developed in the future including a more aesthetically pleasing board layout rather than the coloured squares in the prototype.

The second most popular feature was a high score board, which as well as adding a user requested element to the game, may also be a way of retaining the users attention, with a goal for themselves of getting on the high score board they are less likely to become bored. It may also tempt the user to replay the game.

Different question formats was the third most popular feature. This could include things such as displaying four emails to the user, and have them select the email that is a social engineering attack. An alternative to this could be displaying a single email and have the user select the 'hotspots' that would suggest that it is a social engineering attack.

It can be seen that with the prototype showing potential, if the above developments are implemented in a future development, participation should increase and ideally so will the awareness levels of those who play.

5 References

Bennet et al. *Object Oriented Analysis and Design*. 2nd Ed. London. McGraw-Hill

Gartner. 2007. *Gartner Survey Shows Phishing Attacks Escalated in 2007* [online] Available: http://www.gartner.com/it/page.jsp?id=565125 Date Accessed: 14/01/09

Microsoft. 2007. *What Is Social Engineering?* [online] Available: http://www.microsoft.com/protect/yourself/phishing/engineering.mspx Date Accessed: 14/01/09

Sky. 2009. *Facebook Scam* http://news.sky.com/skynews/home/technology/ facebook-Scam-Ive-Been-Mugged-In-London/Article/200908315363182 Date Accessed: 21/08/09

Comparing Anti-Spyware Products

W.Martins and S.M.Furnell

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

Abstract

Spyware has been more of a threat to the home user than other malicious software for the motive behind its creation which has been the tracking of the user and his activities on the Internet alongside the stealing of his personal or confidential information. As a result of this threat, various anti-malware products have been introduced to remove spyware from home PCs. This research examines the effectiveness of present day anti-malware products in removing spyware from a test computer. The results suggest that the removal capabilities of the products are unsatisfactory and indicate there are compelling reasons for more thorough detection and removal of spyware from home computers.

Keywords

ASEPs, Anti-Virus, Registry Keys, Spyware.

1 Introduction

For the computer user, the Internet is an increasingly dangerous place by the day. Where once all a user had to fear was the threat of viruses, present day trends paint a more sombre picture of an amalgamation of adware, worms, viruses, Trojans, spyware, and root kits the home computer is at risk of encountering once connected to the Internet. In an age in which increasing amounts of personal and confidential information is being stored on the home computer, the preponderance of malware on the Internet harbours significant risks. This growth in malware threats and the corresponding shift, by malware authors, from “ego trips” to pecuniary motives portends a significant risk of loss of trust in the Internet with potential damaging implications for e-commerce in particular.

Numerous studies however indicate the pace of malware prevalence and subsequent infection of home computers is on the increase. A 2008 Internet security study by Webroot (2008) for instance, reported a 500% increase in web borne malware compared to 2007 alongside another study estimating the infection of 35 million computers each month by malware (Pandalabs 2009). It is in this environment fraught with risks the computer user navigates.

Though, as earlier mentioned, user awareness of computer security is on the increase (F-Secure 2009), studies have repeatedly indicated security awareness and knowledge is still lacking, even among advanced users (Furnell et al. 2007). Additionally, while it has been a standard security recommendation for users to

avoid adult and 'warez' websites of which users are at greater risk of malware infection, there is compelling evidence that users are still at risk of infection when they visit legitimate websites (BBC 2009). Home computers are adjudged to be at greater risk of infection compared to corporate computers as a result of user habit to use their computers whilst logged in as administrators and the administrative restrictions enforceable on corporate computers are absent in home computers. It is in light of these short-comings, greater emphasis is placed on the ability of anti-malware products in protecting the home user from the menace of malware. This paper details a research undertaken to investigate the effectiveness of present day anti-virus products in removing spyware from a computer.

2 Methodology

2.1 Test Bed Preparation

For the test, Windows XP service pack 3 was installed on a system along with Microsoft Office 2003 and Adobe reader. All operating system and application updates were subsequently installed. To confirm all updates had been applied, the vulnerability tools - Microsoft baseline security analyser (MBSA) and Secunia personal software inspector - were run against the system. Additionally, the system was scanned with an anti-virus program which was later removed.

2.2 Anti-virus Product Selection

Due to the fact that most standalone anti-spyware products have been integrated into anti-virus products, anti-virus programs were downloaded from various anti-malware vendor websites. The list of anti-virus vendors was obtained from the Microsoft site (2008). The anti-virus products selected are as presented below:

Anti-Virus Products	Version
Eset NOD32	4.0.437.0
F-Secure	9.00 build 149
Kaspersky	6.0.3.837
Malwarebytes	1.39
Panda	9.00.00
Sophos	7.6.10
Vipre	3.1.2775
Webroot	6.1.0.128

Table 1: List of Anti-Virus Products Selected

2.3 Test Tools

For the successful conduct of any test involving malware, tools are required to monitor and record the creation of files and registry keys by the program and to monitor the state of the system prior to spyware infection and after spyware removal.

To accomplish this objective, a collection of freeware and shareware system utilities, comprising registry and file monitoring tools, were adopted for the study. The tools were selected based on a track record of implementation in malware forensic analysis and incident response (Aquilina et al, 2008) and various Internet sources. Malware has been known to compromise the integrity of system utilities. To ensure the integrity of the tools selected would not be compromised by the spyware programs during the course of the study, a MD5 hash was taken of all tools before the installation of the spyware samples and then compared with another MD5 hash after installation.

Additionally, tools of similar functionality were selected. This was for a variety of reasons. Paramount was a bid to ensure result consistency and integrity. For instance, in a scenario in which a single tool is adopted, the integrity of any results obtained is based on the assumption that the program correctly captured or interpreted the required data. In the circumstance where the data capture process or interpretation is suspect, the integrity of the study is put to question. Secondly, the strengths of a single tool may be restricted in certain areas of operation and unable to provide a comprehensive overview as required.

The selected tools are as follows:

- **Autoruns**: A startup program monitor. Used to display which programs are configured to run during system bootup or login.
- **Regshot**: A freeware system comparison tool. Used to compare the changes to the registry and file system prior to and after the installation of a program.
- **Regsnap**: A shareware system comparison tool. Also offers the same functionality as Regshot.
- **InstallWatch**: Used to track system changes as a result of program installations.
- **Hijackthis:** Used to generate an in depth report of the registry.
- **Pstools**: A collection of command-line utilities used to monitor the processes running on a system.
- **Process monitor**: A system monitoring tool. Used to view real-time registry and file/process activity on a system.
- **Process Explorer**: Utility used to list the processes running on a system and the handles and dynamic link libraries (DLLs) loaded.
- **R-Drive Image**: A disk imaging tool. Used to create disk images for the study.
- **Rootkit revealer**: A rootkit detection utility.

2.4 Sample Selection and Installation

Spyware is installed in a system in a variety of ways among which are through drive-by downloads when users visit infected websites, through spyware bundled with free or shareware applications, or through the delivery of spyware as a payload of other malware onto a system.

For the test, samples of spyware/adware were identified and collected for the test. A crucial aspect of any malware test is the identification and confirmation of the samples to be used in the test (Antispyware Coalition 2008). Additionally, identified samples should be of a wide variety and appreciable number for statistical relevance (Marx and Morgenstern 2008). The samples used for the test were of various categories: adware, spyware, potentially unwanted programs such as jokes, Trojan-Spy, file sharing tools and rogue anti-malware applications. Overall, the samples were fifty-five in number.

The samples were identified and selected using a number of internet sources such as the malware databases of anti-malware vendors. For instance, the anti-malware, Emsisoft, lists adware/spyware programs along with the websites which host them. Another resource which was utilised was the malwaredomain list site (2009) which lists websites that host malware or exploits.

To reduce the risk that the samples collected contained any other unknown malicious components, the samples were uploaded to the online virus scanner, Virustotal (2009) for confirmation of the authenticity of the samples.

2.5 Test Execution

A snapshot of the system was taken and an image of the system was taken and stored as a master copy. The spyware samples were then installed on the system and the system rebooted so as to ensure full installation. On reboot, a snapshot of the system state was taken and its image saved. This image was used for subsequent comparison tests with various anti-virus products and the two snapshots were compared to determine the files and registry keys created or edited by the spyware programs.

Internet access was enabled during the installation of the samples and disabled afterwards. Spyware when first installed on a system may update its components or download additional components. Internet access was enabled concerning this and disabled shortly afterwards. Internet access was disabled so as to reduce the risk of system inconsistency due to the risk of download of additional malicious components after the snapshots would have been taken. Internet access was subsequently enabled solely for the purposes of anti-virus updates after product installation and disabled afterwards.

Each anti-malware program tested was configured for full scanning and the system was scanned three times. Full scanning was enabled as a result of the various default configurations of anti-malware products. For instance, a vendor may prioritise speed over efficiency in setting default configurations while another may configure the default scan as a full scan. As such, results from a study in which the anti-malware products are tested based on the default configuration are likely to be flawed (Harley and Lee, 2007). Taking this into consideration, full scanning was configured on all the tested anti-malware products. The products were also configured to remove all traces of malware without prompting. In cases where the delete option had to be selected manually, it was chosen. The delete option was selected so as to gauge the success or failure of the products in removing the spyware. The study was undertaken using the default user account, the administrator.

The system was scanned three times by each product to ensure thorough removal of suspected programs. Additionally, the samples were left on the desktop to determine the removal capabilities of the anti-malware program concerning uninstalled spyware.

3 Results and Analysis

Malware when installed into a system places its files in critical areas of the registry and file system. These areas are commonly referred to as the Auto-Start Extensibility Points (ASEPs) (Harriman 2006). The installation of the samples resulted in the creation of registry keys in to these locations as well as in other areas of the registry. As the samples adopted for the purposes of the study were of various types, it was observed that both the spyware and adware programs installed more files when compared to the Trojan-Spy samples which resulted in the creation of few files and registry keys. For instance, one of the spyware programs was observed to create no less than seven registry keys in the ASEPs.

Overall, the installation of all the samples resulted in the creation or modification of critical registry keys and files. Sixty seven registry keys were created along with three hundred and eighty files. The anti-virus program was then installed on the system and run for a total of three times. On completion, a snapshot of the system was taken and then compared with the snapshot of the system taken after the installation of the samples. The results comparing the effectiveness of the products are displayed in Figure 1.

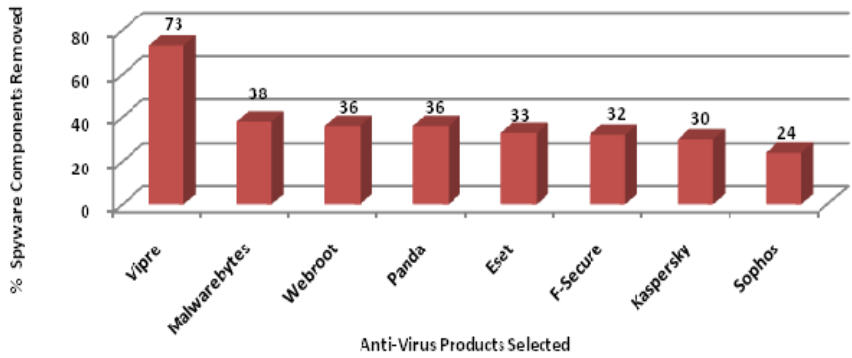


Figure 1: Spyware Components Removed

Anti-virus products are expected to detect and remove malware threats. This is accomplished through the termination of processes and removal of files and registry keys. As shown above, the removal capabilities of the anti-virus products suggests there is room for improvement. The performance of the products was below average, with the exception of the Vipre product which was observed to be the most effective product in the removal of both spyware files and registry keys. Additionally, as depicted in the below Figure 2, the number of processes still active after completion of the tests shows the computer is still at significant risk from malware.

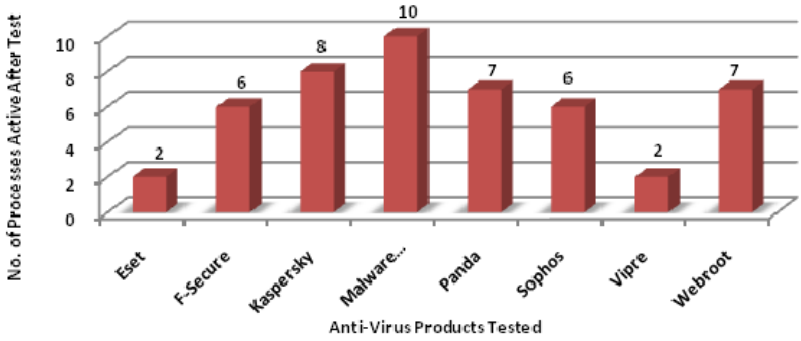


Figure 2: Processes Active after Test Completion

These results raise troubling issues. Foremost, the low rate of removal of spyware components and presence of active spyware processes suggest users are still at risk of spyware. This is particularly worrisome as there are greater expectations on anti-virus products to protect users as most users may not have the required technical expertise or knowledge to supplement the use of anti-malware products. As such, these users may undertake their normal activities on the Internet with a false sense of security.

Additionally, the results indicate the inability to effectively detect the spyware components is not peculiar to one product. This suggests a weakness on the part of the anti-malware industry as a user would still remain unprotected from spyware regardless of the product he were to select.

Further results from the research indicate the removal process of the spyware components are not as thorough as may be expected. As earlier highlighted, anti-virus products are expected to remove all registry keys that are created by spyware or edit the values of the keys if removal would disrupt the legitimate operations of the computer. Figure 3 details the percentage of registry keys which were left intact despite the removal of files associated with the keys.

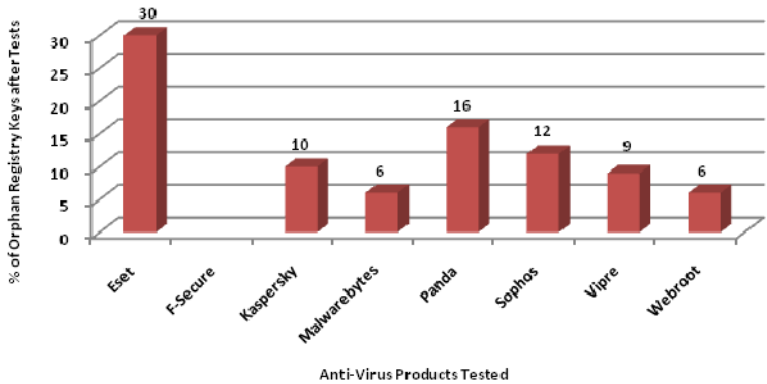


Figure 3: Orphan Registry Keys after Test Completion

As displayed in the above figure, only one anti-virus product ensured no orphan registry keys were left. The prevalence of the orphan registry keys has undesirable implications for both the user and the anti-virus vendor particularly where the keys execute programs automatically on user logon or system startup. For the user, the appearance of error messages on the inability of an application to run on user logon or system startup may cause uncertainty and lead the user to believe that his computer supposedly fixed by an anti-virus product remains faulty. On the other hand, the user may be inclined to believe the anti-malware product was ineffective in the removal of the risks on his computer. In a scenario where the user switches to a different anti-virus product and experiences similar occurrences, there remains the possibility the user may become discontented with the anti-malware industry and subsequently abstain from using the Internet.

4 Conclusion

The importance of anti-virus products for the protection of home computers from malware cannot be over-estimated. Studies have shown users lack the means or knowledge to protect themselves from the threat of malware thus placing substantial responsibility on anti-malware products. The research conducted to examine the effectiveness of present day anti-virus products in removing spyware components from a computer suggests the products may not remove spyware components as may be expected by users. As such, users are still at significant risk of spyware regardless of the anti-virus products selected and may either proceed to browse the Internet under an assumption of false security or desist/limit use of the Internet after experimenting with various products.

The research also suggests anti-virus products may not remove spyware components in a thorough manner as incidences of orphan registry keys were observed to be predominant among the products. The existence of such keys may trigger error messages which may be troubling for users and may result in unintended commercial consequences for anti-malware vendors. Overall, this research has underlined the risk users may still face despite the adoption of anti-malware products.

5 References

Aquilina, J., Casey, E., and Malin, C. (2008) *Malware Forensics: Investigating and Analysing Malicious Code.* Massachusetts: Syngress.

Anti-Malware Testing Standards Organisation (AMTSO) (2008) *the Fundamental Principles of Testing.* Available at: http://www.amtso.org/documents/doc_download/6-amtso-fundamental-principles-of-testing.html (Accessed: 4 January, 2009)

Antispyware Coalition (2008) *Considerations for Anti-virus Product Testing.* Available at: http://www.antispywarecoalition.org/documents/20080417testing.pdf (Accessed: 2 January, 2009)

Autoruns (2009). Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009

Emisisoft. (2009). Available at : http://www.emsisoft.com *Accessed: 10 June, 2009.*

Harley, D. and Lee, A. (2007) 'Testing, Testing: Anti-Malware Evaluation for the Enterprise', *10th Annual AVAR International Conference, Seoul 2007.* Available at: http://www.eset.com/download/whitepapers/TestingTesting(May2008).pdf Accessed: 10 January, 2009.

Harriman, J. (2006) 'A Testing Methodology for Antispyware Product's Removal Effectiveness'. *15th Annual EICAR Conference, 2006.* Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/testing_methodology_for_antispyware_removal.pdf Accessed: 26 July, 2009

Hijackthis (2009). Availabe at: http://us.trendmicro.com/us/home/home-user/ Accessed: 11 June, 2009

Install Watch (2009). Available at: http://www.epsilonsquared.com/installwatch.htm Accessed: 11 June, 2009

Malware domain list.(2009). Available at: http://www.malwaredomainlist.com Accessed: 10 June, 2009

Marx, A. and Morgenstern, M (2008). *System Cleaning: Getting Rid of Malware from Infected PCs.* Available at: http://wwww.virusbtn.com/virusbulletin/archive/2008/06/vb200806-system-cleaning (Accessed: 10 January, 2009) Registration required.

Microsoft Baseline Security Analyser (2009). Available at: http://www.microsoft.com Accessed: 10 June, 2009

Microsoft (2008) *List of Anti-virus Software Vendors.* Available at: http://support.microsoft.com/kb/49500 Accessed: 10 July, 2009

Pandalabs (2009) *Annual Report Pandalabs 2008.* Available at:

http://pandalabs.pandasecurity.com/blogs/images/pandalabs/2008/12/31/annual_report_pandalabs_2008_ENG.pdf (Accessed: 23 June, 2009)

Process Explorer (2009). Available at: http://technet.microsoft.com/enus/sysinternals/default.aspx Accessed: 10 June, 2009.

Process Monitor (2009). Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009.

Pstools (2009). Available at: Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009.

Secunia Personal Software Inspector (PSI). Available at: http://secunia.com/vulnerability_scanning/personal/ Accessed: 15 July, 2009

R-Drive Image (2009). Available at: http://www.drive-image.com/ Accessed: 11 June, 2009

Regshot (2009). Available at: http://sourceforge.net/projects/regshot/ Accessed: 10 June, 2009

Regsnap (2009). Available at: http://lastbit.com/regsnap/ Accessed: 10 June, 2009

Rootkit Revealer (2009). Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009.

Virustotal (2009). Available at: http://www.virustotal.com. Accessed: 15 July, 2009

Non-Intrusive Identification of Peer-to-Peer Traffic

A.Ulliac and B.V.Ghita

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

Abstract

This research study a new way of identifying hosts and connections involved in peer to peer traffic without requiring analysing the payload. The P2P use more and more encryption and port number randomization. Therefore the traditional classification based on signature identification used by deep packet inspection systems is not longer efficient. This study provides a new solution to identity connections of a host which are related to a peer to peer exchange. The final output is to make able to command a firewall able to block only connections of a host that are classified as using peer to peer without blocking all its traffic.

Keywords

Networking, peer to peer, detection, supervised neural network

1 Introduction

Since ten years, the usage of peer to peer protocols significantly grown to permit an easy way to exchange data with personal broadband connections. It was more and more required to monitor and control the usage of those protocols. This is because it generates a lot of overload on the network infrastructures and could be involved in illegal exchange of copyrighted materials. Therefore, it has been able to use signature detection to classify the packets. This increasing of monitoring has motivated the protocols designed to make them evolving in order to escape the classification tools. Therefore new versions of those protocols use port number randomization and encipher the packets payload.

In this paper will be shown how the new algorithm is design and an evaluation will be made in order to identify its benefits and its limitations.

2 Background of payload vs. non payload analysis

2.1 Payload analysis

The payload analysis is the traditional methodology to classify the packets over a network and has been demonstrated as being efficient (Sen et al., 2004). For instance, Snort, the IDS using Deep Packet Inspection, has rules making able to identify some commonly used peer to peer protocols. For instance bittorent exchanges are identified with a specific character string into the packets. This methodology has revealed some limitation over the time. First it is not flexible and

needs to write specific rules for every single protocol and rewrite rules following the evolution or variations of a protocol. Then it is inefficient to identify a protocol when the data is encrypted.

2.2 Non payload analysis

However, previous studies have already shown that statistical analysis can be an efficient response to perform an identification not based on packets payload. Various solutions have been experimented. The first one (Karagiannis et al., 2004) is based on the design of a state machine without requiring payload. However this solution shows limitations on flexibility because of constants variables into the algorithm. Then more studies based on statistical algorithm, using various forms of neural networks or Bayesian algorithm shown their efficiency (Fuke et al., 2007; Chen et al., 2009).

2.3 Discussion

The objective of this research is to provide a new solution, first to identify internal hosts using peer to peer clients, then for each of them to identify on by one which connection is involved in this peer to peer traffic.

3 Methodology and data

3.1 Methodology

The algorithm uses a supervised neural network system. It provides flexibility and is fast at classifying data once the learning stage has been realised. The principle of the learning stage is to provide couples of inputs and outputs to the neural network. Then it will build a network structure describing a pattern of the data in order to automatically classify to the right output considering the input. Then during the execution stage, the algorithm will process input parameters to send them to the trained neural network that will provide a classification with an estimation of the accuracy. This estimation could be use later in order to evaluate the efficiency of the algorithm or if a rule should be apply on a network firewall.

3.2 Data

Two main sets of data are used for the purpose of this research. The first one (traces 1) is a sample of two categories of traces containing respectively peer to peer or some other type of network flow. The peer to peer is from torrent and emule network which represent about 90% of the market share in Western Europe (ipoque, 2007). It is used to train the neural network and to perform the evaluation of the algorithm. The second set of data (traces 2) is made from an ISP in New Zealand, provided by the University of Waikato. It is used to perform evaluation on unknown traces in order to evaluate the efficiency of the algorithm on realistic data.

4 Supervised neural network to identify P2P traffic

4.1 First part of the analysis -- Overall peer to peer detection

The first part of the algorithm take every connection related to a host during a certain period of time in order to process them in their own context. The algorithm generates four inputs for the neural network, and then two outputs are obtained at the end of the processing.

4.1.1 Ratio between the number of external IPs and external ports contacted

Peer to peer protocols use port number randomization. Therefore this attribute can be used to identify them. It reviled that each remote host proposes to download on a different port number. With 65,535 different ports, there are 0.0015% of chances to have two remote hosts transferring data from the same port number. This result that when having peer to peer, the average ration between the number of different remote peers and the number of different ports used to connection to distant machine is about 1.

$$Ratio = \frac{number\ of\ remote\ IPs}{number\ of\ different\ remote\ \ ports}$$

4.1.2 Ratio between replies from peers compared to the number of requests from the internal host

The usage of peer to peer reviled that many connections from the internal host failed when using peer to peer clients. It shows that only 40% of requests receive replies. This rate is over 80% for users only connecting to central servers. This comes from that every peers registered on trackers files are not online on the same time, when the peer to peer client tries to contact them. The second reason could be explained by recent events. For instance The Pirate Bay (torrentfreak, 2008) claimed that they added random IP address onto trackers to make very difficult investigations on trackers illegally hosting copyrighted contents. So the client when starting to contact the IP from this list will also try to contact the randomly added addresses.

$$Ratio = \frac{\sum Replies\ from\ externals\ hosts}{\sum Requests\ from\ the\ internal\ host}$$

4.1.3 Mean value of port numbers used to communicate with external hosts

Most of commons network services use well identified ports number. Most of them are under 1024. Therefore, peer to peer which is using random ports number have a large distribution of values. So the average value of every external ports used by internal hosts to download from peers is high.

$$mean = \frac{\sum remote\ hosts\ ports\ number\ value\ for\ each\ connection}{total\ of\ connections}$$

4.1.4 Standard deviation value of port numbers used to communicate with external hosts

The randomization of ports number also makes the standard deviation of the port number growing. If the ports number are distributed on every ports that can be allocated, the standard deviation will be about 30.000 which is what shown the experiments.

$$SD = \frac{\sum_{i=1}^{i=n}(X_i - mean)^2}{total\ of\ connections}\ ;\ X_i\ is\ current\ the\ i^{th}\ port\ number$$

4.1.5 Reporting of the results

Figure 1 shows the various relations explained in the section 4.1.1, 4.1.2, 4.1.3 and 4.1.4.

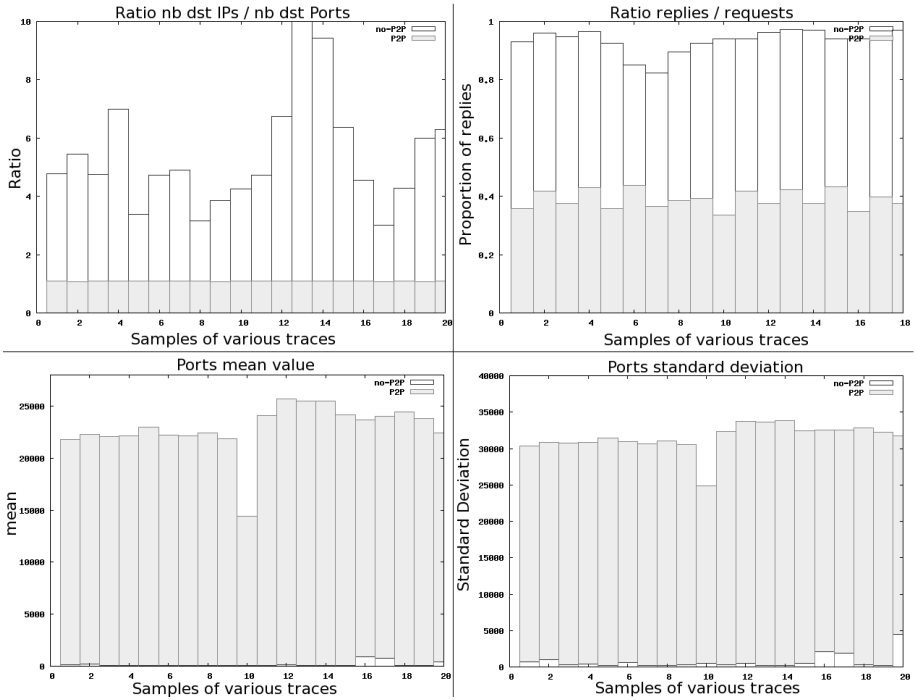


Figure 1 Analysis of the 4 parameters of the overall classification

4.1.6 Output

The output will determinate if the next part of the algorithm will be processed. It provides the probability to have to peer to peer within the group of connections that just have been processed.

4.2 Second part of the analysis – One by One connections classification

This part of the algorithm takes one by one, each connection related to a host in order to mark the one using peer to peer. The aim is to restrict specifics connections of a host without blocking all its traffic. This part of the algorithm generates 3 inputs to the neural network, which are the download and upload throughput, and the outgoing packet frequency of the connection.

