Advances in

Communications, Computing, Networks and Security

Volume 9

Editors

Paul S Dowland

Steven M Furnell

Advances in Communications, Computing, Networks and Security Volume 9

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

2010 - 2011

Editors

Dr Paul S Dowland
Prof. Steven M Furnell

School of Computing and Mathematics
Plymouth University

ISBN: 978-1-84102-320-5

Printed in the United Kingdom

Preface

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

The publications in this volume are based upon research projects that were undertaken during the 2010/11 academic year. A total of 24 papers are presented, covering many aspects of modern networking and communication technology, including security, mobility, coding schemes and quality measurement. Specifically contributing programmes are: Communication Engineering and Signal Processing, Computer and Information Security, Computer Science, Computing, Network Systems Engineering, and Robotics.

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

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

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

Prof. Steven Furnell and Dr Paul Dowland

School of Computing and Mathematics
Plymouth University, May 2012

About the School of Computing and Mathematics

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

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

Prof. Steven Furnell
Head of School

Contributing Research Centres

Centre for Robotics and Neural Systems

Head: Professor Angelo Cangelosi
Email: angelo.cangelosi@plymouth.ac.uk
Research interests:

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

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

Centre for Security, Communications and Network Research

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

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

http://www.cscan.org

Contents

SECTION 4 Network Systems Engineering

SECTION 5 Robotics

Section 1

Communications Engineering and Signal Processing

Turbo Codes: Interleavers Types

M.Boulan and M.A.Ambroze

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

Abstract

One of the most important and critical component in achieving good performances with iterative decoding of Turbo codes is the choice of the interleaver. Indeed the interleaver is a key component because it allows the decoded extrinsic information to be nearly independent of the observed data in the decoder. This publication describes the structure of different types of interleavers and their behaviour thanks to a turbo encoder simulator developed by the author himself.

Keywords

Error correcting codes, Turbo codes, interleaving, iterative decoding, MAP decoding, BCJR, Recursive Systematic Convolutional codes

1 Turbo codes

Turbo codes were discovered in 1993 by Claude Berrou and his team (Berrou et al, 1993). The typical parallel structure of a Turbo encoder uses two identical Recursive Systematic Convolutional (RSC) codes, separated by one interleaver (Figure 1).

The weight distribution of these codes being close to random codes, their performance is remarkable. However, these codes have a low free distance and lose lot efficiency for a low Signal to Noise Ratio. Therefore, an optimal interleaver has to improve the weigth distribution and the minimal distance of the Turbo code. Thus the interleaving function plays an important role on the performance of Turbo codes.

The purpose of the interleaver is to offer each encoder an uncorrelated (random) version of the information, resulting in parity bits from each independent RSC encoder.

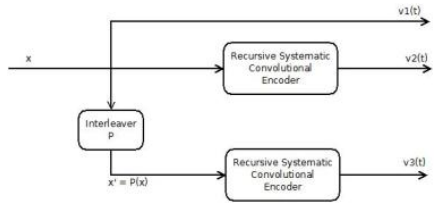


Figure 1: 1/3-rate Turbo encoder

2 Turbo decoding

There are two main algorithm to decode the code message. One is a modification of the well-known Viterbi Algorithm (Viterbi, 1967) and is called Soft Output Viterbi Algorithm (SOVA). It consists in finding the most probable output sequence by drawing the Trellis diagram. The other one is the Maximum A Posteriori Algorithm (MAP), which is often referred to as the BCJR (after Bahl, Cock, Jelenik and Raviv) who proposed it in 1974 (Moon, 2005). MAP is very similar to the Viterbi Algorithm but while Viterbi computes the maximum likelihood codeword (a priori), MAP computes the a posteriori probabilities of symbols.

SOVA and MAP are usually comparable, however the MAP algorithm is used in the most of Turbo decoders because it minimises the bit error probability (Rekh et al, 2005).

3 Interleaver Types

3.1 Block Interleaver

The interleaver the most widely used is the block interleaver, also called rectangular interleaver. It considers the initial positions are written row-wise in a matrix L1*L2. These positions are permuted by reading column-wise the matrix.

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Interleaver(i)	0	5	10	1	6	11	2	7	12	3	8	13	4	9	14

Table 1: Block interleaver, L1=3 L2=5

Ramsey (1970) proves we can construct an optimal block interleaver by choosing L1 (number of rows) and L2 (number of columns) such as:

- L1 + 1 and L2 are prime
- L1 + 1 < L2.

Therefore the case above (Table 1) is an optimal block interleaver.

3.2 Diagonal Interleaver

The diagonal interleaver is a modification of the block interleaver (Morelos–Zaragoza, 2001). Instead of reading column-wise, the matrix is read diagonally from left to right and top to bottom.

0 (start)	1	2	3	4
5	6	7	8	9
10	11(end)	12	13	14

Table 2: Diagonal process

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Interleaver(i)	0	6	12	1	7	13	2	8	14	3	9	10	4	5	11

Table 3: Diagonal interleaver, L1=3 L2=5

3.3 Helical Interleaver

The helical interleaver is also another version of the block interleaver, proposed by Adrian Barbulescu and Silvio Pietrobon (1994).

0 (start)	1	2	3	4
5	6	7	8	9
10	11	12	13	14 (end)

Table 4: Helical process

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Interleaver(i)	0	6	12	3	9	10	1	7	13	4	5	11	2	8	14

Table 5:Helical interleaver, L1=3 L2=5

4 Results

Figure 2. shows the results of the simulation for different types of interleavers (Block, Diagonal & Helical). The chosen interleaver size is 125 (L1=5, L2=21) for each of them. The simulation consists in encoding a 125-length message with a 1/3-rate Turbo code, then modulate the encoded message, add noise and finally decode it with a BCJR decoder (8 iterations).

From the simulation we find that the diagonal interleavers give the best performance.

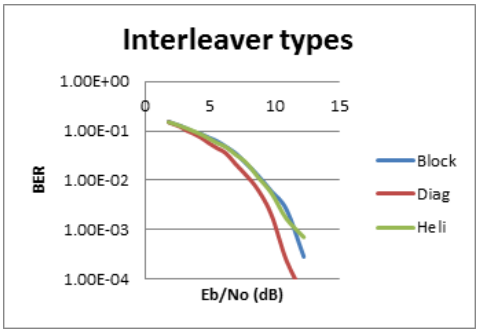


Figure 2: Interleaver types

5 References

Berrou, C., Glavieux, A., and Thitimajshima, P., (1993) Near Shannon limit error correcting coding and decoding: Turbo codes. *IEEE International Conference on Communications*, pages 1064-1070.

Barbulescu, S.A. and Pietrobon, S.S., (1994), Interleaver Design for Turbo codes. *Electronic Letters*, 30(25), 2107-2108.

Moon, T.K. (2005), Error Correction Coding: Mathematical Methods and Algorithms, Wiley.

Morelos–Zaragoza, R.H., (2001), The Art of Error Correcting Coding. Wiley.

Ramsey, J., (1970), Realization of Optimum Interleavers. *IEEE Transactions on Information Theory*, 16(3), 338-345.

Rekh, S., Subha, S. and Shanmugam, A., (2005). Optimal choice for turbo codes. *Academic Open Internet Journal, Vol. 15, 2005*

Viterbi, A., (1967), Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. *Information Theory, EEE, 13, apr 1967*.

The Implications of Social and Technological Developments in Emerging Mobile Technologies

S.A.Kumar and P.Filmore

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

Abstract

Over the last few years the telephone devices have played a vital role for the communication of society. The development of cellular and mobile phones started to grow in a wide manner which resulted in other applications of mobile devices. The growth is forecasted to have a massive difference in the future. A short-term study was made and a simpler method to examine the details of the technologies and influences of mobile phones and development paths has been made out from the sources of all the information available.
The data collected is tabulated based on the current presence of technologies and forecast of technologies. The tabulation also includes the forecast of development paths. From the tabulated results it is observed that technologies will be increased in the country of United States. The U.S and Great Britain are predicted to have the 5G technology in the near future and the U.S nation may also possess robots in every homes in the future say within seven to 10years. Great Britain, India, China and Middle Eastern parts will move closer to technologies such as mobile wallet, mobile health care and 3D learning in the future. The country of China is forecasted to have 4G technology soon, next year and the Chinese will have mobile wallets in the next few years. According to the forecast done, India is predicted to launch a social network for educational purpose for students. The Middle Eastern countries may launch 4G technology similar to China. Africa will show less concentration in the development of future trends due to their famine conditions. This research is totally based on the focus of forecasting technologies and the paths of development.

Keywords

Mobile phones, forecast, technologies, development paths

1 Introduction

Communication at a longer distance became much more convenient since the invention of telephone. People were able to communicate with each other in the world with the help of telephones. In the twenty first century, telephones became a part of everyday life for a billion people. Later the development of cellular phones, cordless phones was noticed (Katz, J.E. and Aakhus, M., 2002). These were based on analog FM technology and currently mobiles are the highlight in the telephone field (Stuber, G.L., 2005). Lots of new applications have been seen in the upcoming mobiles.

Latest phones have got the feature of even watching television videos and news. Smaller and compact size mobiles with the current characteristics are becoming even

more popular and this made the public to completely move towards the mobile technology. A thorough study on the collection of the developing technologies from all the available sources and forecasting even the minute technologies used in each development are done. Also a detailed study of various impacts such as the social, economic and political impacts of the mobile technologies is discussed.

1.1 Technological Forecasting

Technological forecasting is a prophecy of the forthcoming features of convenient technologies, methods or developments. In a period of prompt technological amendment, the corporate procedures should be related to the complete estimate of future technology. Recognized logical techniques are accessible to aid people to formulate sensible predictions of technology. The estimates arranged by these approaches can be freely elucidated to others and are more tolerable to non-technological administrators. The forecasters study about the machines, techniques, functions and processes involved in a developing application. (Martino, P.J. 1993)

1.2 Current Mobile Technologies

The two main booming technologies in the present world are internet and mobile devices. Wireless technology is in the range of conflicting systems. This technology is present from ancient age to communicate between the computers without wire. The most common wireless technology is Wi-Fi, Bluetooth, Infrared and Wi-Max (Dhawan, 2007). Mobile banking offer channel to perform services online in mobile devices. According to You et al (2006), a mobile robot based on Bluetooth expertise is surprising the current mobile technology world. The healthcare industry helps in getting the benefits of telemedicine. Growth will be observed in the UMTS and mobile Internet based m-Health systems (Istepanian, 2003). Latest improvement in mobiles has directed to the residence healthcare application.

1.3 Forthcoming Technologies

The PC or laptops do not have Intel inside; instead they possess a chip devised by the Cambridge. This chip is called the ARM (Kelly, 2011). JANET 3G, permits educational and inspire staff to contact dynamic sources as study facts, computer-generated learning surroundings and reference library collections on the move (Turner, 2011). Mobile Cloud Computing denotes to an arrangement where both the data storing and data device happen outside the mobile device (Perez, 2009). Blackberry is all set to introduce a fresh tablet known as the Playbook (Mclnnes, 2011). The latest surprise for the mobile field is that the Vodafone Company is all set to launch its new mobile phone- Vodafone 555 Blue. A new application for mobile devices has been developed by the NASA. This application will be available only on mobile phones based on Android. Online shopping technique was introduced for the people to feel convenient and easy with shopping goods and it was welcomed by the society. Following this there is development of mobile shopping. Technology has developed so much that human brain can be closely duplicated by a microchip.

Figure 1: BlackBerry PlayBook tablet (Mclnnes, 2010)

Figure 2: NASA's application (Warman, 2011)

2 Methodology

The methodology adopted in this is the qualitative research method in which all the data about the various mobile technologies are collected. The information is collected based on the focus of mobile technologies and various influences of countries in the forthcoming years. In this project, the influences such as the Political, Economic and Social for few countries in the future years are discussed of few nations.

3 Countries in the Future

3.1 China

Housing is dominant in the country's revenue. The income of the nation is growing high and is believed that the economy of this country is large than America since few years. The private economy is developing significantly. The citizens of China are no aliens to entrepreneurship. The administrators and officials of China concentrate and focus on next few decades. The country has also decided to turn away its future funds and assets from the United States and wants to make sure of the welfare of China's money possessions. The earnings in the metropolitan cities of China are very high when compared with the earnings in the rural area. It is predicted that only after few years, a reasonable sharing of the incomes will be provided to the citizens. The country also has substitute for Facebook, the social network called Renren. This website has nearly 5million customers each month.

3.2 United States

IT system has turned out to be a part of predictable insight. There are disputes going over the grade of the administration of America. The discussion was on the American government liability indicating that there is a one in three possibility downgrade in America's credit ranking by 2013. The United States of America has a sluggish economy and unemployment is seen around 9% and the housing market is almost crushed. It is predicted that China will surpass the largest economy, America. It is also forecasted that in the end of this century (Gardiner, 2011). This forecast was based on the debt crisis of the United States. It is also predicted that Sarah Palin will

be the next president. The Google+ site will be improved with the installation of gaming which will help them to gain more users.

3.3 India

It has been said that the country has not succeeded in controlling bribery, corruption and public borrowing, gone behind on infrastructure and proven powerless to make conclusions. The country is under corrupted administrations when it comes to political. The busiest metropolitan of Indian nation is the Mumbai city. The administration has announced to launch the new development plan (DP) in 2016. The city of Rajasthan will launch a social network which will comprise of education and theory learning stuffs for kids (Economic Times Tech, 2011).

3.4 United Kingdom

The growth is getting flattened. The downgrade is due to the suspension of work of the top carmakers. The government will upgrade the rail system by launching a coastline from Great Western and east coastline. Modifications in nursing sector and television sector will be seen in the following years.

3.5 Africa

The economy is going down with famine and drought. There is no proper trade and activity in the continent. Millions and millions is been lost by some Mobile Telecom Corporations and unlawful lotto workers. The society of the continent is totally in a bad state. The disabled persons are ill-treated and not considered. Another factor threatening the society of the continent is raping of women and slavery is increasing too. With all this, poverty is haunting the continent and assistance is needed for the people.

3.6 Middle East

The economy of Middle Eastern part depends on the exports of lubricants to other countries. Patriarchal economy is taken place in the countries. The nations of the Middle Eastern parts are set to get the approval of overseas trading in the future. Arabism is undertaken in terms of management. Construction of hotels and restaurants will be in the future by the government the administrations believe that this will enhance the growth of the nations. The nations lack in education and learning. It is predicted that there will be measures taken in the future for improving education.

4 Results

From the tables shown in figure 3 it is observed that China will be the leading economy in the near future and politically strong too. The United States of America is forecasted to go down economically and the government will launch employment plans for the growth of the nation. In terms of economy, India is stable and ready to purchase technologies. Politically the country is under corruption and terrorism. United Kingdom is predicted to slow down in future and government will take

measures to bring down recession. Similar tabulations have been done for Africa and Middle Eastern countries. Africa is the one which is sluggish and is forecasted to decline in future. Middle Eastern parts are forecasted to concentrate on innovation and increase their economy. So the overall view is that technology is predicted to develop more in the countries with the support from the administrations of countries.

CHINA

	ECONOMY	POLITICAL	SOCIAL	TECHNOLOGIES
PRESENT	Production is high in China which the foremost plus for the nation	Politically the country has good relationship with the United Nations	There are currently no access to social webs such as Facebook, Twitter and Google+	Currently China is not concentrating more on technology yet it tops the list of supercomputers
	Exports (porcelain) are more to North America and Europe	Both China and America are recently tied up with few combined declarations	At present there are availability of domestic webs- Renren and Weibo	3G technology available
	GDP is currently 9.28%	The government is involved in world peace-making which makes it politically strong by having better bonding with other nations		No much improvement in the field of technology
FUTURE	The debt crisis of Europe will affect the future economy of China	Inspite of the declarations the Chinese government may cancel their exports with America due to the debt crisis of U.S	People will use more mobiles than the computers in the future	Robot workers will be seen in the future
	The future GDP Of the nation will be nearly 19billion in the next few year	There will be more exports to other nations possibly India	More population and less farming will be done	Version 3 and Version 4 of Bluetooth will be available
	China will overtake the United States in the following future and will rank as the No.1 Economy	Production will be increased more		4G technology will available in future

Figure 3a: China

UNITED KINGDOM

	ECONOMY	POLITICAL	SOCIAL
PRESENT	The economy is slowing down and losses are observed	Government is failing to avoid unemployment	People move towards technology
	Top car makers suspended employments which affects the economy	Currently the government's age for pension is 65	Current population is high
	Additional bank holidays and the Royal Wedding which included spending affected the economy	The management has not worked on the rail transport system to few cities	Social networks are used majorly in the nation
	Investments in the forthcoming Olympic games is also one of the reason for the slowdown of growth	No preventive measure taken for economic losses	Wiring television available in the nation
FUTURE	Few measures like the adult education is predicted to happen for the betterment of ecology	As outcome of private divisions, forecasting is that there may be employments of around 2.5million in the future	Climatic changes will lead to numerous deaths of people in future
	It is forecasted that the measures will be taken to withstand the changing weather conditions which reduces the growth	The management will cut electricity to the cities of England in the next few years	Population will increase more than current
	Recession will be seen in the near future	The government will shut down the coal power plants in the country of Britain	Nursing sector will get modified in the future
	The bank of England will cut charges in interest in the future and HP will buy autonomy which will enhance the economic growth	The age of pension is raised to 66 by the administration and will be under implementation in the future	Digital television will be launched in the future

Figure 3b: UK

INDIA

	ECONOMY	POLITICAL	SOCIAL
PRESENT	The country has gone down by a tenth dollar this year in stock markets	India is undergoing terrorism and	Poverty and scarcity is found common in the nation
	Cement, Property and construction has faded in their turnovers	No examinations taken by the members of parliament before nomination	Currently the nation is one among the top five countries in terms of population
	Rubber and tyres give good turnovers	BJP and Congress parties are in war and do not take any steps for the nation's growth	All the social networks such as Facebook, Twitter and LinkedIn are available
	Few states like Gujarat offer good economy to the nation by farming	Corruption and bribery is haunting the nation	4G technology is absent
FUTURE	China and few countries will agree to export goods to India	Terrorism will be more in future	It is predicted that the poor and needy will be given assistance and poverty will be eliminated
	Few short term and long term growth measures will be taken in the future for improvement of economy	It is expected that be that the members will take the examination before nomination in the future elections	Increase in population will be seen in the near future and it is forecasted that India will overtake China in population
	The Reserve bank will increase the main charge of interest by 25	Steps will be taken to eliminate corruption and bribery	Development of new social webs for education is predicted to happen in the following years
	The economy due to farming is predicted to increase by 6 to 7%	Predictions are that there will be new development plans for the political betterment of the nation	Huge number of internet users will be from India in the future

Figure 3c: India

UNITED STATES

	ECONOMY	POLITICAL	SOCIAL
PRESENT	Though known to be one of the strongest economy, recession taking place currently	Government is not taking steps for controlling recession and downgrade	The richest people of the world such as Bill Gates and few others are residents of this nation
	Currently debt crisis in the nation	Management is slow even in approving civil agreements which is one of the reason behind slowdown	Citizens offer 12.4% of their earnings to the country
	Current GDP -1.8%	Republicans and Democrats are in war	Overcrowding and accommodation is bringing down the economy
FUTURE	America will be surpassed by China.	Forecasted that Sarah Palin will be the next president	It is predicted that funds will be provided for the middle class citizens in the future
	The GDP is forecasted to go down due to debt	The administration of United States is expected to come to an end in next few years	The overcrowding transportation is predicted to get lessened by effective circulation of goods
	Universal economy strategies to be revised in the future for the economy to function	Measures should be taken by the management to sustain the agreements with other countries	In the following few years, it is forecasted that there will be modifications in the women's health care system
	The slowdown of economy will affect the whole global economy in future	Overall it is forecasted that the nation will go down in the next few years	The Google+ site will be improved with gaming in the near future

Figure 3d: United States

From figure 4, it is observed that America will top the list in the development of technologies followed by India, China and Great Britain. These nations are forecasted to concentrate more on technologies in the following future. Africa will be slowing down and will not show development in innovations.

COUNTRY	CURRENT TECHNOLOGIES	FORTHCOMING TECHNOLOGIES	REFERENCES ON FORTHCOMING TECHNOLOGIES
CHINA	• 3G technology • Mobile learning • Mobile banking • e-learning • e-health	• 4G technology • Mobile wallet	China has got hold of an arrangement to launch 4G. See Alex., (2011) Country of China will possess the mobile wallet technology in the following future. See Tan. F., (2011)
UNITED STATES	• 3G technology • 4G technology • Mobile wallet • Mobile learning • e-health • Playbook	• 5G technology • Robots in office and home • Walt Disney Mobile for Kids	Apple will launch the 5G technology in the American nation in a short span. See InfoBarrel, (2011) The students from Cornell University have developed an algorithm for the robots to recognise objects and is predicted that it will be launched in the U.S in future. See Aron. J., (2011) The Walt Disney will launch a mobile package for kids in the following future. See Baig. E. C., et al (2006)

Figure 4: Part of the final table

5 Discussion

From the results and analysis done, China is a country which concentrates more on production and ranks as one of the top economies in the world. In terms of production the nation of China tops the list. In United States, technologies and resources emerge from the American nation's production. Known as one of the strongest economy of the world, the government is strong in enhancing the growth as well increase the use of technologies. India is mutually developed in both technology and economy. When it comes to Africa, the continent is totally down at present and is difficult for them neither develops nor purchase technologies in the future. The countries of Middle Eastern part do their living on fuel and lubricant resources.

5.1 Future Work

With the technologies budding almost every day, more information can be gathered on technologies. This research is wide ranging and future research can be done by adding every day updates on technologies and statuses of the countries on a website. Any student or researcher who wishes to continue this research with designing a website must know the idea of technological forecasting.

The researcher can have fields such as technological forecasting, present technologies in world and the influences of nations in world. The researcher should be skilled in website programming languages for designing the website. Furthermore, there can also be addition of an option for a small survey link so that users can drop in their ideas and expectations on how technologies should be in the future. With this readers can gain information more easily instead of searching for information on each country. The society will be aware what's new in their nation. Technological forecasters can be active on this website, to know the expectations of people and can fulfil the expectations.

6 Conclusion

From the research and the results it is forecasted that the technologies which will be available for the people in the future are mobile wallet, mobile shopping, mobile healthcare, Facebook phone, social website for education, 3D learning, data miming and chip replicating human brain. It is forecasted that they may be presence of robots in each home and office in the future.

From the results, it is also observed that China will be the top among the nations in the world. The production of china will increase more which will lead the country to top the list the list. The United States of America is expected to be surpassed by China in the future. Economically the gross domestic product is forecasted to go down due to the debt crisis of the nation. Indian nation will have goods and trading from other countries like China in the future. The economy of the country will enhance by farming. The political leaders will upgrade few short and long term goals for the betterment of education in the future. There will be more terrorism in the future. The country of Great Britain will move closer to recession in terms of economy and is predicted that there will be measures taken to withstand the factors affecting the economic growth. The continent of Africa is predicted to go down economically and the gross domestic product will remain the same as the current. It is forecasted that the economic growth may be likely improved with the incomes from mining. The Middle Eastern parts of the world are predicted to set overseas and abroad agreements in future. This may improve the growth of the countries in future.

From the development paths of the countries taken in research, Africa, India and China are predicted to enjoy the facility of 4G technology in the future. The countries of United Kingdom and United States will go one step ahead and will launch the 5G technology. The nations of Middle East are predicted to have 4G technology and mobile wallet in the future.

7 References

Gardiner, K. D., (2011), "China's One-Child Policy: What Does the Future Hold?", *China Musings.Com* Available at: http://chinamusings.com/2011/05/27/chinas-one-child-policy-what-does-the-future-hold/ accessed on: 6/8/11

Istepanian, H.S.H., and Lacal, C.J. (2003). "Emerging Mobile Communication Technologies for Health: Some Imperative notes on m-health", *Proceedings of the 25th Annual International Conference of the IEEE EMBS, Cancun, Mexico*

Katz, J.E. and Aakhus, M. (2002), "Perpetual Contact, Mobile communication, private talk, Public Performance", revised ed., London: Cambridge University, pp. 139-209

Kelly, S., (2011), "The Future of Mobile Technology", *BBC Click* Available at: http://news.bbc.co.uk/1/hi/programmes/click_online/9464939.stm accessed on: 20/7/11

Martino, P.J., (1993), "Technological Forecasting for Decision Making", 3rd ed., Ohio: McGraw- Hill Publication, pp. 92-220

Mclnnes, K., (2010), "More Details about Upcoming BlackBerry Playbook Tablet", *Blackberry cool* Available at: http://www.blackberrycool.com/2010/09/27/more-details-about-upcoming-blackberry-playbook-tablet/ accessed on: 22/7/11

Perez, S., (2009), "Why Cloud Computing is the Future of Mobile", *Read Write Web* Available

Stuber, G.L., (2004), "Principles of Mobile Communication", 2nd ed., Massachusetts: Kluwer Academic, pp. 135-286

Turner, B., (2011), "Janet 3G Announced for Mobile Learning", *Tech Watch* Available at: http://www.techwatch.co.uk/2011/04/26/janet-3g-announced-for-mobile-learning/ accessed on: 20/7/11

Warman, M., (2011), "NASA Official App for Android", *The Telegraph* Available at: http://www.telegraph.co.uk/technology/mobile-app-reviews/8651433/Nasa-Official-App-for-Android.html accessed on: 20/8/11

Study of Communication and Data Interfaces in Earth Observation Satellites Based on their Focus of Application

G.T.Selvan and P.Filmore

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

Abstract

Over the last decades the earth observation data has played an important role for the well being of society and the earth as a whole. This dependence of the human race on the space data is ever increasing and expected to have a massive breakthrough in various needs and applications in future. This study attempts to identify and analyse the instruments and other technologies used in all the earth observation satellites till date, tabulating them with their characteristics and their significance. This study is done based on the secondary qualitative information collected from committees, organisations and data available free on the web. A brief study was made and an easier and better method to analyse the details of earth observation satellites has been figured from the review of all the information available. All the information gathered is tabulated according to the focus of their application i.e. land, water, atmosphere and disaster of the instruments carried by the earth observation satellites designed. This method would prove useful for the researchers and other users, mainly students which would give them an idea about the instruments and technologies comparison for the various satellites that are used for a particular focus. This research which is done on the focus of earth observation satellites on the earth summarises the different communication technologies used between earth and the observation satellites. Moreover the best method and the effective technologies has been analysed which is resulted from the table that had been created. Finally the researched information is distributed to the users through a website for access.

Keywords

Earth Observation Satellite, Satellite data, Applications

1 Introduction

Geographic information acts as a basis for understanding the geographic space from the spatial information collected by satellites. Society has now changed to a geo-information society with access to internet and mobiles associated with spatial and earth observation data. The data which is collected about the earth's resources are analysed and are used for the well being of the society (Kainz, 2005). Every satellite is designed specifically for a particular purpose or to serve an application with special sensors and instruments supporting them. Development in the telecommunication technologies and recent trends in sensor technology has made it possible to build small satellites to have the same potential as the large satellites and this has created an opportunity for all countries to develop their nation with some

research in space technology and earth observation (Karatas, 2009). British company, Surrey satellite technology help in providing small satellite missions for operational and commercial purposes. They help in designing communication payloads and launching them for many commercial applications including the earth observation and imaging (SSTL, 2011).

2 Earth Observations Dominance

Satellite imagery and other remote sensing data's are analysed from various organisations and surveys which are made with the information retrieved. Some of the private companies like Space Imaging, Orbimage, DigitalGlobe, GlobeXplorer, Spot Image, ImageSat International, and EarthSat use the imaging information from the earth observation satellites and are used by the governments and other organisations related to remote sensing for numerous applications (Luccio, 2005). Demand in the society has increased because of the increased web portals publishing, and the companies compete each other to provide the society with the latest images and data retrieved from these earth observation satellites.

There are numerous developments in this field of earth observation with many breakthroughs in the technology and the instrument being used. One of the crucial developments was the use of the multispectral sensors and which used the infrared and microwave regions to monitor the earth surface. A example is Nimbus which concentrated on bringing the details of the ocean topography, ice sheets. The sensors consists of the cameras, infrared and microwave radiometers and spectrometers, colour scanners and back scatter sensors Another breakthrough in the technology came with the emergence of the SAR (synthetic aperture radar) which can sense through the cloud cover and can gather details about the height, scattering properties of the land cover from knowing the time delay between the emission and return of the signals (Tatem et Al, 2008).

Earth observation by satellites is basically an application driven programme which concentrates on certain special applications and these satellites are sent on certain application driven motives. Some of the major applications on which remote sensing satellites concentrate are the agriculture, land use, forestry, urban development, environment, geology, coastal resources, marine resources, snow, glacier, volcanoes, disaster monitoring, mitigation and infrastructure development (Navalgund et Al, 2007). Earth observation on land, atmosphere, water and natural and dangerous hazards have become more important thus developing society and its awareness of all the issues, particularly reducing the losses due to these hazards and protecting the global environment.

Evolution of satellite data to the mobile phones and other climatic events assistance from the satellites and applications of the space data motivated my research over this study of earth observation satellite and technologies. With ever increasing climatic disaster like cyclone, floods, earth quakes, volcanic eruptions with almost all have now been forecasted and are helped for reconstruction and analysing the effects through the data observed from the satellite. Thus knowing that the data collected from the earth observation satellites and other space data are used to assist the research findings and analysis by the space organisation had resulted in the interest

over the technologies they use and the instruments they have for monitoring the earth.

3 Categorisation Based on Focus

This research is based on the two main questions and they are:-

1. What are the satellite missions that are designed specifically for earth observation and the corresponding interfacing technologies that help for a particular application?

2. How to summarise all the satellites and the corresponding instruments, in order for a clear understanding of all the technological and communication interfaces in these earth observation satellites?

The study method that is used determines the ways to answer these two questions and is based on the focus of the earth observation satellite on the application. Though the satellites and instruments can also be divided based upon their orbits, wavelength regions etc. Here they are done on their basis of their focus of application in this research. The main objective to have these categories based on focus is to have a clear idea of the processes, instruments and technologies that is being used, usually for the same application with some advancement in order to retrieve the data and work on post processing. The other main reason for using the classification in terms of using the tabular columns is that if the research was done in studying the technologies and other specification of a satellite with some tabulation for each satellite or a sensor instrument, then this would end up with many pages of data for analysis. But using this method of tabulating the technological details with respect to their application, author (1) did not have the necessity to have a long table and the user can navigate and research the satellite details with their application of their need which makes easy for the further researchers and students to understand the interfacing technologies in the earth observation remote sensing satellites.

This research on the instruments and technologies of the earth observation satellite was started by taking the list of all earth observation satellites that are present in space till this date and thus identified the possibilities of the classification of all the satellites in order to make the research useful for the further researchers to understand the study of instruments and technologies that are used for monitoring. It thus came to a result of classifying the satellites based on their application focus would help, as there were no previous study and classification that have been done with respect to this focus. Then, all the technological details of each earth observation satellites, where gathered in order to find a way to tabulate the different satellites with their focus. Figure 1 shows part of the table developed which classifies satellites in terms of their application focus i.e. on land, water, atmosphere and disaster.

EO SATELLITE NAME	FOCUS ON LAND	FOCUS ON WATER	FOCUS ON ATMOSPHER	FOCUS ON DISASTER
ACRIMSAT			✓	
ADEOS(MIDORI)-1	✓	✓	✓	
ADEOS(MIDORI)-2	✓			
AISSAT-1		✓		
ALOS	✓			✓
AQUA		✓		
ASTER		✓	✓	✓
AURA			✓	
BELKA	✓			
CALIPSO			✓	
CARTOSAT 1	✓	✓		
CARTOSAT 2	✓			
CBERS 1,2	✓	✓		
CBERS 3,4	✓			
CHAMP	✓		✓	
CLOUDSAT			✓	
COSMO-SKYMED				✓
EARTHPROBE/TOMS			✓	
ENVISAT	✓	✓	✓	✓
ERS 1	✓	✓	✓	
ERS 2	✓			
FENG YUN			✓	
FORMOSAT 3	✓			
FORMOSAT 5	✓			
GEO EYE	✓			
GOSAT				✓
GRACE	✓			
ICESAT		✓		
IKONOS 2	✓			
IMS-1	✓			
IRS A,B	✓	✓	✓	✓
IRS C,D	✓			
JASON-1		✓		

Figure 1: Part of the table showing earth observation satellites based on focus. (A-J shown, compiled-December 2010)

4 Methods adopted for classifying

The author (1) classified the focus of the earth observation satellites into four main categories which the author believes are more useful and they are land, water, atmosphere and disaster, as almost all the earth observation satellites was covered under these categories. After identifying the main categories author (1) made several discussions with author (2) to identifying the different fields for tabulation, required for the better understanding of the interfaces in satellites. They are the communication technologies which discusses about the uplink, downlink and other spectral bands with their frequencies. Next field is the data processing where the data

rate and information regarding the data compression, conversion are discussed for every instrument carried by the satellite. Applications of every instrument and the web links for further information are added as it would give a better understanding.

Separate tables are created for each focus of application. When the table is created for the application focus on land, the following satellites which concentrate for the application of land monitoring are identified from the table that were created during analysis of the focus of different earth observation satellites. Thus the different sensors that the satellites of our interest carry are researched and finally the instrument that the satellites use for the purpose of land monitoring is found and tabulated. Other sensors which concentrate on other application such as water or atmosphere other than land are not included in the land table.

Several sources are researched for the various technologies and the mission's websites and books are studied to identify the different methodologies and other technologies that they use for the land observation. Thus the communication technologies and the data processing and other data related processing methods are studied to classify them and tabularize them for the clear understanding of the information researched. But sometimes some sensors have multiple applications, which are thus included in more than one category based on their focuses. Similarly three other tables are created for every application focus containing all the communication technological interfaces details with their information related to data processing and thus proving with their significance towards their application focus using the same method that was adopted for the focus on land.

5 Website Designing

Figure 2: Web pages

Finally a website is created using a PHP and CSS script and edited with Adobe Dreamweaver as a means of making this research to reach the students and others user for easy access and be helpful. The use of the hyperlinks makes the information

access easy and the screenshots are shown in figure 2. The website is created with various tabs that would give clear understanding of the research that has been done. Basic information tab is included in the website in order to include all the basics of the remote sensing and their technologies discussing about the satellites, orbits, sensors and electromagnetic spectrum. Video links and pictorial representation of the concepts are added to make the website more users preferable and thus making the concept reaches the user and students effectively. Separate web pages are created for each and every focus application and their corresponding technology that are discussed in the table such as instruments, communications, data and application. All the summarisation done as a result of the research is included in the website with all the web links which helps the users to get more information about the earth observation satellites and their instrument technologies.

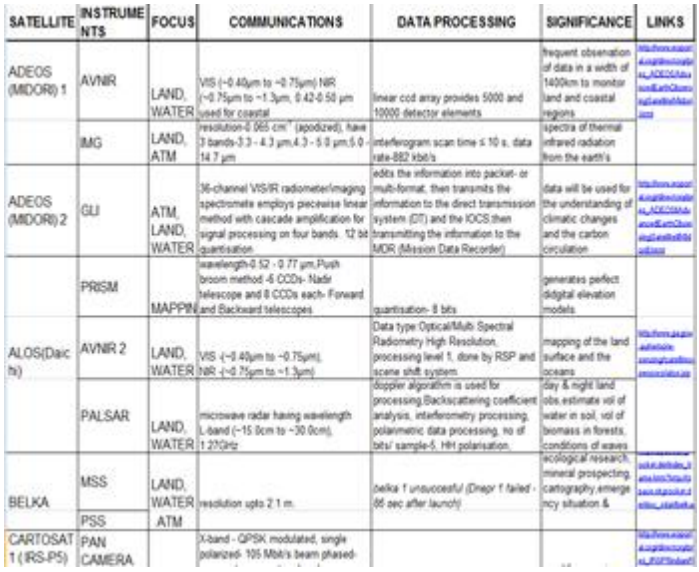
6 Difficulties

Various difficulties happened during the decision making of identifying the methods to tabulate these earth observation satellites considering the different option in hand. This was a challenging task, as when deciding the different fields that need to be used in order to bring details that would be necessary to perform a detailed study about the different interfacing technologies in the satellites. There were some difficulties in making the website more dynamic and thus left for the future work. Moreover there were no access to most of the satellite data and hence this needs more research over several books, archives, organisational reports, space agency website to retrieve the technological details that were needed for the summarisation in the tables.

7 Results

From the table shown in figure 3 that has been designed with all the interfacing communication and data processing details as a result of the research gives more comparison of the different methodologies that the earth observations satellites contain perform their activities. The instrument detail gives the details of the various sensors that are used for the application of land, water, atmosphere and disaster, thus clear for the researcher and users to understand the different sensor used for different application. The communication technology infers the different bands that the satellites operate for the downlink and uplink with their transmission frequencies. The band L is the preferred band by the land observation satellites as this help in monitoring the land cover, surface moisture and vegetation and they are not affected by the dew particles compared with X and C. The land monitoring uses the HV and VH polarisation when compared to the HH and VV because the vegetations are not distinguishable in the latter. This band provides the resolution of up to 25m. Moreover from the table that had been resulted it is very clear that the S band is used for the TT&C (telemetry, tracking and control) and used for the communication links for the supporting instruments. Ka band is the preferred band for the monitoring of the surface temperature and operate in 37 GHz. Ku band is the preferred band for the radar altimeters and thus help in determining the earth parameters from the distance from the radiation gets reflected and operate in 13.8 GHz. C band is also preferred for the land monitoring and being in the middle of the microwave bands, is considered for more applications where resolution is not more concerned. X band is

the preferable band for the imagery and this can provide up to 5m resolution. The X band is used for its low wavelength and high resolution provided and thus can be used by the satellites to provide high resolution imagery of the earth's resources. Moreover this band have the ability to observe tiny particles and thus used for the weather observation and tiny water particles and aerosol in the atmosphere. Thus from the table it is found that most high resolution imagery and tiny article observation application for the satellites are done through the X band.



SATELLITE	INSTRUMENTS	FOCUS	COMMUNICATIONS	DATA PROCESSING	SIGNIFICANCE	LINKS
ADEOS (MIDORI) 1	AVNIR	LAND, WATER	VIS (~0.40µm to ~0.75µm) NIR (~0.75µm to ~1.3µm, 0.42-0.50 µm used for coastal	linear cod array provides 5000 and 10000 detector elements	frequent observation of data in a width of 1400km to monitor land and coastal regions	
	IMG	LAND, ATM	resolution-0.065 cm^{-1} (apodized), have 3 bands-3.3 - 4.3 µm,4.3 - 5.0 µm,5.0 - 14.7 µm	interferogram scan time ≤ 10 s, data rate-882 kbit/s	spectra of thermal infrared radiation from the earth's	
ADEOS (MIDORI) 2	GLI	ATM, LAND, WATER	36-channel VIS/IR radiometer/imaging spectrometer employs piecewise linear method with cascade amplification for signal processing on four bands. 12 bit quantisation	adds the information into packet- or multi-format, then transmits the information to the direct transmission system (DT) and the IOCS,then transmitting the information to the MDR (Mission Data Recorder)	data will be used for the understanding of climatic changes and the carbon circulation	
	PRISM	MAPPIN	wavelength-0.52 - 0.77 µm,Push broom method -5 CCDs- Nadir telescope and 8 CCDs each- Forward and Backward telescopes	quantisation- 8 bits	generates perfect didgital elevation models	
ALOS(Daichi)	AVNIR 2	LAND, WATER	VIS (~0.40µm to ~0.75µm), NIR (~0.75µm to ~1.3µm)	Data type Optical/Multi Spectral Radiometry High Resolution, processing level 1, done by RSP and scene shift system	mapping of the land surface and the oceans	
	PALSAR	LAND, WATER	microwave radar having wavelength L-band (~15 0cm to ~30 0cm), 1.27GHz	doppler algorithm is used for processing,Backscattering coefficient analysis, interferometry processing, polarimetric data processing, no of bits/ sample-5, HH polarisation.	day & night land obs.estimate vol of water in soil, vol of biomass in forests, conditions of waves	
BELKA	MSS	LAND, WATER	resolution upto 2.1 m.	belka 1 unsuccesful (Dnepr 1 failed - 66 sec after launch)	ecological research, mineral prospecting, cartography,emergency situation &	
	PSS	ATM				
CARTOSAT 1 (IRS-P5)	PAN CAMERA		X-band - QPSK modulated, single polarized- 105 Mbit/s beam phased-			

Figure 3: Part of the Table designed for satellites and their corresponding instruments (Focussing on Land)

The modulation techniques that were found from the table shown in figure 4 infers that QPSK is the more preferred modulation technique for various satellite communications used for the purpose of earth observations because of its optimum bandwidth and power requirements. This table also gives details of the various scanning techniques used such as whiskbroom, cross scanning etc by the satellites for various applications. The data processing columns from the table tabulates the details of the various data rates that the earth observation satellites use for various application such as digital data, images etc. This gives the information of the quantisation rate which is used for the processing of data. Some information regarding the data levels that the satellites have for processing the data have been retrieved from the satellite. From the various information tabulated in the results, the data rate that these satellites use for the earth observation had been increased to several Mbps from the older earth observation satellites like Landsat and this is seen from the usage of the X band which allow higher data rates in the order up to 500Mbps in Terra Sar-X which are used for the high resolution transmission to the ground station. The significance gives the idea of the various purposes that these instruments are used for the earth observation applications with the web links giving more idea towards the instruments and satellites.

Thus the results produced by this research give the various technological details needed for the communication and interfacing in a tabularized way for the better understanding of the earth observation satellites.

8 Future Work

The research can be improved in future with updating the information in the table that has been presented in this research. This research is very broad and so further research can be done for each application, focussing on more details of the instruments and explaining the technologies in detail individually. Focus can also be made on the antenna types and other data formats. Finally the website that is created as a means of making all the research findings and presenting all the details to the society can be improved by adding the facility of having a database of all the sensor details and technologies and providing the website with a search option making it more easier to navigate and get more details. This research can also be expanded with updating the satellites and their corresponding details as this work concentrates only on the satellites which are significant in the field of earth observation up to date.

9 Summary

Thus this research gives the study of all the communication and data interfaces present in the earth observation satellites tabulated and organized with respect to their focus on land, water, atmosphere and disaster. A website has been created in order make all the details available for access by students and other researchers.

10 References

Kainz, W., (2005) 'Geo-Information, Earth Observation, and Their Role for Society' Recent Advances in Space Technologies, 2005.Proceedings of 2nd International Conference, 9-11 June 2005, pp: 83- 86.

Karatas, Y., (2009) 'The Place of Small Satellites In Fulfilling The Earth Observation Requirements of a Developing Country', Recent Advances in Space Technologies, 2009. RAST 09. 4th International Conference, 11-13 June 2009, pp: 333 – 339.

Luccio, M., (2005) 'Earth Observation Goes Mainstream' Earth Observation Magazine 2005, available at: http://web.archive.org/web/20070801122924/www.eomonline.com/EOM_Aug05/article.php?Article=department01 [accessed on July 28, 2010]

Navalgund, R.R., Jayaraman, V., Roy, P.S., (2007) 'Remote Sensing Applications: An Overview', Current Science, volume 93(12), pp: 1747-1766.

SSTL (2011) available at: http://www.sstl.co.uk [accessed on January 2011]

Tatem, A., Goetz, S., Hay, S., (2008) 'Fifty Years of Earth Observation Satellites' available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2690060/ [accessed on July 28, 2010]

Section 2

Computer and Information Security

Educating Social Networking Users

P.Nair and M.Papadaki

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

Abstract

"*Privacy is dead, and social media hold the smoking gun." – Pete Cashmore, Mashable CEO*
"Social networks aren't about Web sites. They're about experiences." – Mike DiLorenzo, NHL social media marketing director.
Since the turn of the 21st century, there have been many developments in the technological world, developments and findings that may not have necessarily improved the way the world lives, but definitely have changed and revolutionised the way it works . The Internet itself has changed so much from being a service designed for CERN scientists to communicate amongst themselves to a global phenomenon (Anderson, 2007). And now with the rise of Web 2.0 or simply a second much better version of the Web, people are getting more and more dependent on the Web for everything that they do. The participatory nature of Web 2.0 along with its user friendly design and outlook meant that it became an endless repository of dynamic information and information exchange into which anybody can both add to as well as take from (Sharma, 2011). Many services like blogging, interactive and target centric advertisements and product placements, e-commerce soon started to blossom due to the advent of Web 2.0 however none of them could profit as much as social networking sites did during the last half a decade.
In this project an effort will be made to educate users about the potential threats involved on social networking sites by creating a Flash based game designed in the format of a quiz. The users will be put in make believe situations where they will have to answer questions based on their existing knowledge of social networking sites and its functionalities. The users through the game will also be made aware of additional facts that can further help their security measures against the threats on social networking sites. The game will be sent to a selected group of participants and the results will be collected for analysis purpose. The results will be studied in depth to evaluate the success of the game and whether creating awareness by using interactive medium is a good choice over other means like designing posters, making videos, lectures, seminars etc. Based on some of the scenarios a few solutions and changes will be suggested to the already existing precautions and measures. The results of the game shows there is a scope for more user responsibility in creating awareness and users are open to similar awareness based initiatives instead of the tried and testing ones like video and seminars. Users were also seen to better react to situations if they were able to co-relate it with similar situations.

Keywords

Social networking sites, SNS, security, Awareness, game, educating

1 Introduction

Social networking sites or SNS have been expanding the most amongst all Web 2.0 services (Leitner and Grechenig, 2008), however the threats involved in SNS have

also been expanding at the same phenomenal rate, with cyber criminals making SNS as one of their preferred targets. Social networking sites on their part know that it is essential to keep hold of the users and provide for their safety, making sure that they improve security and devise new methods to keep away the cyber criminals. But the fact remains that the main reason that cyber criminals thrive so much on social networking sites is due to the fact that the efforts put in to protect the users by the sites is not been reciprocated by the users themselves. Lax security measures combined with not adhering to the proper social networking etiquettes with regards to sharing of personal information has meant that it is the end user that is the weak link when it comes to the fight against cyber criminals. The digital age of today comes with a paradox, that of accepting wholesome changes and getting the latest developments with just a mouse click, however it comes at the expense of losing the identity and privacy of oneself, besides opening oneself to a multitude of attacks (John, 2010) It is this internal conflict and chaos that the cyber criminals are exploiting to good effect for their own good

The aim of the paper is three-fold, i) getting a clear picture of the existing scenario with respect to areas like privacy and security issues and the extent of the problem, studying out the factors that are hindering the area and developing a solution ii) designing and developing an interactive game that will bring awareness to the scenario and lastly iii) evaluating the success of the game.

2 Existing Scenario

Users are very careless with their personally identifiable information (PII), nearly 40 per cent of users had displayed information such as birth date, while a quarter of users with children had posted some information about their children on social networking sites(Consumer Report, 2010).Acquisti and Gross(2009) have shown with the help of a few details it is possible to guess someone's social security number(SSN). The popularity of social networking sites with people all over the world has made it a favored spot for cyber criminals to spread their chaos (Walsh, 2011). Oversharing(of information and content) and weak privacy settings are rampant amongst users on social networking sites with users at risk against threats like phishing, identity theft, data breaches, loss of locational privacy, real life threats like stalking, paedophilia, robbery etc.

User is under threat from all sides, i) including his own known contacts/friends, ii) from third party applications and policy changes of social networking like Facebook photo tagging (Cluley, 2011) and iii) lastly from his/her ignorance and neglect. There are other types of threat on social networking sites XSS (cross site scripting) attacks, facial recognition technology related threats. Threats on SNS can be divided into the vectors that they target and attack, like privacy related attacks , drive-by download/payload related threats like malware, spyware etc., identity related threats and real life threats. A table charting the type of threats and the solutions that can be implemented to stop those threats from occuring can be as seen in Figure 1.

Solutions

Threats	Avoid oversharing	Tweak privacy settings	Anti-virus/ user system changes	Changes in site policy, design etc.
XSS			**X**	**X**
Phishing			**X**	**X**
Location tagging	**X**	**X**		**X**
Identity theft	**X**	**X**		**X**
Facial recognition	**X**	**X**		
Real life threats	**X**	**X**		**X**

Figure 1: Threats versus solutions

3 Game Design and Results

The game is designed in the format of a quiz-based game where the user's knowledge will be put to test by social networking sites based scenarios. The scenarios have been developed keeping in mind the various scenarios and threats aggregated from the section Existing Scenario. As such the game will have 8 questions of different formats and divided into 5 scenarios.

Scenario 1: Importance of passwords and and the need for password awareness

The top 5 most commonly used passwords that were revealed during the hack attack on Gawker websites included passwords like 123456, password, 12345678, lifehack and qwerty (Broida, 2010). Passwords like these could mean that even the best privacy and security settings wouldn't be able to save a user from getting his account hacked and all of his information stolen.

Scenario 1 contains 3 questions which are questions which basically tests the user's knowledge on password strength, password reusability and having unique passwords.

Scenario creates awareness on threats like dictionary attacks and brute force attacks, which can lead to the user's password being guessed or cracked and could lead to the user's account getting compromised and misused for a wide variety of purposes.

Scenario 2: Phishing and identity theft protection

Scenario 2 touches on the topic of phishing based emails and sites. There is only one question in this scenario in which given a situation, the user is asked to judge whether the mail originating in the situation is a phishing mail or not. Users are advised and warned about the dangers of phishing sites as well that look very much like the original site exceot for a few unnoticeable changes which sometimes is enough for a naïve or a new user to become a victim of an identity theft.

Scenario 3: Oversharing and privacy settings

Scenario 3 has two questions that concerns oversharing and privacy settings, the two questions were clubbed into one scenario because one can prove that if sharing information and privacy settings are considered two entities then it is enough for one the entity to exist such that the other entity can be neglected and thus limiting the damage that can be caused as well.

For example : If Alice has set her privacy settings such that no one but her trusted friends and contact can only see her information then it means she can share any information she wants without being in too much risk as no one else but her friends can see those information.

The two questions in this scenario tests the user's knowledge of what should be shared with only friends and contacts and what should be shared with everyone (public view)

Scenario 4: Privacy Policy

Scenario 4 containing just only one question tests the user's knowledge of the privacy policy document often found on SNS' that tells the users of the way in which the user's personal information is used by the site, where it is stored, what to do if the user wants his personal information taken back etc.

Being aware of privacy policy and its contents can save a user from data breach and data being viewed and used by third party apps which can then cause all sorts of problem

Scenario 5: Child Protection on Social Networking Websites

The last and final scenario judges a user's knowledge of child protection mechanisms and measures in existence on SNS'. Livingstone, Olafsson and Staksrud (2011) have only surveyed kids in European countries and found that an unusually high number of kids are on social networking sites flouting age restrictions and often end up sharing too much information on the sites. Although many users won't have kids, the sheer number of people on the Internet means that the user will atleast know some people in his contact list who will have kids and it is important to be aware of the threats that can happen on SNS these days.

The question tests the user by asking him/her if they can spot whether in a made up situation, an underage kid is lying about his age online

At the end of the game, there are some questionnaire that is used for the purpose of demographical analysis besides getting feedback on the game and some background information on the user.

4 Results

Total of 30 people played the game and the age and gender wise break up is as follows (the numbers in bracket denote the percentage of the total):

Men : 17 (56.66%), Women : 13 (43.33%)

18-24 age group : 18 (60%)
25-34 age group: 4 (13.33%)
35-44 age group: 6 (20%)
45-54 age group: 2 (6.66%)

The scenario wise break down of the results is as seen in Table 2.

Scenario	Right Answer	Wrong Answer	Need for awareness
Scenario 1	50%	50%	Moderate
Scenario 2	86.66%	13.33%	Very less
Scenario 3	66.66%	33.33%	Less
Scenario 4	33.33%	66.66%	Definite need for awareness
Scenario 5	80%	20%	Less

Table 2: The table is tabulated as the percentage of total users out of 30 who gave the right and wrong answers

From the results one can see that there is a definite need for awareness in Scenario 4 where the user needs to be made aware of the privacy policy.

The high percentage of people who got questions 5 and 6 in Scenario 3 were able to do so because the questions were such that there were related to each other. In fact a high percentage of users who got Question 5 also managed to get Question 6 right.

This proves that it becomes easier to create awareness if situations can be co-related and the user is made aware of it.

4.1 Questionnaire analysis

The users were asked whether they have come across before such awareness based games on the same topic and 80 per cent of the users said they have never across such a game before, while the 20 per cent who had come across such a concept were among the highest scorers. **This proves that those who had come across such a content before were perhaps well informed of the threats and hence were able to score high marks**

The game manages to create some awareness and something new for the users when asked in a question 50 per cent of the users agreed to the fact that games like this were a better concept and more effective in creating awareness than watching a video or a seminar on the same topic. In terms of evaluating the success of the game this statistic says a lot.

It came as no surprise that people who agreed or strongly agreed that they have good knowledge of the way computers and social networking sites work were some of the higher scorers in the quiz with an average score of 69.64 %

This proves that people who have a technical background or a general idea of the way computers and the Internet works are less at risk online than say someone who isn't so good with computers and Internet.

In the next question as well, it doesn't come as too much of a surprise that users who said that they find it difficult to find information on the Internet related to such security threats were in fact some of the low scorers in the game.

5 Conclusion

The game showed that there are certain areas where user awareness is still not as good as one would want it to be, for example areas like password protection and usage. The paper also proved that users must be given more responsibility when it comes to creating awareness amongst each others. Users who had come across a similar awareness related game were some of the high scorers in the game, hence proving that not only being aware of a threat makes you more knowledgeable but also you tend to be in a position to teach others the same. A positive response was received with regards to the concept of using a game to create awareness as half of the users taking part in the game felt that the idea was a better one than creating awareness on the same issue using a seminar or video.

6 Future Work

There is definitely a lot of potential for future work on this particular thesis and the development of the game. The users through the questionnaire have accepted the game as a new and novel way of creating awareness better than some of the existing means like watching a video or attending a seminar on the same topic.

7 References

Acquisti, A., Gross, R.(2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences of the United States of America,* 106(27) pp.10975-109780

Anderson, P. (2007). What is Web 2.0? Ideas, technologies and implications for education. *Proceedings of the JISC Technology and Standards Watch, Feb 2007*. [online] Available at: http://www.jisc.ac.uk/media/documents/techwatch/tsw0701b.pdf [Accessed on 16 June 2011]

Broida, R.(2010). Password Choices [online] Available at : http://www.bnet.com/blog/businesstips/the-gawker-leak-how-to-protect-your-business-from-poor-password-choices/9976 [Accessed on July 16 2011]

Cluley, G.(2011). Facebook changes privacy settings for millions of users - facial recognition is enabled [online] Available at: http://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/ [Accessed on 29 June 2011]

Consumer Reports (2010). Social insecurity. What millions of online users don't know can hurt them [online] Available : http://www.consumerreports.org/cro/magazine-archive /2010/june/electronics-computers/social-insecurity/overview/index.htm [Accessed on 24 June 2011]

John,N.(2010). Does WikiLeaks have any privacy issues? [online] Available at: http://privacy.sociothink.com/?p=110 [Accessed on 16 July 2011]

Leitner, P., Grechenig, T. (2008). Social Networking Sphere: A Snapshot Of Trends, Functionalities and Revenue Models. *Proceedings of the IADIS International Conference on Web based communities 2008.* Amsterdam, The Netherlands, 24-26 July 2008.

Livingstone, S., Ólafsson, K., Staksrud, E. (2011) *Social networking, age and privacy.* EU Kids Online, London, UK.

Sharma, P. (2011). Core Characteristics of Web 2.0 services [online] Available at : http://www.techpluto.com/web-20-services/ [Accessed on 10 July 2011]

Walsh, S. (2011). Top 5 Reasons Why Spammers Love Social Networking [online] Available: http://www.allspammedup.com/2011/08/top-5-reasons-why-spammers-love-social-networking/ [Accessed on 5 August 2011]

Evaluating the Effectiveness of Free e-Safety Software

D.D.Padmini and S.Atkinson

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

Abstract

The young children are increasingly using the Internet every day; they are involved in a variety of online activities ranging from learning to social networking and more. Researches indicates that the more children use the Internet the more they are exposed to risks online. Parents, Schools and other stakeholders are worried about this. Among the many solutions including parental supervision, usage policies, awareness initiatives, etc; the use of E-Safety products for safeguarding children is considered as one of the most important ways to reduce the risks to children when they are online. This report aims to look at the various available free to use solutions and to measure their effectiveness against a carefully designed framework that enables the evaluation of filtering software in a broader scope and focus in relations to the children's online risks.

Keywords

Filtering Software, Parental Control Software, Internet Safety, E-Safety, Cyber Bullying, Cyber Bullying Prevention, Prevention of online Harassment, Online bullying, Internet Harassment, Violence online and free Software.

1 Introduction

The current rapid growth of access to Internet for the young people and the children are unprecedented in this technological era of Internet tablets and Internet enabled mobile devices, Laptops and Personal Computers, etc. Governments and other organizations and parents are increasingly being aware of the benefits the Internet has to offer and several countries and other initiatives by different sort of organizations and institutions are promoting the use of the Internet and the information technology in schools. Internet provides new opportunities for children to explore, collaborate and communicate to enhance their learning experience.

Children use the Internet for a wide range of activities; different activities include the usage of Internet for; school work, watching video clips, playing Internet games, instant messaging, social networking, sending or receiving emails, reading news, downloading or sharing movies, music, videos or pictures, blogging, etc. These online activities along with the benefits they offer also poses a number of risks and threats and may expose the children against these online risks and threats. Cyber bullying, pornographic content, grooming, hateful or racist content, etc (Livingstone et al, 2010; Optem, 2007).

The existing research report also indicates that there are a wide range of risks associated with the children"s use of Internet; the frequency of access, cultural and social aspects, and the amount of time spent, etc. all contributes to the possibility of online children being under risk (Livingstong and Haddon, 2009). The slow pace in which the stake holders keep up to ensure the protective measures (such as awareness about the risks, regulations and safety protection, parental understanding, etc) is another vulnerability; the children often gain access to Internet before such infrastructures are even planned (Livingstone et al, 2010).

Contrary to the beliefs and the projected images by the digital advocates; many children still do not have adequate enough resources to explore the Internet properly in-order to exploit the benefits (Helspera and Eynon, 2010). In this technology age, the necessity of providing adequate resources and facilities for children to enhance their digital literacy skills are important and vital, the promotion of the digital literacy without proper safety measures may result in exposing children to unintended risks and threats.