4.2.1 Throughput of the connection between the two peers

The throughput between to hosts gives interesting information about the type of host involved in the exchange. Personal broadband access provides lower bandwidth and usually an asymmetric connection. For example, in UK, 80% users access the internet with ADSL (broadband-finder, 2009). So it will explain that the throughput of the exchange between two peers will never be at maximum at the upload bandwidth of the remote peer and not at the download bandwidth of the local host. So the average download throughput will be defined by the average upload bandwidth provided by ISPs. Throughput estimation formula:

$$Throughput = \frac{\sum_m^n s_i}{\Delta T} \text{ with } \Delta T = t_n - t_m$$

4.2.2 Average outgoing requests packet frequency from the internal host

The frequency of packet sent from the internal host to external peers is a good indication if the connection carries download or upload of files. It has been made the observation, that the frequency of packets is lower when there is a human interaction. So this parameter will exclude every connections involving human control like for instance web browsing or instant messaging. The frequency estimation formula is:

$$Freq = \frac{1}{\Delta T} \text{ with } \Delta T = \frac{\sum_1^N t_n - t_{n-1}}{N}$$

4.2.3 Output

The final output is an estimation of the probability of having P2P on the current analysed connection from the host. It provides a couple of values (defining a connection) which are an external IP and its remote port associated to it if the estimation reveals that it is part of P2P traffic.

4.2.4 Reporting of the results

The figure 2 illustrates the comparison of throughput and bandwidth values.

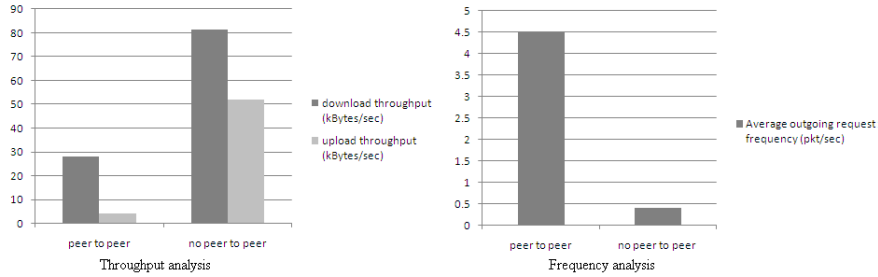


Figure 2: Analysis of the parameters of the connection by connection analysis

4.3 Summary of the algorithm

```
Capture N packets from a host

set i 11 with ratio dst IPs / dst ports on the external host
set i_12 with ratio replies / requests from the internal host
set i_13 with mean of the destination ports number to the external host
set i 14 with standard deviation of the destination ports number to the
external host

do neural network analysis with i_11 i_12 i_13 i_14

if p1 < threathold 1 //p1 is the neural network output probability on
p2p
   Stop
else
   // Here start the second part of the algorithm
   for each connection

      if connection has only request packets without reply from remote
host
         skip analysis

      set i21 with ingoing average throughput from the internal host
      set i22 with outgoing average throughput from the internal host
      set i23 with outgoing average packet per seconds from the
internal host

      do neural network analysis with i_21 i_22 i_23

      if p2 > threathold_2 //p2 is the neural network output
probability on p2p
         connection contain peer to peer
         apply filtering rule
      else
         connection does not contain peer to peer
```

5 Evaluation

5.1.1 Buffer optimisation

In order to process the input parameters of the neural network, the size of the packets buffer should be identified. This size will influent on the accuracy of the detection, on the memory size and on the processing power required. Experiments were made by gradually increasing the size of the buffer, from 50 to 2,000. It shows that the

reliability increases with the buffer size. According to the result reported in the Figure 3 the size of the buffer reach a accuracy limit around 1,000 packets.

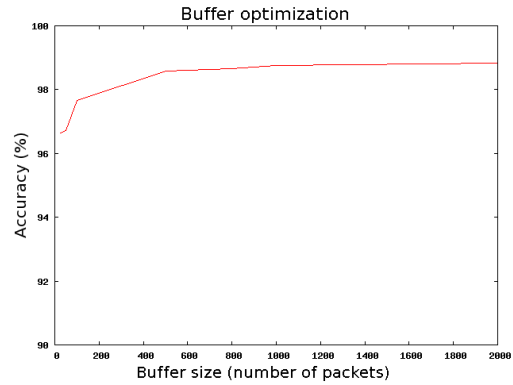


Figure 3: Classification accuracy depending on the packet buffer size

5.1.2 Evaluation of the algorithm

A first evaluation was made with the traces obtain from a 1Gbyte trace obtain from a personal gateway in front of two hosts. The host using peer to peer is detected with an average accuracy of about 98% with a standard deviation of 0.7. Then the host not using peer to peer is also classified with an accuracy of about 98% with the same standard deviation of 0.7.

The reliability of the classification of the second part of the algorithm has been processed with the same data than previously. This analysis is done on connections without requiring the context, so the same sample traces than the previous evaluation have been reused. The result is lower with about 84% of true positives. It has a larger variation around the average which is higher, with a standard deviation equal to 14.5. The Figure 4 shows this accuracy on 30 various sets of data coming from the traces 1.

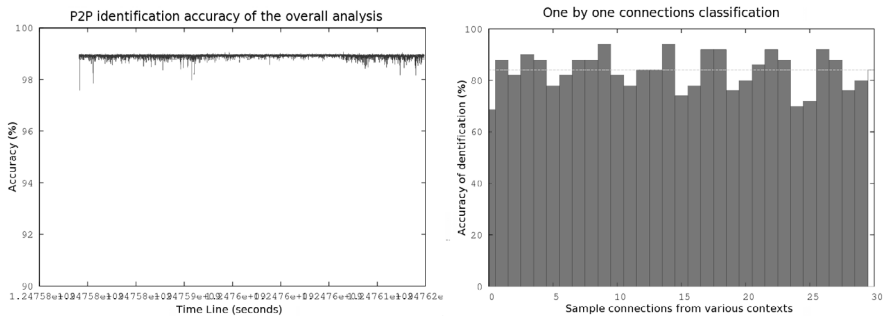


Figure 4: True positive rate on overall and one by one connection identification

5.2 Evaluation with New Zealand ISP traces

An evaluation has been made with unknown data retrieved from an ISP. It comes from a more realistic environment with more noise. The detection accuracy of peer to peer on overall detection is lower with about 85% of true positives than with the samples containing mainly peer to peer. However the true negative rate is higher, with 98%, and closer to the previous experiments. The difference can be explained by the more important quantity of noise on the network.

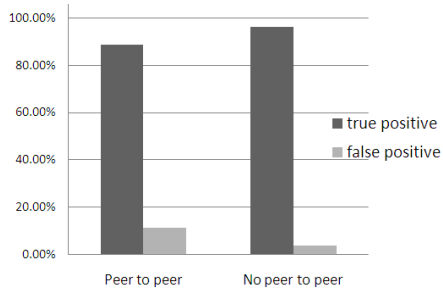


Figure 5: Evaluation of true and false positive on the traces from the New Zealand ISP

6 Discussion and implementation

6.1.1 Discussion and analysis of limitations

The algorithm is efficient when used on a gateway to identify which hosts are exchanging data on peer to peer networks. According to the evaluation tests it can vary between 85 and 98 % of accuracy depending on the noise on the network.

6.1.2 Implementation

An experimental prototype has been realised for the purpose of the research. All the analysis and output graphs are made from its output. Basically there are two ways to perform the analysis. One is offline, by analysing traces after they have been saved, and the second one is operating online. The offline analysis is useful for reporting users connected to peer to peer networks and is not intrusive. The second part of the algorithm identifying single connections is less useful in this case. But the second capability is to be able to perform online analysis to make able to stop, monitor or apply quality of service to the connections of a host (e.g. it is possible to build iptables or iproute2 rules). For this the output of the algorithm provides a couple of information which is a remote host IP with the destination port associated to it.

7 Conclusion and future work

This research shown that with a supervised neural network, it is possible to identify hosts using peer to peer on an internal network. Then the identification of peer to peer on a single connection has been made available.

On a future work it might be interesting to improve the classification methodology on single connections. This study tries to use the supervised neural network for both parts of the detection, but new statistical methodologies can be experiment to detect the peer to peer protocol on a connection.

8 References

Chen, Z., Yang, B., Chen, Y., Abraham, A., Grosan, C. and Peng, L. (2009) "Online hybrid traffic classifier for Peer-to-Peer systems based on network processors", *Applied Soft Computing,* Volume 9, Issue 2, 2009, Elsevier Science Publishers B. V., ISSN: 1568-4946.

Fuke, S., Pan, C. and Xiaoli, R (2007) "Research of P2P Traffic Identification Based on BP Neural Network", *Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing*, Volume 2, 2007, IEEE Computer Society, pp75-78, ISBN: 0-7695-2994-1.

ipoque (2007) "Internet Study 2007", http://www.ipoque.com/resources/internet-studies/internet-study-2007 (Accessed 4 August 2009).

Karagiannis, T., Broido, C., Faloutsos, M., and Claffy, K. (2004) "Transport Layer Identification of P2P Traffic", *Internet Measurement Conference,* 2004, ACM, pp121-134, ISBN:1-58113-821-0.

Maurizio Dusi, Manuel Crotti, Francesco Gringoli, Luca Salgarelli (2008) "Detection of Encrypted Tunnels across Network Boundaries", *IEEE International Conference on Communication*, 2008, IEEE Computer Society, ISBN: 978-1-4244-2075-9.

Robert L., H. (1994) *Neural network principles*, 1994, Prentice-Hall, ISBN: 0131121944.

Sen, S., Spatscheck, O., and Wang. D. (2004) "Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures", *International World Wide Web Conference*, 2004, ACM, pp512-521, ISBN:1-58113-844-X.

TorretntFreak (2008) http://torrentfreak.com/the-pirate-bay-tricks-anti-pirates-with-fake-peers-081020/ (Accessed 4 August 2009).

WAND Network Research Group (2009) "WITS: Waikato Internet Traffic Storage", http://www.wand.net.nz/wits/ (Accessed 15 August 2009).

Section 3

Robotics

Balance Control of a Humanoid Robot – ZMP Preview Controller

A.Maussion and G.Bugmann

Centre for Robotics and Intelligent Systems, University of Plymouth, Plymouth, UK
e-mail: G.Bugmann@plymouth.ac.uk

Abstract

Since the robotics exists, legged robots and especially anthropomorphic robots are great of interest. The fact that they could work in a human environment and perform the same tasks as a human person put them at the centre of all the attentions. Nevertheless, before to try to achieve some human tasks, some major problems like walking smoothly and controlling the equilibrium of the robot when he is moving have to be solved in order to be sure that the humanoid robot will evolve with safety in his environment.

These researches have explored a solution to the problem of balancing control of a humanoid robot which involves a ZMP preview controller using the inverted pendulum as dynamic model. Experiments have been lead on a real humanoid robot to validate the overall controller as a stable gait generator.

This publication starts by describing the ZMP preview controller applied in these researches. Then some details about the implementation and the test equipment are given. Finally, the results of experiments run on a Bioloid robot are presented.

Keywords

Humanoid robot, walk, balance, controller, preview controller, gait generator.

1 Introduction

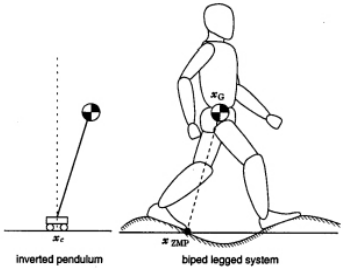
Humanoid robotics is one field of the robotics which made people dreaming but also a field with infinite application possibilities. For decades, a lot of anthropomorphic robots have been built in order to develop this field and study basic features such as the balance control. The list of examples could be long. Some of them are just made of a pair of legs like BIP-2000 by Espiau and Sardain (2000) while others look like a real human with a complete body such as HRP-1S (Yokoi et al. 2004) or HRP-2 (Hirukawa et al. 2007). Nowadays, humanoid robots are also able to perform some kind of run like the last robot from Toyota Partner Robots (Hornyak 2009).

A lot of different approaches have been made concerning the walk and the balance control. Most of them are based on stability criterion like the ZMP which was first introduced by Vukobratovicj and Jurwij (1969). This stability criterion as been expressed by Huang et al. (2001) as follow : "*The ZMP is defined as the point on the ground about which the sum of all the moments of the active forces equals zero*". If this point stays in the limits of the support polygon drawn on the floor by the feet, it guarantees the stability of the feet.

Some controllers are simply based on the ZMP (Takanashi Laboratory 2006) and adjust the gait of the robot by taking in account the actual state of the robot. In order to have a feedback of the position of the ZMP, simple calculation can be made like the one presented by Li, Takanishi and Kato (1991) using two force-moment sensors. Another solution, which is the basis of the presented researches, is based on a method using a ZMP tracking preview controller following a ZMP reference also used by Kajita et al. (2003) in simulations which gave very promising results. The presented researches have gone forward the cited works by implementing and testing a ZMP preview controller directly on a real robot.

2 ZMP preview controller

Biped walking pattern generation by using preview control of Zero-Moment Point was first introduced by Kajita et al. (2003). A preview controller is a controller which is based on the predictive control or Model Preview Control. This type of controllers is used to control complex systems by predicting his behaviour. The behaviour of the system is given according to a dynamic model, the inverted pendulum model in the case of the presented researches.



$$\ddot{y} = \frac{g}{z_c}(y - y_{zmp}) \Leftrightarrow y_{zmp} = y - \frac{z_c}{g}\ddot{y}$$

$$\ddot{x} = \frac{g}{z_c}(x - x_{zmp}) \Leftrightarrow x_{zmp} = x - \frac{z_c}{g}\ddot{x}$$

Figure 1: The inverted pendulum model (Sugihara, Nakamura and Inoue 2002) and its dynamic equations. x and y represent the CoM coordinates and g is the value of the earth's gravity acceleration.

The function of the preview controller is to determine the minimum jerk $\dddot{x}_{CoM}$ it is necessary to apply to the system at the instant k to follow a reference behaviour given by ZMP_{ref}. The output of the preview controller is calculated according to the series of the next N states, where each state takes T, the period of sampling which gives the overall preview period : N x T. In order to get, as output of the preview controller, the ZMP reference required, the preview period needs to be longer than a certain value, 1,2s in the case of the simulation performed by Kajita et al. (2003). If this condition is not respected, the preview controller will fall behind the reference and lose it. The ratio R/Q allows to balance between the minimization of the jerk and the tracking of ZMP_{ref}. The following equation, given by Kajita et al. (2003), resumes the statements previously presented.

$$\min_{\dddot{x}_{CoM_k}, \dddot{x}_{CoM_{k+1}}, \ldots} \sum_{i=k}^{\infty} \left(\frac{1}{2} Q \left(x^{real}_{zmp_{i+1}} - x^{ref}_{zmp_{i+1}} \right)^2 + \frac{1}{2} R \, \dddot{x}^2_{CoM_i} \right)$$

ZMP_{ref}, the ZMP reference is computed through a series of footprints themselves calculated according to the path the robot has to follow, its overall requested speed and some robot physical measurements. Each step is positioned along the path and separated from the previous step of a pre-defined distance. During the single support phase, the ZMP stays at the centre of the foot. In the double support phase, the ZMP is moving from the centre of the previous support foot to the centre of the next one and stays in the support polygon. By this way, a reference, like the one displayed in the figure 2, is generated and provided as input of the preview controller.

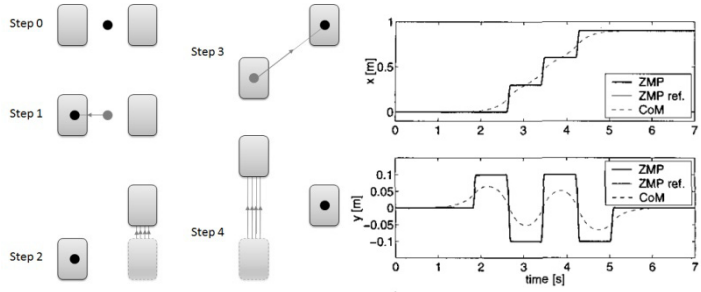


Figure 2: A series of footsteps and the ZMP theoretical trajectory. ZMP reference on X-axis and Y-axis (Kajita et al. 2003).

The calculation of the jerk can be simplified by the solution purposed by Wieber (2006) which involves matrixes iterative calculation. $X_{CoM_k} = (1 \quad 0 \quad \cdots \quad 0) X_{CoM_k}$ where

$$X_{CoM_k} = -\left(R_x^T R_x + \frac{\alpha}{\beta} I_{N\times N}\right)^{-1} R_x^T \left(R_x A_{CoM_k} - X_{ZMP_k}^{ref}\right)$$

According to the output of the preview controller and the inverted pendulum model, it is possible to deduct the next state CoM position, which will, along the time, produce the gait of the robot.

Moreover, Wieber (2006) discovered that for a preview period T = N x P where P is the sampling period and N is the number of preview periods, both parameters N or P can be adjusted as long as the global preview period is at least equal to T without impacting on the output result. This possibility allows to balance between the reactivity of the controller facing a perturbation and the calculation time induced by N x N matrixes calculations.

It is also very interesting to notice that the left part of the X_{CoM_k} equation, which is an NxN matrix, is constant and can be pre-calculated, while the right part of the equation is just an Nx3 matrix and is relatively easy to calculate. This specificity will really make the implementation running faster.

3 Implementation and test robot

The overall implementation of the proposed project can be split in three levels with specified tasks for every one of them. The two lower levels have been built as a sort-of a library in order to be re-usable in future researches. The higher level has been built in components which can be simply activated or deactivated.

The controller is the highest part in the software levels, the one which controls the robot and performs the balance by using functions available in lower software levels or specific built functions dedicated to the controller implementation. The controller is called periodically at a period P in order to perform the balance control of the robot. Figure 3 shows the architecture of the controller.

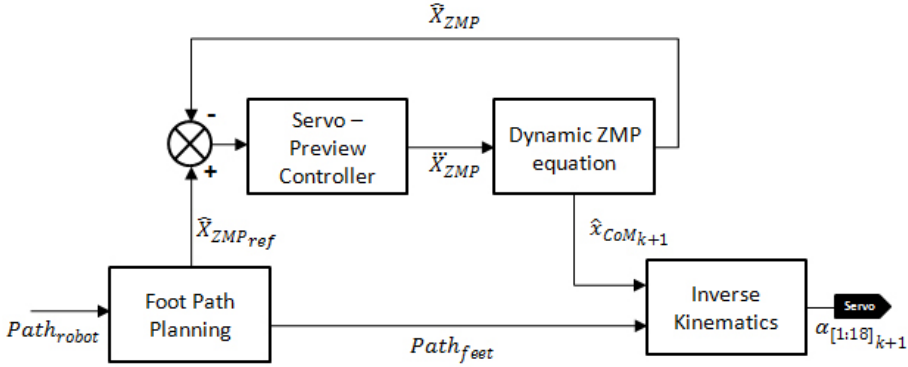


Figure 3: Architecture of the controller.

Middle level software is comprised between the low level and the high level. This part of the software is made of several classes which will support every high level package by providing simple functionality such as the share of memory, matrix calculation, a XML based log module, inverse kinematics or a periodically called basis for controller development.

Low level components of the software are equivalent to drivers. Their role is to make the interface between the hardware and the upper layer of the software by providing simple functions. This type of implementation allows separating the role of each part of the software which provides an easy way to make the software portable. This part of the software highly depends on the processor target used.

During the presented researches, a Colibri module on a development board has been used to control the robot. The Colibri is connecting to the peripheral bus through an interface board based on a bridge chip. On the Colibri side, the SPI bus is used to communicate to the interface board at 1,8Mbps. On the robot side, the serial bus is used at 500kbps.The test robot is a commercial Bioloid robot with 18 DoF which heights 35cm and is built of 19 blocks.

4 Results

The first tests have been run without any feedback from a sensor. In this configuration, the system is equivalent to an open loop controller. With this configuration, the robot is able to perform a smooth walk in a very stable way.

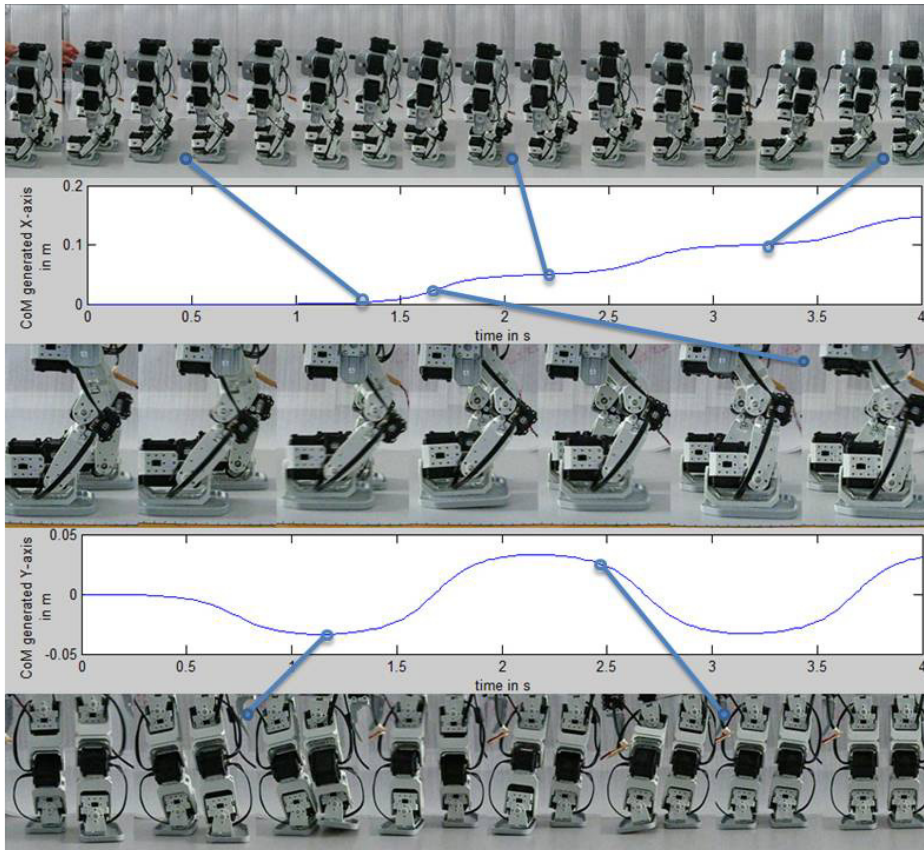


Figure 4: Robot gait obtained on X and Y-axis.

The support leg is driving the CoM motion while the leg which is lifted is slowly reaching its next position taking in account the other leg move. Every step has been defined to get a length of 8cm in the controller and produces real 8cm steps even in spite of light servo linearity problems. The robot avoids falling during the single support phase by switching all his weight i.e. his CoM, on the support leg.

During some tests, the robot was not really walking straight forward. This problem can come from multiple sources. The first one can be simply the linearity of the servos which cannot be the same for every servo and so the motion on one leg can differ from the other leg. The second origin could be the type of surface the robot is walking on. A first series of tests have been performed on a sort of plastic surface very slippery. A second series of tests performed on wood plane which gives better

results with less drift and confirms that the surface type has an impact on the robot path.

Another interesting point is that the preview period highly depends of the height of the CoM. In the case of the Bioloid robot which has a lower CoM height than the robot used by Kajita et al. (2003) and Wieber (2006) during simulations, a short preview period of 0,62s (31 x 20ms) appears to be enough for the preview controller to follow the ZMP reference. By comparison, a preview period of 1,2s has been used by Kajita et al. (2003) and Wieber (2006). This fact makes the preview controller more suitable for small robots because it is easier, and so faster, for them to perform the calculations.

5 Conclusion and future researches

After having run some tests, it appears that the preview controller is well situated to control, in a stable way, the test robot. Concerning the calculation consumption, it is even better with smaller robots which are the case of the Bioiloid robot.

However, these tests just concerned the fact that the system is able to generate a stable gait and not the stabilisation part due to the fact that no feedback has been used. The presented experiments validate the inverted pendulum model which, obviously, can be used as reference model for the Bioloid robot. They also validate the gait generation by the preview controller which is able to follow the reference given in input. Finally, the kinematics has been validated in a real case study.

Future researches will have to focus on the study of the stabilization side of the preview controller when the robot is facing perturbations. It could be also interesting to design foot soles which do not involve sliding in order to minimize the effects on the overall trajectory of the robot.

Even if, future tests could show that the controller is not enough alone to face strong perturbations, it could be one of the main part of a balance control system completed by different stabilizers acting on precise parameters. Moreover, it could also be easily improvable by, for example, changing the model of the simple inverted pendulum by another one, more complex.

The results of the preview controller suggest good prospects concerning his use in balance control.

6 References

Espiau, B. and Sardain, P. - 2000 - “The Anthropomorphic Biped Robot BIP2000” - IEEE International Conference on Robotics & Automation 2000.

Hirukawa, H., Koyanagi, K., Hattori, S., Morisawa, M., Nakaoka, S., Harada, K. and Kajita, S. - 2007 - “A Pattern Generator of Humanoid Robots Walking on a Rough Terrain” - IEEE International Conference on Robotics and Automation 2007.

Hornyak, T. - 2009 - “Toyota robot gets antsy, starts to run” – [online] [last visited the 5th August] [http://news.cnet.com/8301-17938_105-10303411-1.html]

Huang, Q., Li, K., and Nakamura, Y. – 2001 – “Humanoid walk control with feedforward dynamic pattern and feedback sensory reflection”. IEEE International Symposium on Computational Intelligence in Robotics and Automation.

Kajita, S., Kanehiro, F., Kaneko, K., Fujiwara, K., Harada, K., Yokoi, K., and Hirukawa, H. - 2003 - “Biped Walking Pattern Generation by using preview controle of Zero-Moment Point. AIST, Japan

Li, Q., Takanishi, A. and Kato, I. - 1991 - “A Biped Walking Robot Having A ZMP Measurement System Using Universal Force-Moment Sensors” - IEEE/RSJ International Workshop on Intelligent.

Sugihara, T., Nakamura, Y. and Inoue, H. - 2002 - “Realtime Humanoid Motion Generation through ZMP Manipulation based on Inverted Pendulum Control” - International Conference on Robotics & Automation 2002.

Takanashi Laboratory, 2006 - “Multi Purpose Biped Locomotor WL-16RIII Waseda Leg-No.16 Refind III” – [online] [last visited the 10th August] [http://www.takanishi.mech.waseda.ac.jp/top/research/parallel/]

Vukobratovicj, M. and Jurwij, D. - 1969 - “Contribution to the Synthesis of Biped Gait” – IEEE Transactions on bio-medical engineering, vol. BIIE-16, n°. 1.

Wieber, P.B. - 2006 - “Trajectory Free Linear Model Predictive Control for Stable Walking in the Presence of Strong Perturbations”

Yokoi, K., Kanehiro, F., Kaneko, K., Kajita, S., Fujiwara, K. and Hirukawa, H. - 2004 - “Experimental Study of Humanoid Robot HRP-1S” - The International Journal of Robotics Research 2004; 23; 351.

Computer Vision for Human-Robot Interaction on RoboThespian™, a Humanoid Robot

P.Pagnard and T.Belpaeme

Centre for Robotics and Intelligent Systems, University of Plymouth, Plymouth, UK
e-mail: T.Belpaeme@plymouth.ac.uk

Abstract

This paper explores how visual processing can serve as input to the behaviour of a humanoid entertainment robot. The paper reports on the background of the importance of the Human-Robot Interaction and the different abilities that robots can acquire using a vision system and their possible applications in our environment. This paper is describing how the HRI of the RoboThespian™ can be improved by the computer vision.

We wish to focus on a robust image processing technique: the face detection. Details of the method are provided in the technical part of the report. Algorithms are provided and early experiments are described. The paper includes a description of the tools used during the project and the future tasks to achieve in the project.

Keywords

Face Detection, Haar-like Features, AdaBoost Classifier, RoboThespian, Human-robot Interaction

1 Introduction

Humanoid robotics has become an important field of research the latest years.