2 Young children's online activities and parental concerns

The current young generation is popularly mentioned as the Internet-Generation; they use and adopt new media and technologies fairly faster than their parents and other elders; mostly because of the immense amount of influence of technology in their education. So many researchers are conducting research on related topics such as the 'Online Usage', Access, Age and Gender differences and activities of different genders and ages and so on (Livingstone and Haddon, 2009). Many studies shows that; even-though there are very good effects of technology being used in education; it also turns out that there are a vulnerable population of children online. Without proper awareness, knowledge and control sometimes the children can be mislead to threats and may be abused online in several ways. Afore mentioned statements from some of the research outcomes confirms this concern.

Some statistics show that the amount of children using Internet is rapidly growing; In the EU 27 about 75 % children use Internet (children of age range 6 to 17), ranging from less than half of the children (about 45%) Italy, 50% in Greece and Cyprus, 91% in UK and Sweden, 93% Netherlands and Denmark and 94% in Finland (Livingstone and Haddon, 2009; Ofcom, 2009); catching up with the trend, parents are also increasingly being introduced to Internet and using it (Euroberometer, 2008/9). Many of the parents are aware of the potential threats that their children may be exposed to while they are online. More than 92% of the 9-16 year old children use Internet almost every day (Livingstone et al, 2010); it is increasingly becoming embedded in their daily lives.

The findings of a report by EU Kids Online also shows that 22% of 11-16 year olds have been exposed to one or more types of potentially harmful user- generated content: hate (12%), pro-anorexia (11%), self-harm (8%), drug-taking (7%), suicide (5%). 14% of 9-16 year olds have in the past 12 months seen images online that are "obviously sexual – for example, showing people naked or people having sex (Livingstone et al, 2010). The other major threats a child might encounter while using Internet may be : Internet Addiction, Obscene and Illegitimate Contents online

such as Porn and Hate content or Violent content, Self Harm or Suicide encouragement communities, Gangs or other troublesome groups, Violent Gaming, etc (Livingstone et al, 2010; Hasebrink et al, 2009; Byron, 2008; Euroberometer, 2008/9).

The EU Kids Online research findings based on a survey of around 23,420 children indicates that 85% of the children use the Internet at home, among them 60% of the children use the Internet in the living room or other public room at home. About 48% of children use it in their bedroom or in another private room (Livingstone et al, 2010).

A Flash Eurobarometer study indicates 60 % of parents were concerned about the possibility that their children might be a victim of online grooming or their child being bullied by other children (54%); another interesting fact that the parents who did not use Internet themselves are the ones who worried most about such risks. A minority of parents also worried that their child might have access to information about self harm, suicide or anorexia (39% were very worried and 16% were rather worried) (Euroberometer, 2008/9).

The examination of these facts indicates that the children are increasingly using internet on a daily basis and many of them are exposed to harmful content or other sorts of risks during their online activities. Parents are very much worried about the fact that their children might encounter risks online. Several Parents also take precautions such as Parental Supervision or use of E-Safety Software, etc.

3 E-Safety software for a safer internet environment for children: an evaluation of effectiveness of freely available products

E-Safety software are used by several parents, schools and other stakeholders to protect children from online risks; however there were only a few studies related to the children‟s online safety and E-Safety software is done.

Hunter (2000), eTesting Labs (2001), San Jose public library (2008) have evaluated different filtering products; the focus of their research varied and the focus was on first amendment friendliness of the filtering products, ability of the software to block objectionable content based on the „Department of defence‟s‟ criteria and the ability to block pornographic content respectively. However all these studies were differed in context and scope and failed to address the various children specific risk categories.

A new study of freely available E-Safety software which will cover the scope and context to cover children specific risks to include content, contact and conduct risks a child may be exposed to during their online activities is done. A framework that is designed to address both these specific types of risks that focuses on children and the administrative capabilities of the software that might be useful for the parents is created and a random stratified, balanced (1:1 ratio) of objectionable and non objectionable contents and URLs were chosen from different content categories to

test the effectiveness of the software based on the framework. The chosen Products are: K9 Web Protection, Golden Filter Pro, Pareto Logic PG Surfer and AOL Parental Controls

Through six phases of evaluation (Ease of Obtaining the Software, Administrative Capabilities, Products‟ Effectiveness for monitoring and blocking communication

channels, Products‟ Effectiveness for filtering Search Engine Results, Products‟ Effectiveness of filtering URLs, Products‟ Effectiveness of Blocking advertisements) the software are carefully examined to measure their effectiveness.

The program K9 Web Protection demonstrated a very good ability to refine the search results and in blocking the search engines; It had a very good 96% of accuracy in blocking objectionable URLs and a 94% accuracy rate in correctly accessing the non-objectionable content. The highest Correct Blocking Ratio among the chosen products is 0.96 and that was scored by the K9 even when it is lacking in several desired administering capabilities. GF Pro and Pareto logic PG surfer software were found to demonstrate poor performances and an accelerated rate of over blocking and under blocking. With almost majority of the desired features that frame work demanded and the competing ability to filter out objectionable content and other similar features with lowest under blocking and over blocking ratios the AOL Parental control software demonstrated a steady performance and proved to be one of the best free solutions available around for the windows computers. It also seamlessly integrate with the Windows User accounts and enables the parent to create separate user accounts for each children and create profiles based on the age groups. It was also noticeable that the Correct Blocking Ratio is higher and the Incorrect Blocking Ratio was lower for the software which indicates the high effectiveness.

With 0.96% Correct Blocking Ratio; even without many of the desired administering capabilities the K9 web protection is the most effective filtering software among the reviewed products; however considering the fact that it lacks many of the major administrative capabilities that the framework demanded the AOL Parental Controls software, which has almost all the desired administrative capabilities, 0.80 Correct Blocking Ratio and a comparatively effective (0.10 over 0.60) incorrect blocking ratio has a major lead and can be considered as one of the best almost complete and packed with features product freely available to use.

4 Conclusion and Future work

Through the next four evaluation phases it is learned that there is not a single panacea solution available in the free sector; however AOL Parental Controls was found to be the most effective free solution among the compared few with majority of desired features and administrative capabilities. K9 Web Protection was the nearest with features and the capability of blocking various categories; however it seriously lacked most of the major administrative capabilities the framework demanded. It is also noticeable that the ability of these software to block the advertisements are very low and in the case of GF Pro it is nil.

Even though there are several disadvantages (mostly in terms of the administrative capabilities); AOL Parental control and the K9 Web Protection software seem to be a fairly good choice for those who are looking for a free solution. However this said it is pertinent that there is no complete solution currently available to address all these risks, but Prevention is always better and thus making use of these solutions will only reduce the Risks for children.

Recent Research Indicates that the use of mobile devices to access the Internet is increasing (Livingstone et al, 2010; Euroberometer, 2008/9), also the upcoming new technologies , increasing use of social networking (Livingstone et al, 2010), and even the arise of web 2.0 based new communication channels, etc are all increasingly making it difficult to secure the children online. Children are also increasingly using the Internet for creating content and publishing photos, videos, blogs, etc. Research on these areas can be carried out in these dimensions in future. Another interesting topic for future research is the Open Source Enterprise class solutions for E-Safety. There are only a very few reviews of Enterprise range Open Source Solutions that can be used by schools, small organizations, etc to effectively protect the children from online threats for example Smoothwall, Squid and Dans Guardian together can be used as an effective filter; the open nature of these technologies also make it a more interesting aspect as more research on this direction may result in an increase in attention to these products in this context (E-Safety) and will result in betterment of these products to reflects the suggestions of the research out comes. Many schools and small organizations will be benefited by such research as it can help them save money that they might be investing in similar commercial products.

5 References

Livingstone S, Haddon L, Gorzig A and Olaffson K (2010). Risks and Safety on the Internet: The perspective of European Children. Initial Findings. LSE London: EU Kids Online. p1-121.

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K (2009). Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. 2nd ed. London: LSE, London: EU Kids Online. p1-112.

Optem (2007). Safer Internet for Children; Qualitative study in 29 European Countries: Summary Report. Luxembourg:EC: European Commission : Directorate General Information Security and Media. p3-77.

Livingstone, S., & Haddon, L. (2009). Final Report (Kids Online Opportunities and risks for children). Bristol: The Policy Press. p3-127.

Helspera EJ, Eynon R. (2010). Digital Natives: Where is the evidence? British Educational Research Journal. 36 (3), 503-520.

Weiss CH (1998). Evaluation : Methods for studying programs and policies. 2nd ed. New Jersey: Prentice Hall, Inc.. p180-339.

Byron T (2008). Safer Children in a Digital World. Nottingham: DCSF Publications. p1-226.

Hunter, C.D. (2000). Internet Filter Effectiveness : Testing Over and under inclusive blocking decisions of four popular filters. Proceedings of the 10th Conference on Computers, Freedom and Privacy : Challenging the Assumptions. 1 (1), p287-294.

Heins M, Goldberg D and Waldman M (2006). Internet Filters A Public Policy Report. 2nd ed. New York: The Brennan Center for Justice. p1-87.

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

Houghton-Jan S (2008). Internet Filtering Software Tests: Barracuda, CyberPatrol, FilterGate, & WebSense. USA: San Jose Public Library. p1-21.

Christian, W., Dawson. (2009) „Projects in Computing and information Systems : A students guide", Pearson Education Limited.

Bullying Statistics Website (2009). "Cyber Bullying", available at http://www.bullyingstatistics.org/content/cyber-bullying.html, last accessed: 9/6/2010

Grey D (2001). The Internet in School. London: Continuum Books.

Ofcom. (2009). Children"s and young people"s access to online content on mobile devices, games consoles and portable media players. Available: www.ofcom.org.uk/advice/media_literacy/.../online_access.pdf. Last accessed 31 May 2010.

Korte, W.B., Hüsing, T.. (2006). Benchmarking Access and Use of ICT in European Schools 2006: Results from Head Teacher and A Classroom Teacher Surveys in 27 European Countries. Current Developments in Technology assisted Education. 3 (1), p1652-1657.

Euroberometer Analytical report (2008, 2009) "Towards a safer use of the Internet for children in the EU- a parents" perspective", available at http://ec.europa.eu/public_opinion/ flash/fl_248_en.pdf , Last accessed: 1/6/2010.

Safeguardingchildrenbarnsley.com. (2009). E-Safety. Available: http://www.safeguardingchildrenbarnsley.com/sgc/professionals/E-Safety. Last accessed 10th Sep 2010.

Carr N (2010). The Shallows: What the Internet Is Doing to Our Brains. USA: W.W. Norton and Company. p1-276. [20] Tamar Lewin. (2010). Teenage Insults, Scrawled on Web, Not on Walls. Available: http://www.nytimes.com/2010/05/06/us/06formspring.html. Last accessed Jun 5 2010.

Livingstone, S. and Helsper, E.J. (2010). op cit. [22] Livingstone, S. and Bober M., (2005), "UK Children Go Online, Final report of key project findings", available at http://www.lse.ac.uk/collections/children-go-online/UKCGO_ Final_report.pdf Last accessed 06-06-2010

Prensky M. (2001). Digital Natives, Digital Immigrants. On the Horizon : MCB University Press. 9 (5), p1-6.

Europa Information Society . (2009). Towards a safer use of the Internet for children in the EU – a parents" perspective. Available: ec.europa.eu/public_opinion/flash/fl_248_en.pdf. Last accessed 10 June 2010.

Factors Affecting Information Security Behaviour

A.Rajendran, S.M.Furnell and T.Gabriel

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

Abstract

The reason behind inconsistent acceptance and compliance level of employees within organisation has been hard to understand. Personality, organisational culture and environment are said to be the reasons behind such inconsistent compliance behaviour of an employee. But aspects such as personality, socio-organisation factors, educational best practice are been neglected till date during the ongoing training of employees for betterment of acceptance and compliance behaviour. Initial study targeted the likely relation between socio-organisation factors and personality of a person, which gave out the likely process that initiates the security behaviour out of an employee. A model is designed, which best describes and includes all possible influence an employee might get and derives the security behaviour of the employee based on it. The model exhibits a nature to advocate, what causes an employee to behave the way they do. Organisation can make use of this to differentiate security compliant employee with the non-compliant employee and produce effective mitigation plans.

Keywords

Personality, socio-organisation factors, training, compliance behaviour, Information Security.

1 Introduction

With the recent technological advancements and increase in security threats, the importance of sticking with the security focused policies is high on recognition much more than previously it was. A number of studies held so far have suggested that the success of security policies and controls will ultimately depend upon the levels of acceptance and compliance among the underlying staff. A well designed and implemented security system still as to rely on the people it was meant to govern, the human factor importance is significant in this scenario. A fact worth mentioning is that the majority of the troubling incidents related to security had the human factor playing a crucial part, this also led researchers term humans as the weakest link in an organisation. One can implement technical solutions for the related issues, but we still fail to control and handle human factor (Gonzalez et al. 2002; Vroom & Von Solms, 2004).

Compliance behaviour of an employee within an organisation is something of wide range. It is very much inconsistent, so that the researchers who tried to interpret the compliance behaviour of employees came up with number of categories to assume the level of compliance levels. Furnell & Thompson (2009) had developed eight compliance level ranging from culture to disobedience and went on to say that

employees could be mapped in any of those level of compliance depending on the security behaviour they exhibit.

The cause for such discrepant compliance behaviour is said to be personality and socio-organisation factors surrounding the employee. Research purpose was drawn upon the above two reasons, to find the process of resultant security behaviour and subsequent compliance of an employee. The major topics considered include lack of user awareness, personality as a filter, organisation culture, environment, education and importantly deriving a mechanism that derives compliance behaviour of person, which an organisation can later use.

2 Background

2.1 End user behaviour

End user behaviour has been a major concern and organisations are now turning their head towards human factor. Organisations are becoming aware of the major incidents occurring due to the involvement of human element in security breaches. Employees are the cause of highest rate of abuse within an organisation. To add on top of that, 60%-80% of all network misuse is perpetrated by people inside the organisation (Woodhouse, 2007). Major surveys such as CSI (*Computer security institute*), BERR (*Business Enterprise and Regulatory Reform)* and ISBS *(Information Security Breaches Survey*) concur with internal threat in the form of human. The solution for such incidents may seem to be with organisation's security practices and implementation of security policy, but the significant activity of non-compliant behaviour due to personality indifference and external influence would lead to ineffectiveness of security policy.

2.2 Lack of employee awareness

Lack of effectiveness or ineffective nature of the security policy can be attributed to lack of awareness among employees. Effectiveness comes, when every user is aware of what they do and their respective consequences of their actions, awareness does not rise from self-realisation alone. Awareness among users should be cultivated by organisations security training and security culture. Ruighaver et al. (2007) argue that organisational culture plays an important role in end user activities, and suggest it should be a process of continual development rather than a one-time process, which many organisations fail to address. Security awareness is the basis of preventing all major threats from causing damage or even from happening itself. Organisations are most benefitted from employee's awareness and most affected due to employee's lack of awareness. Malwares comes into an organisation with the help of employee within the organisation. Lack of awareness constructs this sort of actions from employees, which confirms the fact people commit mistake not the computers (Lacey, 2009).

3 Organisation culture

Organisation culture or corporate culture is a deep aspect, which is entwined upon each section of an organisation. The organisation culture exist whether management or employees within an organisation aware of it or not. Vroom & Von Solms (2004) state that, organisation culture is about shared ideas between staff, the norms followed, and system structure which enforces its values followed on staff. This in turn becomes a network of learned behaviour, which flows from top level of organisation to bottom level of organisation. Organisation's security culture is a sub form of organisation culture. It is created out of influence from organisation culture and could also be created by the unknown factors outside of organisation. Security culture is defined from the fact, how members within an organisation are conscious of security and follow it (Woodhouse, 2007). This may not necessarily be with the ideals of organisation and how organisation wants their member's security orientation to be. Organisation's culture is an influence that extends its reach on organisational security culture and may obstruct change. So organisation culture could be the single most important factor in deciding the success or failure of the organisation and to think security culture could be affected by organisation culture one need to proceed cautiously.

4 Socio-organisation factors

All the facts and illustration relayed so far highlighted the importance of human factors and organisational factors role, which are highlighted by many studies undertaken so far in improving information security (Lacey, 2009; Dhillon & Backhouse, 2001; Vroom and Von Solms, 2004). Human factor and organisation factor combined are known to be Socio-Organisational factor. Socio-organisational perspective is way forward for betterment of information security rather than the technical and functional aspects of information security (Dhillon & Backhouse, 2001). Socio-Organisational perspective is significant, since technologies ensuring information security are designed, maintained and operated by human agents in an organisation. So it is necessary to understand these socio-organisational factors in order to deliver the assessing mechanism dealing with compliance behaviour.

Socio organisation factors in others words can be described as an influencing factor that works in conjunction with personality of the person. Humans pose such critical threat due to their nature of susceptibility to external pressure applied on them. Influence can be from anywhere as put forward by Lacey that 'Local roles, environments and business objectives shape user attitudes and behaviour' (Lacey, 2009). This describes the importance of the influence factors outlined in matters dealing with information security. The much discussed organisation culture in itself is an influence factor, which could motivate employees within the organisation towards security culture. It has a strong influence on organisational security, which might lead to obstruct change in positive or negative direction (Nosworthy, 2000). Security practices and policy in place also has huge interest in how security orientations of staff are influenced. The extent, a staff understands security policy have impact on security breaches of an organisation. The security policies that are appropriately worded and well intentioned lead to less security breaches (ISBS, 2010).

4.1 Local roles, environment, and mentoring

Local roles might be the employee job role in itself, which could alter the way they comply with information security. Environment includes influence from those who are around us including colleagues, friends and families. Yuen et al. (2009) had taken influence in context of workplace and other in their home. In the organisation context the most influencing factors are security culture of an organisation (e.g. group effect, peers and etc,), and ability of a person. Whereas in home environment, family, peer, mass media influence, perceived usefulness and self-efficacy plays a role in determining outcome of person's security behaviour (Yuen.et al. 2009). Mentoring and training was largely considered as solution for improving security orientation of employees in an organisation. Gabriel (2010) in his work had similar views to spread security awareness among colleagues by means of mentoring. This method was adopted since Gabriel believed colleague behaviour to be more effective and influence the outcome of the other employee's security behaviour.

4.2 Learning Theories & training

Training and educating staff is for their own betterment as well as betterment of organisation that trains their staff. The effectiveness of training varies from person to person. Every employee has different of opinion in the way they want to be trained. That's where the learning theories come into play due to the individual difference in personality. People learn efficiently in their preferred way of learning and tend to change ones behaviour permanently; these learning come out of one's own experience rather than from external body states (Landy, 1985). Learning theories address the way people learn and it is about how behaviour patterns develop from social environment. Armitage et al. (2007) in their work provided the support to learning theories despite shortfalls in it. The learning theory is helpful in understanding the insights of how people learn though it cannot be seen as an exact blueprint of learning nature.

5 Personality as a filter

The personality of a person is the prime factor in security orientation of an employee, which changes the outcomes of all the inputs that feeds into them (Gabriel, 2010). As a human one would find a resilient nature towards change in terms of security, which is a major factor in non-acceptance and non-compliance behaviour. With further research, personality as a prime factor in resisting change turned to be a filter rather being a blockade of security orientation. For example training from an organisation does not go completely ignored, some part of the security facts do get into the employee mindset and they begin to follow as they see it fit or appropriate to them. The personality of person does not bear a direct consequence on security behaviour. The security behaviour of a person is resultant of personality combined with organisation or organisation independent variables. Employee attitude towards compliance and security behaviour arise in conjunction with organisational constraints imposed and psychological process involved within an employee.

6 A model for understanding security behaviour

The process of how personality and socio-organisation factors could lead to a resultant behaviour was described so far. The concerned learning theories, in the way employees get addicted to or affiliated to certain methods of learning were discussed as part of educating them to improve compliance behaviour. From this point on, a model that could lead the organisation or management in identifying the employee compliance behaviour shall be out laid.

A group of 8, IT security professionals from diversified backgrounds in Plymouth University were carefully chosen and invited in conducting of a focus group. *The head of ICT, head of records management, senior HR advisor, IT security research student, System & middleware manger, IT security & Privacy senior lecturer, researcher on relation between personality & security behaviour, head of school of computing and mathematics (project supervisor) and a ICT staff* were the participants invited. The agenda set at the focus group was to validate and enhance the initial model created, which best describes the socio-organisation factors surrounding an employee's personality within organisation and outside of organisation. The outcome of focus group was pleasing since, every participant acknowledged the concept of the model in front of them. With due discussion and questions raised some of the influencing factors were questioned but finally every factor were accepted to have an impact on employees one way or the other. Also some suggestions regarding omitted factors were added to help improve the model.

Issues concerning influence factors having conflict of interest among them were raised. Especially the credibility of perceived benefits as a non-workplace influence factors were subjected to intense criticism, but it was made clear that initial realisation of personal and group benefit come outside of organisation and was added without any change. Noticeable change included of adding colleague behaviour and supervisor/management leadership under *workplace interaction* category and inclusion of *wider awareness* influence to accommodate external scenarios which an employees are aware off. Figure 1 is the refined research model by taking into account the feedback of focus group participants. The model describes key factors of possible influence and tries to explain the process behind the security behaviour of an employee. The influence categories within the model are described below to bring forth the nature of each category considered.

- *Job characteristics* - The job factors such as varied role, job satisfaction, pressure of important task at hand and managing time exerts influence over the staff, on how they end up following IT security. This influence may be positive or negative depending upon on the situation. E.g. jumping guidelines due to concentrate on job at hand

- *Organisational factor* - This generally relates to the positive influences that may be exerted over employees by the organisation in the form of security policy, security training. Even employee aware of organisations disciplinary procedures and security monitoring can make a difference in final actions. E.g. security policy in place could be used as a driving factor to educate and train.

- *Workplace interactions* – The way colleagues or supervisor behave within organisation could influence the action taken by the employee coming in contact with them by means of idealised influence and intellectual stimulation. E.g. supervisor/management, getting in regular touch with their employee and encouraging them to follow IT security guidelines.

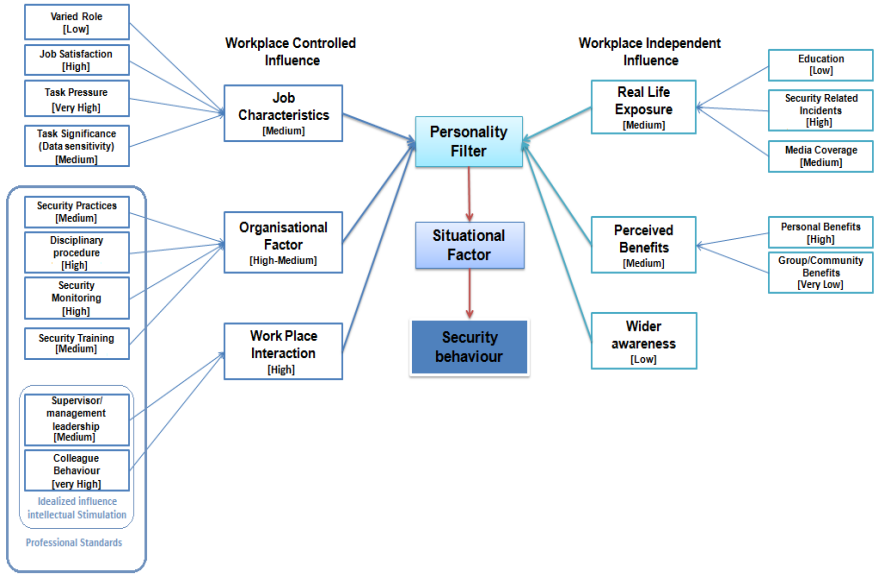


Figure 1: A framwork for understanding security compliance

- *Real life exposure* - The exposure to the security and related incidents that a person has experienced in real life or through education or through a friend can influence how they may react in future. Even media coverage could play a part in it. E.g. malware infections, social networking incidents, phishing incidents and etc

- *Perceived Benefits* - This refers to the personal or community benefits employees are aware off by means of self realisation and follow IT security accordingly. E.g. using strong passwords to protect files or website accounts.

- *Wider awareness* – External scenario that could change security orientation of an employee, when they come to know such things. E.g. Change in cyber law

6.1 Weightage of influence factors

As seen in the figure 1, Weightage of influence factors were given, in order to showcase the extent each influence factors within the research model have an impact on a person. During the focus group participants were targeted with questions related to the way they perceive some of the influence factors and their impacts, so each participant's perception were taken as feedbacks in the way they sounded it. The Weightage were given based on the feedbacks given by participants of focus group

and in consideration of the previous research works. Though most of the influence factors were rated based on the above stated conditions, but few influence factors were unexplored topics. In order to give a complete idea for the observer of the research, assumptions were made by correlating the influence factors with the impact it could have and Weightage were given in accordance with that. The assumptions may be wrong at times and could lead in wrong directions, but one must bear in mind these assumptions were made for guidance. These are the expected results rather than the obtained results, once the model is fully developed and ready for implementations all these assumptions made can be verified.

7 Conclusion

At present the created research model is a tool to understand compliance behaviour of an employee rather than a fully-fledged mechanism that can measure compliance behaviour immediately. Though, with further improvements it can become a fully-fledged mechanism to evaluate likely capability and commitment in relation with IT security. The model is a tool that explains how various influence factors within organisation and outside of organisation have an impact on an employee, and also explains how the system of personality within a person works and reacts to such external influence.

One may ask how does personality and influence factors can be related. In all due likeliness, personality have two distinguished facets namely consciousness and agreeableness. These two personality facets are put forward by researchers (Cellar et al. 2001; Shropshire et al. 2006) as the two facets that have high probability of relation with IT security compliance. Then one must assume that the level of agreeableness and consciousness is directly proportionate to the person's likely capability to get influenced by the external influence factors. This in turn affects the compliance nature of the employee within organisation. So once the organisations test the personality aspect of an employee through numerous personality tests available and also get the likely result of influence factor, the understanding would be much accurate to pin point issues behind behaviour of a person and train them based on those results. In the present state of the model, it is not possible to accurately pin point the exact issue behind behaviour of a person instead an organisation can use it to understand the likely scenarios a person can get influenced by and expect the nature of compliance behaviour and train the employees accordingly.

The outcomes obtained from the extensive research made were pleasing to see, though the same cannot be said about the implementation part of the research model created. The implementations of the research model were stalled to later date due to the limited time and resources. Broadness of influence factors and relatively unknown measurable nature of the influence factors were another reason in delay of implementation. But once implemented the extraction of fruitful deliverables out of this model are not constrained in a particular direction and can fit the needs of organisation, the way they see it fit.

8 References

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

Cellar, D. F., Z. C. Nelson and C. M. Yoke (2001). "The five factor model: Investigating the relationships between personality and accident involvement." Journal of Prevention & Intervention in the Community 22(1): pp43-52.

Dhillon, G., and Backhouse, J. (2001), "Current direction in IS security research: towards socio-organizational perspectives", Information Systems Journal 11, pp127–153.

Furnell, S.M., and Thompson, K, L., (2009), "From culture to disobedience: Recognising the varying user acceptance of IT security", Computer Fraud & Security, Volume 2009, Issue 2, pp5-10

Gabriel, T., (2010), "Personality Type – a valid indicator of security champions?". Master thesis: University of Plymouth.

Gonzalez, J and Sawicka, A, (2002), "A Framework for Human Factors in Information security" , WSEAS international conference on information security, Rio de Janeiro, Brazil

ISBS, (2010), "Information Security Breaches survey" http://www.infosec.co.uk/files/isbs_ 2010_technical_report_single_pages.pdf. (Accessed on 19/01/2010)

Lacey, D., (2009), "Managing the Human Factor in Information Security", Chichester: John Wiley & Sons

Landy, F. L., (1985), "Psychology of Work Behaviour", The Dorsey press.

Nosworthy, J, (2000), "Implementing information security in the 21st Century – do you have the balancing factors?" Computers and Security 19(4): pp337–47.

Ruighaver, A. B., Maynard, S. B., and Chang, S., (2007), "Organisational security culture: Extending the end-user perspective", Computers & Security 26: pp56 – 62

Schein, E.H. (1999), "The corporate culture survival guide", San Francisco, California, United States of America: Jossey-Bass Publishers.

Shropshire, J., Warkentin, M., Johnston, A. C., Schmidt, M. B., (2006), "Personality and IT security: An Application of the five factor model", Proceedings of the Twelfth Americas Conference on Information Systems, Acapulco, Mexico, August 4-6

Vroom, C., von Solms, R., (2004), "Towards information security behavioural compliance", Computers and Security 23(3):pp191-8.

Woodhouse, S., (2007), "Information security: End user behaviour and corporate culture", 7th IEEE International Conference on computer and information technology, pp767-774.

Yuen B. Ng., Kankanhalli, A., Yunjie, X., (2009), "Studying users' computer security behaviour: A health belief perspective", Elsevier: Decision Support Systems 46 , pp815–825.

Graphical Interface for Watermarking

R.R.N.Eeshan and M.A.Ambroze

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

Abstract

Watermarking is a method which is use to hide the data or identifying the data within in the digital multimedia such as Images, Videos, and audios. In this paper the discussion is focused on the watermarking of digital images. Digital watermarking is becoming more popular mainly for embedding undetectable and detectable identifying the marks such as author and copyright information. This research aim is to represent the graphical interface for watermarking techniques. . In this project, the digital watermark is using visible and invisible watermarking technique is designed and discussed. Invisible watermarking using least significant bit (LSB) technique is implemented; the image is to be watermarked has number of pixels, each pixel is represents with the binary system, which is structured to create a digital plane. LSB bits of pixels shows randomness and will not affect the original image even after the bit is changed. We can replace a bit with watermarking metadata. Visible watermarking is visible even after the image is embedded on the original image. This process is implemented in java for graphical interface, where GUI was implemented to provide an easy to use interface that allows easy comparisons of images, and reliable on watermarking techniques.