This project takes part in a bigger project about a humanoid robot, named RoboThespian™. This project is realized by the company Engineered Arts. RoboThespian™ is a life-sized humanoid robot, an automated interactive actor. It has three major applications: to meet and greet visitors, to interact with the public, and to perform pre-programmed sequences. This robot is exhibited in several museums all over the world and is programmed to interact in several languages. A user interface has been created to allow the visitors to communicate with the robot. Until now, the actions the robot does are pre-programmed. That can be when it performs or when visitors configure it themselves and change its mood or ask multiple choice questions. Adding the vision to that robot would increase its realism a lot. Indeed, that would add some random behaviour. The main tasks of the project are to detect face and motion in order to track people in front of the robot.

This paper explains the importance of Human-robot interaction nowadays and reports several techniques of implementation of face detection before explaining the chosen algorithm. Results are discussed in the last part.

2 Human-robot Interaction

The literature about computer vision is relatively rich. It contains many texts and algorithms concerning the manipulations and the transformations of image data. However, it was only 30 years ago that the first computer had processed large sets of data, so we can say that computer vision can be considered as immature.

In terms of full-scale computer vision applications which involve motion estimation, depth recovery, and scene interpretation, fairly limited progress has been achieved. Indeed, no system has managed to react exactly as a human. These algorithms are brittle. If the input changes a little from what was expected, computer vision often fails. Computer vision is related to many areas, including biology, psychology, information engineering, physics, maths, entertaining and computer science. Using and developing robotic technology allow people to be more efficient and productive or can avoid people to do boring or monotone tasks [Kidd, 1992].

The basic goal of HRI is to develop principles and algorithms to allow more natural and effective communication and interaction between humans and robots.

3 Related Works

Many face detection techniques have been developed and generally using one of these approaches: knowledge-based, feature invariant, template matching, and appearance-based [Yang et al, 2002]. As shown in Figure 1, these methods can be classified into two categories: the Feature-Based Approach, considering the face geometry, skin colour and visual features from the input image, and the Image-Based Approach, considering the face as a whole entity to detect.

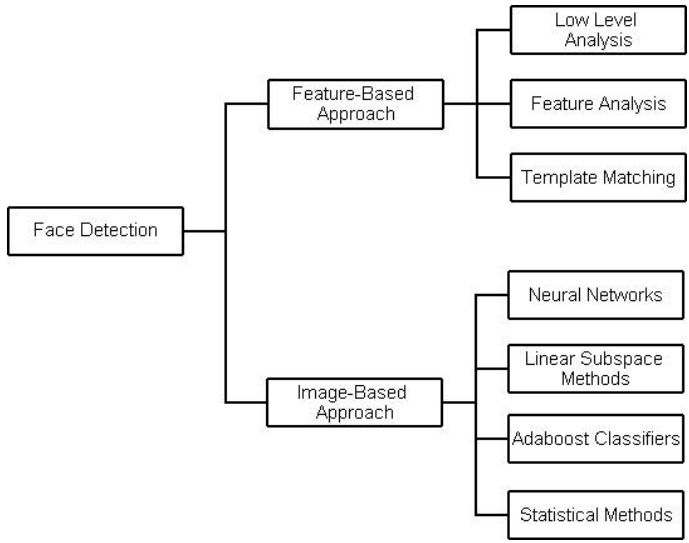


Figure 1: Face Detection divided into two different approaches

3.1 Feature-Based Approach

The feature-based Approach can be then divided into three parts. The low-level method deals with the segmentation of the pixel to obtain information about the properties of the pixel, such as its colour [Terrillon et al., 2000]. The feature analysis uses more global parts of the face, such as the eyes, the mouth, and the geometry of the face (De Silva et al., 1995). This method can provide the location of the face. The last level, which uses templates matching, has been created in order to locate non-flexible parts of the face, such as the lips or the eyebrows.

3.2 Image-Based Approaches

Contrary to the feature-based approach which uses feature and geometrical information about the object to be detected, the image-based uses examples of the image representation. Indeed, the feature-based approach is limited to simple conditions. Problems can be observed when faces are not seen from the front. Faces are now detecting using examples of face patterns and non face-patterns. As the face knowledge is not used anymore, errors due to the geometry of the face are avoided.

Four main subsystems are included in the image-base approach: The linear subspace method (Turk and Pentland, 1991), the neural networks (Rowley et al., 1996), and the statistical approach.

4 The communication between the robot and the server

IOServe is an Input/Output service. All the various configuration options used to configure what IOServe does can be configured from a PHP web page.

All data goes through IOServe. That is how everything happening to the robot can be controlled. IOServe is very comprehensive and flexible. It handles all hardware modules, remote and local communications, error reporting, recording and playback of motion data. It can be configured to work with multiple buses of different types. It also provides a configuration interface for hardware modules and an abstraction layer for mapping data from various sources to various targets.

To run the program of face detection to move the eyes of the robot (cell phones' screens), IOServe is configured to send a packet to the file containing the program that instructs it to send coordinates back to IOServe. IOServe then sees these coordinates as two inputs. From its configuration, it sees that it must forward the values to the Outputs which are physically on other computers, (the Colibris in the robot's head) and that it must put the coordinates into packets and send them to these computers. They are put into UDP packets in the same format as those between the program file and IOServe. The Colibris process the information to change the position of the eyes.

5 Haar-like Feature algorithm

A single pixel does not give more information than the illumination or the colour received by the camera at that location. A recognition process can be much more efficient if it is based on the detection of features that encode some information about the class to be detected. That is the case of the Haar-like features which encode the contrast between regions of the input image.

One of the main problems of computer vision is the time of computation. The integral image is a data structure which allows rapid summing of subregions. It was invented to increase the process time of the image.

The library OpenCV provides an algorithm, the Haar classifier, using Haar-like features. The classifiers based on Haar-like features seem to be really successful in the use in object detection tasks. Haar-like features was introduced by Viola et al. (2001) and improved by Lienhart and Maydt (2002).

This algorithm has been very popular since it has been created. This is mainly due to the fact that it handles very well accuracy and evaluation speed. The advantage of this algorithm is that it can be trained with many kind of object to detect whatever the object to be detected.

5.1 Learning Classification Functions

The Viola-Jones detector employs AdaBoost and organizes it as a rejection cascade, where each node of the cascade is an independent boosted classifier, a "weak classifier", designed to have a very high detection rate and poor rejection rate.

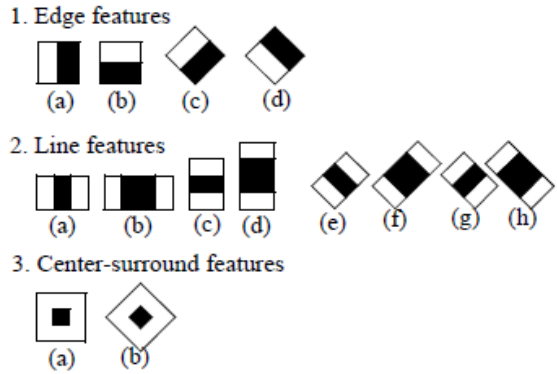


Figure 2: Prototypes of simple haar-like and center-surround features (Lienhart and Maydt, 2002)

The input image is scanned and for every location of the image, an independent decision is made about the presence of a face or not. That leads to a very large number of classifier evaluations. That number is about 50,000 for a 320x240 image. Using the Adaboost algorithm, a set of independent classifiers is trained from the

selection of a small set of features. Although all features can be computed efficiently, analysing the entire set of features is computationally too expensive. Each classifier is a simple function made from rectangular sums compared to a threshold. At each stage, the weak learning algorithm designs a single rectangle feature in order to have a very high detection rate (99,9%) at the cost of many false positive (50%).

The haar-like features used by the classifier are shown in Figure 2. It is made of 14 feature prototypes, including 4 edge features, 8 line features and 2 centre-surround features. All these features are scaled in every direction in order to provide a complete set of features. They can be computed at any scale and any location in constant time using the integral image.

5.2 Cascade of Classifiers

In order to increase false detection rate while preserving the efficiency, the classifier is divided into a cascade of weak classifiers [Viola and Jones, 2001]. Each node of the cascade represents a multitree boosted classifier, which only can return a binary response: Yes or no. The cascade of trees is represented in Figure 3. At the beginning of the cascade, easy classifiers, using few features, are trained to detect almost all positive regions while rejecting many non-face regions. That algorithm, using the rejection cascade, can greatly reduce the computation, because most of the regions studied terminate quickly in a non-face region.

6 Tests

6.1 Tests on the laptop

A data set of numerous images containing faces has been created. It includes many facial expressions, hats, glasses, people with different skin colours, single person or groups. A little part is represented in Figure 3. This data set has been taken on the Internet.

Figure 3: Set of images for face detection

Globally, results are good. When the image contains only a face, the algorithm is able to detect it without error. In the case of friends or family pictures, with at least, five persons, it happens that non-face regions are detected. Indeed, as the classifier is very complete, some shapes can mistakenly look like a part of a face and so be detected.

Where the algorithm failed was in the case of profile faces, or when moustache, glasses, or hairs hide too many features of the face.

Regarding the AdaBoost approach, the following conclusions can be drawn:

- The over complete set of Haar-like features shows the efficiency of the algorithm for face detection. Furthermore, the use of the integral image method makes the computation of these features efficient and achieves scale invariance. Lienhart and Maydt (2002) extended Haar-like features to increase the detection of non-frontal face. This method was used to improve the face detection of the robot.

- Adaboost learning can select best subset from a large feature set and construct a powerful nonlinear classifier.

- The cascade structure significantly improves the detection speed and effectively reduces false alarms.

It is important to ensure that the efficiency of the algorithm, according to the angle of the detected face, is good. The tests have been done on several persons and reduced to two faces which match with the maximum and minimum cases. These results are less good than the reality. Indeed, pictures of faces were taken at different distances and then rotated using a software. The rotation blurred a little the face, so they were less seen than in reality.

The face is not detected before 25 centimeters because the head is bigger than the window captured by the camera. Then, the faces have around twenty degrees on each side and are still detected. The performance decreases from two meters. An important thing is while the faces are detected, they always a rotation freedom, although when they are far

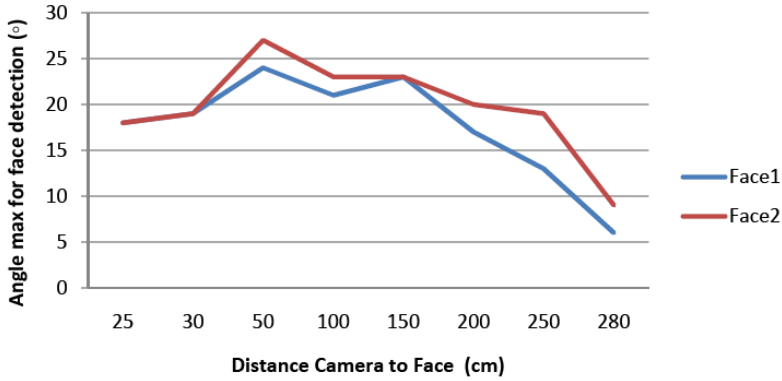


Figure 4: Test on the efficiency of the algorithm to detect leaning faces

The following curves represent the working range of the algorithm according to the brightness. Some tests to check the efficiency of the face detection to face the constraints the floodlight. The aim was to see the range where the robot is able to detect people. The values in the curves are the maximum and minimum distance the algorithm performs well. At these distances, the faces are detected reliably. There is

a little margin between the time the robot sees perfectly people and when it does not see anyone.

For brightness between 70 and 190, the algorithm is still able to detect faces from 25 centimetres and until at least two metres. An important thing has to be considered. RoboThespian™ is exhibited in a museum, so people cannot come too near it. They will not be near 25 centimetres. Besides, visitors will tend to bring them to the robot's attention in order to see its reaction. A distance of two metres or 2,5 metres should be enough in a museum for the face detection.

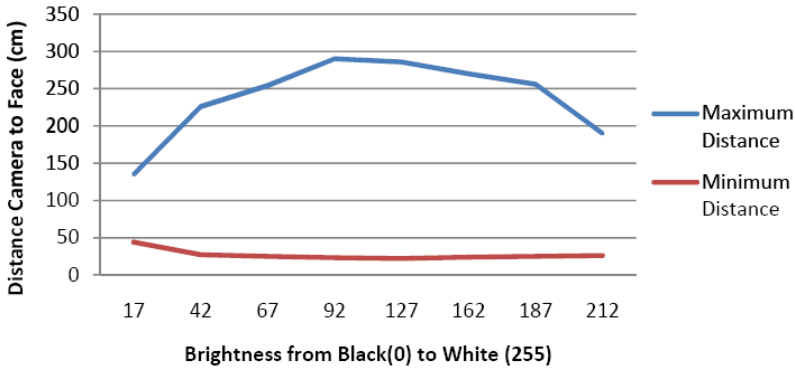


Figure 5: Tests on the efficiency of the algorithm about different illuminations

6.2 Tests on RoboThespian

The code of the face detection has been implemented on RoboThespian to see the compatibility between them. The outputs of the program are coordinates. Using two Colibris located in its head, the robot computes data (the coordinates) coming from the main computer running the program using UDP. Because the transfer of the data takes times, the program is running slower than on a laptop. Besides, the Colibri in the head of the robot has to process the information (the coordinates) into an action.

As seen in Section 4, everything goes through IOServe. It was difficult to change the code in order send the coordinates from the program to IOServe using UDP. Furthermore, the format of the file given by the camera of the robot was not compatible with the files OpenCV can handle. For a future work, the entire code, including the UDP service and conversion of data is owned by Engineered Arts.

The results obtained were good. The robot was situated in the premises of Engineered Arts, which were very bright. Indeed, there are windows on the ceiling which cannot be CACHES and so let enter lots of light. Many tests on the capability of the robot to detect at different distances, brightness or backgrounds were made. RoboThespian was able to detect people until about 2.5meters. Better results were obtained with a black DRAP behind the persons than without. The orientation of the robot was changed in order to vary the illumination of the faces.

The robot is able to follow people if they are in its field of vision. The selection of the biggest face performs well. However, it sometimes loses the face it is tracking. It can be due to the illumination or the speed of the robot. Indeed, the program is real time although the robot is sometimes a bit late. As someone was moving, it sometimes happened that the eyes of the robot were stuck in a position, where the last face was detected, during one second and then the eyes moved again. That was probably more due to the Colibris speed or the time of transfer between the main computer to the robot than the software.

Globally, the program performs well on the robot although it is not perfect.

7 Conclusion

This project gives a contribution for the development of the humanoid robot, RoboThespian™, for an autonomous part.

This paper presented an approach for real-time face detection using computer vision techniques. This system can be very useful in a context of Human-robot interaction. In the environment of a museum where use to be exhibited RoboThespian™, it is able to perceive the presence of a person, and then detect his face in order to track him with the eyes or the head. That gives to the robot the ability to seem more human, which is one of the most important factors of the Human-robot interaction. The algorithm is robust to variations of scale, illumination, pose and noise of the camera.

8 References

Bradski, G. and Kaehler, A. (2008), “Learning OpenCV: Computer Vision with the OpenCV Library”, O'Reilly Media, Inc.

Kidd, P.T. (1992), “Design of human-centred robotic systems in Mansour Rahimi and Waldemar Karwowski” (Eds.) Human Robot Interaction. Taylor and Francis: London. 225-241.

Lienhart, R., and Maydt, J. (2002), “An Extended Set of Haar-like Features for Rapid Object Detection”. In: *IEEE ICIP 2002*, Vol. 1, pp. 900-903.

Rowley, H.A., et al. (1996), “Neural Network-Based Face Detection”. In: Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp. 203-208.

Turk, M. and Pentland, A. (1991), “Eigenfaces for recognition”, *J. Cog. Neurosci.* **3**, 71–86.

Viola, P., and Jones, M.J. (2001), “Rapid Object Detection Using a Boosted Cascade of Simple Features,” *IEEE CVPR*.

Hand-Eye Coordination on a Humanoid Robot: Gaze Control

T.Rodier and P.Culverhouse

Centre for Robotics and Intelligent Systems, University of Plymouth, Plymouth, UK
e-mail: P.Culverhouse@plymouth.ac.uk

Abstract

The development of humanoid robots created a new need in term of interaction with the environment. These robots have to be able to analyze their environment (vision system, different kind of sensors etc...), and then act in consequence (grasping an object, following a target etc...) in a totally autonomous way.

This publication describes the implementation of some algorithm to improve the interaction of a humanoid robot with its environment: a gaze control algorithm and an image stabilization algorithm. They have been implemented and tested on the bunny robot, developed by the University of Plymouth. The results of these tests will be presented at the end of the paper.

Keywords

Humanoid robot, Hand-eye coordination, Image stabilization, Gaze control.

1 Introduction

The purpose of having efficient hand-eye coordination for a robot is to enable it to interact with its environment. Unlike the robots used in industry (on an assembly line for example) which are programmed to do always the same task, the humanoid robots that are dedicated to entertainment have to be able to interact with their environment. This interaction can be split in two parts: the analysis of the environment (vision system) and then the action of the robot due to this analysis (movement of the head, the arms). Coordinating these two things is the objective of the hand-eye coordination project. This particular phase of the project is to control camera gaze.

The hand-eye coordination (i.e. controlling the robot moves with its vision) is something quite new in the robotic world and it is far to be as efficient as the human hand-eye coordination. Indeed, for a long time, the vast majority of the robot population had operated in factories where the environment is adapted to the robot. Because this environment is perfectly controlled, the robot doesn't need applications such as the vision or other sensors. So this is a big area of robotics that has not been very developed, but things are changing. As recently as 1970 and the work of Shirai and Inoue (1973) on controlling a robot position using a visual feedback, people started to work on robot vision control of manipulators. This domain is complex and made more difficult by inaccuracies of servo motors, 'give' in mechanical structures and imprecise estimates of position given by current visual analysis methods. For

example, a paper untitled “A tutorial on visual servo control” (Hutchinson et al, 1996) presents the development of the visual servo control methods from 1973 to 1996.

More recently, other hand-eye coordination projects have given good results. First, the COERSU robot (Jafari and Jarvis, n.d.), which is not a humanoid robot but just hand-eye coordination, permits it to grasp objects. The robot created by Jarvis (2000) is a humanoid robot that interacts with human, and allows it to recognize human gesture and 3-D objects through its camera system. There are other examples of hand-eye coordination for example (Ma and Su, 2003; Hager et al, 1995).

2 The Bunny robot

The Bunny robot is a humanoid robot developed by the University of Plymouth and used by students who studied human-robot interaction. The arms and the legs of the Bunny robot are made with the servos from the Bioloid kit developed by Robotis, but the torso and the head of the robot have been designed and built in-house.

These are the elements that composed the torso (see figure 1):

- A plastic skull, attach to the torso at the level of the neck.
- Eight servos (SuperTec Digital Titch 44) placed in the head.
- Two cameras in the eyes of the robot under X and Y servo control.
- A FPGA board. The FPGA used is an Altera Cyclone III. The FPGA board is the “brain” of the head. It controls all the servos of the head and receives the data from the camera. The Cyclone FPGA is situated on a board, which contains other components such as an X-Y gyro, and the ports connected to the servos.
- Two arms composed of 3 servos Dynamixel AX-12 from Robotis.
- A Colibri board. It has been developed by Toradex and uses Win CE 5.0. It is linked to the FPGA by a 8-bit parallel handshake bus known as the Byte bus. It directly controls the servos of the arms via a RS-485 serial bus. It also received camera video streams from the FPGA.

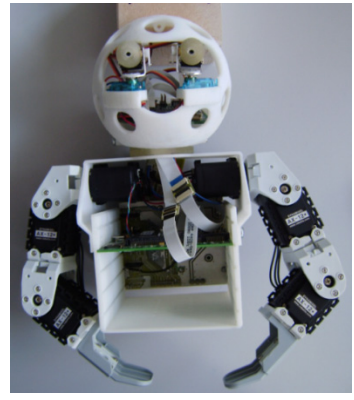


Figure 1: Photo showing torso and skull of the Bunny robot showing one Colibri processor in the torso.

3 Gaze control and image stabilization

3.1 Gaze control

Here, the objective is to use the gyroscope properties of the accelerometer placed on the FPGA board. The gyroscope gives two values in outputs which are proportional to the inclination angle. When the head of the robot moves at the level of the neck, the rest of the head moves with it. In consequence, if the eyes were fixed on a point, because of the movement of the head they will not be staring at the same point. So the objective is to compensate the movement of the head by acting on the eye servos so they will stay focused on the same point. To do so, we just have to take the information about the movement of the head from the gyroscope and to use it to give a new position to the servos of the eyes.

To do so, a hardware description written in VHDL has been implemented on the FPGA to treat the signal from the gyroscope and calculate the corresponding angle, which will indicate the new angle that must be given to the eyes.

3.2 Image stabilization

The cameras (OV7760FSL from Omnivision) stream pixels at a rate of one pixel per 41.6ns. These are organized by column and row. So it is possible to analyse a sub-set of columns to estimate the vertical motion of the camera. Indeed, it is important to consider the possibility of the FPGA in term of memory limitation, so it would not be possible to analyze the whole picture. In consequence, only the columns next to the central column of pixel will be analyzed using a 5x5 patch.

The objective is to take a patch of pixels on the first image from the central columns and then trying to find the equivalent patch on the following image and record its position on the image. Because only vertical translational motions are of interest, only the row will change, so by calculating the difference between the two rows of a patch on two different images, the head motion can be estimated and then servos controlled to compensate for the motion. The comparison between the two images will be implemented by a cross-correlation.

The implementation on the FPGA can be separated in two parts: the processing of the images and their correlation-based comparison.

The interface with the camera had already been designed previously. It processes the signals send by the cameras. These signals are three clocks:

- PCLK, which is the pixel clock frequency (24MHz).
- Vsync, which goes high at the end of each frame. The camera processes 30 frames per second.
- Href, which is high from the first byte to the last byte of a row.

These signals are processed in the ‘SyncProcessor’ block. It gives in output information which is essential to know which pixel of the data is being processed,

with its position (row and column). Having these information will then permit to compare the two images and detect the position of the patch on the image.

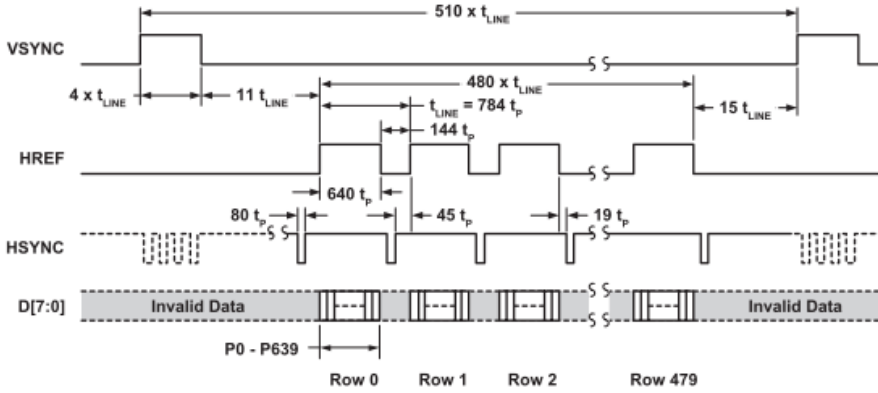


Figure 2: The three signals from the camera

The ‘Uclk’ signal at the output of the ‘SyncProcessor’ block is very important because it is the one which is used to enable most of the process that will permit to analyze the images. ‘Uclk’ reaches the high level for the first chrominance U for each pixel. Indeed, the color information from the camera is YUV encoded, and the correlation will be done on the U channel pixels. This is why the ‘Uclk” signal has been chosen to enable the following processes.

The images will be analyzed using a 5x5 pixels patch. Besides, because the objective is to do image stabilization, two successive pictures have to be processed. The patch of the actual picture has to be compared with the patch of the previous picture. To do this, the patch of the previous picture (time t-1) will always be taken on the same part of the image. By default, that will be in the center of the image so the position of this patch will always be known. The patch is situated in the area analyzed which is between the columns 315 and 320, and is limited in this area between the rows 235 and 240 (see figure 2).

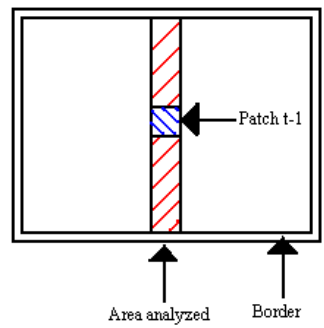


Figure 3: Reference patch

To understand how the images are processed, it is essential to understand what happens at the level of the 'PatchColumnProcessor' block. Because the patch have a size of 5x5 pixels and that two images have to be processed, there are 10 input and 10 output dedicated to this on the 'PatchColumnProcessor' (5 for each image). The pixels from the camera are sent to two inputs of this block so they are processed in parallel. Indeed, because we need two patches, one of the simplest ways is to fill these two patches at the same time, and then to delay one of them so the correlation will always be done between the actual and the previous image.

We will see later than inside this block there are 50 'lpm_dff' functions which represent the 50 pixels that compose both patches (25 each). The principle is that every time a pixel arrives in the block, it goes through 5 'lpm_dff' function and then arrived at the output. They are five rows of five registers; it permits to stock the 25 pixels. Finally it is send back directly in the 'PatchColumnProcessor' in the following input and will follow the same way again, until all the 50 pixels have been processed.

Because there is only a 5 by 5 (25 pixels) patch for an image, it has to be a sub-window of the image in order not to process pixels that are outside the area of interest. As explained before, the area analyzed is just 5 columns of pixels situated in the center of the image, it corresponds to the column from 315 to 320 (the image size is 480x640). The border of the image also will not be analyzed. To do so, there is a block in the VHDL code called 'ControlEnable'. It creates all the signals that will permit to enable the 'PatchColumnProcessor' and its components.

In the following process which is in the 'ControlEnable' block, the Enable signal is set high when the 'ColumnEnable' and 'RowEnable' are high (which means that it is outside the border of the image) and when the column is between 315 and 320. 'UclkEN' is the signal generated by the 'SyncProcessor' block; it is set to one when for the first U of each pixel.

The border of the image which is not analyzed is a 5 pixels border. So the 'RowEnable' signal is high when the value of Row is between 6 and 474, and the 'ColumnEnable' signal is set high when the value of Column is between 6 and 634.

For the reference patch situated in the center of the images, it is activated when the rows are between 235 and 240 and when the columns are between 315 and 320. This signal permits to control the registers which store the pixels of this patch.

There is also a 'PatchEnable' process. The 'PatchEnable' signal is set to one when the two patches for the images have received all the pixels. So at this moment, the comparison between the two patches can begin.

Inside 'PatchColumnProcessor' are five shift registers for each input as can be seen in figure. As with the other shift registers, they are all clocked on 'PIXclk' ('DFF_clk') but only enabled by the Enable signal from the 'ControlEnable' block. It is important to notice that the two groups of 25 registers are not enabled by the same signal.

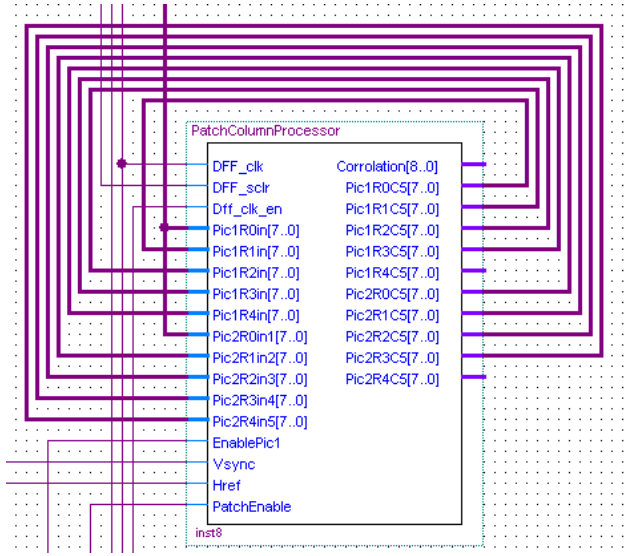


Figure 4: The 'PatchColumnProcessor' block.

There is also a clear signal (‘DFF_sclr’). There are five lines of shift registers like this for each of the pictures, which correspond to a total of 50 registers (see figure 4). The principle of each line is that a pixel goes through it and there is a delay of one clock between each registers. The output of each line is one of the outputs of the block, which is linked to the input of the following line.

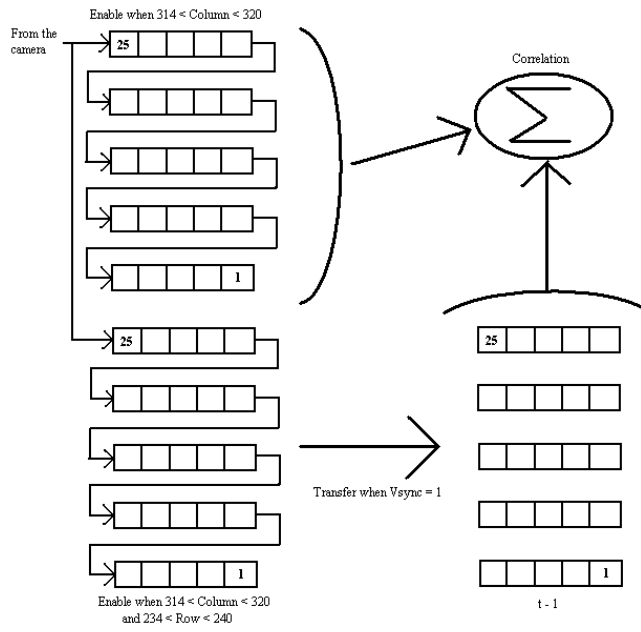


Figure 5: Scheme of the images process.

After all this operations, there are now 50 registers full of pixels, but these are pixels from the same image, and they need to be from two successive images to be compared. That is why there is another group of 25 registers which will store the pixels from the reference patch. It is enabled by the 'Vsync' signal, which means that at the end of each frame, all the pixels from the second group of registers will be loaded in a third group of 25 registers, which will permit to delay them with the new pixels loaded in the first group of registers. To makes these clearer, the following scheme represents the different registers and their interactions (see figure 5).

Here we can see that the correlation is done between the reference patch which contains the pixels from the center of the image and which is delayed by one, and the registers which contain the pixels of a patch situated is the analyzed area. Then, the comparison will permit to find the position of the reference patch on the actual image.

4 Tests and results

The result of the test of the gaze control is good. The tests show that the eyes pitch servos react well to the moves of the head and compensate them. But a simple visual analysis of the result is not enough. By analyzing the signals in the FPGA, interesting information has been revealed. First, there is a very good precision for very small motion of the head, which indicates that the program works properly. But more imprecision appears when the head moves on a larger angle. This comes from a combination of different reasons:

- The mechanical system: the mechanism that controls the eye pitch is quite rigid, so it happens that the action of the servo is not completely reflected on the eye.
- The speed of the servos: the servos are limited to 60 degrees per second. That can have a wrong influence on the whole system, especially in case of fast motion and wide angle.
- The limitation of the gyroscope: the signal send by the gyroscope is not perfect. First, it last 10ms, which imply that there is a certain acquisition time. This acquisition time has to be added with the time for the FPGA to process the signal and act on the servos. Besides, the gyroscope is very sensitive to every move, so it is not really constant even if the robot doesn't move.

The implementation of the vision analysis algorithm presented in the part 3b will permit the Bunny robot to have efficient image stabilization. The gaze control already implemented using the gyroscope gave good result but with a lack of precision. This algorithm is ideal to complete this gaze control and correct the imprecision.

5 Conclusion

The gaze control presents interesting result, and the implementation of the vision algorithm should permit to reach a very good precision.. All the theoretical part and

the implementation had been presented in this research, but there are still more tests to do. This research presents the first step of hand-eye coordination, but much more algorithm and function could be implemented such as feature detection algorithm, or object recognition. The arms could also be used to grasp objects for example.

6 References

Hager, G.D., Chang, W-C. and Morse, A.S., (1995) "Robot hand-eye coordination based on stereo vision", IEEE Control Systems Magazine, 15(1), pp. 30-39.

Hutchinson, S., Hager, G.D. and Corke, P.I., (1996) "A tutorial on visual servo control", IEEE Trans. Robot. Automat. 12 (5).

Jafari, S., and Jarvis, R., (n.d.) "Eye-to-hand coordination: a coarse-calibrated approach".

Jarvis, R., (2000) "Interactive hand-eye coordination between a human and a humanoid", International conference on intelligent robots and systems.

Ma, H. and Su, J., (2003) "Uncalibrated robotic 3-D Hand-eye coordination based on the extended state observer", International Conference on Robotics and Automation, Taipei, September 14-19.

Shirai, Y. and Inoue, H., (1973) "Guiding a robot by visual feedback in assembling tasks", Pattern Recognition, vol. 5, pp. 99-108.

Bipedal Robot: SLAM Pre-Processing

R.Tallonneau and P.Culverhouse

Centre for Robotics and Intelligent Systems, University of Plymouth, Plymouth, UK
e-mail: P.Culverhouse@plymouth.ac.uk

Abstract

Simultaneous Localization And Mapping, or SLAM, is the capacity for a system to create and update a map of the environment while keeping track of its current position in this map. Different sensors can be used in order to extract the information from the environment such as laser range finder or video camera. The information is then processed using a filter in order to estimate the positions of the landmarks and of the camera. This paper presents a set of experiments based on a single camera running on an embedded computer. The state estimation is done by an Extended Kalman filter. The feature initialization is realised using the inverse depth parametrization. Several vision algorithms, including the Shi-Tomasi corner detector and SURF, have been tested and compared.

The software presented is able to map the environment but it is not fast enough to run in real time on the embedded computer. Several optimizations are proposed at the end of the document as guideline for future works.

Keywords

Monocular SLAM, Inverse depth parametrization, Extended Kalman Filter

1 Introduction

The SLAM problem is one of the techniques which will lead to the geographical autonomy of the robots. The first works, for example by Smith et al. (1987), were mostly based on sensors such as laser range finders and sonar. These sensors usually provide a 2D map. The more recent work, for example Lacroix (2006) and Davison et al. (2007), are now based on digital video camera. Much work is currently focused on creating a reliable SLAM algorithm able precisely to map large field of view precisely whilst accurately estimating the position of the camera.

A camera has many advantages compared to the laser range sensor, being cheaper and smaller. They provide much more detailed information and they are similar to the human eyes (Lacroix, 2006). The SLAM is composed of several problems.

The landmark extraction is the detection of key points (the landmarks) in the real world via their projection on the image plane.

The tracking of the landmarks is the recognition of a landmark in several frames. This requires a description of a feature robust to change in scale, orientation and brightness.

The state estimation is the computation of the observations in order to estimate the motion of the camera and he positions of the features. The state estimation can be realised with several methods such as a particle filter and an Extended Kalman Filter. It is assumed that the environment is static, so objects that moves within the field of view add noise features that will contribute to conflicting estimates of the camera.

The solution presented in this paper is based on the Extended Kalman filter described by Davison et al. (2007). Several feature detectors and descriptors have been tested and compared and the position of a landmark is estimated with the inverse depth parametrization (Civera et al. 2008).

2 Features detector

The detection of images features is realised using the Shi-Tomasi detector (Shi and Tomasi, 1994). In addition, these features are also described using the SURF descriptor (Bay *et al.* 2008). The Shi-Tomasi detector gives results really close to the Harris Corner Detector (Harris and Stephens, 1988) used in several successful implementations of Visual SLAM, for example by Davison *et al.* (2007), but it has the advantage to be more robust in rotation.

The matching process to recognize a feature in two images taken at different times is a complex problem. An issue is the Kalman filter, used to estimate the position of the camera as well as the positions of each features, assumes a perfect matching. The matching is realised using the predicted position of the landmarks and the current camera's position: it is assumed that the feature does not move too much between two consecutives frames. Moreover, the response of the detector is used and compared to the previous response. In one set of experiments, the SURF descriptor was used to reject the mismatch, in another image patch correlation was used.

A number of problems are introduced by the vision algorithm, these are:

- non-detection of a detectable landmark
- non matching when the matching is possible
- matching with a bad landmark

The experiments have shown that the matching based on the SURF descriptors can cause mismatching. Moreover, the position of the features is sensitive to the noise and can shift to a near pixel. While this is not important for most of the tracking system, the Kalman Filter can drift and loses its convergence if the errors are too important. In order to make the matching more accurate, a correlation of image patches around the features has been implemented. These patches, with a size of 21 by 21 pixels, give a good convergence of the estimated map. But this solution is slower than the matching based on the SURF descriptor because the correlation has to be done for each pixel in a region close to the position predicted by the Kalman filter.

3 Inverse depth parameterization

A single camera cannot provide directly the distance between the camera and a feature. This depth can only be estimated when the camera moves and the apparent position of the feature is modified.

The 3D coordinates are represented by 6 values:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} + \frac{1}{\rho_i} m(\theta_i, \varphi_i)$$

Being $(x_i\ y_i\ z_i)^T$ the coordinates of the camera when the landmark has been detected, ρ the estimated inverse depth and θ and φ the angles between the camera and the landmark. The initial value given to ρ is responsible for the apparent scale of the map. This value and its associated uncertainty are set to cover the semi-infinite ray in the direction of the landmark by a non-null probability. When the camera moves, the coordinates of the pixel corresponding to the landmarks modify the values (Figure 1). These modifications are calculated by the Kalman filter. Details about the calculations are presented by Civera et al. (2008).

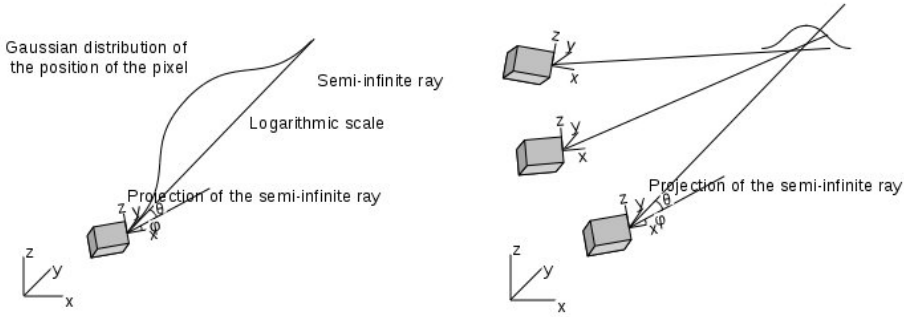


Figure 1: Initial estimation of the position and evolution after several moves

A camera usually suffers distortion due to the lens and to the fabrication process (Azad et al. 2008). Therefore, any point observed by the camera is the projection of the landmark using a non-perfect pin-hole camera and corrections must be applied in order to compensate the distortions. The two-parameter radial distortion model (Mikhail et al. 2001) has been implemented. This method requires the knowledge of the focal length and of the pixel dimensions.

4 Extended Kalman Filter

The estimation of the map is done using an Extended Kalman Filter. An extended Kalman filter is an extension of a classical Kalman Filter in order to handle the non-linear systems (Robertson 2007).

The motion model for the camera is a "constant acceleration, constant velocity" similar to the experiment of Davison et al. (2007). This method handles sharp changes of displacement of the camera as it can occur for a hand-held camera.

The pseudo code below describes the main loop of the algorithm

```
state_vector x;
covariance_matrix P;
while(true){
       frame = grab_new_frame();
       predict_camera_pose(x);
       h = predict_measurment(x);
       y = matching(h, frame);
       update(x, P);
       check_consistency();
       if(sizeof(y) < IDEAL_NB_FEATURE){
              find_new_features();
              add_new_features(x, P);
       }
}
```

The function *check consistency()* has been added to the classical Extended Kalamn filter framework to detect and removes the weak features. A weak feature is a feature detected less than 6 times in the ten frames after its first detection. This procedure is to reduce the size of the state vector and handles moving objects.

5 Experimental results

The software has been written in C using the openCV library (OpenCV n.d.). It has been tested on a laptop running the Debian distribution Linux and on a BeagleBoard (an embedded computer with a 600MHz ARM processor) which is running the GNU/Linux based Angstrom Distribution.

5.1 Experimental setup

A dataset has been created in order to precisely measure the difference between the estimated positions and the real positions. This dataset is a simple translation of the camera in an indoor environment. Moreover, several datasets are available on the Internet, e.g. the datasets of Davison *et al.* (2006) and Civera *et al.* (2006).

5.2 Feature extraction

While the time to process the Shi-Tomasi and the Harris corner detector are smaller than the time to process the image patch correlation, the quality of the results are worst. Indeed, the matching realised by these two methods cannot be based only on the position of the corners because these vary too much. Moreover, using an external descriptor such as the SURF descriptor, does not remove all the problems of matching.

The matching based on the correlation between image patches gives good results. The size of the image patch is directly responsible for the good quality of the matching but is proportional to the processing time.

Another important point is the distribution of the features on the images. The results are better when the features are over all the images. See the Figure 2, for the comparison of the results on the same dataset (Davison *et al.* 2006). This also means that a camera with a big field of view will give better results than with a camera with a low field of view.

Figure 2: Comparison between the Harris Corner detector (left) and the Shi-Tomasi detector (right). The dataset comes from Davison *et al.* (2006)

Only few features are tracked in the image. Experiments have shown that tracking 16 features gives good results while limiting the computational load.

5.3 Depth Estimation

The estimated depth for a feature is modified when the camera moves. The Figure 3 shows the evolution of the estimated depth and the associated uncertainty for two landmarks.

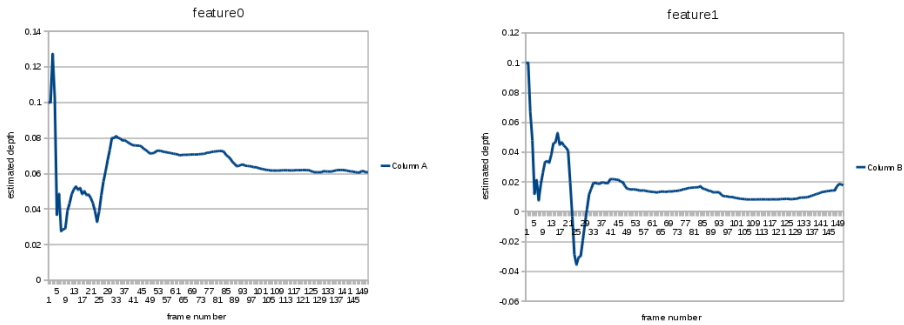


Figure 3: Evolution of the estimated depth for two different features

It is worth noting that the feature can be estimated with a negative depth. Moreover, the link between all the features is visible around the frame 85, when both features are subjected to the same shift.

5.4 Time consideration

The goal of the project is to provide a solution that could fit into a small humanoid robot of about 50cm. The SLAM algorithm therefore could be modified in order to use the information from the robot such as estimated displacement or distance between the robot and a feature using the stereo-vision system. Moreover, such a robot will not have a great speed therefore the differences between the consecutives frames will not be important. But the algorithm must be real time.

The table below shows the time measurement for the main sections of the algorithm. The tests have been realised on a BeagleBoard (2008). This system is based on a 600MHz ARM processor and 128MB RAM. The system runs on Linux Angstrom distribution. These results can be compared to a laptop with an Intel Core 2 Duo 1.5GHz processor running a Debian Linux distribution. The dataset contains 150 images with a resolution of 240 by 320 pixels.

	Laptop	**BeagleBoard**
Shi-Tomasi	16ms	122.7ms
Matching by image patch	Between 30ms and 300ms	Between 500ms and 4s 462
Add new feature (1^{st})	293µs	1770µs
Add new feature (20^{th})	9.236ms	167ms
Update (1^{st})	5ms	91ms
Update (20^{th})	16.5ms	349ms
Prediction (1^{st})	3ms	45ms
Prediction (20^{th})	6ms	192ms
Measurement prediction	4-8ms	20-75ms
Display map	2ms	10ms
Total time (less verbose)	25s 790	5m 38s 29

The times have been measured using the built-in function including in the C standard library.

The time consumed by the matching function is really dependent on the image and on the quality of the estimated depth. The more the apparent displacement is important, the more the time will be important.

The main time consuming processes are the update process and the correlation based matching. It is easy to reduce the time taken by the update process by applying minor modifications to the covariance matrix instead of updating it entirely for each frame.

The correlation is a slow process but can be easily implemented in a FPGA or in the DSP of the BeagleBoard.

5.5 Mapping

The mapping process can be visualised in real time with the software (a 2D top down view only) or with an external Matlab script for a 3D view. The figure 4 shows an example of a map created with the software. The estimated path of the camera is shown by the blue line. In the experiment, the camera moves in a straight line, then rotates around its axis and go back in the direction of its starting position.

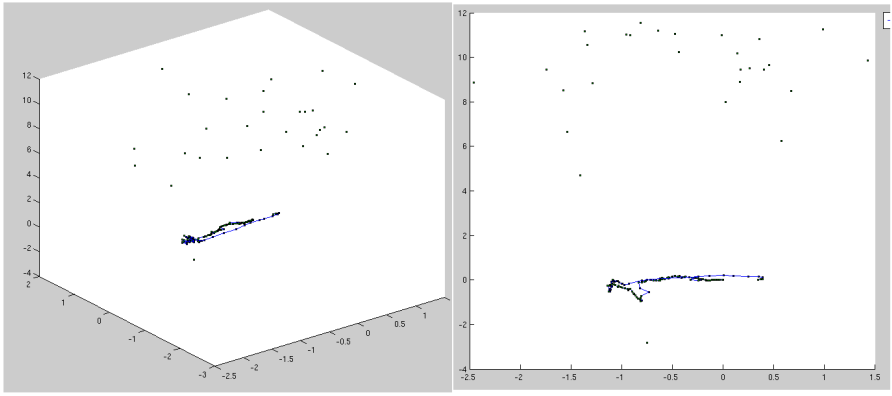


Figure 4: estimated map and path drawn using a Matlab script

6 Conclusion and future work

The solution presented in this paper describes a SLAM pre-processing algorithm. The information given by the algorithm allows extracting landmarks in the world and predicting their positions through several frames. Moreover, it is also able to give an estimation of the displacement of the camera. Because, no pre-defined pattern is used, the map is true to a given scale. The precision of the estimation still have to be measured, while the apparent shape of the world is correct no estimations of the errors between the real world and the calculated one have been assessed as yet.

The main limitation of the algorithm is the time to process. This time increases with the number of landmarks. In order to have a better real time solution, higher order level objects should be tracked. The tracking of a screen for example would require only 1 feature not 4 for example. Moreover, it is possible to create a map composed of several sub-map and work only with the sub-map.

7 References

Azad, P., Gockel, T., Dillmann, R. (2008), *Computer Vision Principles and Practice*, Elektor, 1 edition, 2008.

Bay, H., Ess, A., Tuytelaars, T., Van Gool, L. (2008), "Speeded-Up Robust Features (SURF)", *Computer Vision Image Understanding*, vol. 110, no. 3, pp. 346-359.

Civera, J., Davison, A., Montiel, J.M. (2006), "Slam using monocular vision dataset". Accessed online 23 July 2009. URL: http://www.robots.ox.ac.uk/~SSS06/Website/index.html

Civera, J., Davison, A., Montiel, J.M. (2008), "Inverse depth parametrization for monocular slam.", *Robotics, IEEE Transaction*, vol. 24, no. 5, pp. 932-945.

Davison, A., Reid, I., Molton, N., Stasse, O. (2007), "Monoslam: Real-time single camera slam", *Pattern Analysis and machine Intelligence, IEEE Transaction*, vol. 29, no. 6, pp. 1052-1067.

Harris, C., Stephens, M. (1988), "A combined corner and edge detector", *Proceedings of the Fourth Alvey Vision Conference*, pp. 147-151.

Lacrois, S. (2006), "Cartographie et localisation simultanés par vision en robotique mobile.", PhD Thesis, LAAS/CNRS, Toulouse.

Mikhail, E., Bethel, J., McGlone, J. (2001), "Introduction to modern photogrammetry", New-York, Wiley.

OpenCV (n.d.), Open source computer vision library, accessed online 23 June 2009. http://opencv.willowgarage.com/wiki

Robertson, P. (2007), "Introduction to slam simultaneous localization and mapping", Cognitive Robotics course on MIT, accessed online 25 February 2009. http://ocw.mit.edu/OcwWeb/Aeronautics-and-stronautics/16-412JSpring-2005/LectureNotes/

Shi, J., Tomasi, C. (1994), "Good features to track", *Proceedings of the CVPR'94, Computer vision and Pattern Recognition, IEEE Computer Society Conference,* pp. 593-600.

Smith, R., Self, M. Cheeseman, P. (1987), "Estimating uncertain spatial relationships in robotics.", *Robotics and Automation. Proceedings. 1987 IEEE International Conference*, vol. 4, pp. 167-193.

A Four-Filter Approach to Navigable Space Mapping through Stereo Vision

Z.Y.Woo and G.Bugmann

Centre for Robotics and Intelligent Systems, University of Plymouth, Plymouth, UK
e-mail: G.Bugmann@plymouth.ac.uk

Abstract

This paper presents a working stereo vision system that is able to build a clean occupancy grid map from a noisy disparity map. The system is capable of producing disparity map at least 10 frames per second on an Intel® Duo Core™ 2 Processor with 2.40 GHz laptop. The common disparity noises are the mismatching errors and low light noise on stereo images. Those noises can be eliminated by applying four difference filters. The first and second filter is low pass filter and they are applied to the disparity map and the grid map. Then follow by the third and final filter to clean some obvious random errors on the grid map.

Keywords

Webcam, Dynamic Programming, Navigable Mapping, Stereo Vision.

1 Introduction

The main goal of this project is to allow the robot to identify the amount of free space available in front the stereo cameras. The environment that robot operates can be at indoor, outdoor, unstructured or unknown environment. In order to achieve this, the robot needs to be able to retrieve as many information as possible from the scene.

In most robot navigation application, robot is commonly used at least a sonar transducers or laser range sensors as their main sensors. For example, Lizarralde et al (2003) and Burgard et al (1996) were use odometric and ultrasonic sensors to localise and navigate robot in unknown environment. Another approach in using ordinary sensor for navigation has been carried by Montano et al (1997). It used 3D laser sensor where it was attached and it was able to rotate in order to abstract 3-dimensional information where the system is able to locate object or obstacle. So, it has the ability of avoiding obstacle, self localisation and also building map.

The disadvantages of these sensors are, they are expensive and they are difficult to capture information of the entire scene instantaneously. Also, they are unable to allocate the obstacle boundary or identify the obstacle shape in high resolution. A new approach in overcoming the above disadvantages, some researches had been carry out by using only stereo camera.

Murray and Little (2000) Murray and Jennings (1997) were using Triclops trinocular stereo vision to navigate and explore unknown environment. It used sum of absolute difference (SAD) matching algorithm to obtain environment depth information and

build an occupancy grid map while exploring environment. Murray and Little (2000) presented a number of methods used to filter disparity noise like spike removal on a SAD disparity map.

In this project, we used stereo vision to plot an occupancy grid map where the map will includes the shape like the wall, obstacle and corners. Beside this, it is also able to detect any hole on the floor or objects below the floor level. The grid map will clearly illustrate the free navigable space based on the above specifications.

This paper is organised as follows: Section 2 describes the architecture of our system like the properties of the webcams. After an overview of the system, Section 3 briefly describe the stereo calibration, rectification and matching. Then Section 4 describes how the system converts 2D data to 3D and plot into top-down view map and grid map. In Section 5 describes the four different filters used to filter the disparity noise. Finally the section 6 contains the conclusion and future work on this project.

2 The System Architecture

We used two Logitech® Pro 5000 webcams as our stereo cameras and a laptop with built-in Intel® Duo Core™ 2 Processor at speed of 2.4GHz. A TP-2100 CAMLINK tripod with 3-way pan head is used mainly to hold the stereo cameras but it is also useful in providing a good adjustment on the cameras head angle. A special made housing was build to hold both cameras firmly to ensure they are always separated by 70mm. Figure 1(a) shows the final build housing with both webcams installed. The Logitech® Pro 5000 has focal length and the horizontal VoF of this camera are 3.7 mm and 51° respectively. Finally our programme is written in C++ and we had implemented OpenCV (Source Forge, 2009) library as our image processing tool.

3 Stereo Calibration, Rectification and Stereo Matching

The stereo calibration and rectification must be carried out before applying stereo matching on stereo images. This process is mainly used to identify the intrinsic and extrinsic parameters of the two cameras. In our system we used a 7x5 square chessboard which was printed on A4 paper and we used OpenCV's calibration library, *CvCalibFilter* to calibrate our stereo cameras. A number of guidance was found from MontiVision Image Technologies (2009) on how to correctly calibrate both cameras. We had decided to set the calibration to take up to 25 different perspective views on the chessboard in order to minimise the calibration errors.

We had chosen cvFindStereoCorrespondence() library as our stereo matching algorithm from OpenCV. The algorithm is capable of producing minimum of 10 frames disparity map per second at resolution of 320x240 pixels on our laptop. It is using effective dynamic programming strategy to compute the disparity map and it also has unique ability in handling untexture objects, occlusion and precisely preserve object's shape. Without these abilities we are unable to produce good disparity map in unknown environment.

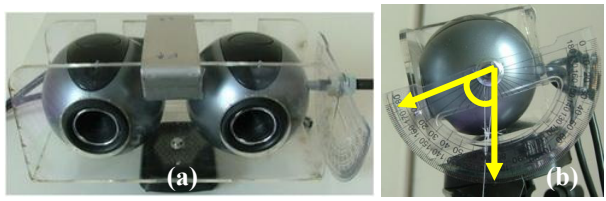


Figure 1: (a) The stereo cameras housing (b) Measuring head angle using protractor

Figure 2: Disparity map of a basket with high texture floor and low texture wall.

Figure 2 shows two images: left image is the source image capture by left webcam where the right image is the disparity map base on the left image. According to the disparity map, the matching algorithm had done a good job in handling large amount of untexture wall and preserve the shape of the basket.

4 3D Scene Reconstruction: The Occupancy Grid Map

Parameters	Description	Symbol	Units
Focal Length	Both cameras should have similar focal length	f	Millimetre
View of Field(VoF)	Horizontal axis view angle	θ_h	Degree
Base Distance	Distance separated by two cameras	b	Millimetre
Image Width	Width of Left Image Resolution	W	Pixel
Cameras Head Angle	The angle between the camera stand and principle line	α	Degree
Cameras Height	The height from ground to cameras	H	Millimetre

Table 1: 3D Reconstruction Parameters

To plot occupancy grid map, we need to transform the 2D data captured by stereo cameras into 3D coordinate. Therefore, the disparity map is needed to find the depth distance on each pixel. The depth distance always measure from the camera head directly to object point because the depth, Z is always parallel to principle ray of left camera. In some situation, we need the head angle vary between 70° to 90° and the depth distance will be different. So, we had created universal equations that handle different head angle. Table 2 included all equations from finding the initial depth, actual depth, height and width on each object's point. Some of the important parameters terms are define in Table 1. The focal length is 3.7mm, horizontal view angle is 51°, base distance is 70mm and the head angle is measured by the protractor which is attached on the left webcam.

The occupancy grid map will consists of three difference colours where they are indicating three difference objects. The black colour represents obstacle either above or below ground and white colour represents free navigable space. Lastly, the grey colour represents the obstacle continuity hypothesis.