Keywords

Least Significant bit, Graphical user Interface (GUI), digital watermarking

1 Introduction

In recent years, Multimedia technologies have become increasingly sophisticated with in the rapidly growing internet which allows Images, audio and videos. According to this there are several problems that are related with security, copyright, and so on. Especially the important factor was to protect the rights of the owners with different watermarking techniques in multimedia distribution. The copyright define for copyright protecting and secure the intellectual property rights. In this, if copyright have some problems where the other persons claimed that they own the multimedia objects like images, audio and videos. So to solve this kind of problems copyright had been adapted to digital watermarking techniques which embed the hidden metadata, information, or secret information in a host image (Kutter and Hartung, 2000). Where this allows someone to identify the original owner rights or in case of illicit duplication of purchased materials in which the buyer is involved. Digital watermarking is an effective technique for protecting these rights. There are several domains in the digital watermarking techniques one of which is frequency domain and spatial domain. Spatial domain is the earliest watermarking techniques the simplest example is to embed the watermark into the least Significant bit (LSB) of the image pixels, this technique has a relatively low capacity of information

hiding. And in frequency domain approach can be embed more information bits and it is relatively robust to attacks. This technique inserts the direct watermarks in a host image by changing the pixels values and increasing the bits information (Hanjalic et al., 2000). Our goal was to design and implement the watermarking methods and determining the process of adding/ embedding, extracting the watermarks. In this we have proposed one of the methods with a GUI for watermarking by using visible and invisible watermarking technique is designed and discussed. Invisible watermarking using least significant bit (LSB) technique is implemented; the image is to be watermarked has number of pixels, each pixel is represents with the binary system, which is structured to create a digital plane. LSB bits of pixels shows randomness and will not affect the original image even after the bit is changed. We can replace a bit with watermarking metadata. Visible watermarking is visible even after the image is embedded on the original image. So additionally we have created a graphical interface (GUI) that would allow the users unfamiliar with java which is JDK 1.6 used for adding different features as well as extract watermarks and evaluate their respective robustness based on a few morphological image attacks. Where GUI was implemented to provide an easy to use graphical interface that allows simple comparisons of images, and reliable on watermarking techniques.

2 Related works

Generally, copyright will present the ownership of the multimedia object. It uses the watermarking technique, which is use to protect its copyright of the digital media (Hy et.al., 2006) In order to achieve the purpose of watermarking techniques for protecting the rights of the owner and also the technique should meet the following requirements:

- Robustness: Depending upon the applications the digital watermarking can support different levels of robustness towards the changes that has made to the watermarked content. If digital watermarking is used for the ownership rights identification then the watermark should be robust against any modification. In the real world environment, no such perfect watermarking method is implemented and it is not clear yet whether a perfectly secure watermarking method exist (cox *et.al, 1997*, Fridrich *et.al, 1998)*. The watermarks should not be degraded or destroyed with the respective robustness based on a few morphological image attacks.

- Imperceptibility: The embedded watermark is invisible by both statistically and perceptually and does not alter the aesthetics of the content that is watermarked. It is very difficult to distinguish the difference between the original image/medium and the embedded one for human eye. The basic concept of the visible watermarking is simpler when it is compared with the invisible watermarking. The main advantage of using the invisible watermark is that in does not lower the quality on the content.

- Inseparability: Even after the digital material (it can be text or an image) is embedded with watermark separating the content that is used for the watermark to retrieve the original content is not possible.

3 Implementation

The implementation is divided into two approaches, visible watermarking using basic watermarking techniques, and invisible watermarking using least significant bit (LSB) in spatial domain.

The implementation of visible watermarking, a visible watermark means that it is visible to the user and the information could be anything like text, logo or image. It is a process that can add/embed secret message on to the image; the secret message could be anything like text or an image over an original image. In this process the embed text can be placed anywhere on the original image from any position, in this we can change the visibility of the embedded text or image, and also has the process of changing the font and size of the text, it has different features of scaling the text or an image. In the above figure A, we can see the actual process of embedding the text or an image in to the original image to get the watermark image. These types of image will have the 8 bit image as a cover image and the input of the file to be embedded is the actual image could be colour image. While in visible watermarking is not that sure for watermarking for different application like copy writer because the algorithm cannot be kept covert. The goal was to design and implement the watermarking methods and evaluate the process of displaying and scaling and determining the right flow of events for watermark embedding, adding the covert message So additionally graphical interface (GI) that would allow the users unfamiliar with java to add evaluate their respective robustness based on a few structured images. The output using GI will be explained in result part. Figure 1 is a pictorial representation which shows the flow of visible watermarking.

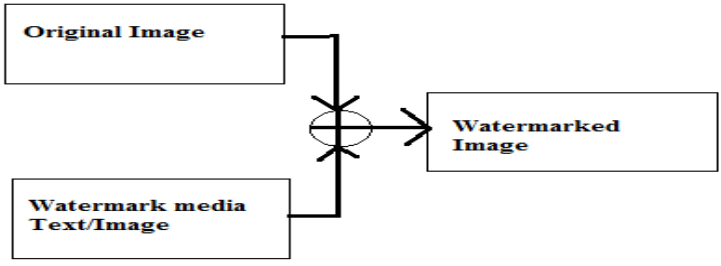


Figure 1: For embedding/adding the watermark on to the image.

Secondly, invisible watermarking using least significant bit, least significant bit is used for visible watermarks; it is the simplest method in hiding the covert message in the original image. Least significant bit is based on the substitution method. The LSBs of pixel of a cover image to the covert image from watermark noise. It embeds the watermark into the least significant bit (LSB) of the image pixel. Adding/embedding and extraction is done by using correlation of both the images. The main advantage of using this technique is, it has a relevant low information hiding capacity, and the disadvantage is that it can be erased by lossy image compression.

3.1 Spatial domain technique

Spatial method analyses the information from the spatial can be viewed from the point of information, where it scatters the information in such a way that the data cannot be easily detected in spatial domain watermarking. The spatial technique has different methods of using pixel, by changing the value of the pixel or alters the lower level bit of the pixel so that the image should not lose the quality (Wolfgang et.al., 1996). One of the methods of data hiding exploits least significant bit (LSB) plane, it has a direct replacement between the cover images. The message and LSB watermark bits will adopt the logical and arithmetic combinations. The image is watermarked in such a way that by selecting the randomly 8x8 blocks of the pixels of the image, it is the earliest watermarking techniques are of this kind, and the simplest example is to embed or add the watermark into LSB of the image pixels. The other features using pixel is adding a positive number to the one of the sub group where the image is grouped into two sub groups (pitas, 1996).

3.2 Watermark Insertion

Embedding the process of the LSB watermarking process, the original image is in vecterized form, this means that it is converted into the matrix form. Then each byte of the image is taken and replaces with the last bit of LSB to the secret information that is watermark image of the each bit. Then the secret image also access the each pixel to convert into the matrix form, then they convert into arrays of bits in binary's of 0s and 1s, and replaces with the least significant of the bit, the output is the watermarked image. It shows that the original image is embedded in to the covert/ secret image that is shown in the figure 2. Figure 2 shows the overall flow of the watermark insertion.

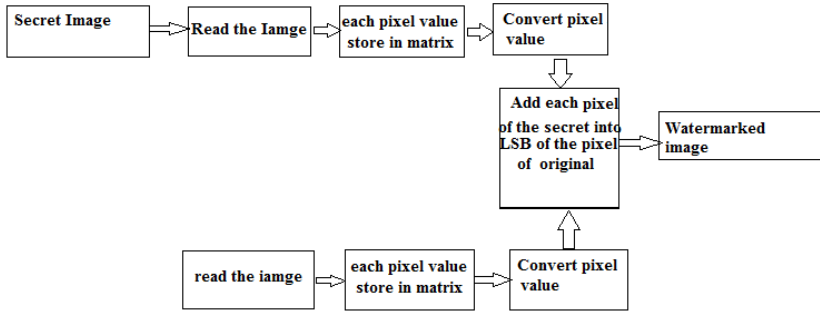


Figure 2: Watermark Insertion

3.3 Watermark extraction using LSB.

It is the similar way of extracting the watermark but in reverse way of doing it. It is the process of finding and extracting the similar bits for both the image like, original and the watermarked image. In this process, after the least significant bit is extracted from both the images, the output is in the form of bytes, and then they are grouped to

obtain the watermarked information. This is the process of extraction this can be found from the figure3.

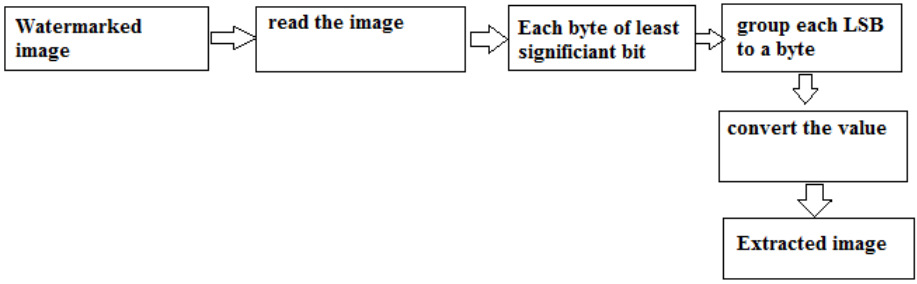


Figure 3: Watermark Extraction

4 Implementation Results

Based on the investigation and implementation we have obtained some results which are discussed in detail as follows.

As mentioned earlier, visible watermark interfaces with the image and can be annoying. It can be easily removable, but the quality will be affected. This was designed to show how the interface is happening between the embedded processing like text and image onto the original image. This is a basic watermarking process that is been implemented using the graphical interface for watermarking. It will show how the interface take the input and process it or in other way adds the covert data in to original image. It has different functionalities that will be explained using Figures. In figure 4, we can select the image by clicking on the browser. We can preview the selected original image. In the functional panel we can select the type of secret message to add/embed on the original image the message could be text or an image.

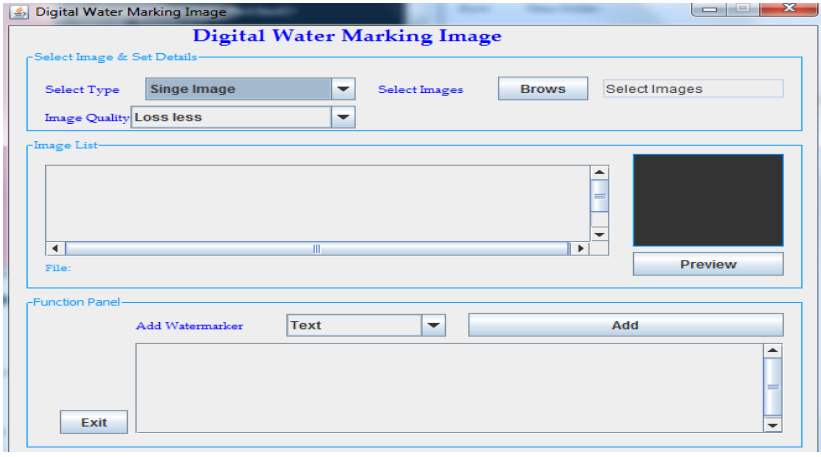


Figure 4: GUI for visible water marking

There are some options for setting the size, font, pixel position, image position, and also can change the visibility options like maximum visibility to minimum. This is the basic implementation using basic visible watermarking technique. The main reason using this technique was to explain the visible watermarking process, how the text or image is embedded on the original image. These images cannot be extracted; there is no software for the extraction process in this method.

In this process a text is embedded in the original image which is visible. In figure 4.8, we can see the text to embed. The difference can be seen from Figures 5 and 6. This is to show the actual process of watermarking technique for visible watermarks. The changes can be made on the written text like increase the size, change the font, change the colour, position of the text to be placed, and the visibility of the text.

Figure 5: Original image

Figure 6: Embed text

From Figures 7 and 8 we can see that how an image is embedded on to the original image. In this we can change the visibility of the embedded image, set the positions of the image. This is to show where the image is been embedded visibly.

Figure 7: Original image

Figure 8: Embed image

5 Results for invisible watermarking

This section will show the results that grained for the LSB watermarking that was implemented. Here JPEG file are used for the cover image as well as watermarked image. The size of the file taken here was 24bit 256*256 colour versions for the original image, 8bit figure the watermark image is been added/ embedded in the original image, it's like adding original image + watermark. This watermarked bit is not visible to the human eye, this process of watermark is called invisible watermark. The image looks same as the original image even 16*16 for the secret image for the least significant bit. The output of the file is resized to the 8bit 16*16 which is very small.

In figure 9, we can see the original image that was selected. And in this the watermark is a predefined image is (J) that is been added to the original image. On clicking the button, insert watermark into the image, the watermark gets embedded into the original image. In this process 24bit 256*256 original image is used. And the water image is smaller size 8bit 16*16. This is mainly used for inserting the logos of the organisations so that it should be secret. In Figure 10, we can see that embedded watermark, in this the main part of interface is that it takes the input process it and sends back the output to the user. In this when the covert image is added to the image.

In figure 11, this is the extraction of the watermark, when we click the extract watermark form the image in figure 10, we can see the covert image is been extracted from the original image is been shown in figure 11.In this we can see the extracted image which was (J), this was extracted from the figure 10 to get the same results, which was embed in figure 9. We can see that extracted image and watermark image was same.

Figure 9: Original image

Figure 10: Hidden image same as original

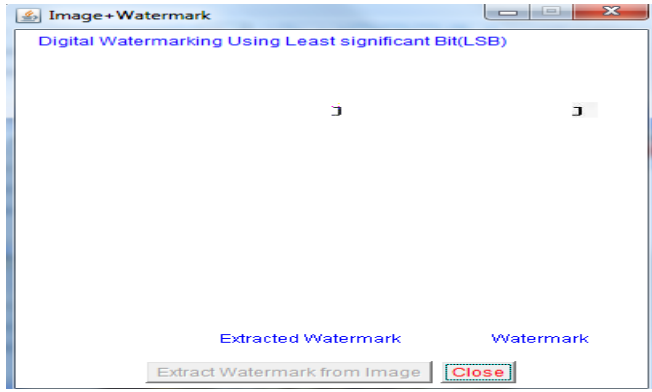


Figure 11: Extracted image

6 Conclusion and future work.

Form the above analysis and discussion for watermarking techniques that are visible and invisible. These techniques perform adaptive measures in embedding the covert message in to the original image where they can be easily achieved. When dealing with the images, it is more useful to approach the matter form the visual position, where the GUI makes visual application much easier. As GI allows us to compare and contrast the original image and the embedded one this is easier to compare the image, and also monitors the illegitimate user by make copies. These methods are successful watermarking in the perspective of reliability and cost. Watermarking is a powerful technique of hiding the data in other files without altering the cover image noticeably. In future this work can be improved by extracting the visible watermarks, and can also introduce the lossy, and lossless visibility watermarking for the quality levels. And there is another important transformation called as Fast hadamard transformation which was not discussed in depth. This is found to be more robust and efficient approach for digital watermarking of digital images; this is used to scale the watermark coefficients in the similar range to the coefficient form hadamard coefficient of the sub blocks of the container image. This research work can be further be improved by improving the security and the robustness.

7 Reference

Cox I. J, Kilian J Leighton F.T and Shamoon T. “Secure spread spectrum watermarking for multimedia,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, December, 1997

Fridrich.J, “Robust digital watermarking based on key,” In Proc. of the International Information hiding Workshop, 1998.

Hartung, F. (2000). Introduction to watermarking techniques. In S. Katzenbeisser & F.A.P. Petitcolas (Eds.), Information hiding techniques for steganography and digital watermarking. Boston: Artech House

Hanjalic, A., Langelaar, G.C., van Roosmalen, P.M.G., Biemond, J., &Langendijk, R.L. (2000). Image and video databases: Restauration,watermarking and retrieval. Amsterdam: Elsevier

Hy.M,Lou.D, and Chang.M. Dual-wrapped digital watermarking scheme for image copyright protection. Computers& Security, 26:319–330, October 2006.

Pitas, "A method for Signature Casting on Digital Image," Proc. Of ICIP, Vol. 3, pp.2 15-2 18, 1996.

Wolfgang.R and E. J. Delp, "A watermark for digital images," *Proceedings of the 1996 International Conference on Image Processing*, Lausanne, Switzerland, Sept. 16-19, 1996, vol. 3, pp. 219-222

Security on Mobile Devices: A Survey of Users' Attitudes and Opinions

J.E.Symes and N.L.Clarke

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

Abstract

With greater number of people using mobile devices than desktops over the last few years has left many subscribers using the same functionalities which are found on desktop computers but with little security features to protect them from risks and attacks. This paper presents the survey results of over 300 subscribers, which evaluates their attitudes and opinions about mobile security, as well as their perception towards future security features on mobile devices. It is clear from the survey's results that there is an apparent difference between users wanting more security features on their mobile device but not currently using what is available. With 68% of the survey respondents either 'somewhat concerned' or 'very concerned' about mobile security and 63% of the participants wanting more security features on their mobile device, this prompts issues for further investigation. Furthermore, despite users becoming more concerned and aware of security threats and risks on mobile devices, 43% are not taking any precautions to protect their devices from unauthorised access.

Keywords

Mobile device, user survey, mobile security.

1 Introduction

The evolution of mobile devices has changed dramatically over the last few years and brought a revolution to the functionalities and services that mobile devices are able to offer. As a result, mobile devices have similar levels of capability as desktop computers; however the security being utilised is not the same or unavailable for mobile devices. With over 5 billion mobile connections (GSM Association, 2011) and an increase in risks and attacks occurring on mobile devices, a significantly increase in risks towards sensitive information stored on mobile devices exists.

The importance of security on mobile devices is difficult to calculate, especially as trends show that some subscribers are making a complete switch from desktop to mobile devices (IBM, 2008). In fact, according to a recent survey, it indicated that people would consider a mobile device over a PC for Internet access (IBM, 2008). This is also backed up by the statement from Gartner PC stating that, *"by 2013, mobile phones will overtake PC's as the most common web access device worldwide"* (Gartner, 2010). As a result, with many web-based applications accessible via mobile devices, security needs to be of high-quality to prevent security breaching from occurring.

While technically it appears security is lacking, a requirement exists to better understand what people use the technology for and what aspect of security they currently use. A previous survey has gathered information about users' attitudes towards security on mobile devices, (Clarke and Furnell, 2005) yet with the increase of 3G networks and the use of the mobile Internet, a similar up-to-date survey has been created. This has been compared to Clarke and Furnell (2005) survey to help examine the changes in subscribers' usage, needs, attitudes and opinions about mobile security.

The paper will be organised as follows. Section 2 reviews and discusses the major results and conclusions from Clarke and Furnell survey. Section 3 describes the general traits of the survey respondents including their mobile usage, current security features being used, their attitude and awareness toward mobile security. Section 4 provides a general discussion to the findings and a comparison between the two surveys. Finally the paper ends with a conclusion.

2 Review pervious work

A survey was conducted in 2002-2004 by Clarke and Furnell which concludes that subscribers are not using security features to help protect them from security breaches. Of its 297 surveyed participants, 66% used PIN codes on switch on, yet 85% of respondents would favor additional security for their device.

Clarke and Furnell found that fingerprint and voiceprint recognitions were the most widely known techniques among their survey respondents. Overall, with the exception of facial recognition, their results show that if a respondent was aware of a technique, there was a greater than 60% chance that they are willing to use it on their device. This suggests that if users were aware of an authentication technique, then a majority would be willing to use the technique (Clarke and Furnell, 2005).

Features	Percentage of respondents
Text Message	97%
Telephony	95%
WAP Services	36%
International roaming	36%
Information services	26%
Email	22%

Table 1: Usage of mobile devices in 2002-2004

Another important result from Clarke and Furnell survey was current usage of mobile handsets during their survey took place. In 2002-2004, as seen from table 1, text messaging and telephony dominate the mobile usage at this time. However, other features such as WAP services and information services were used by over ¼ of the subscribers. During these two years, when the survey took place, functionalities on mobile devices such as email were on the increase. Today with the changes in functionalities as well new features such as 3G network and the mobile Internet has prompted research to obtain up-to-date information on the attitudes and

opinions of users toward mobile security. Whilst the technology has changed over the last 7-9 years in terms of function, has there been a change in terms of security?

With this in mind, a survey was conducted and distributed to understand the user's attitude towards current and future security on mobile devices. The survey was conducted over 3 months via an online questionnaire and promoted via emails, links on websites and flyers.

3 A survey of subscribers' attitudes and opinions

3.1 Survey participants

As a first step in assessing the end users view of mobile security, the survey attempted to gain a fair and un-bias set of results from a distribution of participants from all ages. However, figure 1 clearly shows that in particular, 56% of respondents were in the 18-25 age bracket.

Although this is likely to skew the results, this age range is similar to Clarke and Furnell survey where 71% of their participants were in the 17-24 age group (Clarke & Furnell, 2005). Therefore since trends were concluded from comparing these two surveys, age factor is not as large as it might initial appear.

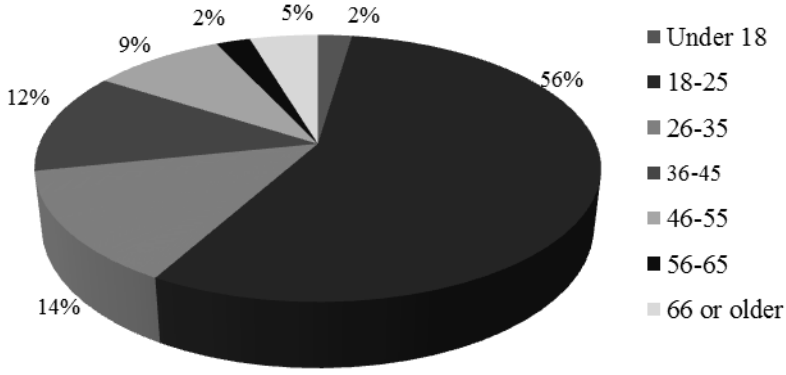


Figure 1: Percentages of participants' age

The distribution of gender was quite spread out in this survey. 55% of participants were male while the remainder where female. In terms of statistical analysis, this is quite a fair approximate of users, with males a little higher than females.

3.2 Usage of mobile technologies

To help improve mobile security the survey analysed the respondents' perspective on current handset usage. The findings in relation to mobile usage revealed that the

most used feature is SMS. This was closely followed by browsing the Internet, telephony and social networking as seen from figure 2 below. There seems to be a change in mobile usage with and dramatic increase of features such as Internet and applications occurring today compared to the past. These popular features use either the network providers 3G services or more commonly now – WiFi, both of which were limited or not available when Clarke and Furnell survey took place. Other past surveys seem to echo the most widely used feature as SMS while other features such as video calling or MMS fall somewhat behind (GSM Arena mobile usage report, 2011; Kennedy et al., 2007& Clarke &Furnell, 2005).

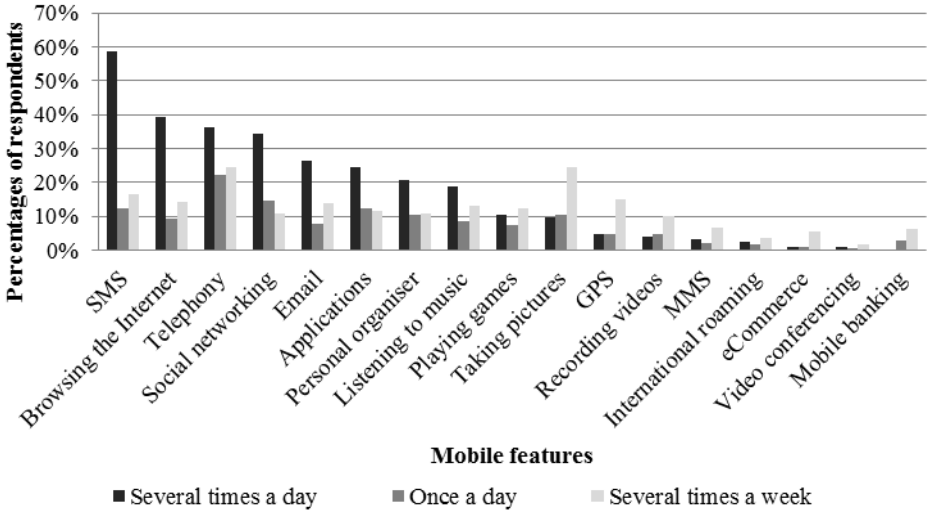


Figure 2: Mobile device usage

3.3 User's attitude

When respondents were asked if they are concerned about the security on their mobile devices, 68% of participants were either 'somewhat concerned' or 'very concerned', as shown in Figure3. Not surprisingly, IT professionals with a degree education or higher, where more concerned than non-IT professionals. Either way, from the data gathered from the survey, it is clear that the majority of subscribers are concerned about mobile security. This plus the fact that 63% of survey participants would like additional security on their mobile device, prompts issues for further investigation to identify issues of user awareness of mobile security and considerations to improve the security on mobile devices in the future.

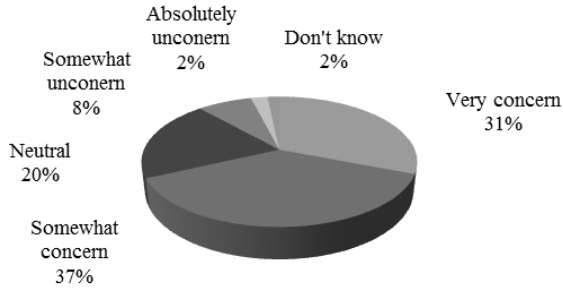


Figure 3: Security concerns of survey participants

The survey also attempts to determine the perceived importance of several factors when choosing a mobile device. The results suggest that features such as Internet usage or applications matter more to users than security when choosing a device. These results conflict with each other, since it seems that users would like additional security on their mobile devices and concerned about it, yet when purchasing a new device, other features are more important than security.

3.4 Security procedures currently implemented on mobile devices

Figure 4 presents the percentage of respondents who currently use security features on their mobile device. It reveals that backing up contacts and other personal data is the most commonly used security features used on today's devices. However less than half of respondents carry out this simple procedure which serves to highlight an important issue. This security feature is available to perform on all devices, but less than half of subscribers are using it. Additional hardware such as SIM card readers or USB cables are often required to carry out this feature, yet newer devices do not come with these in the handset boxes. Subscribers have to buy additional hardware to perform this security feature which is inconvenience and therefore not all subscribers perform this procedure.

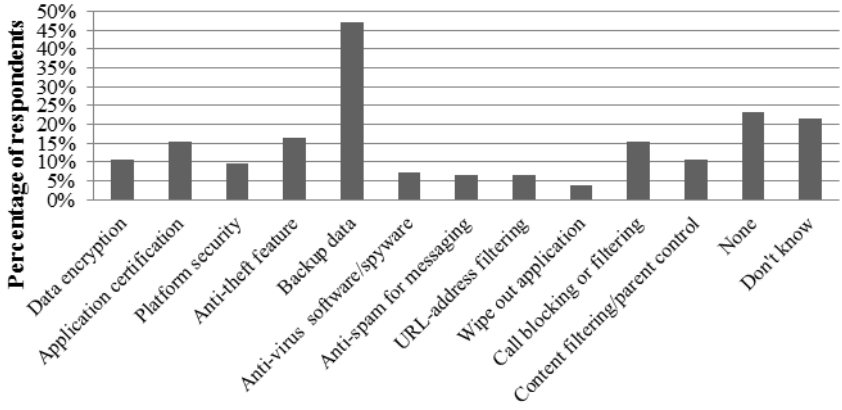


Figure 4: Security features implemented on mobile devices

Many desktop computers automatically perform anti-malware scans yet from the complete set of results only 7% of the survey participants use anti-malware software on their devices. When participants were asked to rank what they believe is the most likely to cause of data misuse, malware came second to stolen devices from a list of choices available. This suggests that subscribers are indeed security conscious, but are not using countermeasures or procedures to prevent it from occurring on their device.

Some may argue that with few malware on mobile devices at present, is there a need for anti-malware protection software on these portable devices (Goode, 2010). Yet like many security procedures, it is better to have it in force before the attack occurs rather than adding it later when the damage may have already occurred. In addition, with more data being stored on mobile devices such as bank details and confidential emails, this motivates hackers and malware writers to create new malware to access this data. Therefore in the future, there will certainly be an increase in malware in mobile devices (Goode, 2010).

3.5 Usage use of PIN-based authentication

PIN-based authentication is quick and easy method that works on nearly all devices. When respondents were asked if they used PIN-based authentication, 32% used a PIN code on standby, while 44% used power-on PIN's.

However, even those who use PIN codes were not necessarily doing so properly. If a PIN code is shared like 26% of users in 2002-2004 (Clarke and Furnell, 2005) or not changed regular, then some may say that PIN-based authentication is not effective since it can be guessed using social engineering, dictionary attacks or brute force attacks (Kennedy et al., 2007). Therefore, the more often the PIN code is changed the more secure the mobile device will be. From the survey results, as seen in table 2, 14% of respondents change their PIN code monthly while 10% change their PIN codes yearly. However, 58% have never changed their PIN code. This suggests that PIN based authentication, which is available on nearly every handset, presents some major challenges in terms of correct usage.