Head Angle, α	Range from 70° to 90°
Vertical Angle, β	$\left(\frac{image_{height}}{2} - Pixel_{coord}\right) \cdot Pixel_{angle}$
Depth from Camera, Z	$z = \frac{b \cdot f}{d \cdot \lambda} \quad where\ \lambda = \frac{2 \cdot f \cdot \tan\left(\frac{\theta_h}{2}\right)}{w}$
Virtual depth base on β and Z'	$Z' = \frac{Z}{\cos(\beta)}$
Distance between object & camera base, Z''	$Z'' = Z' \cos(90° - (\alpha + \beta))$
Object Height, h	$h = H - Z'' \tan(90° - (\alpha + \beta))$
Horizontal Angle, γ	$\left\lvert\left(\frac{image_{width}}{2} - Pixel_{coord}\right) \cdot Pixel_{angle}\right\rvert$
Width, x	$z \cdot \tan(\gamma)$

Table 2: 3D Reconstruction Equation

5 The Four Filters Algorithm

In order to plot a clean and reliable grid map, we had design four unique filters to eliminate unreliable noise from disparity map. The first filter used in the disparity map is mainly to eliminate pixel with inconsistence disparity value. Where the other three filters are used to filter any obvious and inconsistence obstacle points appear in the grid map.

5.1 Low Pass Filter on Disparity Map

This filter reads the disparity value on each pixel to compute the *Logic(t)* used in Equation 1. The following rules are used to determine the *Logic(t)*:

Current disparity value at coordinate$_{ij}$ ≠ Previous disparity value at (i, j) Then,
***Logic(t)** = 1 otherwise **Logic(t)** = 0.*

$$reliabilityDisp_{ij}(t) = \alpha_c \cdot reliabilityDisp_{ij}(t-1) + (1 - \alpha_c) \cdot Logic(t) \quad \textbf{(1)}$$

where coefficient, $\alpha_c = 0.9$

Then the logic is feed into Equation 1, and the *reliabilityDisp$_{ij}$(t)* of each pixel will update overtime. If particular pixel value vary over time then the *reliabilityDisp$_{ij}$(t)* value will become smaller. Figure 3 shows the behaviour of a low pass filter. According to the figure, the *reliability$_{ij}$* value is higher when disparity value at coordinate$_{ij}$ is constant at 70% of the time. A threshold of 0.9 is applied to filter any pixel with *reliabilityDisp$_{ij}$(t)* less than the threshold. So, those unreliable pixels along

the edge of the disparity map as shown in Figure 2 will be filtered. Figure 4(b) shows the result of a grid map after applying this filter.

5.2 Low Pass Filter on Grid Map

The second filter is applies on the grid map where it uses exactly the same equation as Equation 1 and same coefficient but it used difference rules. The concept of the second filter is similar to the first filter but instead of detecting the value changes, we used obstacle and non-obstacle appearance to determine the *Logic(t)*. The rules are:

Grid Map value at coordinate$_{ij}$ = ***obstacle*** *then* ***Logic(t) = 1*** *otherwise* ***Logic(t) = 0***

$$reliabilityGrid_{ij}(t) = \alpha_c \cdot reliabilityGrid_{ij}(t-1) + (1-\alpha_c) \cdot Logic(t) \quad (2)$$

Again, same threshold of 0.9 is applied to filter those unreliable pixels. Figure 3 shows if the pixel changes too often (duty cycle = 30) then the *reliabilityGrid*$_{ij}$ is smaller compare to those stable pixels (duty cycle = 70%). So, the *reliabilityGrid*$_{ij}$ is useful to effectively eliminate those unreliable pixels whiles plotting the grid map. Figure (c) shows the result of a grid map after applying this filter.

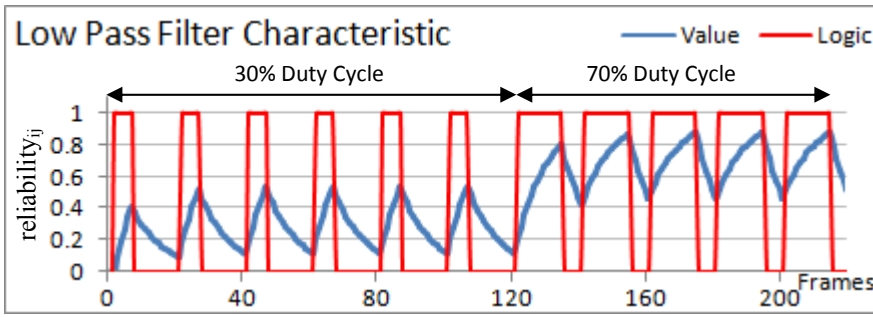


Figure 3: Low Pass Filter Output behaviour at 30% and 70% Duty Cycle over frames

5.3 Pixel based Filter

After applying the above filters, the grid map still contains some random flashing noise. This noise had some common patterns like they are normally appear to be away from other groups of points (when head angle is less than 90°) or they are normally surrounded by small amount of 'neighbour' points. These 'neighbour' points are most likely to be shorter (either 2 to 3 pixels horizontally).

According to the above observations, we can delete any obstacle point which it is connected to only one or two obstacle point along horizontal line. For those deleted obstacle points, they will received a *Logic(t)* = 0 and their *reliabilityGrid*$_{ij}$ value will be updated by Equation 2. As a result, their *reliabilityGrid*$_{ij}$ values are becoming smaller over time and they can be filtered by the grid map threshold (Refer to Second Filter).

This filter produces better result on a grid map with head angle at 90°. This is because the noises in grid map with less than 90° head angle has difference patterns. So, another filter in needed on difference grid map. Figure 4(a) shows a grid map after applying this filter and the result looks clean with a clear navigable path between two obstacles. Figure 4(d) shows the result of a grid map at head angle less than 90° after using this filter. The result show it is not as clean as Figure 4(e) which it is using window based filter (Describe on next section).

5.4 Window based Filter

The third filter used to filter points that those noise are spread in randomly with low concentration among them. This filter is more suitable when cameras head angle is less than 90° because obstacle points are normally diffuse with high concentration due to the disparity map discrete effect. So, we had introduced a fix window with a size of 5x7 (height x width) and a threshold of minimum of (*window's width – 2)* neighbour obstacle points. The rules that the filter used are:

(1) *If any obstacle point falls on the boundary of the window, no action is taken on pixels lied along middle row.*

(2) *If found neighbour obstacle points <= window's width – 2, then apply Equation 2 with* ***Logic = 0*** *on the pixels along middle row of the window* and overwrite those obstacle points as ground point.

The window starts scanning from the top left grid map. On each scan, it will carry the above rules and actions. When it is done, the window will move one column to right for next scanning. It will stop until end of the grid map. Figure 4(e) shows the final result of the grid map after applying first, second and fourth filter.

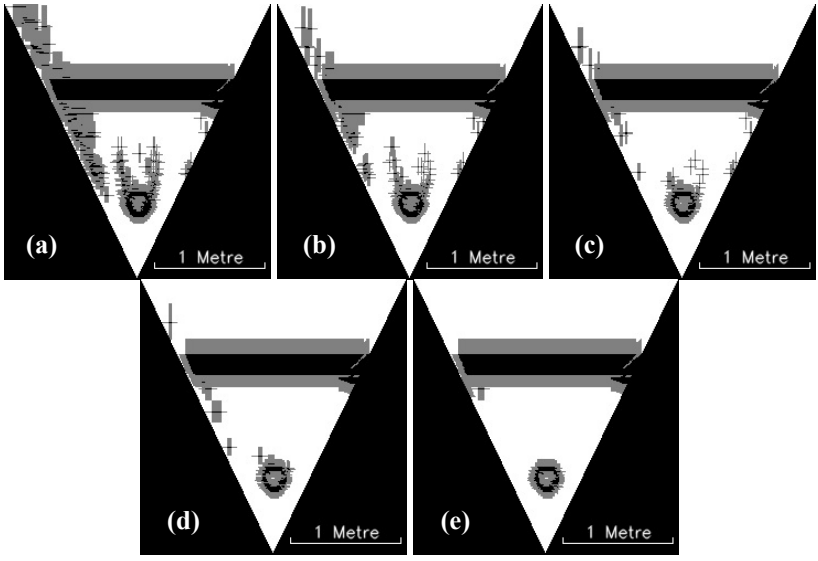


Figure 4: Filtering Grid Map through Four Difference Filter Stages

Figure shows the grid map when head angle is at 70° and it shows the result after difference filter is used. Figure 4(a) shows the grid map without any filter. Figure 4(b) shows the result after applying the first filter on disparity map then Figure 4(c) shows the grid map after applying first and second filter and most noisy obstacle were being removed. Then we apply either pixel-based or window-based filter to eliminate remaining noise on the Figure 4(c). Figure 4(d) shows the grid map after applying pixel-based filter and Figure 4(e) used window-based filter. By comparing result in (d) and (e), it shows that when using window-based filter on this grid map produce cleaner and reliable result.

5.5 Improving Grid Map

A clean grid map is obtained but some improvement is required on the map in order to accurately present a navigable space to a robot. The improvements are applying a boundary of 50mm on any obstacle points and implement the obstacle continuity hypothesis. The obstacle continuity is recalculated by adding ± 0.5 disparity value then plot a gray colour on the grid map. Two final grid maps are shown in Figure 5. In Figure 5(a) it uses first, second and third filter and it shows a clear path between the brown cupboard and the bed. Figure 5(b) uses first, second and fourth filter. It shows a slanted shape of a rectangular box and the wall behind the box also clearly display in the map. We had set a height threshold to filter out height's error caused by the discrete effect from disparity map. So any points below 50mm and higher than -50mm are eliminated and they will not be plotted on the gird map.

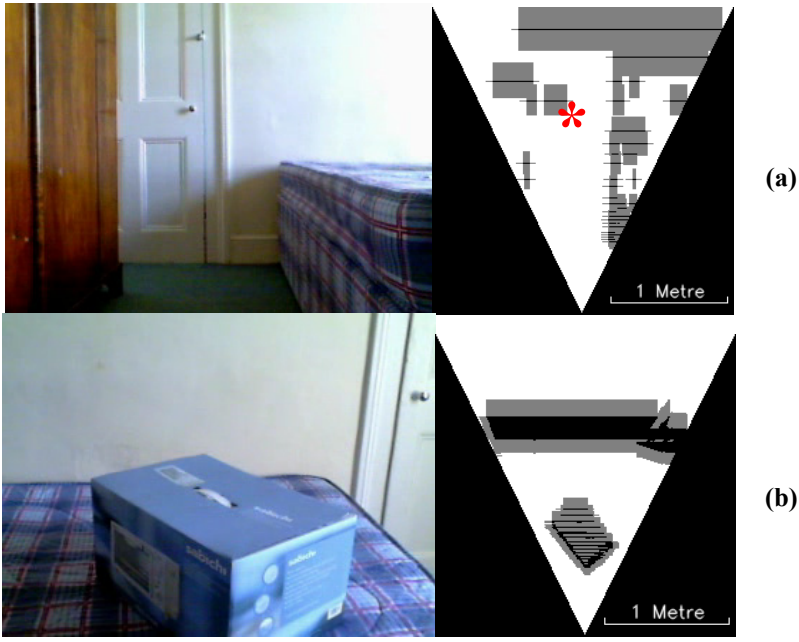


Figure 5: (a) Grid Map with Head Angle at 90° (b) Grid Map with Head Angle 70°

5.6 Discussion

Two grid maps shown in Figure 5 had illustrated the two difference patterns map. We noticed the grid map with head angle at 70° have many points concentrated around other horizontal line and formed the shape of the box. This is because of the discrete effect on the disparity map. The top grid map shows noisier than bottom grid map. This is mainly due to the quality of the disparity map. In Figure 5(b) there is large high texture background under the box and this reduced the mismatch error in the disparity map. Besides Figure 5(a) has large amount of untexture background that it increases the potential of mismatching errors especially on the floor surface. The top grid map does show a small error which it is found near to the wall and mark as red * where it should be a free navigable space.

6 Conclusion and Future Work

In high texture environment, our filters' algorithm works well in filtering out noisy disparity value but it is difficult to remove large amount of mismatching noise when it is in low texture environment like Figure 5(a).

Due to the time limitation, there are a number of challenging tasks needed to be carried out in future. The first challenge is the difficulty of the robot operates in low texture environment. Even thought, current matching algorithm is able to handle untexture objects but the disparity map remain many invalid and unreliable random flashing disparity value on the disparity map.

The second difficulty is where the system is unable to plot a reliable grid map from a long range view especially corridor with large untexture wall. Due to the untexture issue, the disparity map become discrete value along the walls. Therefore we are unable to accurately plot the actual wall position and fail to recognise the structure of the building.

7 References

Burgard, W. Fox, D., Hennig, D. and Schmidt, T. (1996). Estimating the absolute position of a mobile robot using position probability grids. *In Proceedings of the Thirteenth National Conference on Artificial Intelligence*, Menlo Park

Lizarralde, F., Nunes, E.V.L., Liu Hsu and Wen, J.T. (2003). Mobile robot navigation using sensor fusion. *Robotics and Automation, 2003. Proceedings. ICRA '03. IEEE International Conference on*, vol. 1, pp. 458- 463.

Montano, L. and Asensio, J.R. (1997) Real-time robot navigation in unstructured environments using a 3D laser rangefinder, *Intelligent Robots and Systems. IROS '97., Proceedings of the 1997 IEEE/RSJ International Conference on* , vol.2, pp.526-532

MontiVision Image Technologies, (2009). *MontiVision DirectShow SDK Documentation: How to Calibrate / Undistort a Camera.* [Online] [Available at: http://www.montivision.com/support/documentation/frames/index.html?page=source%2Fhowto%2Fhow_to_calibrate_camera.htm]

Murray, D., Jennings, C., (1997). Stereo vision based mapping and navigation for mobile robots, *Robotics and Automation, Proceedings., 1997 IEEE International Conference on*, vol.2, pp.1694-1699.

Murray, D. and Little, J., (2000). Using Real-Time Stereo Vision for Mobile Robot Navigation. *Autonomous Robots*, Vol. 8, No. 2, pp. 161–171.

Source Forge, (2009). *Open Computer Vision Library.* [Online] [Available at: http://sourceforge.net/projects/opencvlibrary/] [Accessed: 10th February 2009].

Section 4

Computing, Communications Engineering and Signal Processing & Interactive Intelligent Systems

A HOX Gene Developmental System for Evolutionary Robotics

S.V.Adams and M.Beck

School of Computing, Communications and Electronics, University of Plymouth
e-mail: M.Beck@plymouth.ac.uk

Abstract

In Evolutionary Robotics, Developmental Systems can be used to facilitate a more complex mapping between the genotype and phenotype as they aim to mimic the biological processes of embryological development and growth. This paper describes the development of a new developmental system based upon Hox gene theory which is self-contained but also intended for use in a full evolutionary system. The biological rationale for the Hox model, its implementation using the Growth Grammar software application GroImp and the results of experimentation with the model are described and show that a variety of insect-like morphologies can be generated with only a few changes to the model parameters.

Keywords

Artificial Embryogeny, Developmental System, Evolutionary Robotics, Hox genes, GroImp.

1 Introduction

An important aim in Evolutionary Robotics (ER) is to create more biologically plausible agents with greater adaptive capabilities. However, increasing the complexity of evolved agents to achieve this may mean that there is a greater computational overhead in generating them. Evolving a more biologically realistic agent body and brain (phenotype) requires a more complex genetic representation (genotype) if there is to be a direct mapping from elements in the genotype to features in the phenotype. Using an indirect mapping such as a process that mimics embryological development and growth is one solution to this. Such a process can be designed to incorporate principles seen in nature to specifically facilitate the evolvability and adaptive capabilities of the agents. ER has already made use of developmental systems and many researchers such as Sims (1994a, 1994b), Bongard and Pfeifer (2001), Hornby and Pollack (2002) and Hornby et al. (2003) have found that such processes can enhance the evolvability and performance of agents.

A key aim of the current work has been to develop a novel software system for 'growing' the morphology of simulated robotic agents which incorporates principles from recent thinking in the field of Evolutionary Developmental Biology, in particular Hox gene biology. Over the last few decades research has shown that 'Homeobox' or 'Hox' genes, a relatively small subset of the genome common to all animal species plays a fundamental role in the early development of the embryo and

the resulting animal morphology. Changes in the number and genetic regulation of Hox genes almost certainly play a part in the changing complexity and diversity of animal forms over evolutionary timescales (Carroll et al., 2001). These genes are highly conserved by evolution and exist in the genomes of all animals despite the wide variety of seemingly unrelated forms.

The relevance of Hox genes to ER is not a new idea: some researchers have already acknowledged their key role in morphological development processes (Lund et al., 1997; Bongard, 2002; Stanley and Miikkulainen, 2003) but as far as this author is aware there have not yet been any attempts to directly model Hox genes in an ER research project. There is a wealth of material available from the Developmental Biology literature which can be used to develop abstracted models that are suitable for implementation in a computer simulation.

Section 2 of this paper describes the biological principles behind the Hox model and its implementation as a GroImp Relational Growth Grammar program. Selected results from experimentation with the model parameters are presented in Section 3 and the paper concludes with a brief assessment of the model and its potential use for future ER work.

2 The Hox Developmental Model

2.1 Key Biological Principles

The model is based on the fundamental developmental processes of the fruit fly, *Drosophila Melanogaster* and has been specifically designed to generate biomimetic insect-like body plans. In order to simplify the complex biological detail for implementation, three key aspects were selected:

2.1.1 Establishing the Body Axis

The first stages of *Drosophila* development include the establishment of the Anterior(head)-Posterior(tail) or A/P body axis. This phase is not initiated by Hox genes, but is controlled by 'maternal' genes (from the maternal genome only) and their gene products. The genes interact via a Genetic Regulatory Network (GRN) and set in motion subsequent processes which cause Hox expression.

Three maternal genes are known to be key players in establishing the A/P axis: The **caudal** gene expresses a gene product (**cd**) which is expressed uniformly in the developing embryo. The **bicoid** gene product (**bcd**) is expressed initially at the anterior end only and the **nanos** gene product (**nan**) is expressed initially at the posterior end only. As the gene products diffuse **bcd** represses the **caudal** gene and causes an A to P gradient of the **cd** gene product. The gene product **nan,** also has a repressing effect on the **bicoid** gene which reinforces the gradient of **cd** from P to A. The concentration gradients thus impose a sense of direction on the developing body axis.

2.1.2 Development of a Segmented Body by 'Zones' of Hox Expression

The early experimental work of Lewis (1978) established that Hox genes play an important role in constructing the body plan in *Drosophila*. Lewis found that Hox genes exhibited **colinearity**: the order of the genes on the chromosome corresponded exactly with their spatial expression in the A/P axis in the developing embryo. Figure 1 illustrates this and shows the *Drosophila* 'HOM-C' homeobox gene cluster along the bottom of the diagram with each gene represented as a shaded square.

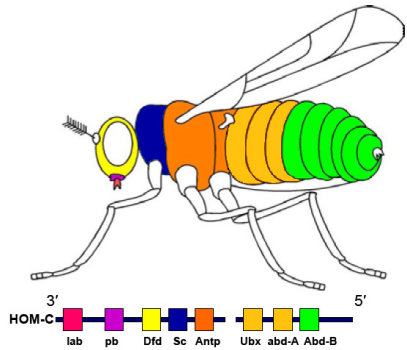


Figure 1 – Hox gene expression in Drosophila Melanogaster (Adapted from Fig 2.Lappin et al.,2006)

The top part of the diagram shows the areas of corresponding gene expression along the *Drosophila* body axis. This Hox 'ground plan' controls the type of body segments that develop as well as later appendage development.

2.1.3 Limb Development

Once the body axis and ground plan have been laid down, limb position and number can be determined. Essentially the effects of Hox 'selector' genes which have been expressed in a particular segment in the ground plan (as in Fig. 1) combined with positional information from the body axis controls whether or not appendages develop in that segment and also what type they will become. A non-Hox gene **distal-less** is expressed in the ventral (lower) parts of all body segments and is required for proper limb development. The action of selector Hox genes **Ubx** (Ultrabithorax) and **Abd-A** (Abdominal-A) repress **distal-less** and therefore only allow limb development on the anterior part of the thorax: note that the body areas corresponding to **Ubx** and **Abd-A** in Figure 1 show no limbs.

2.2 Characteristics of the Developmental System

Stanley and Miikkulainen (2003) coined the term 'Artificial Embryogeny' (AE) to describe the study and creation of artificial developmental systems and their review describes possible approaches which range from biologically detailed up to high-level abstracted representations. A high-level grammar based AE approach was selected for the current work: the proposed developmental system was not intended

solely for the purpose of studying biological systems, but instead to be integrated into a larger evolutionary system for evolving and studying robotic agents. Furthermore, the biological processes under consideration are fairly new in their application to Evolutionary Robotics; therefore too much detail at this stage would have been a hindrance to identifying and applying the key principles.

Many previous works in ER have used approaches where the developmental system rules are evolved (Bongard and Pfeifer, 2001; Hornby and Pollack, 2002; Hornby et al., 2003). In the current work the developmental system itself is not evolved but has been designed so it can be incorporated into an evolutionary system. Development paths in the model do not change, for instance, always the same genes interacting with each other in the same way. However, the model also has a level of indirection: the effect of the gene interactions are controlled by levels of transcription factors (gene products) which are controlled by parameters passed to the GRN rules, and these values *can* potentially be evolved.

2.3 Implementation

For the current work the open-source modelling package GroImp (BTU Cottbus Website, 2008) was chosen as the implementation platform. Although GroImp was originally designed for plant modelling, it has also been used for some ALife applications (Kniemeyer et al., 2004). GroImp implements the concept of Relational Growth Grammars (RGG) which are essentially extended L-Systems. RGGs further extend the basic 'string' grammar rewriting capabilities of traditional L-Systems to graphs, thus allowing for more complex models of development.

The methodology for creating the RGG Genetic Regulatory Network structure is based upon the principles used in the example code 'ABC of plant morphogenesis' provided with the GroImp software (Kniemeyer et al., 2004) and has been adapted to model the biological principles described in Section 2.1.

2.3.1 The GRN RGG Implementation

RGG programs are Object-Oriented, therefore elements of the GRN and relationships between them are modelled as objects, or 'modules' in RGG terminology. The objects in the developmental system implementation are as follows:

2.3.2 Gene

This object represents a generic gene, and is associated with one parameter, the gene Activity (base level of production of its transcription factor).

2.3.3 Factor

This represents a generic gene transcription factor and is associated with two parameters: the initial concentration of the transcription factor and the decay rate.

2.3.4 Activates

This is a special object which represents an interaction between a gene and a transcription factor. It has two parameters: The Specificity (affinity) between the factor and a target gene, and the Maximum Activation Rate of the interaction. Although this object is called Activates it can represent activation (positive value for Maximum Activation Rate) or repression (negative Maximum Activation Rate) interactions.

2.3.5 Somite

Represents an undifferentiated body segment, and takes one parameter: the type of segment it will develop into.

2.3.6 Body

Represents the entire 'body plan'. This object takes no parameters, but forms the highest level in the developmental hierarchy to which Somites are attached as they develop.

There are two other elements in the RGG program which are not strictly objects as they represent informational relationships in the GRN and do not take any parameters. This type of element is called an 'edge' in RGG terminology:

Encodes – represents the association between a gene and the transcription factor it produces.

Factors – represents the entire collection of transcription factors in the network.

The GRN is initialised by means of an **Axiom** statement. This has the same function as in an L-System: it is the starting 'rule' or conditions upon which subsequent rules operate. Figure 2 shows the RGG code implementing the Axiom statement for the model in this work. The RGG code sets up a model of the three maternal Genes which control body axis development: **caudal**, **bicoid** and **nanos**, and their respective gene Factors **cd**, **bcd** and **nan**. Rules are also set up which govern the gene interactions: each gene product activates its own gene; **bcd** and **nan** repress the **caudal** gene and **nan** represses the **bicoid** gene. In the case of limb development a more simplified gene model than the true *Drosophila* case is used. The **distal** gene product (**dll**), as in its biological counterpart, controls whether limbs are developed or not. The **abda** and **abdb** genes and their products fulfil the role of Hox selector genes and help modulate limb development in body segments.

As the RGG program is run, the GRN develops and the relative concentrations of the maternal gene products change due to a combination of processes represented by other RGG rules: continued expression of a factor by its parent gene, activation/repression of a gene by other gene factors and decay of gene factors.

Gradients of the various gene products are established over time and new body segments are created according to the current gene product concentrations, thus creating a 'virtual' Anterior/Posterior axis.

A primordial Somite can develop into one of three types of segment, **ROST** (for the Rostral or head end), **ABDA** (middle abdomen) or **ABDB** (tail end). A **ROST** segment is always created first in the body plan and initialises the GRN with the set of gene factors as shown by the last line of the Axiom statement in Figure 2.

When a new Somite is created during growth, its type is determined by the gene Factor concentrations at the time of creation using a simple set of conditional statements:

```
IF nan > 120)  THEN TERMINATE
IF bcd > cd  AND  cd > nan  THEN  ROST
IF cd > nan  AND  cd > bcd  THEN  ABDA
IF nan > cd  AND  cd > bcd  THEN  ABDB ELSE ABDA
```

These rules are a loose interpretation of the principles of development seen in *Drosophila* but are considerably simplified from the true situation which involves many more Hox and non-Hox genes which interact to determine body segment type. A 'termination' condition which is used to stop development has been incorporated but this has no direct analogue in the actual biological processes.

```
Axiom ==>>
        // Create the three maternal Genes and their Factors:

        caudal:Gene(0.1) -encodes-> cd:Factor(2, 0.001),
        bicoid:Gene(0.00000001) -encodes-> bcd:Factor(30, 0.5),
        nanos:Gene(0.00000001) -encodes-> nan:Factor(2, 0.0005),

        // Set initial Activation/repression of genes by factors:

        cd -Activates(0.000000001, 50)-> caudal,
        bcd -Activates(50, -100)-> caudal,
        nan -Activates(50, -50)-> caudal,

        bcd -Activates(0.0003, 50)-> bicoid,
        nan -Activates(80, -5000)-> bicoid,
        nan -Activates(10, 50)-> nanos,

        // Create the three Genes controlling limb development

        distal:Gene(0.1) -encodes-> dll:Factor(50,0.1),
        abda:Gene(0.1) -encodes-> aa:Factor(30,0.5),
        abdb:Gene(0.1) -encodes-> ab:Factor(20,0.0005),

        dll -Activates(10,10)-> distal,
        aa -Activates(10, 30)-> abda,
        ab -Activates(10, 10)-> abdb,

        // Create the initial body plan

        ^ Body Somite(ROST) [-factors-> cd bcd nan dll aa ab] ;
```

Figure 2 – The RGG Axiom for the Hox GRN Model

The presence of the **distal** gene product, **dll** is required for proper limb outgrowth and the factors produced by pseudo Hox genes **abda** and **abdb** (**aa** and **ab**) control limb type. As the body axis develops over time gradients of the limb gene products are also established and limbs are developed and classified as fore and hind limbs according to two simple rules which are very much simplified from the true *Drosophila* processes.

```
IF aa < dll  AND  ab < aa  THEN  FORELIMB = TRUE ELSE FORELIMB = FALSE
IF ab < dll  AND  aa > ab  THEN  HINDLIMB = TRUE ELSE HINDLIMB = FALSE
```

As in a true Hox ground plan, segment type also controls limb development. **ROST** segments cannot develop limbs, only fore limbs develop on **ABDA** segments and hind limbs on **ABDB** segments. Although the number of segments, and thus, limbs can be variable, the boundaries delineating where fore and hind limbs can start are preserved. Depending on the relative gene product concentrations limbs may be absent on some or even all segments.

3 Testing and Results

The Hox developmental model was tested by investigating the effect of changing selected GRN parameters of some genes and observing what effect this had on the resulting morphology. Of particular interest was how much change at the genotypic level was necessary to cause a significant change in the phenotype as this would give an indication of the potential diversity that could be generated if the developmental model was incorporated into an evolutionary system. The 'baseline' set of parameters is as shown in the RGG code of Figure 2.

Changes were then made to only one or two of the parameters at a time and the resulting change in limb morphology was noted. Figure 3 shows the baseline morphology (3a) and the results of three tests (3b-d).

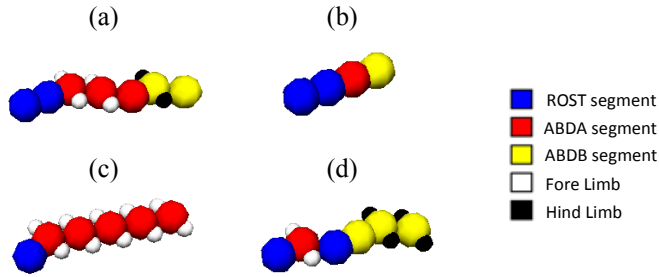


Figure 3 – Examples of morphology changes during testing

3.1 Repressed Development

Altering the behaviour of the **nanos** gene by increasing the initial concentration of the **nan** Factor from 1.0 to 3.0 and reducing the **nanos** termination concentration from 120.0 to 70.0 has the effect of truncating the development of the body axis

as shown by Figure 3b. In this test the initial concentration of the **dll** factor was also reduced from 50.0 to 30.0 and represses limb development completely.

3.2 Enhanced Development

Increasing the starting concentration for the **caudal** gene Factor **cd** by a large amount from 12.0 to 70.0 and also increasing the **nanos** termination concentration from 120.0 to 150.0 has the effect of enhancing the development of the mid-axis **ABDA** segments as shown in Figure 3c. Additionally, increasing the starting concentration of the **dll** factor from 50.0 to 70.0 and increasing the decay rate of the **ab** factor from 0.0005 to 0.5 results in limb development on all segments apart from ROST segments where limb development is not allowed.

3.3 Disrupted development

Figure 3d shows the effect of increasing the starting concentration of the **nan** gene Factor from 1.0 to 2.0 and decreasing the starting concentration of the **cd** gene product from 12.0 to 2.0. This results in segments generated in an incorrect order at the anterior end. Also, extra **ABDB** segments have been generated.

4 Conclusions and Future Work

This work has shown that the proposed Hox developmental model has been successfully created as an RGG program within the GroImp application. Using the features of GroImp meant that it was relatively straightforward to take a simplified, yet biologically plausible abstraction of some of the key processes of early *Drosophila* development and code them in a software model which could be used for exploring these principles. Experimentation with the GRN parameters showed it was possible to generate a variety of different combinations of body segments and limb arrangements with a few parameter changes. The values of the gene parameters for the regulatory network were determined and modified in a somewhat empirical fashion, so for the Hox model to be of practical use to Evolutionary Robotics an obvious direction for future work is for the genes and their parameters to be encoded in a simple genome and evolved using a genetic algorithm before passing into the RGG regulatory network to generate morphology.

5 References

Bongard, J. C. (2002) 'Evolving Modular Genetic Regulatory Networks' in: *Proceedings of the 2002 Congress on Evolutionary Computation (CEC2002)*, IEEE Press: 1872-1877.

Bongard, J. C. and Pfeifer, R. (2001) 'Repeated Structure and Dissociation of Genotypic and Phenotypic Complexity in Artificial Ontogeny' in: Spector et al. (eds.), *Proceedings of the Genetic and Evolutionary Computation Conference, GECCO-2001*, Morgan Kaufmann: 829-836.

BTU Cotbuss grogra.de Website (2008) http://www.grogra.de/ (Accessed multiple times during September-October 2008)

Carroll, S. B., Grenier, S. and Weatherbee, S. (2001) *From DNA to Diversity*, Blackwell Science, Massachusetts, USA, ISBN 0-632-04511-6.

Hornby, G. and Pollack, J. (2002) 'Creating High-Level Components with a Generative Representation for Body-Brain Evolution', *Artificial Life* **8**: 223-246.

Hornby, G., Lipson, H. and Pollack, J. (2003) 'Generative Representations for the Automated Design of Modular Physical Robots', *IEEE Transactions on Robotics and Automation* **19**(4): 703-719.

Kniemeyer, O., Buck-Sorlin, G. and Kurth, W. (2004) 'A Graph Grammar Approach to Artificial Life', *Artificial Life* **10**: 413–431.

Lappin, T., Grier, D., Thompson, A. and Halliday, H. (2006) 'HOX GENES: Seductive Science, Mysterious Mechanisms', *Ulster Medical Journal* **75**(1): 23-31.

Lewis, E.B. (1978) 'A Gene Complex Controlling Segmentation in Drosophila', *Nature* **276**(5688): 565-570.

Lund, H., Hallam, J. and Lee, W. (1997) 'Evolving Robot Morphology' in: *IEEE Fourth International Conference on Evolutionary Computation (ICEC'97)*, IEEE Press: 197-202.

Sims, K. (1994) 'Evolving Virtual Creatures' in: *Computer Graphics, Annual Conference Series (SIGGRAPH 94)*, ACM Press: 15-22.

Sims, K. (1994) 'Evolving 3D Morphology and Behavior by Competition' in: Brooks, R. and Maes, P. (eds), *Artificial Life IV Proceedings*, MIT Press: 28-39.

Stanley, K. O. and Miikkulainen, R. (2003) 'A Taxonomy for Artificial Embryogeny', *Artificial Life*, **9**(2): 93-130.

Fingerprints Authentication and File Encryption: Effective Tools for Organisations Information Technology Systems Internal Control

A.Afolabi and M.Tomlinson

Fixed and Mobile Communications, University of Plymouth, Plymouth, UK
e-mail: M.Tomlinson@plymouth.ac.uk

Abstract

Insiders attack and compromises can wreak more havoc on organisations than those from without. Implementing reliable internal controls to detect and prevent internal fraud threats continues to be an obligatory priority. Such controls include, among others, proper person's authentication, access control and electronic data encryption. This paper presents the issues with internal control and describes a developed framework that employs fingerprint authentication techniques plus data encryption processes as effective tools for implementing Information Technology Systems internal control.

Keywords

Biometrics, Encryption, Decryption

1 Introduction

Ensuring the security and privacy of electronic data assets is one of the key concerns facing corporations today. The need to safeguard these assets from both internal and external threats has never been more urgent. A 2007 eCrime watch survey, carried out by CSO Magazine with the U.S Carnegie Mellon University Software Engineering Institute's CERT program and Microsoft; showed that 34% of incidents were insider related, while 37% and 29% were attributed to outsiders and unknown sources attacks respectively. (e-Crime Watch, 2007).

Despite its attendant shortcomings, passwords authentication remain the most popular method employed by most organisations nowadays to provide security and privacy to their sensitive and proprietary digital information. Passwords can easily be guessed, acquired illicitly and illegally, subject to both dictionary and brute force attacks, and also very vulnerable to social Engineering (Bjorn, 2005). It is therefore the weakest link to the security of most electronic-based data.

We present a Fingerprint Biometrics-based authentication method that offer improved security advantage over a password-only-based authentication systems. Coupled with our biometrics authentication, is a password controlled data encryption/Decryption capabilities for electronic data.

1.1 The Problems with password as one-factor authentication

The vulnerabilities of password-based solutions stem from a combination of the following:

- Humans are forgetful and cannot be relied on to maintain highly-ruled based processes
- There are both insiders and outsiders who are intentionally looking for ways to compromise the solution

An average computer user nowadays is faced with so many applications that require authentication by means of 'user name' and 'password'. To cope, he often adopts two gullible approaches; he either keeps a list of passwords or chooses easy to remember common words (Bjorn, 2005). Both ways, the systems is exposed to higher vulnerability and the whole security essence could easily be defeated.

In an attempt to improve security, some systems compel users to select hard-to-guess passwords; some other systems require periodical change of passwords through password expiration policies. However, some systems neither enforce hard-to-guess passwords, nor adopt periodic password changes.

The outcome is usually complex, thus prompting users to either select trivial passwords or write them down where they could easily be acquired by impostors. On rare occasions, where users do not violate security policy in any of these ways, there is a high propensity that they forget their password, thus generating help desk call volume.

One of the proposed solutions to these human-based problems with only password-based authentication systems is to replace passwords with biometric authentication or introduce biometric authentication as secondary authentication means; known (in technical terms) as two-factor-authentication. (Griaulebiometrics, 2008).

2 Brief Overview of Biometrics

To set the scene for this paper, we first begin by a brief overview of Biometrics Technology.

Biometrics, a compound word coined from the Greeks words "Bio and metric" meaning "life measurement" is the science of identifying an individual using his distinctive physiological and behavioural features. Such features include fingerprint, voice, iris, veins, ear, face, gait, signature etc) and have been found to remain invariant over a persons life time.

Biometric features as opposed to Passwords, PINs and tokens do not depend on what you know; it depends on what you are.

The main objectives of Biometrics are user convenience (removes the need to carry cards, remember passwords and PINs), improved security, (difficult to forge), and higher efficiency. Biometric offers the following advantages over other traditional security measures:

2.1 Accuracy and Security

Biometric traits, unlike like passwords cannot be guessed. They require the physical presence of the user and therefore cannot be circumvented through a dictionary or brute force style attack. (Lee *et al*, 1991).

2.2 Non-repudiation

Because of the distinctive (that cannot be shared) characteristics of biometric traits, it becomes easier to tracks users activities in biometric authentication techniques. Whereas, in a passwords or PIN systems, users can easily claim that their password/PIN/tokens was stolen or compromised (Chikkerur, 2005).

2.3 Negative Identification

Biometric can establish whether a person is who he denies being. It can prevent a person from using multiple identities. (Maltoni et al, 2003).

2.4 Convenience

In many authentication environments, a user may have different tokens or passwords. In these cases, biometrics can be used to simplify the authentication process since the multiple passwords or tokens can be replaced by a single biometric characteristic.

In a broad sense, biometrics can be classified into three categories: 1. Physiological, physical measurement such as fingerprints, ear, iris, face etc. 2.Behavioural, such as gait, signature, handwriting, keystroke and voice and 3. Chemical, include composition of perspirations and DNAs. (Chikkerur, 2005)

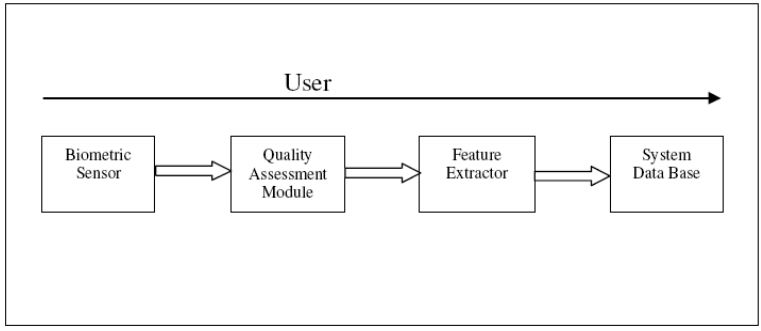


Figure 1: Enrolment

The most important characteristics of biometric traits that make them attractive for people recognition are: *Universality*, everyone possesses the feature(s); *Distinctiveness*, the features contain information sufficiently different from others and can be used to distinguish separate individuals; and *Permanence*, the features remain invariant with time. . (Maltoni et al, 2003).

A typical biometric system comprises of the following modules. As shown in fig.1

2.5 Enrolment

The *sensor* acquire the raw biometric data in form of fingerprint, voice, video, signature, iris etc, the *Quality assessment module* evaluates if the acquired data is good enough for processing, else, it would be discarded and fresh samples are taken, the *Feature extraction module* extracts unique set of features from the biometric signal and the *Data base module* holds the extracted features usually in a form other than the original extracts for the purpose of security. These data could either be stored on local or remote servers.

2.6 Authentication

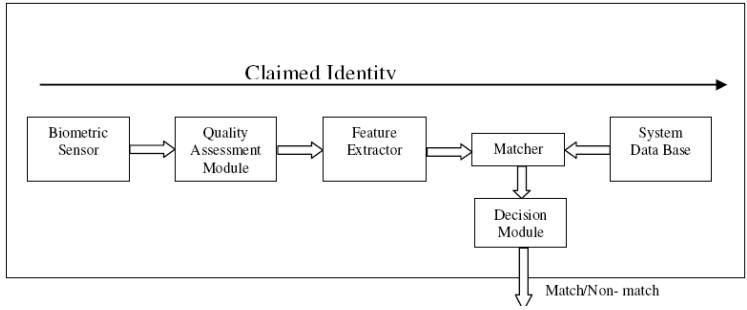


Figure 2: Authentication

The process of authentication is similar to the enrolment process, with two additional modules; the Matcher and Decision modules. The *Matching module* compares the feature extracted during authentication with the store templates and produces match scores and finally the *Decision module* process match scores, resulting in the system authenticating a user or denial.

3 Fingerprint Biometrics

Among human biometric characteristic features that can be explored for the purpose of recognition, Fingerprints is one of the most popular and well researched. A recent report by the Biometric International Group on 'Biometric Revenues by Technologies' revealed Fingerprints taking 28% of the market share after AFIS/Live-Scan's 39% . (IBG, 2009).

A fingerprint is made of a series of ridges and furrows (valleys) on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. (Maltoni *et al*, 2003).

4 An Authentication System Based on Fingerprint Recognition

We designed a simple yet robust (in terms of security) access control and authentication system based on fingerprint recognition together with electronic data protection through cryptography techniques. Our design was implemented using VB.NET 2008 programming language on windows operating system platform. The GUIs were such that users need little or no training to get on with.

4.1 The scenario:

Suppose an organization XYZ, say a banking institution, has on her computer server classified information. Only very few employees have privileged password to access the server either directly or from a remote locations. Not all the employees who have access to server are supposed to be privy to some or all of the classified information. However, there have been a few proven occasions when one or more of the classified information got into the public domain. Investigations to uncover how the information got compromised were abortive; since there were inadequate means to verify who accesses the files with prove of evidence without the culprit being able to deny.

Besides, there is the potential danger of a hacker (both within the organization and external) getting hold of the classified information, which could result into serious damage to the business of XYZ organization.

4.2 Solution Design:

We set out to achieve two goals with our design, they are

- Firstly, an authorized user must be authenticated through fingerprints verification techniques.
- Secondly, provide the capability to Encrypt/Decrypt the classified files with unique password for each file.

The following steps were followed in designing a VB.NET application to address the goals stated earlier:

1. Setting-up a database (using MS access) with two tables: the first to hold the users credentials; name and department and the second to keep enrolled users fingerprint templates.

2. Creating a Windows Forms-based VB.NET fingerprint authentication and file encryption/decryption application project with the following functionalities

i. Initial enrollment of authorized users: usernames and departments.
ii. Extracting the fingerprint templates for enrolled users.
iii. Providing authentication to users trying to access classified information by fingerprint verification techniques
iv. Offering Encryption/Decryption capabilities to verified users accessing the classified information.
v. Password protection for encrypted files.

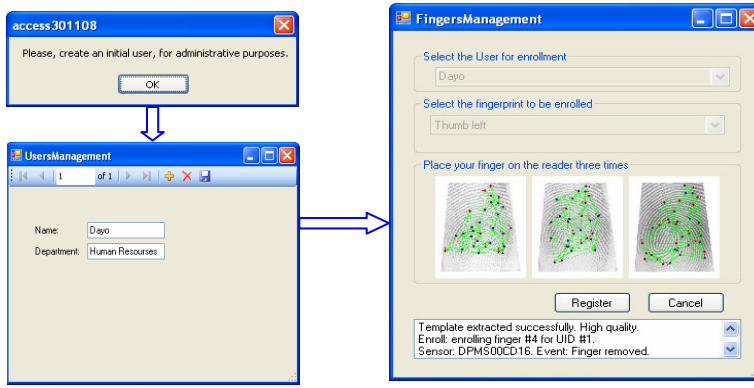
5 Enrolment, Authentication and Encryption/Decryption Interfaces

We have used minutiae based fingerprint recognition techniques based on the algorithm described in Griaulebiometrics, (2008) and data encryption/decryption based on Advanced Encryption Algorithm AES, also known as Rijndael (named after his authors, Ramen and Damen). The Rijndael uses key and block sizes of 128, 192 and 256 bits for encryption. We employed 256 bits key-length and 128 bits block size in our implementation (to conform to the AES specifications). The *Federal Information Processing Standards Publication 197* (FIPS-197) (2006), describes the details of the AES specifications and its implementations.

Our application goes thus: the first enrolled user is assigned administrative rights; he therefore becomes the only user with privileged rights to allow the registration and de-registration of others users.

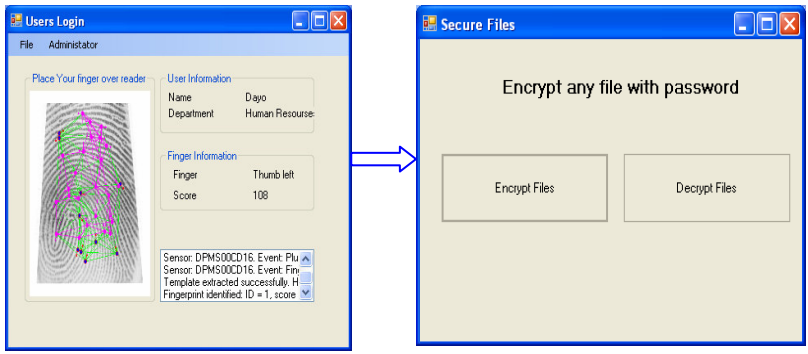
- ✓ *Initially the users' database is empty; hence the first user is created and assigned the role of administrator. He chooses a user name and entered his department.*

- ✓ *His fingerprint is captured thrice and registered in the database. Once he is registered, he is the one who has rights to allow registration of other users.*

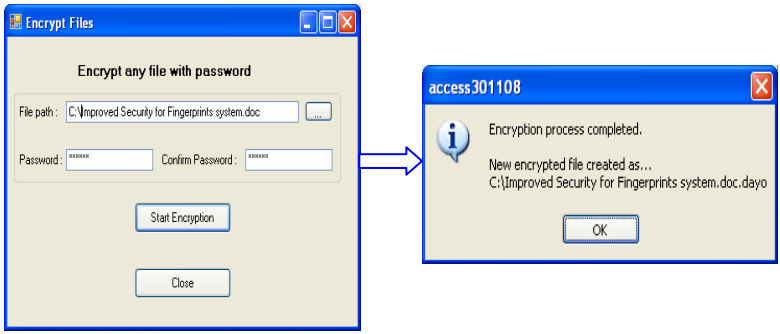


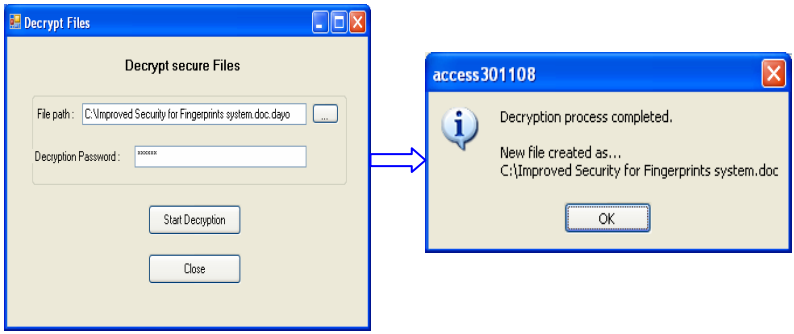
- ✓ *A registered user presents his finger (N.B it must the same as the one used during enrolment); its features are extracted and compared with reference*

templates in the database. A matched? His details are displayed. He then gains access to the controlled (classified) data files via 'Secure Files' (Encrypt/Decrypt) Interface



✓ *Now, He can either encrypt files and add to the classified files or decrypt existing ones, provided he possesses the passwords to do so.*





6 Conclusion

Passwords are less effective -as a tool for providing internal control- today, despite more rigorous requirements. Fingerprint Biometric offers a realistic solution. Fingerprint authentication creates a more secure environment by requiring users to prove who they are through their biometrics traits.

A well implemented fingerprint authentication offers more reliability, greater convenience, cost effective, and best of all, much more security.

Our system could be extended to a distributed network environment to facilitate users' authentication over the network and from remote locations.

To ensure security for the fingerprint templates themselves, cryptography techniques such as demonstrated by Sutcu *et al.* (2002) and Karthik *et al.* (2007) could be employed. The alternative is to store the reference template on smart cards as suggested by Clancy *et al.* (2003) although, this could defeat the convenience advantage fingerprint authentication offers.

7 References

Chikkerur S.S. (2005), Online Fingerprint Verification System. *Master's thesis*, University of Bufalo, the State University of New York.

Clancy T. C., Lin D. J., and Kiyavash N. (2003), Secure Smartcard-Based Fingerprint Authentication. *Proceedings of ACM SIGMM Workshop on Biometric Methods and Applications*, Berkley, USA, November 2003, pp. 45–52.

Bjorn V, (2005), "Solving the Weakest Link: Password Security" -A Comprehensive Review. A DigitalPersona White Paper, February 2005. [Online] Available from http://www.digitalpersona.com.tw/resources/downloads/Weakest_Link_wp_0205.pdf [Accessed 1 January, 2009]

e-Crime Watch (2007), "Over-Confidence is Pervasive Amongst Security Professionals." [Online] Available from http://findarticles.com/p/articles/mi_m0EIN/is_/ai_n27369168 [accessed 29 December, 2008]

FIPS-197 (2001), Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication 197* November 26, 2001

Griaulebiometrics (2008), "Understanding Biometrics" [Online] Available from http://www.griaulebiometrics.com/page/en-us/book/understanding-biometrics/introduction/history [Accessed 20 August 2008]

IBG (2009), "Biometrics Market and Industry Report 2009-2014" [Online] Available from [Accessed 16 December, 2008]

Karthik N., Jain A. K., and Sharath P. (2007), Fingerprint based Fuzzy Vault: Implementation and Performance. *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, December 2007.

Lee H. C. and Gaensslen R. E., (1991) editors, Advances *in Fingerprint Technology,* Elsevier, New York, 1991.

Maltoni D., Maio D., Jain A. K. and Prabhakabar S. (2003), *Handbook of Fingerprint Recognition.* Springer Ed, USA: Springer Science+ Business Media

Sutcu Y., Li Q., and Memon N. (2007), Protecting Biometric Templates with Sketch: Theory and Practice. *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, September 2007.

Implementation of RLS Algorithm

H.V.Ajmera and M.Z.Ahmed

Fixed and Mobile Communications, University of Plymouth, Plymouth, UK
e-mail: M.Ahmed@plymouth.ac.uk

Abstract

An algorithm for recursively calculating the least square solution to adaptive filter, for its implementation on a dsPIC is described in this paper. It shows an unified approach for deriving the fixed-point Recursive Least Square (RLS) algorithm to estimate the optimal set of filter coefficients. The objective is to study implementation effects on the Recursive Least Square algorithm used in the mean-square manner for adaptive filter for a dsPIC. Using the matrix operation as well as the round-off error model, the effects of machine implementation on RLS algorithm has being found out theoretically confirmed by simulation results. The main sources of errors can be thought of: division operation involved in updating filter variables. Due to such errors, the digitally implemented algorithm shows a divergence rather than convergence. A couple of solutions are provided to give better performance, so that the simulated results for filter coefficients for fixed and floating point are found to be similar.

Keywords

RLS algorithm, Finite Precision Effect, Error Analysis

1 Introduction

In recent years, recursive least square (RLS) filters have emerge as a powerful tool for adaptive filtering, prediction and identifying (Haykin, 1996). However, when implemented in a finite precision environment, RLS algorithm can suddenly become unstable and also divergence becomes a problem. A number of papers have being published that deals with the effects that finite word length has on the RLS algorithm (Adali and Ardalan, 1987; Ardalan, 1986; Bottomley and Alexander, 1991). Its always being a difficult issue to analyses such algorithm due to recursive nature of this filter. Consequently, certain simplifications have being made in order to yield useful results. One simplifying approach is to assume that kalman gain is available with finite precision range (Adali and Ardalan, 1987; Ardalan, 1986). A second approach was to bias the round-off error in each filter quantity to achieve a more stable performance (Bottomley and Alexander, 1991). It has also being shown that the prewindowed growing memory RLS algorithm is unstable (Adali and Ardalan, 1987), while other assume that some of the term didn't contribute to the error. All the elements of matrices and vectors in the RLS algorithm will deviate from their correct values due to quantization effects, giving three separate effects: 1) The inverse autocorrelation matrix may become indefinite due to accumulation of the error, 2) Propagation of the error due to recursive use of the algorithm and 3) With use of exponentially forgetting factor, the errors also grows exponentially. The output signal is computed by convolving the input sample with tap coefficients and the weight vector are updated by taking the product of kalman gain with the predicted

error. In this paper, there are no simplifications made. Specifically, 1) Quantized input signal and desires signal are available, 2) Neglect the second order noise term if the magnitude is smaller than 1. The paper is organised as: In section II, the infinite precision RLS algorithm is being discussed, while in section III, fixed-point error are injected into the algorithm with results being reviewed in section IV.

2 RLS Algorithm

The basic aim of the least square algorithm is to minimize the sum of the squares of the difference between the desired signal r(i) and the filter output y(i). An important characteristic of RLS is the computation of the estimate of the inverse correlation matrix from the input data u(i), which helps the minimization process. The adapted coefficient $h_n(i)$, n=0,1,2…N aim at minimizing the given objective function. In the case of the least square method, the objective function is given by

$$\varepsilon(n) = \sum_{i=0}^{n} \lambda^{n-i} \left| e(i) \right|^2 \tag{2.1}$$

$$\text{where, } e(i) = r(i) - y(i) \tag{2.2}$$

and λ is forgetting factor. To find optimum values of the tap-weight vector h(n), it necessary that $\boldsymbol{\varepsilon}(n)$ achieves its minimum value. This is done by taking partial derivative with respect to the tap coefficients h_n. The optimum value for the filter coefficient is obtained when the partial derivative is set to zero. The resulting expression is given by:

$$hn = R_u^{-1}(n) .rdu(n) \tag{2.3}$$

where, $R_u(n)$ and $r_{du}(n)$ are auto correlation of the u(n) and cross correlation matrix between u(n) and r(n) respectively. Using the matrix inversion lemma, and defining term kalman gain, the inverse of the autocorrelation matrix is given by

$$P(n+1) = R_u^{-1}(n+1) = \frac{1}{\lambda} [P(n) - k(n+1)\, uT(n+1).P(n)] \tag{2.4}$$

Using eq. (2.2), (2.3) and (2.4) we develop a recursive solution for updating the least square estimate h(n) for the tap weight at iteration n as follows:

$$hn+1 = h(n) + k(n+1)\, e(n+1) \tag{2.5}$$

Thus, we can conclude that the new estimates of the tap coefficients are calculated based on the inner product of the old estimate and the current input sample.

3 Fixed-Point Implementation of RLS Algorithm

In this section, a fixed point analysis approach is developed to analyze RLS algorithm. The approach develop is clear- model all the round-off errors resulting from fixed-point implementation and depending on this model, build up exact recursive equation for total error in the algorithm. A typical approach towards the modeling is the assumption that addition and subtraction do not introduce any round-off error and this holds true as long as there is no overflow. Thus, for most of cases, the culprit left are multiplication and division, as the source of round-off error in fixed implementation of RLS algorithm. The round-off error in the product of a multiplication can be expressed as

$$f[x \cdot y] = xy + \xi_{xy}$$

where xy is the infinite precision product, ξ_{xy} is relative error and is independent of x,y and also of x·y. Similar result do exist in case of division.