Duration	Percentage of survey respondents
Daily	1%
Weekly	0%
Monthly	14%
Yearly	10%
After Purchase	17%
Never	58%

Table 2: Respondents changing their PIN codes

3.6 Awareness of mobile security

If the user would like additional security on their device, are they aware of what authentication methods already exist on their device? It seems that PIN-based authentication methods are commonly known, but how about the other types of

authentication techniques such as fingerprint scanning or graphical passwords. The awareness of authentication methods is a key area of interest due to the fact that user awareness is hindering mobile security. Therefore, the survey asked the subscribers if they are aware of different types of authentication methods. As seen from figure 5, subscribers are most aware of fingerprint recognition, even though it requires additional hardware such as the fingerprint scanner to function. With this is mind, another question asked the subscribers if they would consider using different types of authentication methods if it was available on their device and again fingerprint recognition scored high. On the all, subscribers would consider using authentication methods if it was available on their device even if they were not fully aware or understand the technology.

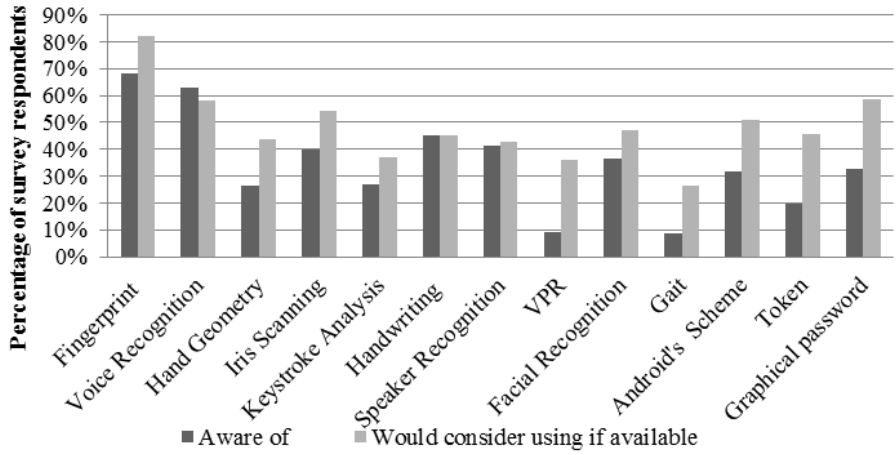


Figure 3: Awareness and considering using of authentication methods

4 Discussion

The survey results suggest that overall; subscribers are concerned about security on their mobile devices and $^{2}/_{3}$ of mobile users want additional security on their devices. However when comparing the difference between certain factors that affect choice of handset, in 2002-2004, security was the second largest factor after battery life (Clarke and Furnell, 2005). However today's results suggest that users are not as concerned about security when choosing a handset, but instead other factors such as Internet usage and applications matter more to users than security. One reason for this may be due to social trends. Subscribers would prefer to have the latest features to 'show off' rather than built-in security features.

	2011 survey results	**2002-2004 survey results**
Power-on PIN	44%	66%
Stand-by PIN	32%	18%

Table 4: changes in the percentages of respondents using PIN based authentication

As seen from table 4, another comparison that is worth discussing is the 22% reduction in power-on PIN that has occurred over a period where the functionality of mobile devices has dramatically changed, serves to highlight the change in how subscribers use their device.

A possible reason could be due to the fact that in 2002-2004, 85% of respondents had their handsets on for more than 10 hours a day. Today, 85% of respondents have their devices on 24/7 and 93% have their device turned on for more than 12 hours a day. Therefore, with so many users not turning their phones off means they are not switching it on. This change in functionality of device may be a major reason why less people are using power-on PIN today.

So why is there a change of attitudes and opinions about security on mobile devices today? It seems that there still remains a gap between security on mobile devices and what the end users would like on their devices, even with the change in functionalities. Some manufacturers today offer security features such as anti-virus software or encryption of data, yet the consumers are not using or aware of it (McAfee, 2009).

One of these reasons why there is a gap between what the subscribers want in term of security and the security features which are delivered on mobile devices is the lack of technological requirements available, such as the limited on-board processing power, memory and battery requirements. Some security features such as biometric authentication would require additional hardware or software. However, some for instance hand geometry, the hardware would be too large, bulky and heavy to include on mobile devices. Therefore, when considering mobile security, one must consider other limiting factors such as the large variety of handsets in addition to the lack of user awareness.

Given the apparent disparity, between users' concerns and wanting more security features but not currently using what is available, another possible reason may be since some security features such as anti-malware or anti-spyware software need to be kept up-to-date with the latest signatures. If not, the anti-malware software becomes out-of-date and the problem of 'mobile blind spot' occurs (Friedman et al., 2008). This major challenge is changing as the survey results suggest that more people are using and keeping their WiFi on all the time. However, many of these security tools only update when connected to a corporate network. Some mobile devices require the user to visit the corporate websites manually. However, on desktop computers, it automatically connects to the corporate network and downloads new updates. This is not the case for all mobile devices. Therefore for certain security features to work effectively without affecting increasing the inconvenience to the user, security features should be able to connect automatically to download updates similar to desktop computers.

Another factor which needs to be discussed further is that many security features are available but are not well advertised. When one buys a desktop computer, it is often next to the latest version of anti-virus software and has a deal where you can buy both at the same time, often with a discount on the software. Yet with mobile devices this is not the case. When a consumer walks into a mobile phone shop, there

are no advertisements about additional security features the device could have. Even network providers' websites do not provide information about additional security features on mobile devices. If security products are not well advertised then the consumers will not be aware of their existence in the first place.

It seems from the complete set of results that users would like security to be present and active when they purchase a device. However, this does not occur on all devices. A reason for this may be due to technological requirement on the handset itself. With processing power and memory being a limiting factor, if certain types of security features were active when purchased, this may make the device slow and inconvenient for the subscriber.

5 Conclusions

With millions of users of all ages from around the world using mobile devices everyday for functions from telephony to mobile banking, has brought security issues that were not present some years ago. The nature of the information stored on mobile devices has placed a necessity for a high level of security. However, with many limiting factors which are hindering mobile security, a compromise between the level of security provided by a technique and the inconvenience to the user is required.

The survey findings reinforce the view that the existing security approaches such as backing up data and the use of a PIN is not a significant approach to this problem. A large majority of users are concerned about security on their devices and want additional security available on them. On the basic of these findings, it is evident that alternative and stronger secure solutions are required for mobile devices. These procedures must be capable of securing access to sensitive data throughout the duration of use, in addition to convenience and cost.

6 References

Clarke, N. L., & Furnell, S. M., (2007), 'Advanced user authentication for mobile devices' *Computers & Security*, 26(2), 109-119.

Clarke, N. L., Furnell, S. M., (2005), 'Authentication of users on mobile telephones- a survey of attitudes and practises', *Computers & Security*, 24(7), 519-527

Friedman, J & Hoffman, D. V., (2008), 'Protecting data on mobile devices: a taxonomy of security threats to mobile computing and review of applicable defences', *Information, Knowledge, System Management,* 7(1-2), 159-180.

Gartner, (2010), 'Mobile Phone Sales Grew 35% in Third Quarter 2010; Smartphone Sales Increased 96%', [online], Available at: http://www.gartner.com/it/page.jsp?id=1466313 (Accessed on 24/11/10).

Goode, A., (2010), 'Managing mobile security: how are we doing?', *Network Security*, 2010(2), 12-15.

GSM Arena, (2011), 'GSM Arena mobile phone usage report 2011', [online], Available at: http://www.gsmarena.com/mobile_phone_usage_survey-review-592p12.php (Accessed on 02/06/2011).

GSM association, (2011), 'Global GSM and 3GSM mobile connections', [online], Available at: http://www.gsm.org/ (Accessed on 22/09/2011).

IBM, (2008) 'IBM study finds consumers prefer a mobile device over the PC', [online], Available at: http://www-03.ibm.com/press/us/en/pressrelease//25737.wss (Accessed on 12/09/2011).

Kennedy, G., Dalgarno. B., Grey, K., Bennett, S., Maton, K., Krause, K. L., Bishop, A. & Chang, R., (2007), The net generation are not big users of Wed 2.0 technologies: preliminary findings, *Proc. Of ICT: providing choices for learners and learning conference 2007*, Singapore, 517-525.

Kurkovsky, S. & Syta, E., (2010), 'Digital Natives and mobile phone: a survey of practises and attitudes about privacy and security' *In Proceedings of the 2010 IEEE International Symposium on Technology and Society: Social implications of emerging technologies*, Wollongong, Australia, June 7-9, 2010.441-449.

McAfee, (2009), 'Mobile security report 2008', [online], Available at: http://www.scribd.com/doc/2987302/mcafee-mobile-security-report-2008 (Accessed on 10/01/2011).

Section 3

Computing
&
Computer Science

Impact of the Consumption of Interpersonal Electronic Content (CIEC) in the Context of Romantic Relationships

S.Barrington and B.G.Sanders

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

Abstract

Technical, social and economic drivers have facilitated the growth of online User Generated Content (UGC). This has raised a number of concerns regarding the privacy and misuse of that data. However, very little research has been conducted to examine the consumption of content that is available through authorised or public channels, in the context of romantic relationships. This research investigates the sources used to obtain interpersonal content, the type of content consumed (e.g. current or archived material), the emotional impact on the consumer, and the efficacy of four proposed application-level features to reduce the consumption of content.

The research was conducted with a sample of 252 participants. The findings revealed that the majority of respondents reported to engage in the consumption of interpersonal content (n=225, 89.2%), the majority of which obtain this content from 2 to 3 different types of sources (n=112, 49.8%), e.g. social networking sites, personal websites and search engines. However, most respondents conduct this type of activity less than once a month (n=107, 47.5%).

The majority of respondents (n=117, 52%) reported to experience some emotional impact (positive and/or negative). Of those who consumed online content, 16% reported to have experienced exclusively negative emotional consequences, such as increased feelings of sadness, anxiety and suspicion regarding their partner's activities. An analysis of the data did not find any correlation between emotional experience and demographic factors, including gender, age, the length of the relationship and the length of time single.

Keywords

Cybersurveillance, Electronic Surveillance, Social Media, Social Networking, Mobile Social Web, Interpersonal Content, Romantic Relationships, Emotional Impact

1 Introduction

It was reported in 2010 that 38.3 million UK adults were 'internet users' (Office of National Statistics, 2010). Web 2.0 developments and the rapid adoption of mobile communication technologies have been significant drivers in the growth of User Generated Content (UGC) (Green and Smith 2004). Further growth of UGC is predicted (Daugherty *et al*., 2008).

The number of adults who joined social networking sites more than quadrupled, from 8% in 2005 to 35% in 2008 (Kennedy, 2009). Facebook is one of the most popular international SNS applications, claiming to have more than 500 million active users (Facebook, 2011). It has been reported that a great deal of highly personal information is shared with the online community (Furnell, 2010). This has raised a number of concerns regarding the privacy and misuse of that data, such as social engineering attacks (Sanders, 2008) and cyberstalking (Reed, 2011).

2 Cybersurveillance

Cybersurveillance is a broad term for a wide range of surveillance activities executed on, or with the aid of various technologies. Peer-to-peer cybersurveillance behaviours include cyberstalking (Spitzberg and Hoobler, 2002), Facebook stalking (Kennedy, 2009), and snooping (Dumpala, 2009). However, there are inconsistent definitions of these behaviours, and terms such as 'stalking', have been applied to a broad range of very different behaviours and practices.

Peer-to-peer cybersurveillance research has primarily focussed on two behaviours; cybersnooping (Phillips 2009) and cyberstalking (Spitzberg and Hoobler, 2002). These behaviours include the use of illegal, unauthorised or specialist surveillance technologies to gain information about another, and in some cases with the intention of causing harm to the individual under surveillance. However, there has been very little investigation of other behaviours on the cybersurveillance continuum such as the consumption of content through authorised or public channels.

Stern and Taylor (2007) found that 30% of respondents used Facebook for investigating ex-partners, 38% for tracking the activities of others, and 40% for monitoring current partners to check for evidence of infidelity. Phillips (2009) found that 83% of respondents monitored their partner's comments, pictures, or messages on social networking sites, and that approximately 65% had used this information to question their partner. It has been asserted that social networking and location-based social networking sites facilitate surveillance (Kennedy, 2009). There is evidence that users do not regularly maintain their personal content online (Walther *et al.*, 2008), which may be a consequence of inadequate auditing and content management.

3 The Impact & Consequences of Consuming Interpersonal E-Content

Online communities and communication applications can have a positive impact on relationships. It has also been suggested that the activity of sharing thoughts and experiences, can bring people closer and help establish common interests (Chen, 2010). Walther (1996) asserts that computer mediated communication can be *hyperpersonal*, i.e. it can facilitate a more enhanced mode of communication than face-to-face methods.

However, it has been reported that the act of observing others can result in mental health problems, paranoia and anti-social behaviour (Atkinson, 2007). The opportunity to observe previous partners may make it difficult to overcome a

breakup, and 'watching' them move on with their lives can exacerbate feelings of loss and distress (Gershon, 2010).

Muise *et al.* (2009) found that when partners are connected to ex-partners or other unknown parties, there is greater opportunity for the development of jealousy and suspicion. Jealousy can threaten self-esteem when individuals are unfavourably comparing themselves to perceived rivals (Guerrero and Afifi, 1998). It has been suggested that offline artefacts relating to former relationships (such as photographs and affectionate messages) were not often made available to new partners before the creation of social networking sites (Bowe, 2010).

A further consequence is the erosion of trust between both partners in the relationship as a result of surveillance behaviour. One may feel disgruntled for being subjected to surveillance, and thus withdrawing from the relationship, whilst the other may become *more* suspicious of their activities because they are more withdrawn (Muise *et al.*, 2009).

4 Method

An online survey technique was employed. Participants were required to be aged 18 or over, a current member of at least one social networking site, and if not currently in a relationship, they must have been in a relationship previously. Those who were *not* in a monogamous relationship were asked questions relating to former partners, and those in a relationship were asked about their current partner.

A pragmatic sampling approach was selected due to practical considerations, although it is acknowledged that the sample generated may not be representative. Participants were recruited through Plymouth University contacts and web-based advertisements (e.g. posts on social networking sites and public discussion forums).

The survey contained primarily quantitative based questions, but included an open question to capture any comments from the participants upon completion of the survey. An extensive search of the literature revealed that a comprehensive, reliable and valid scale for measuring emotional impact does not exist. Loosely based on the principles of the I-PANAS-SF (Thomson 2007), two 5-item subscales of negative affect (NA) and positive affect (PA) were constructed, based on their relevance to the context of romantic relationships. A five-point scale was developed to measure whether the emotion was experienced from 'much more' to 'much less', with the central item measuring no change.

5 Results

A total of 352 responses were received. Precisely 100 were insufficient and thus removed, resulting in 252 responses for analysis. Significantly more females (n=170, 67.5%) than males (n=81, 32.1%) responded to the survey, which may present bias in the results (1 respondent did not disclose their gender) therefore some of the results are split by gender. The age range was between 18 and 63 (mean = 29.7, SD = 9.8). The student (n=123, 48.8%) vs. non-student samples (n=129, 51.2%) were

almost equally distributed. The majority of respondents (*n*=172) were in a relationship (including engaged and married), 66 were single, divorced or separated and 14 were dating or in an open relationship.

The number of respondents who consume interpersonal electronic content was 225 (89.2%), and there was very little difference between the proportions of males (*n*=71, 87.7%) and females (*n*=153, 90%) who reported to conduct this practice. Further analysis of the data showed that there was a significant negative correlation between age and level of e-content consumption (r (*N*=252) = -.400 $p < .001$), indicating that the higher the age, the lower the level of consumption.

Over half of SDO respondents reported to communicate with their ex-partner/s via SNS (*n*=34, 51.5%), and those in a relationship reported the highest percentage of those conducting SNS communication (with their partners, *n*=111, 83.5%). Of the total sample of those who consume interpersonal e-content (*n*=225), the majority of respondents do so less than once a month (*n*=107, 47.5%). Over a quarter of respondents reported to do so either once a day, or one or more times a week (*n*=59, 26.2%). Very few respondents reported to consume data several times a day (*n*=6, 2.6%).

A one-way ANOVA was conducted to analyse the variance of consumption scores between each of the single groups (categorised by the length of time since their last relationship). The results were not statistically significant ($F(4, 61) = 2.264$, $MSE = 103.637$, $p = 0.073$). Statistical analysis revealed that there was a significant negative correlation between the length of the relationship and level of consumption (r (*N*=172) = -.429 $p < .001$).

5.1 Surveillance of Third Parties

Within the single, dating and open relationship (SDO) sample, 89% (*n*=71) reported to consume e-content. Of those, 52.1% (*n*=37) used the site to find out about their ex-partner/s' current partner. In addition, 4 participants said that they would if they had the necessary access. Participants were also asked how applicable a series of statements were to describe their motivation to get information about their ex-partner (question E1). Over half of the respondents (*n*=40, 56.3%) said that the statement "I want to find out more information about my ex-partner/s current partner" was applicable.

Almost a quarter (*n*=46, 26.7%) of those in a relationship conducted a search engine search related to their partner, and 10.5% (*n*=18) related to their partners ex-partners. Overall 32.6% (*n*=56) of respondents accessed at least one of their partners sites (blog/personal website: n=33, 19.2%; social media site: n=33, 19.2%; professional blog/profile n=15, 8.7%) and 13.4% (*n*=23) accessed those of their ex-partner/s (blog/personal website: n=7, 4.1%; social media site: n=18, 10.5%; professional blog/profile n=5, 2.9%).

Just under a third of those in a relationship (*n*=52, 30.2%), used social networking sites to find out about their *partner's ex-partners*. There was however a distinct difference in the responses to this question from those who had access to their

partner's social networking site (*n*=47, 35.3%) and those who did not (*n*=5, 12.8%). Further analysis of the data revealed a significant negative correlation between the length of the relationship and the motivation to retrieve information about their partners former partners, by those with access to their partners SNS content (r (*N*=130) = -.382 $p < .001$).

5.2 Access to Content & Application/Site Features

A bivariate correlation analyses revealed that the results were not statistically significant between the frequency with which mobile/portable devices are used to access online information and the level of online interpersonal content consumption (r (*N*=252) = .105 *p*=.095). However, a weak positive correlation was found between the use of laptop devices and level of interpersonal content consumption (r (*N*=252) = .177 *p*=.005).

Respondents were asked whether any of the following technological changes would reduce their content consumption:

(a) If sites were restricted to display only the last 30 days of information;
(b) If content owners could determine who viewed their information (but not including details about the frequency of visits);
(c) If content owners could determine who viewed their information, including details about the frequency and length of time;
(d) If an alert could be set up to warn users when exceeding a certain period of time on a page.

The only feature which would result in the majority of respondents reducing this behaviour (*n*=105, 46.7%) was item c. However, notably almost the same number of people (*n*=102, 45.3%) reported that there would be no change. Furthermore, 8% of respondents (*n*=18) said that their consumption would increase in this case.

5.3 The Impact & Consequences of Consuming Interpersonal E-Content

The majority of respondents (*n*=117, 52%) reported that there was some impact on their emotions either positively and/or negatively. Those who experienced the least impact on positive and negative affect were those who were in a relationship and did not have access to their partner's SNS content (*n*=16, 66.7%). SDO respondents experienced the most emotional change (*n*=48, 67.6%), and proportionately more reported an exclusively negative affect (*n*=17, 23.9%) than those in a (monogamous) relationship (n=19, 12.3%). Those who were in a relationship and had access to their partners SNS content reported proportionately the greatest positive impact on their emotions (*n*=30, 23.1%). A bivariate correlation analysis showed that the results are not statistically significant between the respondent's emotional affect scores and their level of consumption (r (*N*=225) = -.093 *p*=.164).

6 Discussion

Within the context of romantic relationships, an overwhelming majority (89.2%) of respondents reported to consume interpersonal e-content. Similarly to the findings presented by Tokunaga (2010), there was very little difference between the proportion of males and females who reported to consume this e-content. Despite the large proportion of users who reported to use at least one mobile or portable device daily (to access the internet), there did not appear to be any relationship between the frequency with which they use these devices and their level of interpersonal e-content consumption. This indicates that access to these technologies does not necessarily predict an increase in consumption.

For each of the relationship categories, the *main subject* of the e-content consumed was either their current partner (those in a relationship) or their ex-partner (SDO respondents). Content was consumed on *connected third parties*, i.e. partner's ex-partners or ex-partners current partners, although this was markedly less in comparison to the 'main subject'. However, this demonstrates how content from other members are utilised in information seeking strategies in the context of romantic relationships. This suggests that SNS users' content may be being consumed in unexpected ways and perhaps in ways users would not permit.

However, the data revealed that there was a significant positive correlation between the frequency of communication (with partners/ex-partner/s via SNS) and level of e-content consumption, indicating that the more frequently they communicate, the greater their consumption of interpersonal content. Assuming that the communication was 'direct' communication (as opposed to indirect communication such as second-order information (Gershon, 2010)) this suggests that some respondents are actively participating in the site and not 'lurking' as found in similar studies (Preece *et al.*, 2004). Although participants were not questioned about the level of interaction with connected third parties (such as current partner's former partners), therefore lurking may occur on those sites.

6.1 The Impact & Consequences of Consuming Interpersonal E-Content

As found by Tokunaga (2010), a significant negative correlation was found between the length of the relationship and level of consumption, indicating that the longer the relationship, the lower the level of consumption. This would correlate with other findings that those who are in unstable or new relationships are more likely to conduct surveillance (Persch, 2007).

An assessment of the mean CIEC scores (i.e. the range of sources accessed and frequency with which online content is searched for/viewed) revealed that the group of single respondents with the highest mean score were those who had been single for 1 year to less than 3 years. Furthermore, within this group *every* respondent consumed e-content in this context. One reason why some participants may be consuming online content related to a former partner, after a significant period of time since the relationship terminated, is that some relationships can end amicably (Sprecher and Fehr, 1998) and former romantic partners remain friends post-breakup (Sprecher *et al.*, 1998). In support of this, this investigation revealed that the most

applicable statement to describe the motivation of SDO respondents was 'I am friends with my ex-partner/s, and I use social networking sites to look for information about all of my friends' (78.9%).

Of the 52% that experienced some change in emotion, 18% reported to exclusively experience a positive impact, 16% exclusively a negative impact, and 18% a mixed impact. However, emotions are "…highly complex and subtle phenomena whose explanation requires careful and systematic analysis of their multiple characteristics and components. The major reason for the complexity of emotions is their great sensitivity to personal and contextual circumstances" (Ben-Ze'ev, 2004). For those who experienced a negative change, the precise cause of that change is unknown, and given the complexity of emotions it is likely that it is caused by a number of factors.

Nevertheless it is important to note the findings of Muise *et al.* (2009), who reported that increased time spent conducting surveillance on Facebook, contributed more to feelings of jealousy, beyond other contributory personal and relational factors, which the authors referred to as "…Facebook-specific jealousy". Similarly, Bowe (2010) reported that the content on social network sites can create relational problems, to which there is no 'offline equivalent'. He argues that there would be no such impact before these sites existed.

The respondent's emotional scores were compared with their consumption score, the results of which were not able to find any conclusive evidence that emotional impact was related to the frequency or range of sources used to consume data. Therefore, this research has demonstrated that application-level strategies to reduce the consumption of interpersonal content are not an effective technique to improve user experience in this context. Furthermore, preventing the consumption of interpersonal content would be to the detriment of those who have experienced positive benefits from engaging in this behaviour. In addition, the findings demonstrate that of the four proposed application-level features, only one was revealed as a *potentially* successful method to reduce online content consumption.

7 Limitations and Future Research

An internet-based survey is problematic as there are few opportunities to check the responses for honesty and accuracy. Furthermore, due to a lack of a suitable sampling frame, the sampling methods used were not able to generate a representative sample and therefore may be subject to bias. Terms such as 'romantic relationship' and 'single', were left to the interpretation of the respondent. As reported by Bowe (2010), this may have resulted in great variations in the definition of these terms, which could have impacted on the responses submitted. It is therefore important in future studies that any terms which may be open to cultural interpretations are clarified during the research process. An interview approach may be beneficial in such contexts.

Both the CIEC Scale and Emotional Impact Scale, were not sufficiently evaluated (using factor analysis for example), therefore the quality and accuracy of the results obtained is unknown. Furthermore, it is unclear the extent to which the respondents

were consciously aware of their emotions (in order to be able to accurately reflect on them), or suppressing their emotions (and thus responses) for cultural or other personal reasons. Responses may also have been bias by any negative perceptions of the consumption of online content.

A qualitative methodological approach may be a more appropriate method to examine and assess the experiences of emotion, and context within which they experience those emotions (e.g. personal diaries could be kept by respondents over a period of time (Sprecher et al., 1998)). This approach would be further complemented by Brain Computer Interface (BCI) technologies which can be used to measure emotional state, which may overcome the limitations of response bias as discussed above.

The results have provided an insight into how users source content from multiple sites, and the frequency of the consumption, but little is known as to precisely how much content is being consumed, i.e. how much time do they spend consuming this content, or spend engaging in information-retrieval activities. Further in-depth analysis of this behaviour is required in order to determine and define the different levels of cybersurveillance behaviour on the continuum, their characteristics, methods, similarities, differences and the profile of those who conduct those behaviours. This will serve to benefit academic research as specific behaviours can be isolated and investigated. Research is required to examine the perception of these behaviours in society, whether these behaviours are 'unwanted', and if so in which circumstances, and whether its public perception correlates with its position on the continuum.

8 Conclusion

The results revealed that particular types of e-content have the potential to cause a negative emotional response. This affect may be reduced in three ways; firstly discussing and agreeing on the 'idioms of practice' within a relationship (Gershon, 2010), secondly controlling access to the content, and thirdly controlling the publication of that content. Furthermore, this research supports strategies for increasing user awareness, developing emotional responsive interfaces and conducting further research into the efficacy of existing content management and archiving tools.

9 References

Atkinson, S. (2007) Risk Reduction through Technological Control of Personal Information. Doctor of Philosophy. University of Plymouth.

Ben-Ze'ev, A (2004) Love Online: Emotions on the Internet. UK: Cambridge University Press.

Bowe, G. (2010) Reading Romance: The Impact Facebook Rituals Can Have On A Romantic Relationship. Journal of Comparative Research in Anthropology and Sociology. 1(2), pp.61-77.

Chen, G.M. (2010) Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others. Computers in Human Behavior. pp.1-8. Available at:

http://linkinghub.elsevier.com/retrieve/pii/S0747563210003213 (accessed on 15 January, 2011).

Daugherty, T., Eastin, M.S. and Bright, L. (2008) Exploring Consumer Motivations for Creating User-Generated Content. Journal of Interactive Advertising. 8(2). Available at: http://jiad.org/article101 (accessed on 3 July, 2011).

Dumpala, P. (2009) Who married your ex? Is your gorgeous neighbour available and have bad things befell the bully from high school? Available at: http://thenewblackmagazine.com/view.aspx?index=1935 (accessed on 3 January, 2011).

Facebook, (2011) Press Room. Available at: http://www.facebook.com/press/info.php?statistics (accessed on 3 January, 2011).

Furnell, S.M (2010) Online identity: Giving it all away? Information Security Technical Report, pp.1-5. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1363412710000245 (accessed on 20 December, 2010).

Gershon, I. (2010) The Breakup 2.0: Disconnecting over New Media. USA: Cornell University Press.

Green, N. and Smith, S. (2004) 'A Spy in your Pocket'? The Regulation of Mobile Data in the UK. Surveillance & Society 1(4), pp.573-587.

Guerrero, L.K. and Afifi, W.A. (1998) Communicative responses to jealousy as a function of self-esteem and relationship maintenance goals: A test of Bryson's dual motivation model. Communication Reports. 11(2), pp.111-122.

Kennedy, M.C. (2009) Facebook and Panopticism: Healthy Curiosity or Stalking? Master of Arts. Scripps College of Communication of Ohio University. Available at: http://etd.ohiolink.edu/send-pdf.cgi/Kennedy%20Mary.pdf?ohiou1258038346 (accessed on 5 January, 2011).

Muise, A., Christofides, E. and Desmarais, S. (2009) More Information than You Ever Wanted: Does Facebook Bring Out the Green-Eyed Monster of Jealousy? Cyberpsychology & Behavior. 12(4), pp.441-444.

Office for National Statistics (2010) Internet Use. Available at: http://www.statistics.gov.uk/cci/nugget.asp?id=8 (accessed on 15 March, 2011).

Persch, J.A. (2007) Jealous much? MySpace, Facebook can spark it. Available at: http://www.msnbc.msn.com/id/20431006/ (accessed on 21 November, 2010).

Phillips, M. (2009) You're Invading MySpace!: Predicting the Use of Social Networking Sites for Surveillance in Romantic Relationships. Master of Arts. San Diego State University.

Preece, J., Nonnecke, B., and Andrews, D. (2004) The top 5 reasons for lurking: Improving community experiences for everyone. Computers in Human Behavior. 20, pp.201-223.

Reed, J. (2011) Social network sites 'have duty' to stop cyberstalking. Available at: http://www.bbc.co.uk/newsbeat/14085766 (accessed on 12 July 2011).