The error term e'(i) consists of the difference between a desired filter output r(i) and the fixed-point output of a filter y'(i), where e'(i) is the fixed-point error term. Here h'(n) denotes fixed-point weight coefficients.

$$e'(i) = r(i) - y'(i) = r(i) - h'_n \, uT(i) - \mu(i) \tag{3.1}$$

The optimum value of weight tap coefficients is found out in a same way as done for conventional RLS algorithm and for fixed-point RLS is given by:

$$rdu(n) - \mu du(n) = Ru(n).h'n \tag{3.2}$$

where, $\mu_{du}(n)$ is cross correlation matrix between u(i) and error μ(n). As from the fixed-point model defined previously, the multiplication and division may result in quantization error, denoting the fixed-point kalman gain by **k**'(n + 1) while β(n) as the fixed-point error, the kalman gain is expressed as:

$$k'(n + 1) = k(n + 1) + \beta(n) \tag{3.3}$$

Similarly, the error introduced in the calculation of the inverse autocorrelation matrix is ω(n) and P'(n + 1) as the inverse auto correlation matrix using fixed-point RLS algorithm, then

$$P'(n + 1) = \frac{1}{\lambda} [P(n) - k'(n + 1) \, uT(n + 1).P(n) + \beta(n) \, uT(n + 1).P(n) + \omega(n)] \tag{3.4}$$

Once the fixed-point inverse autocorrelation is calculated, we can then use eq. (2.5), (3.2), (3.3) and (3.4) to update the weight vector by recursive sequence.

$$h'(n + 1) = h'(n) + k(n + 1)e'(n + 1) - \alpha NN(n)h'(n) \tag{3.5}$$

where, $\alpha_{NN}(n) = \beta(n)\, u^T(n+1).P(n) + \omega(n)$. This is the theoretical expression for the fixed-point weight error vector.

4 Experimental Analysis

The section below provides the effect of fixed-point errors on the performance of the RLS algorithm through simulation results. The programs were stimulated in C and MPLAB. The algorithm is based on the equations (3.1), (3.3), (3.4) and (3.5). In the calculation, the inverse autocorrelation matrix is initialized as $P(0) = \delta^{-1}I$, where, $\delta = 0.005$ which ensure that $P^{-1}(n)$ is a positive definite matrix. All the other vectors except the input and the desired response are set to zero. The desired response to the algorithm was a sine wave, while the input response consists of delayed version of the sine wave added with a sine wave of different frequency. The table shown below is calculated for different forgetting factor lambda λ.

Iteration	λ=0.1	λ =0.5
0	0.0000	0.0000
1	0.0000	0.0000
2	0.0371	-0.0413
3	-0.013	0.4645
4	-0.069	0.3786
5	-0.2171	0.4446
6	-0.0514	-0.328
7	-0.0706	0.2280
8	-0.7693	-0.1528
9	-0.395	0.3817
10	-1.233	-0.1596

Table 1: Comparison of μ(i) for different λ

With larger value of λ, the magnitude of error μ remains less than 0.6 and its value remains more stable, although the filter continues to be unstable due to the higher value of μ. The smaller value of λ makes the filter more unstable as compared to higher values of λ, and also sets the maximum value of μ(i). This smaller value of λ has benefit of offering the least value of μ(i). With the smaller value of forgetting factor, the maximum value shown is almost the double of its counterpart.

One of the most important filter quantity is the kalman gain, as the value of k(n) affects all the filter quantities directly. This can be seen from eq. (3.4) used to calculate the inverse of auto correlation matrix and from eq. (3.5), where current tap coefficient vector uses the value of kalman gain. Hence, quantization in kalman gain k(n), would amplify the total error in the filter and severely affect the stability of the algorithm. To see how the errors are manifested in practice, we show the results of computer experiment.

Table 2 shows results for different value of λ at iteration 2. As observed from above, the error vector β(n) increases as the value of the λ is being increased from 0.1 to 0.5.

The variation in the error for the case when λ=0.1 is very small, while the simulation results shows a tremendous growth in the error β(n) for the latter case. This means the magnitude of β could be said to be proportional to λ.

With the presence of inverse autocorrelation, the successive taps becomes decorrelated in RLS algorithm, making the algorithm self-orthogonalizing. The update value of P(n) is calculated using the previous value of P(n), the product of kalman gain and the tap inputs. Table 3 below shows the error ω(n).

λ=0.1	λ=0.5
Iteration 2	
$\begin{bmatrix} 1.9711 \\ -0.8482 \\ 0.0673 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 3.2636 \\ 5.3929 \\ 12.7649 \\ 0 \end{bmatrix}$

Table 2: Comparison of β(n) for different λ

λ=0.1	λ=0.5
$\begin{bmatrix} -2.4592 & -0.5371 & 2.218 & 0 \\ -0.6029 & -0.0188 & 3.8376 & 0 \\ 2.5396 & 4.6352 & 9.7435 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} -3.0142 & -1.5050 & 0.2129 & 0 \\ -1.4353 & -1.4719 & 0.8287 & 0 \\ 0.3748 & 0.7289 & 3.7256 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

Table 3: Comparison of ω(n) for different λ

As the autocorrelation matrix in symmetric, so is the case with the error in it. The values of ω(n) also follows this symmetric property. As seen from the table, ω(n) shows maximum value for the minimum value of forgetting factor λ.

Having calculated all the error in each filter variables, the final step will be to calculate the total error in the tap coefficients affected due to the errors present in the filter variable. In this sense, the errors generated in the filter vectors and matrices are multiplied by different filter variables to produce additional errors. In the eq. (3.5), there is an error $\alpha_{NN}(n)$ which is given as:

$$\begin{bmatrix} 4.078 & 2.5076 & -5.5667 & 0 \\ 10.4329 & 5.1587. & -9.7086 & 0 \\ 27.2169 & 13.9655 & -17.2931 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Table 4: Error $\alpha_{NN}(n)$

The magnitude of the error produce is of order of 10. An error with such magnitude definitely tends to make the filter highly unstable and also losses the convergence property for which the adaptive filter are famous for. This error is then multiplied by the current tap coefficients.

Table 5 shows the amount of the error which is added to the previous tap coefficients to give the new coefficients. In other words, this is the error by which the new taps coefficient will be shifted. One peculiar characteristics of this error is the dependence on the previous tap coefficient as seen in eq. (3.5). In short, the tap coefficients are updated as addition of previous tap coefficients with the product of kalman gain and error e(n), with the addition of the product $\alpha_{NN}(n)h'(n)$.

$$\begin{bmatrix} 3.0379 \\ 4.6637 \\ 6.0451 \\ 0 \end{bmatrix}$$

Table 5: Total Error in Tap Coefficient

There are two problems which can be associated with the error result found out above: Firstly, a fixed-point implementation does not guarantee to prevent the overflow and underflow, a problem which results in nothing but divergence. Secondly, the stability may not be guaranteed. The problem can be solved by preventing the overflows. This can be done either by using floating-point, not possible in our case or by modifying the code. From a designer point of view, a careful fixed-point implementation of the filter is to be developed, so that overflow and underflow are minimized. Secondly, the filter is to be made stable. The following are the way to minimize the error:

- Changing the value of forgetting factor λ

The minimum value for error in β can be obtained when the value of λ is taken to be minimum shown in table 2. Successively, as seen from table 3, with minimum value of forgetting factor the error ω reaches a value of 10 in the first few iteration only. The minimum value for this error can be obtained when the value of the λ is maximum. Successively, as a designer there has to be a trade-off made in selecting the value of the forgetting factor.

- Reducing the value of k by factor of $\frac{1}{2}$

Changing the value of k to $\frac{k}{2}$ and by keeping the value λ=0.5, has the advantage of decreasing the error β and also compensates the error in the auto correlation matrix.

With the above solution in the mind, let us recalculate the errors in different term. Figure 1 below shows the stimulation result for the average mean square error μ(i) against the number of iteration for the original value of kalman gain k(n). This situation sets the maximum value of the average mean square error μ(i), which comes to be more than 2. However, for most of the iteration the error value remains close to 1. Accordingly, this indicates a huge amount of error in the least square solution, which results in divergence. As seen form the graph, there is continuously rise and fall in the value, with a sudden rise reaching a peak value of about 2.4, indicating the instability of the filter.

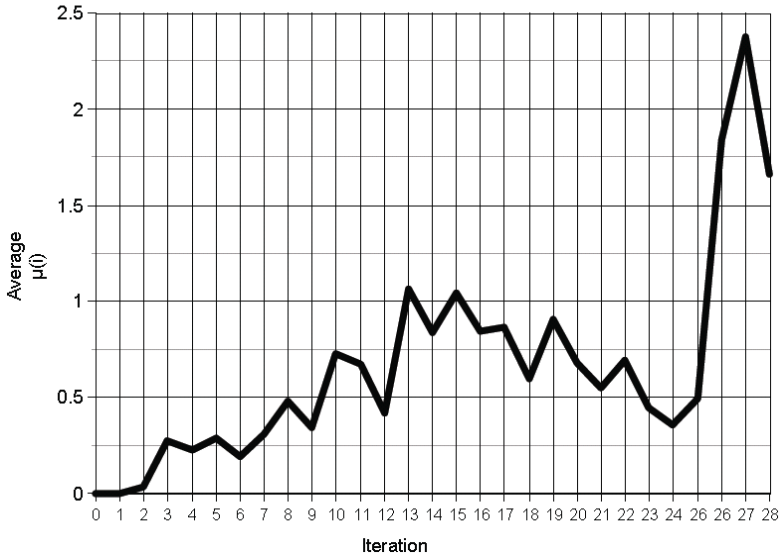


Figure 1: Average Mean Square Error μ(i)

Now let us analyze the graph when the value of the kalman gain is reduced by 2, so that the input to the filter is now $\frac{k(n)}{2}$. It can clearly seen in figure 2 that the value of the average mean square error μ(i) has decreased from the maximum value of 2.4 to a value just less than 1.77. Consequently, the graph seen is more stable and tries to maintain a similar value of 0.75, but at certain iteration the value is doubled then its previous iteration. There is peculiar similarity about both the graphs- at a point there is sudden linear rise followed by liner fall and again linear rise.

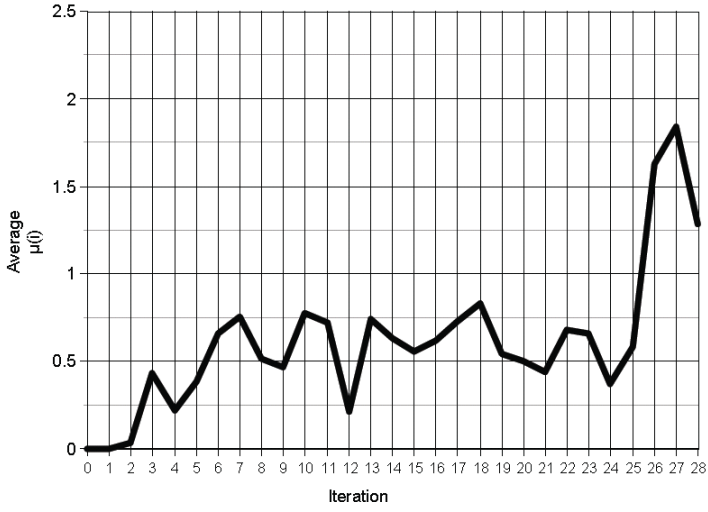


Figure 2: Average Mean Square Error μ(i) for scaled kalman gain

As seen from Figure 2, the error in the μ(i) has decreased. The error in kalman gain β(n) as shown decreases due to scaling and as shown in table 3, with increase in value of forgetting factor the error ω(n) decreases. With these details, the error $\alpha_{NN}(n)$ is calculated as shown in table 6.

When this calculated value of $\alpha_{NN}(n)$ is compared with the previous value, one can easily state that the error had reduced to almost half of the previous one. Now let us compute the total error due to which the current estimate tap coefficients are shifted. This is achieved in the same way as earlier by multiplying the error shown below with the previous tap coefficients.

$$\begin{bmatrix} -0.235 & 3.9352 & -1.867 & 0 \\ 7.8091 & 1.4737 & -3.1074 & 0 \\ 15.7651 & 10.0565 & -7.4675 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Table 6: Error $\alpha_{NN}(n)$ for scaled kalman gain

There is tremendous decrease in the total error as seen in table 7, when matched against the outcome of the simulation performed without the correction in the program. This may due to the reason that the error in the previous coefficient vector may be less as well as the other error has decreased. Performing similar scaling of various filter quantities may help the designer to obtain convergence or convergence may be possible with the above solution after may be 100's of iteration or the error value will be so less that the magnitude may be less than 1.

$$\begin{bmatrix} 0.4504 \\ 0.9807 \\ 1.1111 \\ 0 \end{bmatrix}$$

Table 7: Total Error in Tap Coefficient for scaled kalman gain

5 Conclusion

A surprising divergence is observed on implementing the algorithm on a fixed-point processor. From the mathematical expressions, we can say that the least square solution includes a huge amount of error, confirmed with the stimulated results. From the theoretical expression, it is shown that in equation for optimum filter coefficients, the only error present is the correlation matrix of μ(i) and tap inputs u(i). The expression for least square solution is same as that for infinite precision with finite precision least square solution being the result due to arithmetic operation carried on the finite precision filter quantities plus the error multiplied by the old estimate of tap coefficient. It was shown that the error contribution of certain fixed-point operations increased as the forgetting factor increases while errors due to other operations decreased. The cause of error in some of the variables has being identified, pointing towards the division operation carried out to calculate these

terms. With the above facts, it forces the designer to make trade-off in the value of forgetting factor λ. The value of lambda could be taken equal to 0.5. The β(n) will still show a higher error value. Consequently, the values in kalman gain k(n) should be then reduced by a factor of ½. With this solutions, the error decreases which is shown in table 7.

6 References

Adali, T. and Ardalan, S. H. (1987). “Fixed-point roundoff error analysis of the exponentially windowed RLS algorithm for time-varying systems.” Proceedings of the Acoustics, Speech, and Signal Processing, 1987. ICASSP-87., 1987 International Conference on.

Ardalan, S. (1986). "Floating-point error analysis of recursive least-squares and least-mean-squares adaptive filters." Circuits and Systems, IEEE Transactions on 33(12): 1192-1208.

Bottomley, G. E. and Alexander, S. T. (1991). “A novel approach for stabilizing recursive least squares filters.” Signal Processing, . IEEE Transactions on 39(8): 1770-1779.

Haykin, S. S. (1996) *Adaptive filter theory,* Upper Saddle River, N.J., Prentice Hall.

Graphical Environment Tool for Development versus Non Graphical Development Tool

S.Daniel and P.Filmore

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

Abstract

This paper highlights the differences, advantages and drawbacks of a graphical environment tool for development (LabVIEW) against a non graphical development tool (Java) a text base programming language. The study is centred on the developments and analysis of a sever-client application using these different technologies. To understand the differences between the different technologies, it's really useful to come back to the origins of the human computer interaction and look the differences between the different interfaces. This paper matches then some of the advantage and disadvantage for using these different technologies. It is found that JAVA has advantages in resources as it gives smaller lighter source code and LabVIEW has advantages in time, it is faster and easier to program.

Keywords

Internet, client-server, command line, graphical user, LabVIEW

1 Introduction

First of all, this paper aim to review the difference between a graphical user interface (GUI) programming tool against any other type of programming tools; this will be reviewed around a web application by building a simple client-server application.

In order to compare this technology we must come back to the source; the user interface. It's not the first time that graphical user interface has been reviewed. Since the very beginning of computer, human computer interaction (HCI) has a key role in the computer usability.

The first interface to be developed was the command line interface (CLI) which is a text based environment totally neutral. Its successor; the graphical user interface which replaces most of the command by graphical icon/button reflecting a real life environment. This was followed by natural user interface (NUI) which adds physical interaction with the graphical user interface (ex: Microsoft Surface). Qt this point of time, organic user interface (OUI) claims to adapt themselves to the current application (Chapman, S., 2008).

	Metaphor	Relationship	Control	Flexibility	Behaviour
CLI	Textual	Abstract	Directed	High	Static
GUI	Graphical	Indirect	Exploratory	High-Medium	Dynamic
NUI	Physical	Direct	Contextual	Low	Realistic

Key examples: CLI → Microsoft DOS
GUI → Microsoft Vista
NUI → Microsoft Surface

Table 1: The difference between interfaces (Daniel Makoski, 2008):

1.1 From a user point of view graphical user interface are very common nowadays:

Every computer gets now graphical user interface, even mobile devices have their own graphical user interface. These interface have been develop to help user to match their personal behaviours to the computer by association of symbols, the computer interface looks pretty much as a virtual office you can find the same kind of workspace with the tool used in real life also imitated to fit the needs of computing.

Most of the advantage and drawback have already been surrounded for the basic users.

Makoski (2008) has identified major Key points between command line interface and graphical user interface. These are:

Ease of use New user will have facilities to get into the graphical user interface as it tries to fit the behaviours at the opposite the command line interface will be much difficult to use as you need to memorize the command needed for your action that you intend to do.

Control Even with all the buttons we would, the command line interface offer more control for advance user over the graphical user interface.

Multitasking That is where the graphical user interface gets most of their power, you can display as many information as you want on your display and organize them as you want. It's also possible to control multiple objects at once.

Speed Because the graphical user interface needs to point and click with the mouse the graphical element you want to use, it seems to be slower than the command line when you only need your keyboard and perform action with a single command where you may need several clicks on a graphical user interface.

Resources That isn't a secret graphical user interface needs more resources to load the graphics and manage the interaction whereas the command

line interface needs a minimum of resources to display textual information.

Scripting A command line interface enables to execute small program to automate some of their task. This feature can be find also in the graphical user interface under the name of macro which memorizes the action perform in order to automate them.

Remote access Most of the recent graphical user interface already includes remote access without the need to perform any command line.

2 Evaluation of the technologies

It is useful to compare these technologies:

a) Text based programming language:

Often shortened to code, this programming language is made of text. It could be compared to command line, each line of code represent a specific command line which is process by the compiler to provide the final application. So the developer needs to write himself all the code, text to build an application.

As reference we use Java because it's widely use over the world for creating desktop and web application and well known to be cross platform. Java application can be use as well with Linux, Mac, or Windows and can even be embedded in a web browser; it uses a run-time engine available for these different platforms.

b) Visual programming language:

Also shortened to G language for graphical language, this programming language change totally from the text based programming language as there is no code. Everything is visual, instead of command we have box and wire to interconnect these box together and make a more advance function. It is a dataflow programming; data linked the application are visually connected in the source.

So LabVIEW is the reference for this review. As well as Java it's a cross platform language using its own run-time engine for Linux, Mac, windows and web browser.

c) Client-Server application:

The client-server application is a very basic application which uses the TCP protocol to send and receive data through Internet or a network.

In both Languages Java and LabVIEW, we will produce a server application which sends some data and a client application which receives these data.

2.1 Hypotheses and Measurements

Previous studies on human computer interaction. All the key points previously highlighted are reused there for the comparison between the development languages.

2.2 Common perceptive:

1. Graphical language is easier to use.
2. Text language gives more control.
3. Graphical language allows showing more information (multitasking).
4. Text language is faster to write.
5. Graphical language is heavier.

These hypotheses have all been discovered along general usage of user interface. We are now looking forward to see if these hypotheses are also applicable to the programming languages. Point by point we are going to demonstrate each of these hypotheses to finally conclude which of them is the best and in which circumstances. For each hypothesis, we will measures and compare the result between the languages.

2.3 Methods:

1. Ease of use:
    a. Analysis of my personal experimentation.
    b. Student survey (Mark Yoder and Bruce Black, 2006).
2. Control:
    a. Number of function available.
3. Multitasking:
    a. Review of the programming environment.
4. Speed:
    a. Time to make an application.
        i. Creating source.
        ii. Compiling.
        iii. Deluging.
5. Resources:
    a. Number of lines/blocks.
    b. Source files size.
    c. Computer memory usage.

3 Demonstrations and Experimentations

Ease of use, control and multitasking:

Evaluation of the programming environment.
Working with LabVIEW feel as simple as playing Lego, you just have to pick the block you want connect it to you data and your function is done, personally I felt really confident on LabVIEW after a few hour of trainings where I was feeling a bit confuse at the same time using Java as long as you know how to program Java is

correct, but for a non programmer it we be difficult to remember every command and write the perfect syntax needed for Java. At the opposite, when a newbie in coding can get lost to remember any command in Java, that give great control over the people who masteries these language they can do much more thing than the traditional uses, in LabVIEW we hurt ourselves again the graphical wall which allow us to use only blocks already created. This last point tends to disappear as we can create our proper object, class … but it's still taking more time. Another advantage of graphical programming is the ability to see on the screen all the data that you are working on and their relation, you can easily map your idea on LabVIEW where you need to produce an algorithm even before thinking to start any coding in Java.

LabVIEW source (Figure 1) shows clearly whereas Java source (Figure 2) is less clear, we need to read the comment to understand what it is actually doing.

In another study "a study of graphical vs. textual programming for teaching DSP" Yoder M. and Black B. (2006) intend to find which of LabVIEW or MATLAB another text based programming much closer to LabVIEW in his functionality; student rather prefer to use. They made junior-level student teaching discrete-time signal processing (DSP) on both languages LabVIEW and MATLAB. "Of the 64 students that took the survey, only 3 had learned LabVIEW prior to learning MATLAB." (Yoder M. and Black B., 2006). This can be explained by the fact that MATLAB is required in some other courses.

Table 2 shows the result of this study; almost 3 to 1 student preferred to use LabVIEW. "They say it is easier to learn and more understandable." In another advanced user state "When you know what you are doing, it's much faster to type a program than to select icons from menus and point and click to connect them". (Yoder M. and Black B., 2006). This last result can be applied to most of the text based language and also to Java.

	Matlab	Either/ Neither	LabVIEW
Which language did you learn first?	60		3
Average number of quarters of experience	2.5		1.1
Which language was easier to learn?	11	12	40
Suppose you had some simple task to do, which language would be quicker to do it in?	9	8	47
Which language is better for solving signal processing problems?	14	6	44
Which language do you prefer to use?	7 – strongly 9 – somewhat	7	13 – somewhat 28 – strongly

Table 2: Some results of the student survey (Mark Yoder and Bruce Black, 2006)

Speed:

In term of time of coding this is very **variable form beginner to advance** users. So measuring the time to make the source code on both languages should not provide significant result apart of the user experience. What we can say for sure is that is still

faster to write that pointing and clicking as long as you use only your keyboard. Then when it comes interesting is for the compiling time.

In LabVIEW there is no such thing as compiling, it run the application straight from the block diagram so **no compiling time where** in Java you have to compile you code to produce the final application, this is very short few second depending of you computer but a real drawback compare to LabVIEW.

For the deluging, in both Java and LabVIEW you are able to use breakpoint to stop the application at a specific line or place and variable watcher or probes to observer the current value of data. But due to the graphical interface of LabVIEW it's much easier to **identify problem on a flowchart** than it is in a list of command. The physical positions of the different block help him to target where the problem is. So again LabVIEW seems to be much faster.

Resources:

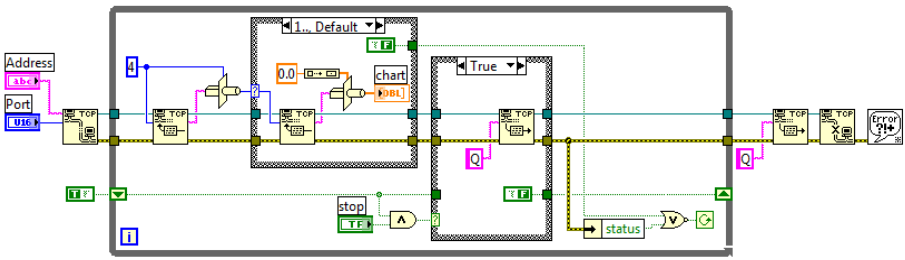


Figure 1: LabVIEW Client

```java
/**
 * Example Client program using TCP.
 */
public class Tclient {

    final static  String    serverIPname = "Localhost";       // server IP name
    final static  int       serverPort   = 3456;              // server port number

public static void main(String args[]) {

    java.net.Socket         sock = null;                      // Socket object for communicating
    java.io.PrintWriter     pw   = null;                      // socket output to server
    java.io.BufferedReader  br   = null;                      // socket input from server

    try {
          sock = new java.net.Socket(serverIPname,serverPort); // create socket and connect
          pw   = new java.io.PrintWriter(sock.getOutputStream(), true); // create reader and writer
          br   = new java.io.BufferedReader(new java.io.InputStreamReader(sock.getInputStream()));
          System.out.println("Connected to Server");
          pw.println("Message from the client");              // send msg to the server
          System.out.println("Sent message to server");
          String answer = br.readLine();                      // get data from the server
          System.out.println("Response from the server >" + answer);
          pw.close();                                         // close everything
          br.close();
          sock.close();

    } catch (Throwable e) {
          System.out.println("Error " + e.getMessage());
          e.printStackTrace();
    }
}
}
```

Figure 2: Java client

I have been able to observe on different source codes (extract: figure 1 & 2), it's quite obvious, the Java version of the client-server application is the smallest just 33 and 37 lines of Java code for this basic version without any graphical interface where LabVIEW accuse 27 and >50 blocks it's also include a small graphical interface. In term of visual space **LabVIEW seem to be again bigger than Java** to shows all the block diagrams code.

The difference become much sensitive when looking at the source file size; around 4KB for the Java source and 45KB for the LabVIEW source it's more than **ten times the size of the text based version**.

For the memory usage; Java need only the java run-time engine to run and don't need the full development kit. To work straight from the block diagram LabVIEW language need to keep the development kit running which take much more memories than a simple run-time. LabVIEW also have the possibility to build an executable application which doesn't need the development kit to work but just a **LabVIEW run-time engine similar at Java**.

3.1 Results and Comments

- ✓ LabVIEW is easier to use than JAVA or MATLAB.
  - ➢ Symbols are easier to recon than reading text.
- ✓ LabVIEW is faster to program than traditional text based language.
  - ➢ Much less error during coding (no syntax).
- ✓ JAVA takes less resources.
  - ➢ Pure text is still smaller than LabVIEW.

4 Evaluation and Conclusion

In the first part of this review we remember have seen the different key point between command line interface and graphical user interface; text based languages were supposed to have more control over the programming be faster to code and be small. And the graphical based languages were supposed to be easier to use and multitask. Finally we break the myth of text based programming is faster. That is the only real change between general interfaces a programming interface.

In the author opinion, the other drawback of LabVIEW against traditional programming is that it takes more resource and gives less control. These are not going to be some serious drawback as for the resources nowadays computers are powerful enough to run any graphical programming environment and running them without any problem. Memory isn't a problem as in the past as memory is now really cheap. The only braking point is the lack of control. LabVIEW is seriously focus on this point and are trying to give the maximum to the user and in each new version they provide more and more feature also the ability to build almost anything as our own block, library, class and much more.

Because it is particularly easy and fast to program under LabVIEW, it's really interesting to use it for **prototyping** software or any application you can just sit and start programming what in your mind and try it straight away without having to spend hours and hour to determine the perfect algorithm or debugging your application in order to make it running.

LabVIEW is a great tool for prototyping, it allows to program fast and test the application as soon as possible then we can use another language as Java or C++ to program the final application and optimize it at maximum which isn't rally the case on LabVIEW. To conclude LabVIEW is perfect to make a prototype but doesn't replace text based language as it need its own run-time less common than other languages as Java or C. LabVIEW is **complementary** to the text based language and help to **save some precious time**.