Sanders, B.G. (2008) An Assessment of People's Vulnerabilities in Relation to Personal and Sensitive Data. Master of Science. University of Plymouth.

Spitzberg, B.H. and Hoobler, G. (2002) Cyberstalking and the technologies of interpersonal terrorism. New Media & Society. 4(1), pp.71–92.

Sprecher, S. and Fehr, B. (1998) The Dissolution of Close Relationships. In Harvey, J.H. Perspectives on loss: a sourcebook. UK: Psychology Press. pp.99-112.

Sprecher, S., Felmlee, D., Metts, S., Fehr, B. And Vanni, D (1998) Factors Associated with the Distress Following the Breakup of a Close Relationship. Journal of Social and Personal Relationships. 15(6) pp.791-809.

Stern, L. A., & Taylor, K. (2007) Social networking on Facebook. Journal of the Communication, Speech, & Theatre Association of North Dakota. 20, pp.9-20.

Thompson, E. R. (2007) Development And Validation Of An Internationally Reliable Short-Form Of The Positive And Negative Affect Schedule (PANAS). Journal Of Cross-Cultural Psychology. 38(2), pp.227-242.

Tokunaga, R. S. (2010) Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. Computers in Human Behavior. Available at: http://tinyurl.com/4v9ol8f (accessed on 15 January, 2011).

Walther, J. B. (1996) Computer-mediate communication: Impersonal, interpersonal, and hyperpersonal interaction. Communication Research. 23(1), pp.3-43.

Walther, J. B., Van Der Heide, B., Kim, S., Westerman, D., & Tong, S. (2008) The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep? Human Communication Research. 34, pp.28-49.

A Comparison of Operating Systems for use on a Self-Powered Server System

B.Bridgeman and D.Lancaster

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

Abstract

In an attempt to establish which operating system is the most suitable for use on a self-powered server system, five of the leading operating systems were analysed on efficiency when related to power dissipation and process creation and management. A set of tests were created and executed on a test system whilst the power consumption on various components of the system was measured. Contrary to the beliefs of many, the conclusions of the tests indicate that the best operating system for the server is Windows Server 2008.

Keywords

Efficient Server System, Computer Power Efficiency, Operating System Power Efficiency

1 Introduction

A project is currently being undertaken at the University of Plymouth investigating the possibility of a self-power server system, where 'self-powered' is referred to as a power source not connected to a mains power grid. As the server will be subject to a potentially limited power reserve, the efficiency of the system needs to be maximised. According to Srikanthan et al (2005) and Kuehlmann (2003), the best way to achieve this is to implement both power efficient hardware and software, which is known as partitioning. Along with a low power dissipation level, the operating system will also have to perform to a high standard and according to Yu (2006), process management is one of the most important and relevant tasks in an operating system. Good optimisation of process creation and management not only helps improve the efficiency of the system, but aids the operating system in running smoothly without lockups.

An operating system is the largest part of software that generally runs on a computer and as such, a suitable and power efficient operating system needs to be implemented on the server system. According to Wakabayashi (2008), the current most popular operating systems for servers are Linux and Windows based. From these two product groups, the most commonly used operating systems on home servers are Windows XP, Windows 7, Windows Server and Linux Ubuntu (Wikipedia, 2011). These operating systems include a range of power management features which can be changed to affect how much power the hardware is consuming. However, none of them were designed with power efficiency as the main focus point. There is

however, another Linux based operating system known as WattOS, which is specifically designed to increased battery life on laptops.

A article by Henderson (2008) reports of a range of operating systems that have been subjected to tests involving power efficiency. The results of these tests concluded than Linux is the most power efficient operating system. Henderson (2008) claims that Linux has a maximum margin of being 12% more efficient than Windows Server 2008.

The experiment will conform of a set of tests that will be completed to assess the power consumption and process management abilities of a computer running the five operating systems mentioned above. Based on the previous research compiled by Henderson (2008), it is expected that the best operating system of choice will be Linux based as opposed to Windows based.

2 Methods

2.1 Operating Systems & Hardware

The operating systems chosen to be submitted to the testing were Windows XP, Windows 7, Windows Server 2008 R2, Ubuntu Server 10 SE and WattOS R3. Each of the operating systems was installed on the same computer after the previous operating systems tests were completed and removed. This ensured the installation location of the operating system had a fair chance to be located in the same sectors of the hard drive, as installation in another sector may have caused different response times from the hard drive. The hardware used throughout the tests remained the same, a summary of which can be seen in Table 1.

Component	Make & Model
Central Processing Unit (CPU)	Intel Pentium P4 2533MHz, 533MHz bus
Motherboard	Asus P4S533-E
Random Access Memory (RAM)	PNY 512MB PC2700
Hard Disk Drive (HDD)	IBM Deskstar 120GB 7200RPM
Network Interface Controller (NIC)	D-Link DG
Power Supply Unit (PSU)	Magna ATX300W

Table 1: Test Computer Specifications

2.2 Benchmarks

As the outcome of these tests will help define which operating system will be used on a server system, the test benchmarks that were chosen were intended to imitate what a server would be expected to do on a day to day basis. Benchmarks were created that could be run across all the operating systems. A list of the benchmarks along with a brief explanation of the benchmark and why that benchmark was chosen can be seen in Table 2 below.

Benchmark	Description
System Idle	Measures the power consumption when the computer is left alone – this is the most common mode for a computer to be in, and as such was chosen to be measured. The power consumed in the idle state can be considered as a constant in the overall consumption of the server.
Constant Ping request from another PC	Measures the overheads of a simple ping request. This test was chosen to help highlight if simple network interactions influenced the power consumption of the computer in any way.
File transfer to server (800mb)	Measures the power consumption when an 800Mb file is being transferred to the server from another networked computer. This test uses the Samba file sharing protocol, allowing files to be easily transferred to the server from other computers within the local network. This test was chosen to see the effectiveness of a Samba file transfer based on overall power consumption.
File transfer to server x2 (2x800mb)	Measures the power consumption when two 800Mb files are being transferred to the server simultaneously from two different networked computers. This test was chosen to highlight the differences in power consumption between transferring a single file and multiple simultaneous files via Samba. As the file transfer is being sent simultaneously, hard disk operations are increased and may cause the process to take longer.
File transfer from server (800mb)	Measures the power consumption when an 800Mb file is being transferred from the server to another networked computer. This test was chosen to highlight the power efficiency differences between sending a file to the server and reading a file from the server. The test also used the Samba file transfer protocol.
File transfer from server x2 (2x800mb)	Measures the power consumption when two 800Mb files are being transferred from the server simultaneously to two different networked computers. This test was chosen to highlight the differences between retrieving a single file from the server and multiple files from the server, allowing comparison between the alternative directions of sending files to the server.
HD Video Streaming	Measures the power consumption when another computer on the network is watching a full HD video file saved on the server. This test was chosen to help indicate how much power it takes to stream a HD video to another computer.
ASP Webpage Request (10 loads per second)	Measures the power consumption when another computer on the network accesses the webpage. The webpage has been coded to return the date and time along with a computed

	value based on the current second and a jpeg image. It has also been coded to automatically refresh the client's browser every 100 milliseconds. This test was chosen to help identify if ASP web requests from other computers to the server caused any major overheads on power consumption.
ASP Webpage Request x2 (2x10 loads per second)	Measures the power consumption when two other computers on the network accessing the same webpage in the above benchmark. This test was chosen to increase the number of requests to the server, increasing the potential stress level of the server.
Maths Stress Test	Measures the power consumption of the component when computing a constant algorithm. The Maths Stress Test was originally written as a Windows Shell Script and as a Linux Bash script. However, due to this not being very fair between operating systems, it was re-written using C++ and compiled on all platforms using the GNU G++ compiler. When executed, the test loops in a mathematical equation of 'x=x*2/2+1' until x reaches a value of 2000, at which point the application is launched five more times simultaneously. The effect causes the computer to become gradually stressed until it is unable to continue due to lack of resources. This test was chosen to test multiple areas of the computer under load, along with the efficiency of the operating system when related to process creating and management. The test is likely to affect the CPU, RAM and HDD differently across all operating systems.

Table 2: Chosen Benchmarks

All the benchmarks were run on the 12v-CPU group. However, only selected benchmark tests were run on the other component groups as little or no change in power consumption between idle and peak load was detected. The benchmarks that were run on the individual component groups along with the duration of the test can be seen in Table 3. The durations shown in Table 3 are a set time calculated to cover completion of the test across the different operating systems. The actual completion of some of the tests (more precisely, the file transfer tests) may be shorter than the given duration. The actual duration of the file transfer tests were calculated after all the testing was completed to help indicate which operating system is the most efficient on that given benchmark.

12v Group (CPU) Completed Benchmarks	Duration of Test (Seconds)
System Idle	1130
Constant Ping request from another PC	200
File transfer to server (800mb)	40
File transfer to server x2 (2x800mb)	96
File transfer from server (800mb)	22
File transfer from server x2 (2x800mb)	92
HD Video Streaming	80
ASP Webpage Request (10 loads per second)	22
ASP Webpage Request x2 (2x10 loads per second)	22

Maths Stress Test	1366
5v Group (PCI + Motherboard) Completed Benchmarks	Duration of Test (Seconds)
File transfer from server (800mb)	23
Maths Stress Test	112
3.3v Group (RAM + Motherboard) Completed Benchmarks	Duration of Test (Seconds)
System Idle	170
File transfer from server (800mb)	30
File transfer from server x2 (2x800mb)	56
ASP Webpage Request (10 loads per second)	13
Maths Stress Test	504
5v HDD Tests	Duration of Test (Seconds)
Idle	380
File transfer from server (800mb)	28
ASP Webpage Request (10 loads per second)	20
Maths Stress Test	500

Table 3: Benchmark Test Groups

2.3 Performance vs. Power Saving

In order to show the full power efficiency spectrum of each operating system, the benchmarks were run twice; once with the operating system setup in its maximum performance mode and once with the operating system setup in its power saving mode. Within the Windows environments, this was achieved by adjusting the Advanced Configuration and Power Interface (ACPI) settings by use of the 'Power Options' utilities found in the 'Control Panel'. On the Linux operating systems, the basic power management controls did not allow for advanced power management. In order to enable access to these controls, a package called 'Granola' was installed. Once this package was installed, the advanced power option could be edited manually be modifying the values within the relevant configuration files. The maximum power mode was setup on all operating systems to make full use of the hardware. The CPU was set to use 100% all the time, the HDD was set to never go to sleep and the power saving modes on PCI devices was set to 'disabled'. For the power saving setting, the CPU was set to use a maximum of 20% of its power in all C-states, the HDD's were set to sleep after one minute of inactivity and the PCI devices were set to use all available power saving modes.

2.3.1 Test Equipment

In order to attain a realistic average result from the tests, measurements of amperage and voltage were taken over a period of time. This period of time was calculated to cover the completion time of the given benchmark in the slowest situation (minimum performance on the least efficient operating system), the times of which can be seen in Table 3. In order to capture these values, a custom volt and amp meter was designed and built; this device has been named 'USBVAM'. This device allows the measurement of volts and amperes to be simultaneously measured at a rate of one sample per second. The measurements can then be automatically stored in a database for a given period of time.

2.4 Component Groups & Connectivity

As it is impossible (without very specialist equipment) to fully isolate the power sources for each of the major components found in a computer, the component measurements were taken based on their supplying voltage rails; in modern computers allow the possibility to separate the core components solely based on the Power Supply Unit's (PSU) supply rails.

The motherboard used in the tests utilized a dedicated 12v supply rail to supply the CPU power via a 4 pin Molex connector, so this was used as the measuring point for the CPU (there was an additional 12v supply rail included in the 20pin Molex connector which was removed completely). The 5v supply rails from the PSU are mapped to the PCI cards and USB sockets. The 3.3v supply rails from the PSU are used to power the RAM along with the other chips on the motherboard that don't utilize the 5v rail. With this in mind, the components that can be measured from the motherboard PSU rails are grouped as the CPU, PCI + Motherboard, RAM + Motherboard. The hard drive was also tested on its 5v rail, as this is the power source used for the IO and head movement. The 12v rail appeared to show constant results regardless of which benchmark was being run, as this rail is used primarily to power the drives motors. As such, this rail was omitted from the tests.

In order to ascertain the measurements, the supply rails from the PSU were cut and the USBVAM ammeter was inserted (the volt meter was also connected to the load side of the ammeter to ground). This allowed the component groups power consumption to be measured in real-time over the given time-lapse for the benchmark. The procedure for running a test was to load the computer to the required state (i.e. booting into the operating system), starting the USBVAM and then performing the benchmark test. The USBVAM was then stopped after the set amount of time for that benchmark had elapsed.

3 Results

During the testing of the operating system, a large number for raw results were compiled (over 52000 logs). To help analyse and publish this data, the results have been summarised down into the form of a table. Table 4 summarises the results ascertained from the set of tests run with the operating system setup in the performance mode. Table 5 summarises the results ascertained from the set of tests run with the operating system in its power efficient mode. Due to the nature of the Math Stress Test and the varying effects it had across the different operating systems, the results have been excluded from the totals in Table 4 and Table 5.

Table 4 and Table 5 list two sets of results for each operating system; the 'A' result and the 'T' result. The 'A' result is the average wattage of the test and was calculated by adding together all samples within the test and then dividing the figure by the number of samples. The 'T' result is the total of all samples and is calculated by adding all the values from all samples together within the test. The reasoning for calculating both the 'A' and 'T' values was to highlight which operating system was more efficient in the file transfer tests, as the duration of these tests was dependant on how efficient the operating system was at transferring the file over a network.

12v Group (CPU) Completed Benchmarks	Windows XP Pro		Win Server 2008		Windows7 Pro		Ubuntu 10 SE		WattOS R3	
	A	T	A	T	A	T	A	T	A	T
System Idle	24.04	27218	23.93	27114	28.24	31911	21.90	24787	22.65	25594
Constant Ping request from another PC	23.70	4787	24.01	4874	23.85	4770	21.98	4439	23.16	4631
File transfer to server (800mb)	34.80	1148	41.84	878	34.31	926	49.82	1793	36.87	884
File transfer to server x2 (2x800mb)	33.95	2919	44.17	1590	35.35	1802	50.57	3539	38.03	1901
File transfer from server (800mb)	46.53	884	41.32	867	34.32	686	46.70	840	39.25	745
File transfer from server x2 (2x800mb)	34.17	2972	38.05	2093	27.33	3498	37.06	2557	28.94	3038
HD Video Streaming	24.37	1974	24.18	1982	23.90	1911	24.24	1963	23.98	1909
ASP Webpage Request (10 loads per second)	25.71	565	24.19	556	25.95	570	26.97	593	26.53	583
ASP Webpage Request x2 (2x10 loads per second)	25.53	587	24.02	576	24.15	531	25.23	603	26.45	581
Maths Stress Test (C++)*	66.21	90449	53.98	73741	38.22	52207	27.80	37976	24.09	32901
Section Average\Total	30.31	43054	31.74	40530	28.60	46605	33.83	41114	29.54	39866
5v Group (PCI + Motherboard) Completed Benchmarks										
File transfer from server (800mb)	6.77	155	6.68	153	6.79	142	6.73	154	6.80	156
Maths Stress Test (C++)*	6.74	755	6.71	751	6.74	754	6.75	823	6.74	754
Section Total	6.77	155	6.68	153	6.79	142	6.73	154	6.80	156
3.3v Group (RAM + Motherboard) Completed Benchmarks										
System Idle	8.66	1472	7.58	1289	7.79	1323	8.14	1383	8.35	1419
File transfer from server (800mb)	9.18	192	8.42	160	8.44	177	9.17	220	9.05	199
File transfer from server x2 (2x800mb)	9.16	198	8.26	404	8.24	1326	8.78	474	8.6	1134
ASP Webpage Request (10 loads per second)	9.13	118	7.93	103	7.97	103	8.21	106	8.65	112
Maths Stress Test (C++)*	9.75	4916	8.42	4245	8.69	4380	8.52	4295	8.51	4287
Section Average/Total	9.03	1980	8.04	1956	8.11	2929	8.57	2183	8.66	2864
5v HDD Tests										
System Idle	1.00	381	1.03	392	0.37	141	0.98	376	0.15	56
File transfer from server (800mb)	3.40	71	3.13	37	2.93	76	2.93	76	3.01	63
ASP Webpage Request (10 loads per second)	-	-	-	-	-	-	-	-	-	-
Maths Stress Test (C++)*	1.04	521	1.21	606	1.18	591	2.06	1030	1.98	989
Section Average/Total	2.20	452	2.08	429	1.65	217	1.95	452	1.58	119

Table 4: 'Performance' mode test results

12v Group (CPU) Completed Benchmarks	Windows XP Pro		Win Server 2008		Windows7 Pro		Ubuntu 10 SE		WattOS R3	
	A	T	A	T	A	T	A	T	A	T
System Idle	23.89	27045	23.93	27087	-	-	21.93	24781	21.88	24730
Constant Ping request from another PC	23.91	4782	23.81	4762	-	-	22.52	4504	22.24	4448
File transfer to server (800mb)	36.03	1369	29.45	1531	-	-	32.91	3719	31.75	1206
File transfer to server x2 (2x800mb)	34.72	2742	30.23	3234	-	-	32.38	7966	32.45	2434
File transfer from server (800mb)	44.76	850	32.05	1281	-	-	32.74	1800	32.20	1288
File transfer from server x2 (2x800mb)	33.58	3290	30.69	3037	-	-	32.71	3662	29.41	3293
HD Video Streaming	25.03	2002	24.33	1946	-	-	24.32	1945	22.67	1813
ASP Webpage Request (10 loads per second)	23.95	526	25.20	554	-	-	28.10	618	28.88	635
ASP Webpage Request x2 (2x10 loads per second)	23.91	526	23.50	516	-	-	26.97	593	27.67	608
Maths Stress Test (C++)*	29.14	39808	28.05	38320	-	-	25.92	35406	25.63	35013
Section Average\Total	29.97	43132	27.02	43948	-	-	28.28	49588	27.63	40455
5v Group (PCI + Motherboard) Completed Benchmarks										
File transfer from server (800mb)	6.74	364	6.76	365	-	-	6.70	362	6.82	369
Maths Stress Test (C++)*	6.78	826	6.71	818	-	-	6.66	746	6.68	748
Section Total	6.74	364	6.76	365	-	-	6.70	362	6.82	369
3.3v Group (RAM + Motherboard) Completed Benchmarks										
System Idle	8.81	1496	8.18	1391	-	-	8.18	1390	8.26	1403
File transfer from server (800mb)	8.95	537	8.38	502	-	-	8.79	527	8.75	472
File transfer from server x2 (2x800mb)	9.22	921	8.40	840	-	-	8.76	928	8.59	1031
ASP Webpage Request (10 loads per second)	8.82	114	8.37	108	-	-	8.82	114	8.46	109
Maths Stress Test (C++)*	9.41	4741	8.30	4182	-	-	8.33	4197	8.52	4258
Section Average/Total	8.95	3068	8.33	2841	-	-	8.63	2959	8.51	3015
5v HDD Tests					-	-				
System Idle	0.33	123	0.72	274	-	-	0.07	25	0.10	36
File transfer from server (800mb)	3.14	65	2.51	108	-	-	1.83	93	1.87	67
ASP Webpage Request (10 loads per second)	1.23	24	0.84	16	-	-	0.3	6	0.1	2
Maths Stress Test (C++)*	1.13	563	0.79	396	-	-	1.17	854	1.38	689
Section Average/Total	1.56	212	1.35	398	-	-	0.73	124	0.69	105

Table 5: 'Power Saving' mode test results

The results from the 'HD Video Streaming' and 'Constant Ping Request' tests appear to have no measurable effect on any of the operating systems (the results are similar to that of an idle system), so it has been concluded that the operations completed within these tests are small enough that the effect on the power consumption of the system is benign. However the results captured from the rest of the tests have shown significant differences between the different operating systems and between the two

different modes of operation for each of these operating systems (the performance mode and the power saving mode).

Although the actual CPU load level was not logged during the tests, it can be estimated by the amount of watts being consumed by the CPU; when the system is idle, the CPU's average power consumption was 24watts and at 100% load, the CPU's average power consumption of 74watts. By working out the range between these two values (which is 50watts), an estimation of the CPU load\activity can be calculated as a percentage. As an example, when the CPU was idle and thus at 0% load, the wattage recorded would be 24watts, at 50% load the wattage recorded would be 49watts and at 100% load would be 74watts or higher.

Performance vs. Power Saving Modes

It is sometimes perceived that because a system has a lower peak current consumption value, it is taking fewer watts to complete the task. However, this may not be true at all; just because the system is indicated to show lower peak wattage's does not mean conclusions can be drawn from it. The duration for which a system takes to complete a task at the lower wattage may exceed the duration seen to complete the same task in the performance mode by such a value, that the low power mode actually consumes more watts overall.

Throughout all the operating systems (minus Windows 7, which was not able to activate the power saving mode on the hardware and as such is removed from this discussion area), the results measured from the idle tests in both the performance and power saving modes remained relatively the same with a value close to 24 watts being consumed (the Linux kernels actually consumed slightly fewer watts with an average of around 21watts, but this value also remained relatively the same between the performance and power saving modes). All the other tests, showed a significant drop in power consumption when compared between the performance and low power modes. In all the operating systems apart from Windows XP, the maximum wattage seen to be consumed by the CPU was capped below 36watts when the power saving mode was activated, 40 watts less than the amount of current drawn when in the performance mode. Windows XP was the only operating system that operated differently by showing signs of selectiveness on when the CPU would be capped to 20%; during the Maths Stress Test, the CPU appeared to be showing similar results to the other operating systems with the power consumption not exceeding 30watts. However, during the file transfer tests, the CPU did not appear to adhere to the set limit and power consumptions almost identical to that seen in the performance mode was captured.

The entire set of tests, excluding the ones related to file transfer, are not measurable against a completion time as they are on-going tests and as such, an answer to whether or not power is actually being saved overall between the different modes is not decipherable from the results. The tests related to file transfer on the other hand do allow for a conclusion to be drawn. These tests include all the vital parts of an operating system including the CPU, RAM, HDD and NIC, which allows for a fully rounded answer covering the computer system as a whole to be established. In the performance mode, the operations involving the transfer of a file 'from the server'

gave a smooth and steady power consumption during the transfer process, which in the case of the CPU very rarely exceeded 50watts (which estimates to around 60% load) at any time during the transfer across all the operating systems. As expected when reading a file from the HDD, the power consumption measured on the HDD rose to its maximum state. However the duration for which the HDD remains in this state was unexpected; it was presumed that the data would be transferred from the HDD to the RAM in large data batches, allowing the data to be packaged up quickly and sent over the network. In reality, on all the operating systems besides Windows Server 2008, the duration the HDD appears to be in its maximum power consuming state is relatively equal to the duration of the file transfer test as a whole. Window Server 2008 is the only operating system that shows the HDD only being in this maximum state for considerably less time than the total duration of the file transfer (as shown in Fig 1). This indicates that all the operating systems bar Windows Server 2008 are reading the data directly from the HDD, creating the TCP/IP packets and then transferring the file.

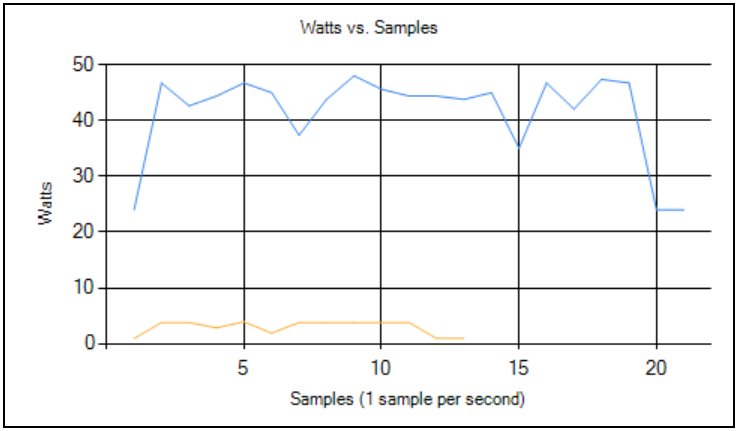


Figure 1: CPU (top line) vs HDD (bottom line) activity on Windows Server 2008 file transfer

Non-continual reads from the HDD can cause delays due to the seeking of the HDD read head. The results seen by Windows Server 2008 indicate the data to be transferred is first being placed from the HDD into the RAM, allowing the HDD to become idle a lot faster and thus reducing the transfer time and overall power consumption. However when compared with the same test run in the power saving mode, Windows Server 2008 showed different results; instead of the HDD activity being a lot shorter than the duration of the CPU activity, it was relatively the same length, indicating it started to work in the in-efficient manner like the other operating systems. This may be a result of a fluke, or there is a change in the file transfer algorithm that causes this to happen in the power saving mode. The other operating systems showed similar patterns to what was seen in their performance mode tests, but with a longer duration of completion and a lower CPU power consumption.

When two files were sent to the server, the CPU appeared to have a lower activity load than when setup in the performance mode. This is caused by the HDD, which when accessing two files, data transfer speed is greatly reduced. This is because the

read head is required to move between the locations of the two files constantly, creating a delay. When tested in the power saving mode, the CPU load is once again showing signs of being capped to 20% in all operating systems except Windows XP. As such, the duration to complete the test is lengthened in all operating systems expect Windows XP, which again showed almost identical results to the tests run in the performance mode. The duration of time that the test was extended by in the power saving mode compared to the performance mode was at a lower ratio than when transferring a single file.

Table 6 was compiled to help define which operating system consumed the least amount of power during the file transfer tests. This table also indicates which operating systems actually consumed more power when in the power saving mode compared to the performance mode. The values in the table are based on a calculation which removes the amount of power that would have been consumed if the computer was in an idle state. This was required to show a true representation of the amount of power the task consumed on its own. The idle power consumption was based on the average power consumption calculated for each operating system in Table 4.

12v Group (CPU) File Transfer Benchmarks	Windows XP Pro				Win Server 2008				Ubuntu 10 SE				WattOS R3			
(PM = Performance Mode, PSM = Power Saving Mode)	PM		PSM		PM		PSM		PM		PSM		PM		PSM	
System Idle Average	23.89				23.93				21.93				21.88			
(D = Duration in Seconds, T = Total Watts)	D	T	D	T	D	T	D	T	D	T	D	T	D	T	D	T
File transfer to server (800mb)	33	359	38	461	21	375	52	286	36	1003	133	802	24	358	38	374
File transfer to server x2 (2x800mb)	86	864	79	854	36	728	107	637	70	2003	246	2571	50	807	75	793
File transfer from server (800mb)	19	430	19	396	21	364	40	323	18	445	55	593	19	329	40	412
File transfer from server x2 (2x800mb)	87	893	98	948	55	776	99	667	69	1043	112	1205	105	740	112	842
Total	225	2546	234	2659	133	2243	298	1913	193	4494	526	5171	198	2234	265	2421

Table 6: Calculated total values for file transfer tests on the CPU group

It can be seen from table 6 that Windows Server 2008 is the only operating system that constantly consumed fewer watts when in the power saving mode compared to the performance mode. This operating system also consumed fewer watts for each test completed in the performance mode than any of the other operating systems. Unexpectedly, Ubuntu appears to give the worst performance of the lot, consuming almost double the amount of power that Windows Server 2008 consumed. Interestingly, WattOS performs much better than Ubuntu and even out-performs Windows Server 2008 in the performance mode tests.

Process Creation and Management

The effects of creating many processes using the Maths Stress Test were different between four of the five operating systems. Only the Linux operating systems (Ubuntu and WattOS) showed almost identical results, which is to be expected as they are both using the Debian kernel. Windows XP gave a poor result when subject to the Maths Stress Test. No longer than half way through the test, the operating system started to throw visual error messages stating that the process could not be created due to a memory exception. This form of behaviour shows that the operating

system is not swapping data to the HDD before starting a new process or as an alternative, waiting for resources to become available before creating the new process. The results from the HDD show that little or no activity took place on the drive, indicating that the operating system was not attempting to sway any data between the RAM and HDD. This indicates that the Windows XP kernel is limiting the reliable number of processes that can be run to the available RAM size.

The result seen in the Windows server2008 tests differ from the Windows XP tests only on the CPU. However the kernel appears to handle the creation of new processes differently as no errors or exceptions were observed during the tests. Instead, the rate at which new processes were created appeared to be related to the completion rate of running processes. This indicates that the kernel is waiting for resources to become available before creating the new process. Another observation was the speed at which the test was being executed; unlike Windows XP which appeared to try and run all open processes at the same time, Windows Server 2008 appeared to halt certain processes, allowing older processes to complete. However, the overall speed at which the processes were being completed did not appear to be as fast as Windows XP.

The Windows 7 operating system responded to process creation and management completely differently than the previous operating systems. Unlike the previous operating systems, Windows 7 was observed to almost ground to a halt during the test period. By comparing the raw data recorded during this test for the CPU and HDD, it is shown that the CPU activity rises, maintains a peak level for a short amount of time and then begins to fall gradually back down to a similar level as the idle test results. The HDD on the other hand appears to become a lot more active at the point where the CPU begins to fall. This suggests that the operating system is trying to swap data between the RAM and HDD to allow room for new processes to be loaded into memory without completing previous. This process of swapping data swamps all other activity on the computer and as such, the CPU cannot continue to process the data.

The next two operating systems to be tested were Ubuntu 10.10 Server Edition and WattOS R3. These operating systems gave very close results to the Windows 7 operating system. Both appeared to become over worked with memory swapping operations, causing the CPU to become almost idle.

The prior discussion about the effect of the CPU related to the Maths Stress Test is in reference to the operating system being setup in the performance mode. When the operating system was setup to use the power saving and the Maths Stress Test was run, the effects seen on all the operating systems (minus Windows 7 which encountered difficulties when entering the low power mode) showed the same patterns of operation. However the duration of time taken for the processor to reach is maximum activity state was a lot sooner than the uncapped performance mode, which in the case of Windows 7 and the Linux operating systems, meant the RAM took longer to become full and thus delayed the memory swapping operations.

4 Conclusions

Best operating system for use on a self-powered server?

All the operating systems tested would have been suitable as the host operating system on the server system. They have all shown similar results in performance, the differences of which probably would not be noticed by an end user. However, the operating systems did perform differently and as a result, the important factor of energy consumption has been affected. Out of the five operating systems tested, two show a clear lead in power efficiency, these being Windows Server 2008 and WattOS. The windows operating system excelled at process creation and management over the other operating systems, but the power dissipation was higher than that seen from WattOS during the file transfer tests in the performance mode. WattOS however, showed that certain tasks consumed more power in the power saving mode over the performance mode and despite consuming less power in the performance mode when compared to Windows Server 2008, consumes more power than its competitor when in the power saving mode. This means the WattOS operating system cannot switch between the performance and power saving modes reliably, which for a power source that may be limited on capacity during certain times is essential. Windows Server 2008 did allow for this and was in fact the only operating system to show a consistent drop in power consumption when in the power saving mode compared to the performance mode. This coupled with the operating showing it has the ability to consume less power than any of the other operating systems and also out-performs all the other operating systems in relation to process management, Windows Server 2008 looks like the best choice of operating system for a self-powered server system.

There might be an even more suitable operating system in existence that has the combined benefits of both WattOS and Windows Server 2008. As of yet, no Unix based operating systems have been tested, so future research can be resumed with the testing of this operating system, continued with the tested of other available operating systems.

5 References

Henderson, T (2008), “Linux captures the 'green' flag, beats Windows 2008 power-saving measures”, http://www.networkworld.com/research/2008/060908-green-windows-linux.html, (Accessed: 02-08-11)

Srikanthan, T., Xue, J., Chang, C.H. (2005), Advances in computer systems architecture: 10th Asia-Pacific conference, Springer, ISBN: 978-3-540-29643-0

Kuehlmann, A (2003), The Best of Iccad: 20 Years of Excellence in Computer-Aided Design, Springer, ISBN: 978-1402073915

Wakabayashi, D (2008), “Microsoft sees Windows gaining server market share”, http://www.reuters.com/article/2008/02/28/us-microsoft-servers-idUSN2748543820080228 (Accessed: 24-08-11)

Wikipedia (2011), “Home server”, http://en.wikipedia.org/wiki/Home_server (Accessed: 14-08-11)

Yu, L (2006), “Operating System Process Management and the Effect on Maintenance: A Comparison of Linux, FreeBSD, and Darwin”, http://www.dcc.ufla.br/infocomp/artigos/v5.2/art06.pdf, (Accessed: 14-08-11)

E –learning and Password Games

R.Gardner and S.Atkinson

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

Abstract

This research built a password game on a current smart phone that aimed to educate children within the topic of security awareness. The pedagogy used in the game is stated as having behaviourist tendencies. Children reported some informed opinions on passwords and used this knowledge to solve clues on appropriate use within a game of hangman. Early indications are that the game performed well and the novelty of the method used in an informal learning scenario is promising. Mobile learning and the topic of games and learning are both under presented in literature, despite the pedagogical benefits that could be brought to students by playing immersive activities that are able to motivate learners.

Keywords

E-learning, mobile learning, games, passwords, security awareness and children.

1 Introduction

This project considers the evaluation of an e-learning game that aimed to educate children in the area of passwords. The device chosen to implement the game was a current generation smart phone; such devices allow users to complete many different tasks and applications and can be considered relatively powerful. Objectives of research also included gauging the attitudes of children in the area of security awareness and measuring the effectiveness of e-learning games.

Passwords are still (despite their age) a very popular method for authenticating users as they engage with technology, in a variety of locations including the internet. Browne (1972) wrote about the commonality of passwords almost forty years ago. There have been different approaches to the means of controlling access such as by using smart cards, tokens or biometrics (Furnell, 2007). However, these options are expensive and not easily implemented for today's internet user. As we use the web we may have a number of usernames and passwords that apply to us and as such form part of our virtual identity. This may cause us some difficulty as we have to remember them, as we go about our tasks and it has not gone unnoticed within the human computer interaction community. Nielsen (2005) states the cognitive problems that result from having to handle this scenario. Password usage is something that may come up as an issue for adults in the work place as companies have an obligation to look after data responsibly under the laws of data protection. The Computer Misuse Act (1990) also reminds us that access to resources must be

"within rights". What though do home users and children in particular know about the importance of passwords?

Although children will be using computers from a very different perspective for example: enjoyment, social networking, games and personal use, passwords remain something that must be looked after. Within computer security the password can be considered the "only line of defence from system intruders" (Bunnell et al, 1997). Through a lack of security awareness and misuse of the password there may be some worrying issues for children, Mark and Ratliffe (2011) defined cyberbullying as:"name-calling, threats, spreading rumour, sharing another person's private information, social isolation and exclusion".

Learning games are a relatively small research area in comparison to the topic of games at large, and require input from several disciplines if they are to work well. For example computer programmers, graphical designers and educators are needed as a minimum. Rooney et. al (2009) used two full time student programmers in their learning game that was based on a 3D graphics model and had graphical input as well as the perspective of lecturers in the area of learning. Brown (2008) records some attributes of game playing that may be utilised in the ultimate learning game; the desire of students to out perform their peers, be immersed in activity for long periods of time, paying great attention and meeting learning objectives as well. Learning games may also be described as serious games and come under the umbrella of e-learning in general. E-learning is a growing industry that has been born out of the popularity of the internet and the changing needs of its users, there are many ways in which it can be implemented. Andrade (2008) defines e-learning as: "the application of information and communication technologies in a wide array of solutions that improve knowledge and performance". Computers have been used in education for much longer than the duration of the internet however, Twining et al (2005) remark that computers have been in the classroom since the 1960s in the United States and within UK schools since the 1970s. Chambers and Spreecher (1980) found using such technology to be of value to learners of all abilities, the student who could learn quickly and those in need of more time; the computer was capable of handling both. However, as with any other form of information technology intervention appropriate software design is important. The term pedagogy is found in literature to describe the theories of learning and teaching, good pedagogy achieves good results for recipients. The internet is a very powerful resource and one in which people have become used to using for information. One form of e-learning is described as "shovelware" and this term from Teo and Gay (2001) merely describes the posting of electronic documents onto the internet. It is not the most valid means of e-learning but is a start.

Educators may have a good understanding of the term pedagogy and so perhaps they should have a role in the process. There are quite grounded methods however across the whole spectrum. The format of the rest of this paper is as follows: firstly the methodology behind our work is presented, a description of the 'password hangman' game designed to meet the security awareness, pedagogical and technical needs of the project is discussed. A brief synopsis of learning theories that we feel have contributed are shown. An evaluation of our results is documented and we close with a short conclusion and statement of further work.

2 Methodology

There were three phases in the project. In the first phase a literature review was undertaken across areas that were considered to be relevant to the research, computer security, games and learning, e-learning, perspectives on learning from the fields of education and psychology. Suitable methods to implement a learning game were investigated, eventually the choice of a smart phone was chosen as these devices support the notion of "anywhere any time learning". Development of the software commenced and although the researcher had a computing background with some commercial experience this was the first time that a major application (or game) had been written on a smart phone. It was ensured however that the pedagogical features were justifiable from ideas that where found in literature. Gaming theories from authors such as Prensky (2001) were also reviewed to ensure that when testing occurred typical features of games such as rules, goals, outcomes and competition were present in the prototype. The learning curve was therefore quite steep. Phase one also sought to find a suitable group of children to test the game. Resources and time available within the scout group restricted testing to four scouts but fourteen members of the scout group were kind enough to complete a password usage questionnaire. These data together provided some interesting points for discussion and cited much of the documented evidence we where able to find across literature. It is not claimed these data are significant but to back our theories we have looked to other work whenever possible. It should be stated that mobile learning is itself a research area Blunt (2009) records the same conclusion for game based learning. Therefore evaluating work is not as straight forward as was hoped. Phase two of the project tied up ethical approval to work with the scouts and finally during phase three write up of work was completed.

3 Description of Password Hangman

To enable children to learn about security awareness some well known principles for good password use (clues) were found from open literature (Furnell, 2007; Cazier and Medlin, 2006) and from publications such as Action for Children (2011) and the UKCCIS (2009). Eleven clues were stored inside the game so that the hangman game had some questions for children to evaluate. When the child did not choose an appropriate letter the game constructed the "hanging post" and hangman character "limb by limb" until the child had either correctly guessed the word or lost their ninth life. The answer to the clue was drawn on the screen as a series of dashes with each letter (or hint) filled in appropriately. Each incorrect guess of letter or word resulted in the loss of a life. By the ninth life the drawing of the frame and hangman character was complete and the game was lost. Upon the placing of the final letter or by taking a straight guess correctly the game was won. An animated graphic showed the result and a more detailed explanation of the question and answer was then presented. In the case of a win this reinforced the answer and also showed some reasoning. The same notion was provided when the child lost.

1. Who can you tell your password? (NOBODY)
2. At all times your password must be what? (CONFIDENTIAL)
3. This kind of password is difficult to guess (STRONG)
4. Don't choose a word found in one of these (DICTIONARY)
5. This word describes password theft. (ILLEGAL)
6. These people may steal passwords (HACKER)
7. With someone else's password you can _ _ _ _ _ _ _ _ to be them. (PRETEND)
8. Change your passwords at least this often. (YEARLY)
9. Don't use this date as a passcode. (BIRTHDAY)
10. This kind of password is difficult to guess (RANDOM)
11. Don't _ _ _ _ _down a password (WRITE)

Figure 1: Questions and answers held within the game

At any time children were able to skip the current clue and move on to the next without penalty. The game did not show the answer that was being skipped (and associated reasoning) but on reflection should have done so as not all learning goals could be met if the children skipped questions.

4 Learning Theory

Behaviourist learning theory represents an established set of principles that can be traced back to the time of Pavlov a Russian psychologist and beyond. He was interested in the notion of stimulus and response, tested with a group of dogs that were trained to salivate upon the ringing of a bell when food was present. Pavlov (Wollard, 2008, p.14) discovered that for a time even when no food was present the dogs would still salivate. The dogs recognised the bells that resulted in the reward of food and were even able to recognise combinations of sound and the shining of light, such that when a light was shone without the bell they would still expect food. Crawford (1998) records also the benefits to human learning when we are rewarded, learning is reinforced. The other side of the theory states that rewards can be withdrawn when we do not meet the learning goal (or a child misbehaves for example). Thus the child in need of reward reverts to good behaviour again. Rooney et al. (2009) cites that games can be very rewarding for players, through scoring and competition. Most behaviourist theory is not concerned with how we may store knowledge the presence of a changed behaviour is sufficient. Constructivists however, consider the acquisition of knowledge to be relative to our existing ideas and experience. Angela (2011) feels that students build up their own knowledge and should be encouraged to solve problems using the theories they currently hold. Constructivism sees the role of educators as one of a tutor guiding students through the course of learning. This can occur through the discussion and modification of existing ideas.

A combination of ideas from these theories, present how learning could be achieved within password hangman. By evaluating the clue children were consistently reinforcing the question being presented and the answer that was being sought. Reward was presented by way of a good score in the game, the opportunity to reach the top of the leaderboard the chance to better a friend. Constructivist theory was also in part used as children were given very little by way of prior knowledge it tested where they were at.

Analysis of the password use questionnaire would later suggest that the children knew enough to play the game. Other theory regarding the use of our senses is also considered relevant to the playing of the hangman game. Visual Auditory Kinesthetic learning (Kátaia, Juhászb and Adorjánia, 2008) considers how we use our senses and any preferences we may have to help us learn. Some may learn best through sound, visual cues or by actually touching and doing the task (kinaesthetic learning). Work by (Fernandez, Simo and Sallan, 2009) found that by using a combination of VAK elements that students were able to enhance their own learning experience (). Password hangman was able to provide children with the opportunity to touch, through the tapping of keys on the screen, and watch the visual reaction within the game. There were limited system noises that also informed users of errors.

5 Results and discussion

A summary of questions and responses used to gauge children's awareness of password safety are shown in the figure below. The small number of respondents (questionnaire n=14, game evaluation n=4) in our sample means that a detailed quantitative analysis of data is not required. The figure below presents an overview of results from the questionnaire.

1) Do you think passwords are important?	Yes (13)	No (1)
2) Why?	Account access	(2)
	Security	(3)
	Protection ->people	(2)
	Information /identity	(2)
	Safety	(5)
3) Where do you use passwords	Laptop	(12)
	Computer	(3)
	School Computer	(7)
	Games website	(10)
	Facebook	(7)

	All above	(5)
4) Do you use a password in >1 place?	Yes (7)	No (7)
5) Do you find it hard to remember passwords?	Yes (3)	No (11)
6) How do you remember passwords?	Memory	(5)
	Kept simple	(3)
	Write down	(2)
	Pet's name	(2)
	Other	(2)

Figure 2: Summary of questionnaire data

When these results are combined with game evaluation data this work has more standing. The first question asked if passwords were felt to be of importance. Reference can be made to computer security literature such as Furnell (2007) who found that users sometimes traded their passwords for rewards such as pens, suggesting that passwords are not always felt to be of value by users. In this work all but one child at least on paper felt passwords were important.

Many of the children were able to refer to the various underpinnings of security that passwords represent. The idea of having an online existence by children was also recognised. Children were able to associate passwords with key terms such as account access, securing information, protecting themselves, and the general principle that passwords make things safe.

These findings have come out of a coding analysis of the response to question two: "please explain why you think passwords are important". From the perspective of the game evaluation it was reassuring that children in the sample agreed. If not, it would have rendered the game pointless.

A later question found that despite being important children did share passwords, with friends and family (going against the advice of Furnell, 2007; Action for Children, 2011). Children were then asked to record details of their use for passwords. A key theme in response from this was twofold firstly that many children used laptops and all children said they used passwords in more than one place. Some children (over a third) remarked that they used passwords in all of the locations that were suggested (laptop, school computer, games website and the social networking site facebook). There were ten additional areas found in the free text response for other password uses. Frequency of password use was noted in literature (Gibson, Renaud, Conrad and Maple, 2009). Using passwords in multiple locations is generally frowned upon, half of the children admitted to this but over three quarters also said that they did not find handling multiple access difficult as noted in literature (Renaud and De Angeli, 2009). Next an open question regarding how they achieved this was posed, with responses generally agreeing with the opinions of literature. Children relied on their memory, (Cazier and Medlin, 2006; Furnell, 2007) kept passwords simple (Bunnell et. al, 1997) and used familiar words such as the name of pets (Cazier and Medlin, 2006).

The second part of our work was able to evaluate the performance of the game itself. Tests were undertaken at the scout meeting an informal experience, with scouts who were not playing the game taking part in their regular activities. The group were used to having useful activities presented within their meeting, recent other activities had included map reading and camping advice. Four volunteers agreed to test the game and were handed a simple instruction sheet that explained their role and key functions that were available within the game. Testing was undertaken for a period of almost two hours although the game was only active for some twenty-five minutes of this period. As noted by Sharples (2009) a log file recorded system activity in black box style, every interaction and game state. The four testers were able to correctly guess the answers to security awareness questions thirteen times. This included the realisation that passwords were confidential (n=4), you should tell "Nobody" your passwords (n=3), hackers may attempt to get hold of your password (n=2) with a password you can pretend to be someone else (n=1), your password should be changed yearly (sic) (n=1), password theft could be illegal (n=1). A full list of clues are given in Figure 1.

Our analysis was able to show that some of the children were also quite persistent in their use of the game as demonstrated by their spelling out of the word "confidential" in answer to the question 'at all times your password must be what?' This was the longest word held within the game and may not have come to mind, however there is not a connection between the difficulty of the clue and length of word being guessed. A short word can be difficult to guess if only one or two letters have been confirmed. One child guessed the word 'hacker' in only 80 seconds, 'confidential' was guessed in 137 seconds. Conversely, another guessed 'confidential' in only 39 seconds with 'nobody' taking 170 seconds.

All of the four testers gave positive reactions as noted was often the case with this form of learning (Schwabe and Goth, 2009; Sharples, 2009). Interesting comments were received by email from one evaluator who provided a reflection about their experience. They wrote that they had learnt about passwords, stated that the game had a good layout, liked the element of competition (Prensky, 2001) liked the collaborative feature of scoring against friends but also asked for increased difficulty and variety in the task. Even though the game had not managed to ask each clue to evaluators during testing, when the clues were repeated over the telephone a month later scout GK was able to give accurate answers to eight of the eleven questions stored within password hangman, a month after the original activity. It is not claimed that this is statistically significant but it would be nice to think that mobile learning could be an immersive technology that is able to facilitate one to one communication and find ways of introducing topics that could be considered dry within the classroom, this hope is shared by Zyda (2007) who would like learning done this way and by Dalsgaard (2005) who hopes for better pedagogies to be forthcoming from e-learning.

6 Conclusion

A description of a relatively new method for education, password hangman has been described and although the use to date has been limited and tested on a small number of children we are encouraged by the results. Games and learning is a promising field for some students who perhaps do not do well using traditional pedagogical approaches. There is also the opportunity that the student who is doing well can do better, become more immersed in activities and see materials from a fresh perspective. Zyda (2007) shares this great optimism. Dalsgaard (2005) sees the chance to improve education through the adoption of e-learning. The resources in this work were by no means exhaustive and the programming skills of a computing masters student where able to build a smart phone game. This ran in an informal environment prompting a group of willing evaluators to consider some security awareness ‘clues’ as noted in publications and literature. Mobile learning and games are still under presented within literature, perhaps because learning and psychological theories and programming can be daunting to those outside of the relevant fields. To this end we strongly suggest a multidisciplinary approach. A brief description of the pedagogical features within the game has been stated. While not perfect, features have built on the notion of reward as suited to games (Prensky, 2001) and behaviourism (Crawford, 1998). Children were able to state their knowledge of passwords on a written questionnaire before trying the game. Not only were they able to play the game using their existing knowledge (known as constructivism) the questionnaire data from fourteen students stated some refined opinions about passwords. Children were (as was anticipated) leading lives requiring credentials in multiple places, much to the displeasure of their memory. For the moment at least the future for the password looks to be secure, no pun intended.

7 References

Andrade, J., (2008) 'Guidelines for the development of e-learning systems by means of proactive questions'. Comput. Educ., 51 (4). pp 1510-1522.

Angela, T. (2011) 'A constructivist approach to new media: An opportunity to improve social studies didactics'. Procedia - Social and Behavioral Sciences, 11 pp 185-189.

Brown, G. (2008) 'The serious side of games'. e.learning age, pp 22-22.

Browne, P. S. (1972) 'Computer security: a survey'. SIGMIS Database, 4 (3). pp 1-12.

Bunnell, J., Podd, J., Henderson, R., Napier, R. & Kennedy-Moffat, J. (1997) 'Cognitive, associative and conventional passwords: Recall and guessing rates'. Computers & Security, 16 (7). pp 629-641.

Cazier, J. A. & Medlin, B. D. (2006) 'Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times'. Information Systems Security, 15 (6). pp 45.

Chambers, J. A. & Sprecher, J. W. (1980) 'Computer assisted instruction: current trends and critical issues'. Commun. ACM, 23 (6). pp 332-342.

Crawford , R. (1999) Teaching and learning IT in English state secondary schools: towards anew pedagogy? Journal of Education and Information Technologies: Official journal of the IFIP technical committee, 4 (1). pp. 49-63. ISSN 1360-2357

Dalsgaard, C. (2005) 'eleed-Pedagogical quality in e-learning'. Eleed-e-Learning and education,(1).

Fernandez, V., Simo, P. & Sallan, J. M. (2009) 'Podcasting: A new technological tool to facilitate good practice in higher education'. Comput. Educ., 53 (2). pp 385-392.

Furnell, S. (2007) 'An assessment of website password practices'. Computers & Security, 26 (7-8). pp 445-451.

Gibson, M., Renaud, K., Conrad, M. & Maple, C. (2009) 'Musipass: authenticating me softly with "my" song'. Proceedings of the 2009 workshop on New security paradigms workshop. Oxford, United Kingdom: ACM, pp 85-100.

Gilbert, J., Morton, S. & Rowley, J. (2007) 'e-Learning: The student experience'. British Journal of Educational Technology, 38 (4). pp 560-573.

Kátaia, Z., Juhászb, K., and Adorjánia, A.K. (2008) 'On the role of senses in education'. Comput. Educ., 51 (4). pp 1707-1717.

Mark, L. & Ratliffe, K. T. (2011) 'Cyber Worlds: New Playgrounds for Bullying'. Computers in the Schools, 28 (2). pp 92-116.

Nielsen, J. (2005) 'Ten Usability Heuristics'. 2005. [Online]. Available at: http://www.useit.com/papers/heuristic/heuristic_list.html (Accessed: 26th January 2011).

Prensky M (2001) Digital Game-Based Learning New York: McGraw-Hill.

Rooney, P., O'Rourke, K. C., Burke, G., MacNamee, B. & Igbrude, C. (2009) 'Cross-Disciplinary Approaches for Developing Serious Games in Higher Education'. Proceedings of the 2009 Conference in Games and Virtual Worlds for Serious Applications. IEEE Computer Society, pp 161-165.

Renaud, K. & Angeli, A. D. (2009) 'Visual passwords: cure-all or snake-oil?'. Commun. ACM, 52 (12). pp 135-140.

Sharples, M. (2009) Methods for Evaluating Mobile Learning. In G.N. Vavoula, N.

Pachler, and A. Kukulska-Hulme (eds), Researching Mobile Learning: Frameworks, Tools and Research Designs. Oxford: Peter Lang Publishing Group, pp. 17-39

Schwabe, G. & Goth, C. (2005) 'Mobile learning with a mobile game: design and motivational effects'. Journal of Computer Assisted Learning, 21 (3). pp 204-216.

Teo, C. B. & Gay, R. K. L. (2005) 'Content authoring system to personalize e-learning'. Proceedings of the 5th WSEAS Int. Conference on Distance Learning and Web Engineering. Corfu Island, Greece: World Scientific and Engineering Academy and Society (WSEAS), pp 105-110.

Twining, P., Evans, D., Cook, D., Ralston, J., Selwood, I., Jones, A., Underwood, J., Scanlon, E., Kukulska-Hulme, A., Dillon, G., McAndrew, P. & Sheehy, K. (2005) 'Should there be a future for Tablet PCs in schools?'. Journal of Interactive Media in Education,

UKCCIS (2009) 'Click Clever Click Safe: The first UK Child Internet Safety Strategy'. [Online]. Available at: http://media.education.gov.uk/

Wollard, J. (2010) Psychology for the Classroom:Behaviourism. Routledge.

Zyda, M. (2007) 'Creating a Science Of Games'. Commun. ACM, 50 (7). pp 26-29.

Geolocation in Mobile Devices – Past, Present and Future

J.Godfrey and N.Barlow

School of Computing and Mathematics, Plymouth University, Plymouth, UK

Abstract

This research paper aims at providing an understanding about the structure, principle and positioning methods in geolocation using mobile devices. Basically, geolocation refers to the process of locating a geographical region using computers or mobile devices that are connected to the internet. With the advancing technology in the mobile phone industry and the internet, the use of paper maps to locate places while travelling is slowly being phased out. Smart phones and other GPRS supported mobile phones have software that enable travellers and other people to easily identify locations without have to use physical maps, which can be monotonous to use if the person does not have a certain level of knowledge of the geographical area to find out their current position. The use of mobile devices to locate different geographical features is increasingly being used because it is fast, effective and very accurate. This paper therefore highlights the basic features, principles, and the positioning methods that are used by the mobile phone's software to locate places. It also addresses some of the ethical and security issues that are associated with this technology, as well as its possible success or failure into the future.

Keywords

Geolocation, GPS, Positioning, Mobile, Cell Tower Triangulation

1 Geolocation Methods

Examples of geolocation methods include Global Positioning System (GPS), geolocation using Mobile Phone Information, and Google Map Mobile (GMM), which is a complete positioning package developed by Google (Dwivedi & Ed, 2011 p17). GPS stands for Global Positioning System, and is owned by the US Department of Defense (Griffin, D., 2008). The system is the only publically available satellite positioning system in operation at present - although there are other systems which have been used in the past, such as the GLONASS system which was launched by the Soviet Union, but is in a state of disrepair as of 2011. The European Union has a system called GALILEO which is not yet launched but hopes to achieve accuracy figures that of the GPS system. GPS was launched in the cold war period by the US, but was released for public use in 1983, but with an accuracy limit of 100m, but this was finally dropped in 2000.

The GPS system consists of a constellation or group of satellites which orbit the earth, and send out their current position to the earth, and measurements of their viewpoint of the earth. A receiver which is located on the ground then receives each of these satellites, or to be more precise, the satellites it can effectively see at that

time, and will be able to work out from the positioning information sent by each satellite the position of the receiver itself on the ground. The information used to calculate the position estimate is usually very precise, which can result in many cases in a very accurate position report on the ground, quite often down to 10 metres accuracy. This means it is the only positioning method which is ideally suited to turn-by-turn navigation, such as is used in satellite navigation systems. A typical GPS unit consists of radio receiver, antenna and CPU, and are often in a very small package. They require a clear view of the sky in order to receive the satellite signals.

With the advancements in technology and the invention of internet enabled devices, it is possible to locate the position of a place using information which is available on the phone, without having to rely on the satellite positioning method. Mobile phone tower signals and WiFi signals (if the smartphone has a WiFi unit built in,) can be used to triangulate the position of a given mobile phone device (Dwivedi & Ed, 2011 p17). It is however not all that accurate to specifically identify the exact region of interest, and for turn-by-turn navigation, satellite positioning is still the only method which is accurate enough for this purpose over a wide area.

GMM works closely like the Google maps website, but it is an application that is specifically designed for mobile devices. It uses built in methods for location finding, and presumably Google has a large database which allows them to use the mobile phone information to work out the location of the user, however this is speculation as Google do not release information on how their system actually works (Pilgrim, 2010 p117). All mobile devices using any geolocation application must always have data connections to the internet to work.

2 Structure and Principle Mechanism

Basically, geolocation applications perform two major functions - they link your current location to other real world locations such as events and restaurants, and report to other users your current position. The geolocation applications that are designed for mobile phones are more effective than those designed for PCs because the data that is received, changes as you change your position (Progri, 2011 p332). Most smartphones that are built by different mobile companies have an inbuilt GPS chip, which works out the current location from the data received from satellites. When you are inside a building and the sky is not clear, mobile geolocation applications will fall back to more inaccurate methods, and use the information obtained from cell towers or WiFi hotspots to approximate your exact position (Dwivedi & Ed, 2011 p17).

Other geological applications use cell site triangulation and local Wi-Fi networks. Using the data obtained from the satellites, positioning is more accurate when outdoors and when the view of the sky is clear. This can be said to be true about mobile devices when used in a car, which is where a lot of people will use geolocation applications (satellite navigation,) and the phone on the dashboard will have a clear view to the sky. However, it does not work well if there is no clear view of the sky, for example if indoors.

Several mobile phone manufacturing industries offer geolocation services. Some of the examples include Foursquare, Gowalla, Brightkite and Loopt. Foursquare Company serves a thousand of users globally (Firtman, 2010 p384). It works with BlackBerry, Palm, Android and iPhone phones. If there is no geolocation application installed in your phone, then it is possible to download them from the Foursquare mobile website. This service provider is able to locate your current position and communicate it back to your friends in other locations. It is also possible to locate restaurants, cyber cafes, bars, offices, parks and other places of interest (Neff & Moss, 2011 p164).

Gowalla works with the same mobile devices just like Foursquare. It has big database of different geographical positions and its users are capable of trading virtual products that they have collected. It also gives its users the opportunity to share real materials that they experience in their lives. Something interesting about its services is that the company is capable of identifying the region you frequently visit, and this gives the users a chance to identify twenty locations they are interested in under the sponsorship of the company. Google has never been inactive when it comes to the area of geolocation, and they working day and night to create more geological applications for most cell phone devices. Twitter and Facebook have also recently updated their sites to provide a means for its users to be able to locate their positions and identify other areas.

With cell towers, a single phone will only be connected to one tower at a given time. This is usually the cell tower with the strongest signal on the phone, which is (in an ideal situation,) the one that is closest to that tower. Every tower has its unique ID consisting of MCC, CID, LAC and MNC (Firtman, 2010 p384). Each country has its unique MNC and MCC while towers have specific CID and LAC. The towers however, are spread over many regions and they are usually instated to provide coverage with areas not covered by other towers. When you notice that you are frequently connecting to one specific tower, it is an indication that you are in the same general area. After identifying the location where that cell tower was received most strongly, it would be easier to identify it later while using the same tower. Google was the first company to launch a database of different geographical locations. Their application called Latitude is an application to share your location with friends, and see their location. It is very easy to use, by pressing "0" on your cell phone, the user's cell tower data is transmitted to Google and your exact location is relayed back. The user's cell tower information is sent to the Google by getting location data from a location API on the device, then LAC, MCC, GID and MNC details from the phone are sent using a HTTP POST request connection to the Google server (Pilgrim, 2010 p117). The latitudes and longitudes are determined at offset-bytes 7, 8, 9, and 10 and 11, 12, 13 and 14 respectively in the form of binary packets (Pilgrim, 2010 p117).