5 References

Blake J. (2009) 'Deconstructing the NUI: The Natural User Interface Revolution', *Deconstructing the NU*, blogger, [online] Available from: http://nui.joshland.org/2009/01/natural-user-interface-revolution.html (Accessed 31 March 2009).

Chapman S. (2008) 'UX Evangelist: Windows 7 NUI: Stepping Beyond the GUI', *UX Evangelist*, blogger, [online] Available from: http://uxevangelist.blogspot.com/2008/06/windows-7-nui-stepping-beyond-gui.html (Accessed 31 March 2009).

Makoski D. (2008) 'Beneath the Surface', pptx, [online] Available from: http://www.microsoft.com/surface/ (Accessed 31 March 2009).

Reyes A. (2008) *Predicting the past*, MP3, Sydney Convention Centre, [online] Available from: http://www.webdirections.org/resources/august-de-los-reyes-predicting-the-past/#description (Accessed 31 March 2009).

Sun Microsystems (n.d.) 'Writing the Server Side of a Socket', [online] Available from: http://java.sun.com/docs/books/tutorial/networking/sockets/clientServer.html (Accessed 30 March 2009).

Yoder M. and Black B. (2006) 'A Study of Graphical vs. Textual Programming for Teaching DSP', Rose-Hulman Institute of Technology, [online] Available from: http://zone.ni.com/devzone/cda/tut/p/id/3798 (Accessed 26 March 2009).

Wong W. (2006) 'Graphical-And Text-Based Programming: Complementary, Not Competitive', [online] Available from: http://electronicdesign.com/Articles/Index.cfm?AD=1&ArticleID=13241 (Accessed 26 March 2009).

Assessment of Speech Quality for VoIP Applications using PESQ and E -Model

H.A.Khan and L.Sun

Signal Processing and Multimedia Communications,
University of Plymouth, Plymouth, United Kingdom
e-mail: L.Sun@plymouth.ac.uk

Abstract

The aim of the paper is to investigate and assess speech quality for VoIP applications using the latest ITU-T standards (i.e. ITU-T P.862 PESQ and G.107 E-Model) and to compare the results with subjective tests results. . The speech quality metrics used in this experiment are MOS-LQS, MOS-LQO and MOS-CQE. The impact of packet loss rate (including packet burstness) on speech quality was investigated based on a VoIP testbed (including NistNET network emulator and XLite/ Skype VoIP terminals). The preliminary results show that PESQ achieves a higher correlation rate (81%) with subjective test results than that of E-model (74%). Some issues related with how to test speech quality properly in the experimental testbed are also discussed.

Keywords

QOS, MOS-LQO, MOS-LQS, MOS-CQE, VoIP, Emulator and NistNET

1 Introduction

Voice over IP is getting popular day by day, due to its obvious benefits. However, with the popularity and growth in the field of VoIP, standardization also became an important part of the industry. VoIP technology is used to transfer voice data over the traditional data networks using a set of protocols specialized for voice communication. Voice over Internet Protocol is growing at a very fast pace. The advantages of this technology are low cost and transfer of other data then just voice (images, video etc) over long distances using computer networks. However, the quality of this service is often compromised with cost and bandwidth. Also, the quality of this technology is affected by network issues like jitter, delay, distortion, packet drop etc. However, to regulate and maintain quality of the service, there are certain Quality Measuring Methods that are used today in VoIP field.

There are many speech quality measurement methods, for example, the ITU-T PESQ and ITU-T E-model, which have been widely used in industry for speech quality assessment for VoIP products and systems. However, it is unclear how well the PESQ and E-model is when compared with subjective test results.

The main aims of this paper are (1) To compare and correlate Objective speech quality (PESQ) and Estimated Speech Quality (E-model) with the subjective method

of speech quality (2) To investigate and analyze the effect of packet loss ratio over the voice quality in an IP network (3) To get a better knowledge of Speech quality measuring methods. Also analyzing and evaluating the reasons behind the unusual behavior will be a part of the project.

For this purpose, we have set up a VoIP speech quality testbed and investigated speech quality using PESQ and E-model and compared the objective test results with subjective test results. The preliminary results show that PESQ correlates better then E-model. The Pearson Correlation that was calculated between PESQ and Subjective tests came out to be 81% while the correlation between E-model results and Subjective results came out to be 74%. During the experiment, we also find that the NistNET network emulator software should be given some time in-order to achieve drop rate that has been specified. We find out that time equivalent to 100 ICMP echo packets take (200 seconds) should be given to the network and NistNET for drop rates up to 20% be achieved.

The remainder of the paper is structured as follows. In Section 2, an overview of VoIP and speech quality measurement methods is introduced. In Section 3, the testbed used in VoIP quality assessment and methodology of testing is presented. In Section 4, test results and analysis are shown for drop ratios of 4%, 8%, 12%, 16% and 20% with loss correlation of 0.3, 0.5 and 0.8. Section 5 contains the conclusions that are obtained after analyzing the results. All the references are mentioned in the end of this paper.

2 Voice over Internet Protocol and Quality Measurement Methods

To define it ,VoIP is set of technologies that is used to transfer Voice data over computer networks rather than traditional PSTN systems(Dudman 2006). If we look into the architecture of Voice over IP, it essentially consists of end points that are capable of converting analogue voice into digital data, a network, a receiving end that would convert digital voice data into audible sound, and a server to register and control all the activities. There are many factors affecting the speech quality in VoIP network (Opticom 2007). There are certain methods that are used to measure the speech quality over an IP network. These methods can be divided into intrusive and non intrusive methods.

ITU-T defines MOS as the values on a predefined scale that subjects assign to their opinion of the performance of the telephone transmission system used either for conversation or for listening to spoken material (ITU.T.Recommendation.P.800.1 2006). MOS is arithmetic mean of all the scores collected in a test. We will take into account the main three types of MOS tests, that are Subjective based testing, Objective based testing PESQ ITU-T P.800 and Estimation based testing, E-model ITU-T G.107.

Subjective scoring is done through the scoring of many subjects. These tests are carried out in a very controlled environment, so that external disturbance elements are not involved. The subjects are presented with a number of degraded samples and are asked to number mark them from 1 to 5, depending on the perceived speech

quality. In objective types of test, the score is calculated from an objective models that predicts the scores as would have done by subjective testing(PESQ 2001). PESQ is an objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs(ITU-T 2007a). PESQ software is modeled and designed in such a way that it can it can analyze certain degradation factors inside an audio file as compared to its reference file.

Estimation based methods of speech quality measurements are usually non-intrusive that are estimated using the parameters of the networks. The method we have used in our project is E-Model , the principal behind the working of E-Model is that the Psychological factors on the psychological scale are additive.(ITU-T 2005). Prediction models like these are useful in network planning and to replace the need for the sample comparison(Horrocks). , E-Model estimates the value from 1 to 100. The equation (Ding and Goubran 2003)by which E-Model is calculated is given below

$$R = R_o - Is - Ie - Id + A$$

R_o is the over all signal to noise ratio including the over all circuit and signal noise effects. A is the advantage factor. Id stands for any delay that can be caused by the network while Ie counts for the packet loss. In this section, we will restrict the theory explanation only for IeI.e. as it is being used in our project and a thorough explanation is required for any reader to understand the concept behind the packet loss calculations. Usually, packet loss is not purely random; in fact it occurs with a conditional probability. Hence Ie, when packet loss is not random, we write it as $Ie - eff$ and defined by

$$Ie - eff = Ie + (95 - Ie) \cdot \left(\frac{Ppl}{(Ppl/BurstR) + Bpl}\right)$$

Where Ppl = percentage of packet loss
$BurstR$ = Correlation of packet loss
Bpl = Packet robustness value

The Ie and Bpl values for different codecs are taken from ITU publication(ITU-T 2007b).The value of BurstR can be calculated using

$$BurstR = \frac{1 - \frac{Ppl}{100}}{q}$$

the equation can be rewritten(Sun and Ifeachor 2004) as

$$R = 93.2 - I_{e-eff}$$

Hence, we will calculate the R values from above equations and we can use (ITU-T 2005)the equations defined in ITU-T Recommendation G.107 to convert R values into MOS values.

3 Testbed Setup and Methodology:

The architecture deployed for our testing is a WAN (Wide area network), that consists of many routes that are lossy and possess delays. However the main concentration in this analysis would be on packet loss in the network. The end points which were discussed are two computers that contain SIP Phones. Below is the general picture of the architecture that we are looking to experiment with**.**

In this testbed, we are using a system that is a network emulator, and will be used to emulate network scenarios with different packet loss. The network emulator that we will use is called NistNET(NistNET 2001). NistNET is used here to introduce delay and packet loss for experimenting different network scenarios i.e. heavy packet loss with high correlation like 0.8 or 80% etc. The NistNET runs on a Linux base Operating System, and here in our testbed, we have used SuSE 9. The main values for packet loss used in our project were 0%, 4%, 8%, 16% and 20% with the correlation probability of 0.3, 0.5 and 0.8.

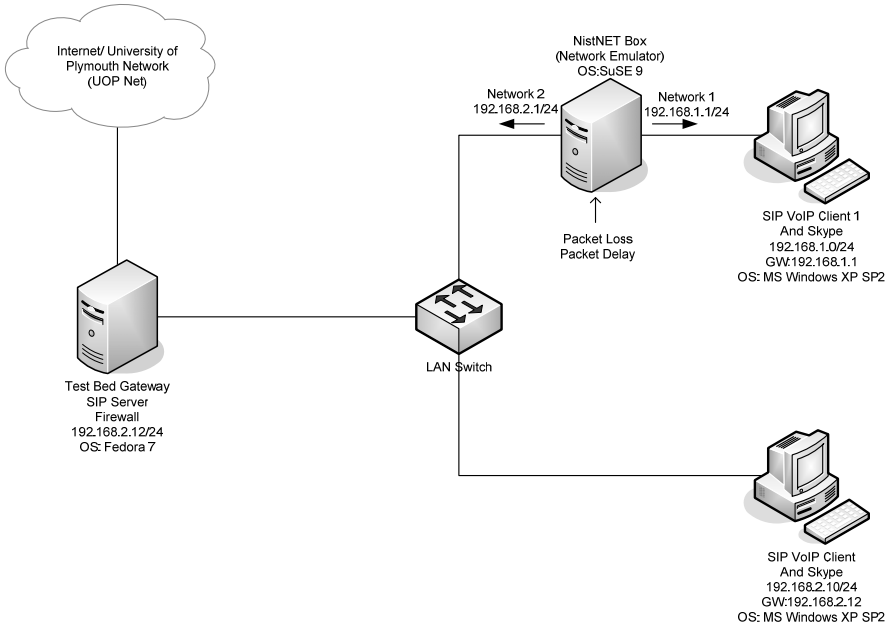


Figure 1: Test bed architecture

The whole network has been divided into two subnets. The NistNET system has two network cards connected to it and each is connected to a separate network. So any data that is moving from network 1 to network 2, as shown in Fig 1, will suffer all those degradations (Loss, jitter, delay etc) as defined in the NistNET box. However, the testbed is also connected to external network through a gateway as shown in the

figure above. The reason behind giving an external network access to the network is to do the testing on the Propriety based P2P VoIP clients e.g. Skype and Google talk, which need their own servers to communicate. However, for the SIP VoIP terminal used in this project is X-Lite which gives us the flexibility of choosing the codecs for VoIP communication. One important factor is to transfer voice sample from the sender to receiving end. For this purpose, a cable who's both ends are 3.5" audio jacks, is used. One end is connected to microphone/audio in port while other is connected to speakers/audio out port of the same system. Thus any audio file played in the system will be directly transferred to the microphone port and thus will be used for input voice sample for VoIP end terminal. Another method is to use virtual cable, that is, software based sound driver, works same like physical cable connected between audio out and in ports. Virtual audio cable can process sound output into the audio input /Line in of the soundcard. We used physical cable for our experimentation.

NistNET is a software based network emulation package that runs on Linux(Khasnabish 2003). NistNET allow a single Linux base system as a router and performs Fire-wall like functions to emulate a wide variety of network base functions(Panwar 2004). The Linux Platform on which NistNET runs in our case is SuSE 9 Enterprise edition. The end clients are the two end systems that are operating on Windows XP. These end systems act as the VoIP end points. The VoIP end terminal software used here were Skype and X-Lite SIP. The gateway is also a Linux base platform that is fedora 7. It also contains two network interfaces; one is connected to the University of Plymouth Network while other is connected to our project network. The IP address for the one interface that is connected to the University network is on DHCP while other is on a static IP. The firewall settings' are the default in the system.

The main aim of the project is to assess and correlate PESQ and E-Model with Subjective MOS results, thus the testing has to be carried out with ITU-T recommended voice sample and observe the results. The below mentioned are the three different methods used to assess the quality of speech or device network.

The samples reach the receiving end after passing through an emulated lossy network. We compare the reference signal with the degraded signal in Opticom Opera software to get the Objective PESQ MOS-LQO results, while in subjective testing; Human beings are used as subjects for grading the quality of the sample.

We took 18 samples, which are in different combination of loss percentage (0%, 4%, 8%, 12%, 16% and 20%) and Loss correlation (0.3, 0.5 and 0.8).The reference sound file (b_f1_eng.wav) was placed in the beginning while the remaining 18 samples were placed randomly in a playlist. Subjects are asked to listen to the files in given order and were asked to mark them in the range of 1 to 5.Later; all scores for a file were averaged to obtain MOS-LQS score.

The methodology we use here is that one system transmits the original sample (reference audio file), while it passes through the NistNET system that introduces the present network parameters (delay loss etc), and then it reaches the other system

where it is recorded and analyzed. So, the transmitting system plays the audio file in any of the ordinary audio player. The Audio out is inserted into Audio In (Microphone) port of the sound card through an audio cable that has both ends 3.5" audio jacks. On the other end of the network, the voice sample is received by the VoIP client, which is recorded either by the built in recorder or by any other software. In this experiment, Audacity software was used for recording with Skype while Built-in recording function was used for X-Lite recording. This file is then used in Opera software with reference to its original audio file to compute PESQ (MOS-LQO) score.

The third part of the testing was to calculate the R value from E model. As we have discussed before that the E-model is basically an estimation of the voice quality that the voice sample will have depending on the network conditions. As the R values are dependent on the network values, we will just consider packet loss and no delay is taken into the consideration. The shortened general E-model equation (Sun and Ifeachor 2004)is given by

$$R = R_0 - I_{e-eff}$$

Where I_{e-eff} is calculated using equations as described in literature review, where R_0 value is taken as 93.2, in this way, we get the values of R for the corresponding packet loss ratio. Also, we know the mapping function of MOS scores to R values. Hence we can use that as well for mapping the R values to MOS values.

4 Test Results and Analysis

Now in this part of the report, we will look into the results of the tests we conducted and will discuss about them. The three types of test we did were with a audio sample file over three different Quality measuring standards in the metrics of MOS-LQS, MOS-LQO and MOS-CQE.

4.1 Objective Tests based on PESQ (MOS-LQO)

We received the following results when objective testing was done

	Table 1				Table 2				Table 3			
Loss	Test 1	Test 2	Test 3	Average	Test 1	Test 2	Test 3	Average	Test 1	Test 2	Test 3	Average
0%	3.32	3.39	3.44	3.38	3.23	3.35	3.26	3.28	3.31	3.03	3.33	3.22
4%	3.01	3.01	2.76	2.93	3.02	3.1	3.1	3.07	2.9	3.15	2.89	2.98
8%	2.48	2.46	2.69	2.54	2.72	2.65	2.55	2.64	2.67	3.02	2.54	2.74
12%	2.35	2.41	2.28	2.35	2.6	2.5	2.52	2.54	2.71	2.73	2.37	2.60
16%	1.98	1.78	1.78	1.85	2.33	2.15	2.59	2.36	2.38	2.4	2.47	2.42
20%	2.19	2.36	2.03	2.19	2.43	2.17	2.47	2.36	1.35	2.25	2.01	1.87

Table 1: Results of objective testing

4.2 Subjective Tests

The results obtained from subjective testing are given as below

Table 1					Table 2					Table 3				
Loss Corr	Loss	Av .MOS-LQS	MOS-LQO	Av. MOS-LQO	Loss Corr	Loss	Av .MOS-LQS	MOS-LQO	Av. MOS-LQO	Loss Corr	Loss	Av .MOS-LQS	MOS-LQO	Av. MOS-LQO
0.3	0%	2.91	3.32	3.38	0.5	0%	2.83	3.23	3.28	0.8	0%	2.92	3.31	3.22
0.3	4%	3.23	3.01	2.92	0.5	4%	2.73	3.10	3.07	0.8	4%	2.80	2.90	2.98
0.3	8%	3.14	2.69	2.54	0.5	8%	2.29	2.72	2.64	0.8	8%	2.97	2.67	2.74
0.3	12%	2.25	2.41	2.34	0.5	12%	2.31	2.60	2.54	0.8	12%	2.40	2.37	2.6
0.3	16%	1.79	1.98	1.84	0.5	16%	2.14	2.15	2.35	0.8	16%	1.61	2.38	2.41
0.3	20%	1.81	2.19	2.19	0.5	20%	1.93	2.43	2.35	0.8	20%	1.39	2.25	1.87

Table 2: Results of subjective testing

4.3 Objective Tests based on E-model (MOS-CQE)

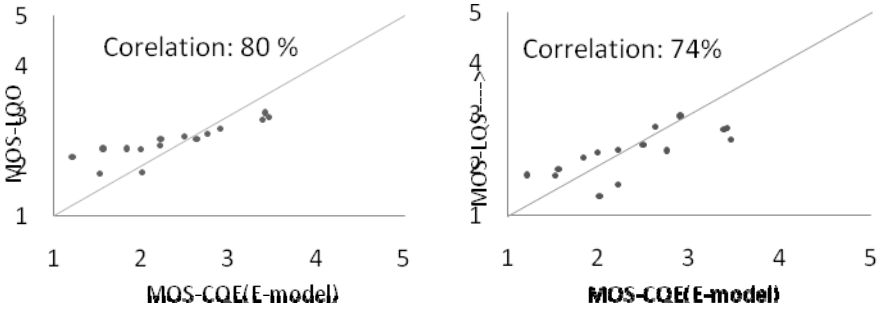
The results obtained from E-Model calculation are as follow

Table 1				Table 2				Table 3			
Loss Corr	Packet Loss	R value	MOS-CQE	Loss Corr	Packet Loss	R value	MOS-CQE	Loss Corr	Packet Loss	R value	MOS-CQE
0.3	4%	65.51	3.38	0.5	4%	66.11	3.41	0.8	4%	67.13	3.46
0.3	8%	51.04	2.63	0.5	8%	53.32	2.75	0.8	8%	56.17	2.9
0.3	12%	38.47	1.99	0.5	12%	43.13	2.22	0.8	12%	48.37	2.49
0.3	16%	27.78	1.52	0.5	16%	35.06	1.83	0.8	16%	42.93	2.21
0.3	20%	18.51	1.21	0.5	20%	28.79	1.56	0.8	20%	38.89	2.01

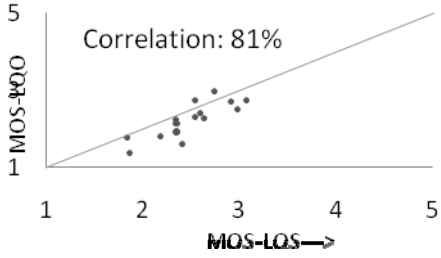
Table 3: Results of Estimation based testing

4.4 Analysis

The first analysis which we will do is the correlation between the three types of Voice quality measures. We have already collected the necessary data in the Testing portion of the project.



(a):MOS-LQO vs MOS-CQE (b):MOS-LQS vs MOS-CQE



(c):MOS-LQO vs MOS-LQS

Figure 2: Pearson Correlation plots between (a) PESQ Objective Values MOS-LQO and E-Model values MOS-CQE (b) Subjective values MOS-LQS and E-Model values MOS-CQE (c) PESQ Objective values MOS-LQO and Subjective values MOS-LQS

The first correlation plot is between PESQ Objective values of MOS-LQO and E-model value of MOS-CQE, in which correlation comes out to be 80%. The correlation between Subjective results MOS-LQS and estimation based E-Model MOS-CQE results came out to be 74% and that is shown in Fig 2(b). Fig 2 (c) is the correlation between MOS-LQS and MOS-LQO. Thus we can see that the objective results have a better correlation as compared with Subjective and Estimate based results. Hence, PESQ objective MOS correlates much better with subjective MOS than E-model MOS.

If we look into the objective test results with correlation of 0.3, there is an interesting point, MOS values increased when packet drop is increased from 16% to 20%. During the testing phase, readings from 0% to 16% were taken continuously, but

NistNET was turned off and on again for 20% loss reading. Hence, when NistNET was started again, the MOS values were not in a continuous fashion but changed. To investigate that, we observed NistNET box with loss correlation of 0.8 with loss percentages of 4%, 8% and 20%. We checked by sending 10, 50 and 100 ping packets through the network and observed that the more the time or packets sent, better the packet drop percentage achieved. For 20% drop rate in NISTnet, the average loss rate in ping packets were 0%, 8% and 21% for 10, 50 and 100 packets sent. Also loss percentages of 4% and 8% were achieved when average packet loss in 100 Ping packets were observed. However, the average loss was not satisfactorily close to the set rate if observed with 10 or 50 ping packets. Therefore, we observed that when time equivalent to 100 ping packets (200 seconds) is given to NistNET before carrying out any test, the average loss rate is almost achieved and results are more accurate.

Another observation that we have was the analysis for the waveform of 16% drop and correlation of 0.3 in the objective testing. We will consider the waveform of the original file first.

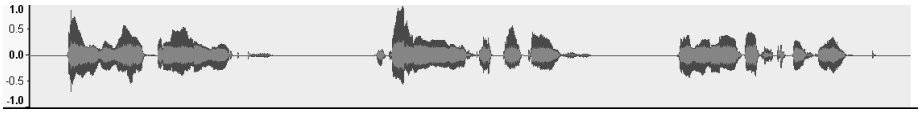


Figure 3: Original waveform

Now we will see the waveform of the file that suffers a loss of 16% with correlation of 0.3.The plot is shown below, which indicates that due to high amplitude at some points, the waveform was clipped.

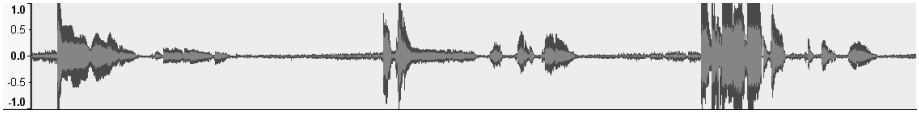


Figure 4: Waveform received from X-Lite

While the original file doesn't have the elements of so high amplitude, some gain was added to the wave file that resulted in the high amplitude and eventually clipping for high amplitude values. Tests were carried out with same parameters, however, clippings or high gain was not achieved. Literature shows that X-Lite has an auto gain function, however, this was checked with Skype and compared with the waveform received from X-Lite, but results show no sign of high gain added by X-lite. Hence, proving that there was some gain added to the incoming speech data, but not from the X-Lite. The waveform for the same parameters as received from Skype is shown below, which resembles the real waveform and no increase in gain is seen.

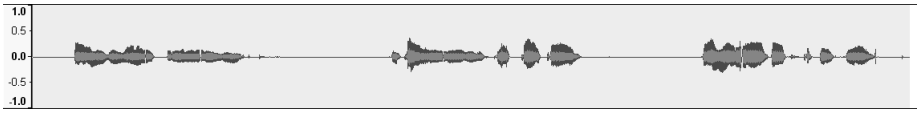


Figure 5: Waveform received by Skype

The reason for the high amplitude of the sound file received was that the system was not calibrated and was sent with high volume or it was the disturbance in the system for example audio cable was not connected properly etc. The standard method for objective and subjective MOS testings require certain calibrations, however, due to time and space constrains, these tests were carried out in a normal Lab environment. Hence we can say that before starting the experiment, the system should be calibrated in order to minimize the error or to localize any type of disturbance that can affect the speech quality. We also used virtual cable instead of physical connection between the input and output of sound card, and find out that the MOS results obtained from Virtual cable are better than physical cable. Hence, in short, system calibration and more use of controlled equipment (software based instead of hardware) should be used in order to minimize the external disturbances that can affect the test results.

5 Conclusion

In this experiment, we correlated PESQ and E-Model with subjective MOS results. A testbed was setup, which resembles a WAN environment. NistNET was used to introduce controlled packet loss in the network. Tests were carried out with two different VoIP end terminals, Counterpath X-Lite and Skype. Standard ITU-T speech sample was sent from one end client to other, and was recorded using audacity software or built-in recorder in X-Lite. The correlation between the Subjective and Objective scores, MOS-LQS and MOS-LQO, came out to be 81 percent. The correlations were measured using the Pearson correlation equations. Similarly the correlation between the Subjective scores (MOS-LQS) and Estimation based scores (MOS-CQE) came out to be 74%. While the correlation between the Objective and Estimation based results came out to be 80%. If we compare the three correlations that we have determined, it's obvious that the Objective scores correlate better (80% and 81%) then subjective or estimation based scores. Thus over all, we can say that PESQ correlate much better than the E-Model. The other conclusions that we obtained from this experiment is about the NistNET (Network emulator) software. We came to an important observation that NistNET should be given enough time (the time of 100 ICMP ping packets echo relies) so that the packet drop rate is averaged at the set rate. This conclusion holds good for packet drop ratios of 20% or less. The final important observation which we obtained from the experiment is that the testbed should be calibrated carefully before carrying out any type of test. For example, there was a high gain input or any cable of the system not connected properly, which introduced this noise and high gain. Due to time constrains, some issues, especially of system calibration were left for future research and analysis. Virtual cable was also used instead of Physical cable that connects the audio out and audio in of the sound card through a driver software. The MOS scores obtained by using virtual cable were better than with physical cable. Hence, we can conclude that

the system should be carefully calibrated for any of the test especially in terms of senders voice gain, and in controlled environment, where external disturbances can be minimized (using Virtual software cable instead of physical one) so that the results achieved are more accurate, or any issue can be localized and analyzed.

6 References

Ding, L. and Goubran, R. 2003. Speech Quality Prediction in VoIP Using the Extended E-Model. IEEE, Ottawa,ON. Available online at: http://portal.acm.org/citation.cfm ?id=1268177.

Dudman, J. 2006. voice over IP:what it is, why people want it, and where it is going. JISC. Available online at: www.jisc.ac.uk/media/documents/techwatch/tsw0604openoffice.odt.

Khasnabish, B. 2003. *Implementing Voice Over IP*. Published by Wiley-IEEE.

NistNET. 2001. NistNET Homepage. Available online at: http://snad.ncsl.nist.gov/nistnet/. (Accessed: 03/03 2008)

OPTICOM. 2007. Voice Quality Testing. Available online at: www.opticom.de. (Accessed: 8/08 2008)

Sun, L. and Ifeachor, E. 2004. New Models for Perceived Voice Quality prediction and their Applications in Playout Buffer Optimization for VoIP Networks. University of Plymouth, Plymouth. Available online at: http://www.tech.plym.ac.uk/spmc/people/lfsun/.

Author Index

Advances in Communications, Computing, Networks and Security

Volume 7

Edited by
Paul S Dowland & Steven M Furnell

This book is the seventh in a series presenting research papers arising from MSc/MRes research projects undertaken by students of the School of Computing, Communications and Electronics at the University of Plymouth. 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 2008/09 academic year. A total of 31 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: Network Systems Engineering, Computer and Information Security, Web Technologies and Security, Robotics, Computing, Communications Engineering and Signal Processing, and Interactive Intelligent Systems.

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.

ISBN 978-1-84102-283-3
90000
9 781841 022833