Geolocation in mobile devices is very effective when locating restaurants, city to city, friends and other countries, but can be ineffective for turn-by-turn navigation, unless the satellite positioning method is used – WiFi and Cell Tower Triangulation are very rarely enough for a navigation system as there are purely never enough towers or routers to reference current position against, even in big cities this would still rarely be accurate enough for navigation.

3 Geolocation and Privacy

Giving your location or address on any internet-based system exposes you to different risks, and thus it means that you will be sacrificing a certain amount your privacy, whether it be one user viewing your data, or the whole world. Sharing your current location with other people through social network could possibly increase the degree in which you are exposed to risks. Geolocation service providers have worked hard to protect their users from being exposed to risks and dangers by publicly identifying their locations, but their efforts have not been successful yet (Progri, 2011 p332). Most of the geolocation applications protect the safety of its users to some extent, but it is not all that effective to fully protect them from potential dangers. The users are thus advised not to post their personal details such as cell phone numbers, email addresses and home addresses on these sites.

Privacy advocates are currently creating general public awareness on the dangers of publicly sharing locations through the social sites. Contrary to this idea, discouraging people from identifying their exact locations at any given time is also a threat to the use of geolocation applications. So it is the responsibility of everyone to be sure of who they are relating to before identifying your location (Progri, 2011 p332).

4 The Future of Geolocation

To this date, geolocation applications are not taken seriously by most people, and it is being used by a small number of people overall globally. This is the reason as to why start-up companies such as Foursquare and Gowalla are incorporating features like games in their services to make it more popular among its users. With the advancing technology, it would be possible to develop and improve geolocation technology, and it will encompass other applications for news gathering and public safety. But when geolocation service providers begin creating applications that allow the users to include their physical locations in messages, privacy and safety issues should remain areas for concern for the foreseeable future unless it is successfully handled (Neff & Moss, 2011 p164).

5 Conclusion

In summary, geolocation applications designed for mobile devices have been established to be more effective than those intended for PCs. This is because they change location as the users move, and so can be used as an effective tracking device, and are portable compared to the average PC. With Smartphones and other internet enabled cell phones, it is possible to locate restaurants, parks, churches and events with ease, and without having to ask for directions from another person.

Mobile devices use the information obtained from cell towers, WiFi access points, or data obtained from satellites. Data received from satellites are effective and accurate outdoors when the sky is clear. However, information from the cell phone towers is effective and accurate in locating a position both indoor and outdoor, albeit much more inaccurate than that of GPS.

An ideal positioning method would be one which combines the three to minimize the serious disadvantages of all three methods, such as clear view of sky, inaccuracies etc. A positioning method which could overcome having a clear view of the sky, and was very accurate, would be a great asset to geolocation and is definitely something which should be researched in the future for great progression of geolocation.

A geolocation application was developed, during a University project by the author of this paper, which was a child/vulnerable person tracking system, which was successful in improving the understanding of geolocation for the author, but not just from a programming aspect – from an ethical and security point of view as well - the research helped to understand such issues which are present with geolocation applications.

Privacy relating to the identification of an individual's location is the biggest challenge that is being faced in geolocation technology. If these issues and concerns are overcome in the future, geolocation applications will become more popular, as people will not be as concerned about their privacy, and there will be less security risks, which will result in the technology being more widely used.

6 References

Dwivedi H, Clark C, Thiel D. *Mobile Application Security.* Chicago: McGraw Hill Professional, 2010.

Firtman M. *Programming the Mobile Web.* Chicago: O'Reilly Media, Inc., 2010.

Griffin, D., 2008. *How does the Global Positioning System Work?* Available at: http://www.pocketgpsworld.com/howgpsworks.php [Accessed 21 Jan 2011].

Neff D. J, Moss R. C. *The Future of Nonprofits: Innovate and Thrive in the Digital Age.* New York: John Wiley and Sons, 2011.

Pilgrim M. *HTML5: Up and Running.* New York: O'Reilly Media, Inc., 2010.

Progri I. *Geolocation of RF Signals: Principles and Simulations.* New York: Springer, 2011.

Privacy Dashboard

M.Tyler-Dimond and S.Atkinson

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

Abstract

Social Networking is taking the world by storm and with over 750 million users worldwide actively using *Facebook* alone, the growth of this phenomenon is staggering. Social networks allow users to interact with each other through posting messages on each other's walls and sharing personal information. In this paper, we observe the threats which are affluent in the social networking world and apply them to the perceived organisational values placed on using social networks. Through observing the threats we analyse the ways in which users attitudes and behaviours towards social networking impacts on the privacy of the organisation as well as the individual. We evaluate the usability of the social networking websites' privacy settings in order to establish how easy it is for users to maintain their desired level of privacy, and discuss the needs for a Privacy Dashboard in order to prompt users to manipulate their privacy settings in order to reduce the level of information they share.

Keywords

Social Networking, Privacy Controls, Privacy Settings, Awareness

1 Introduction

Social networks are now a common sight in the workplace, having been embraced by many companies in order to communicate and gain information on potential employees as well as market products and services to potential consumers. However, these social networks are also being used by employees for personal use in the workplace, and represent a distinct threat to sensitive information as well as acting as a gateway to malicious software. Therefore, this paper will look at the attitudes and behaviours of employees towards social networking websites in order to establish how much information they are sharing online.

2 Background

Although the concept of social networking dates back to the 1960s people were not interested until it was supported technically by the internet (Leonard 2004 cited in Gross and Acquisti 2005). These websites take many forms. It is popular for people who wish to share information through profiles (e.g. *Facebook* and *Linked In*), collaborate on playlists and musical tastes through *Last.fm*, share and comment on photographs using *Flickr* or the most recent trend; micro-blogging on *Twitter*.

Although the way in which people collaborate on these social networking sites differs greatly, they all provide users with the ability to share personal information:

For example, contact details, relationships and interests. Through the information provided on these social networking sites, the user is able to create an online profile or 'persona' which may mimic their offline persona or they could create themselves a whole new personality. However, although these social networks allow users to share their personal information, it is not compulsory to do so. Nevertheless, it has been found that the majority of users fill out these forms (Ofcom 2008). This is because people enjoy sharing their interests and daily occurrences with other users as it provides them with an outlet to share their news, ideas, feelings and interests. However, it is also used as a way to vent anger and can in some cases damage the reputation of the user, as well as other users and potentially organisations. Therefore, it is important to observe users' attitudes and behaviours towards social networking websites in order to ensure that threats to personal as well as corporate information is not revealed.

3 Social Networking Threats

Social networking websites, such as Facebook and Linked In, need to remain cautious over threats to users' data, as with over 750 million active users, *Facebook* needs to ensure that users' personal information is secure as more and more malicious operators target users of social networking sites (Facebook 2011).

3.1 Social Engineering Threats

Social engineering is a term used to describe the psychological tricks used to mislead people into undermining their own online security through social networking sites, and, consequently, into disclosing sensitive information (Sophos 2011).

Methods of deception can influence users to follow links, open an email attachment, click a button, or fill in forms with sensitive personal information. These psychological tricks capitalise on weaknesses in users' online behaviours and lack of awareness in order to spread malware, gain access to sensitive information, and target the users' desires, fears and curiosities exercised when online (Sophos 2011).

However, attacks often take place through phishing and click-jacking scams (Wisniewski, C. 2011; Cluley, G 2011).

Many users are unaware of the level of information they are sharing on social networking sites and with whom they are sharing the information. As can be seen in the Preece vs JD Wetherspoons plc case (Lawspeed.com 2011) many believe that any information they post can only be seen by a certain number of people, mainly close friends. However, this depends on the networks joined, as well as the number of people befriended on the social networking site. Therefore, it is easy to assume that although users claim to be aware of their actions, and the consequences of their actions on these social networking sites, their actions do not fit the 'Attitudes' or 'Behaviours' of someone who is aware of the threats some posts may cause. PR Newswire (2011) surveyed that at least 52% of all social networkers post risky

information on their social networking profile. However, this information is only relevant as far as those who are aware of the risky content they post online.

Realistically, of the other 48%, a proportion of them will not be aware that they have posted any risky content and, therefore, the statistic should be much higher.

4 IT Security and User Acceptance

IT Security for many organisations is an uphill struggle. Those employees which are seeking to comply with security policies implemented need to maintain an awareness of how to avoid causing vulnerabilities, whilst those who are working against security policies need to be made aware of the dangers.

Security Awareness is defined as "An initiative that sets the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of security failure. Furthermore, awareness reminds users of the importance of security and the procedures to be followed" (Primode 2011).

Furnell and Thompson (2009) theorize that employees' attitudes and awareness can prove to be an obstacle to effective maintenance of information security. They apply Schein's theory (1999) that there are three levels of corporate culture and apply it to IT Security policy compliance. It is Furnell and Thompson's belief that "corporate culture is a particularly intricate aspect of any organisation, and can exist whether the management and employees are aware of it or not" (Furnell and Thompson 2009:1).

Therefore, they conceive that culture can be likened to personality as it affects how employees behave in the workplace when unsupervised. It is these collective individuals and their behaviours (artefacts) within an organisation which make up the basis of how employees' values and beliefs impact upon the corporate, or in this case, security culture of the organisation.

The second tier of corporate culture relates to the 'espoused' values. For example, these values would be those which the organisation puts forth through its regulations and policies on security. However, it is important to note that should the regulations outlined in the company's IT policy and the behaviours of employees not run parallel, then the beliefs of the employees will succeed. Therefore, it is important to ensure that employees are made aware of their actions through the use of training and other awareness-raising practices. This will enable the organisation to develop a deeper level of corporate culture through "shared tacit assumptions" (Furnell and Thompson 2009:2). Therefore, the third tier of corporate culture implies that the regulations outlined in the organisation's IT policy and the subsequent behaviours of employees contribute to shared beliefs and work practices which provide unison in the achievement of a common goal.

Therefore, measuring the attitudes and behaviours of employees is crucial to the success of implementing any IT policy within an organisation, as without the compliance of the workforce, the necessary level of security will not be achievable.

5 Attitudes and Behaviours towards social networking sites

Ofcom's research suggests the importance of creating a 'well developed' profile in order to create a distinct and unique online presence. Furthermore, the more information shared within the profile, the more this attracts users to view a profile as it allows them to see a representation of who the user is 'offline', and whether or not they have common interests. Therefore, these profiles frequently contain highly detailed information about the user as although it is not compulsory to fill in this information, it is of benefit socially to the user who will enjoy sharing information about themselves and their interests, plus photographs, and playing online games (Ofcom 2008).

However, previously, social networking information such as religion, sexual orientation, and political views would not necessarily be disclosed to the general public, but instead only shared with close friends. Social networking has changed the modern perception of what is private and what is not. This has lead to 17% of adults communicating with people they do not know through these sites (Ofcom 2008).

Although all users engage with social networking websites in order to communicate, Ofcom have theorized that there are 5 different categories of user who use these websites with different motives, behaviours and attitudes.

Groups	People	Description
Alpha socialisers	a minority	People who used sites in intense short bursts to flirt, meet new people, and be entertained.
Attention seekers	some	People who craved attention and comments from others often by posting photos and customising their profiles.
Followers	many	People who joined sites to keep up with what their peers were doing.
Faithfuls	many	People who typically used social networking sites to rekindle old friendships, often from school or university.
Functional	a minority	People who tended to be single-minded in using sites for a particular purpose.

Table 1: Ofcom's 5 social networking site user categories

Categorising users into these 5 groups makes it easier to create an educated assumption of those who are at more risk to threats caused by social networking websites than others. For example, alpha socialisers and attention seekers especially, are more likely to be those who look to meet new people, and maintain a complete profile, sharing information with everyone instead of filtering their settings. In comparison, 'followers' and 'faithfuls' are more likely to lean on the side of caution, keeping abreast of any information they publically display and keeping their social networks for those with whom they have already communicated.

From the business perspective, an employer or manager of an organisation may wish to review the profiles of potential candidates when recruiting. For example, employers view social networking websites to determine if the applicant would be a suitable match to the company by looking at what information they share with others.

The Ofcom report suggested that privacy and safety issues were not of particular concern to the majority of users and that 44% of users left their privacy settings open by default, either through a lack of awareness, or through lack of manipulation of privacy controls. Ofcom also theorize that the need for 'attention seekers' to have attention is more important than protecting their information.

Giving out information, photographs and other content provides users categorized as 'attention seekers' with a high or confidence boost they need in order to feel popular or attractive. Unfortunately, people who come across as willing to give out sensitive or personal information may be seen as a liability to organisations looking to employ. It may be felt they would not maintain confidentiality of information within their company as such behaviours may be transferred from the personal lives of employees to their professional lives. In the current privacy climate new boundaries have been created by social networking websites, and the borders to these boundaries have not as yet been determined. Therefore, users need to maintain a degree of awareness when determining what information they wish to share openly, especially if it affects other people or organisations.

Consequently, because of the risks involved both to the individual, the organisation, and in some cases wider society, it is vital to establish why a large percentage of users display a lack of concern towards the visibility of their profiles.

Raising awareness of the issues is a fundamental area which needs to be addressed, particularly as users are also prone to assuming that the social networking websites themselves actually ensure that a level of privacy is maintained. However, the reality is that social networks, such as *Facebook*, leave users' privacy details 'open' by default. This not only takes advantage of the users' lack of awareness, it also benefits from users' lack of confidence in their ability to change their privacy settings.

6 Social Networking and Privacy

***Facebook* settings:** *Facebook's* privacy settings are the most complex of all the social networking websites compared. Their privacy settings allow you to customise all the fields which allow you to share information, providing 5 different settings. For example, for all fields including the address field, the user can choose to share information with 'Everyone', 'Friends of friends and networks', 'friends and networks', 'friends of friends', or just 'friends'. Furthermore, within the advanced settings, the user can choose not to share with anyone, or share only with specific people (Facebook 2011).

However, for the average user, who is non-technical, knowing which settings and how to implement them can be a struggle. Therefore, *Facebook* have also implemented an easier way of setting privacy settings, using preset options of 'Everyone', 'Friends of Friends', 'Friends' and 'Recommended' settings which will

automatically update all the field's privacy settings to that standard. *Facebook* also give a table highlighting settings, enabling the user to overview their privacy settings (Facebook 2011).

However, although these added settings have been implemented, *Facebook* is still criticized for its 'opt-in' to privacy culture. For example, when signing up to *Facebook* for the first time all settings are set to share with everyone. In addition, upon implementation of new features, *Facebook* automatically enrols users into the new service, one of which called 'instant personalization' gives access to users' publicly available profile information to selected websites the user has visited (Larkin, E 2010).

***Twitter* settings:** In comparison to *Facebook*'s settings, *Twitter*'s are considerably less sophisticated. However, their type of social networking is not based on sharing personal information in the same context. Twitter is based on micro-blogging: for example, posting comments and status on current events and topics which the user feels strongly about. This allows users to build an online persona through their posts.

In comparison, *Facebook* is based upon building a profile which allows the user to create an online persona by giving information and focusing more on interaction with 'friends' and 'friends of friends'. In contrast, *Twitter* encourages building a network with people of the same interests, and not having as much control on who follows the posts. However, there is a setting which allows the user to control who is able to view their 'tweets' by approving people they wish to share with. Although, this setting is nowhere near as sophisticated as *Facebook's* as it does not allow any distinction between friends and other people who follow you. Therefore, it is more difficult to determine the identity of the follower.

***Linked In* settings:** *Linked In* privacy settings are more sophisticated than *Twitter's,* as they conform to traditional use of social networking and allow the creation of a persona through the sharing of personal information. However, the social networking websites' settings are categorized into 4 sections: Profile, Email Preferences, Groups, Companies and Applications and Account. Within these 4 sections, settings relating to the category are laid out in order to allow the user to customise settings which incorporate privacy settings, as well as sharing of information with accounts on other Social Networking Websites such as *Twitter*.

The first distinction in *Facebook's* settings is that unlike *Linked In*, *Facebook* has a dashboard devoted to the protection of data. This means that users have to check through all 4 sections to ensure that their information is secure. This inevitably would frustrate users.

However, the *Linked In* privacy controls allow the user to choose whether they wish to share their 'Activity Broadcasts'. Sharing 'Activity Broadcasts' allows people to know when the user changes their profile, makes recommendations, or follows companies. As *Linked In* is based on professional contacts, it may be advisable when searching for a job not to share activity broadcasts, as an employer may notice the user is looking elsewhere for new employment. However, the user is also able to

customise their activity feed so that only certain people can see it: for example, 'only you', 'your connections', 'your network' or 'everyone'.

Linked In also provides users with the option to 'opt-out' of advertisements selected for users dependent on their interests or profession. This sort of advertising also takes place on *Facebook*. However, *Facebook* do not provide the option to opt out of tailored advertising, as it provides them with its main source of income. Unlike *Linked In*, *Facebook* also does not directly allow opting out of data sharing with third-party applications either. This is mainly because *Facebook* encourages openness, and wants to be able to provide users with as much functionality as possible. However, in order to deliver this functionality, users may have to share information with third parties so that they can use the service

Therefore, due to the complexity of the privacy settings and lack of awareness of the threats to privacy, it was considered that a prototype application based on raising awareness of the insecurity of settings was needed to allow employees within organisations to protect both their personal information, and that of the company.

7 Prototype: Privacy Dashboard

The prototype addresses the concerns which users commonly have when using websites: knowing what settings are relevant to them and protecting their privacy. The prototype will allow users to engage with the three most recognised and popular social networking sites' (*Facebook*, *Linked In* and *Twitter*) privacy settings, which will allow them to view what information they are sharing with everyone, and provide them with a privacy rating. Furthermore, it will offer them advice on where their privacy settings are at their weakest. The prototype will be designed as an educational tool instead of manipulating settings through the prototype. This allows the user greater flexibility, as changing the settings through the prototype may influence them to implement different settings than they desire. Therefore, the tool acts as an aid which empowers the user to make their own decisions, and provides them with a greater understanding of their settings, rather than the prototype doing all the work for them.

8 Conclusion

In Conclusion, although the vast majority of the public see the lack of privacy as a threat, it has not been deterred them from using *Facebook*, or other social networking websites. Through users' attitudes and behaviours observed by Ofcom (2008) it can be determined that observing which category users' attitudes and behaviours belong to, the organisation can judge the need for training users further in order to protect their own privacy and reputation. However, in order to do this, users need to comply with the policies set by the company. This can be a particular challenge to the organisation as without awareness users will not fully understand the necessity to comply to these policies and, therefore, cause threats to the organisation. Consequently, it is vital that the organisation provides users with the means to become aware of the social networking threats, through training and updates of the latest threats through internal email systems

9 References

Cluley, G. (2011). “Lady Gaga found dead in hotel room? Beware Facebook clickjacking scam”. [Online] Available at: http://nakedsecurity.sophos.com/2011/08/05/lady-gaga-found-dead-in-hotel-room-beware-facebook-clickjacking-scam/ [Accessed 23rd August, 2011]

Facebook. (2011). ‘Timeline’ [Online] Available at: http://www.facebook.com/press/info.php?timeline [Accessed 23rd August, 2011]

Furnell, S and Thomson,K. (2009). “From culture to disobedience: Recognising the varying user acceptance of IT security”, *Computer Fraud & Security*, February 2009, pp5-10.

Gross, R. and A. Acquisti (2005). Information revelation and privacy in online social networks. Proceedings of the 2005 ACM workshop on Privacy in the electronic society. Alexandria, VA, USA, ACM.

Larkin, E. (2010). ‘Can You Really Trust Facebook?’ [Online] Available at: http://www.pcworld.com/article/199162/can_you_really_trust_facebook.html [Accessed 24th August, 2011]

Lawspeed. (2011). “Employee posting offensive remarks on Facebook” [Online] Available at: http://www.lawspeed.com/news/Employee_posting_offensive_remarks_on_Facebook.aspx [Accessed 17th August, 2011]

Leonard, A (2004) ‘You are what you know[Online] Available at: http://dir.salon.com/tech/feature/2004/06/15/social_software_one/ [Accessed 31st August, 2011]

Ofcom. (2008). ‘Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use’ [Online] Available at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf [Accessed 30th August, 2011]

Primode. (2011). ‘Glossary’ [Online] Available at: http://www.primode.com/glossary.html [Accessed 26rd August, 2011]

PR Newswire. (2011). “Consumer Reports Survey: 52 Percent of Social Network Users Post Risky Information”. [Online] Available at: http://www.prnewswire.com/news-releases/consumer-reports-survey-52-percent-of-social-network-users-post-risky-information-92748344.html. [Accessed 23rd August, 2011]

Sophos. (2011). ‘Security threat report 2011’ [Online] Available at: http://www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreport2011wpna.pdf [Accessed 25th August, 2011]

Wisniewski, C. (2011). “Twitter is not charging in October, there is no petition, you're being phished”. [Online] Available at: http://nakedsecurity.sophos.com/2011/08/18/twitter-is-not-charging-in-october-there-is-no-petition-youre-being-phished/. [Accessed 23rd August, 2011]

Section 4

Network Systems Engineering

Evading IDS Detection

M.Batta and M.Papadaki

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

Abstract

Detecting intrusions is an arduous task, and although IDS technologies are getting better with time, it is still not possible to always detect intrusions accurately. IDS evasion techniques are becoming more complex and advanced, allowing them to operate under the radar of an IDS, and thereby bypass detection. The aim of this project is to investigate how easy it is to evade an IDS, and how different IDS configurations can influence its resilience to evasion techniques.

Keywords

Snort, Network Intrusion Detection System, preprocessors, datasets/pcap files, rulesets, fragmentation

1 Introduction

In an ever evolving world of computer systems and networks, complex security threats continue to surface rapidly. Latest firewalls and updated antivirus might be adequate solutions to the most common threats. But, the drawback of these protection mechanisms is that their main focus is on application behaviour and looks, not on examining the content. The attacker can bypass both the firewalls and antivirus simply by transferring data over firewall-accepted protocols or applications. This shows that both these mechanisms provide some level of security, but have their own limitations. Here arises the need for a security device which has the capability to perform all these functions plus to scan the contents of the traffic. Such a device is an Intrusion detection system (IDS) and it acts as a second line of defence (Anderson, 1980).

The purpose of this paper is to investigate how easy it is to evade an IDS, and how different IDS configurations can influence its resilience to evasion techniques. It performs an in-depth analytical study of the various tools and techniques employed to evade the IDS, intending to fortify the defence mechanism with a view to detecting of threats and attacks. It focuses on the pertinence and serviceability to ward-off untoward situations, and recommend pre-emptive measures to address the challenges posed by IDS. This research chooses to use Snort as a network intrusion detection system (NIDS) and enhance it with the latest rule set to detect any incoming attacks or threats.

2 Existing Research

In 2007, Jarle A. Ytreberg tested the resilience of Snort against certain IDS evasion tools such as Nikto. In his research, experiments were performed which tested Snort's alerting capabilities on sending mutated attack packets to a web server. Some weaknesses were discovered in Snort's capabilities to detect certain kinds of evasion attacks. But these could be dealt by creating customized rulesets. It was found that Snort was able to detect around 50% of the attacking packets sent from Nikto. All of the packets used a range of evasion techniques, which ideally should have been detected by Snort and alerted accordingly. When the computer was at its maximum processing speed, 50% of the packets were being dropped. The research also wrote five new rules, which on being implemented; Snort alerted about the dangerous evading packets and most evasion attacks. The research also proposes a new detection method for Snort which stated that the large request strings should be segmented into smaller strings, which would then be analysed individually against the rulesets (Ytreberg, 2007).

But, Snort has certainly improved with time and lived up to its reputation, which has led it to be one of the most popular and successful intrusion detection tools. This was evident by the research done by Ibrahim ALRobia, in 2010, who conducted research to test the durability of Snort against evasion attacks from Nikto. Unlike Ytreberg's research results in 2007, the results of this research revealed that Snort successfully detected all evasion techniques that were employed by Nikto and 104 alerts were flagged whether the test was conducted by single evasion technique or by combining multiple evasion techniques to strengthen the attack. Hence, the research concluded that Snort remained unaffected by the presence of any other application sharing the same processor. However, it also stated that such an improvement to Snort's detection ability was attributed to the preprocessors and Barnyard (ALRobia, 2010).

3 Test Setup and Configurations

In order to test Snort's efficiency, a number of tests, with different Snort configurations, would be performed. Results of these tests would be compared, deliberated upon and analysed; concluding with recommendations for achieving enhanced Snort's performance. In the course of detection process, the research will try and examine if Snort was successfully able to detect the evasion attempts for each dataset by looking into the results generated. Hence, the results of these experimental tests will enlighten users on how secure Snort really is, and what may or may not be its loopholes.

3.1 Download and relevance of pcap files

For a comprehensive investigation of Snort, there was a requirement for 'pcap' or packet capture files which could determine how reliable and efficient, in fact, the latest version of Snort IDS is, when exposed to attacks or threats. For this, it was essentially required that the pcap files consisted of built-in evasion techniques, especially devised to bypass the protection mechanisms of Snort. This would boost

the research to enlighten the users on how secure Snort really is, and what may or may not be its loopholes.

After immense research and many thanks to my supervisor Dr. Maria Papadaki, 23 pcap files were found with Advanced Evasion Techniques (AETs). With these pcap files, this 'Antievasion' website claims to have "discovered a new, dangerous set of evasion techniques that threaten to penetrate even the most sophisticated networks." All these packet capture files and their details are enlisted on the 'Antievasion' website, from where these can be downloaded and used (Antievasion, 2011).

3.2 Modifications made to Snort's default configuration

The modifications that are done to Snort's default configuration would be based on the configuration changes suggested in a blog entry of Joel Ester (Ester, 2011).

Modification 1: Enabling all rulesets

Following are the rulesets which were enabled in this research. In the default configuration of Snort, these rulesets were commented-out (#) or were not in use.

```
# Policy related rules:
 include $RULE_PATH/policy.rules
 include $RULE_PATH/community-policy.rules
 include $RULE_PATH/porn.rules
 include $RULE_PATH/community-inappropriate.rules
 include $RULE_PATH/chat.rules
 include $RULE_PATH/multimedia.rules
 include $RULE_PATH/p2p.rules
 include $RULE_PATH/community-game.rules
 include $RULE_PATH/community-misc.rules
# Extremely chatty rules:
 include $RULE_PATH/info.rules
 include $RULE_PATH/icmp-info.rules
 include $RULE_PATH/community-icmp.rules
```

Modification 2: DCE/RPC2 preprocessor

Following changes are made to the default DCE/RPC2 preprocessor configuration:

```
preprocessor dcerpc2: memcap 102400, events [co ]
preprocessor dcerpc2_server: default, policy WinXP, \
detect [smb [139,445], tcp 135, udp 135, rpc-over-http-server 593], \
autodetect [tcp 1025:, udp 1025:, rpc-over-http-server 1025:], \
smb_max_chain 3, smb_invalid_shares ["C$", "D$", "ADMIN$"]
```

Modification 3: RPC_DECODE preprocessor

Modifications made to default RPC_DECODE preprocessor configuration:

```
preprocessor rpc_decode: 111 32770 32771 32772 32773 32774 32775 32776 32777
32778 32779 no_alert_multiple_requests no_alert_large_fragments
no_alert_incomplete
```

Modification 4: SSL Preprocessor

Following are the modifications made to default configuration of SSL preprocessor:

```
preprocessor ssl: ports { 443 465 563 636 989 992 993 994 995 7801 7702 7900
7901 7902 7903 7904 7905 7906 6907 7908 7909 7910 7911 7912 7913 7914 7915
7916 7917 7918 7919 7920 }, trustservers, noinspect_encrypted
```

Modification 5: HTTP_PORTS

The updated configuration of HTTP_PORTS reads:

```
portvar HTTP_PORTS
80,311,591,593,901,1220,1414,1830,2301,2381,2809,3128,3702,5250,7001,7777,
7779,8000,8008,8028,8080,8088,8118,8123,8180,8181,8243,8280,8888,9090,
9091,9443,9999,11371]
```

Modification 6: ORACLE_PORTS

The modified and updated Oracle configuration line now reads like this:

```
portvar ORACLE_PORTS 1024:
```

Modification 7: stream5 preprocessor

Default configuration of stream5 preprocessor is modified to:

```
preprocessor stream5_global: max_tcp 8192, track_tcp yes, track_udp no
# preprocessor stream5_tcp: policy first
preprocessor stream5_tcp: policy first, use_static_footprint_sizes, detect_anomalies,
overlap_limit 1
# preprocessor stream5_udp: ignore_any_rules
```

This modifications done to the stream5 preprocessor's default configuration is based on the document written by Richard Bejtlich on "Snort's Stream5 and TCP overlapping fragments". These changes will cause Stream5 to alert when it sees at least one overlapping TCP segment (Bejtlich, 2007).

4 Results and analysis

Beyond doubt, the test results proved that modifications made to Snort's default configuration have indeed enhanced Snort's capability of detecting and alerting evasion attempts. The 22 datasets acted as a polestar to keep a vigilant eye on Snort's performance after each and every modification. The following graph 1 recapitulates the results obtained by performing the various modifications in Snort's default configuration:

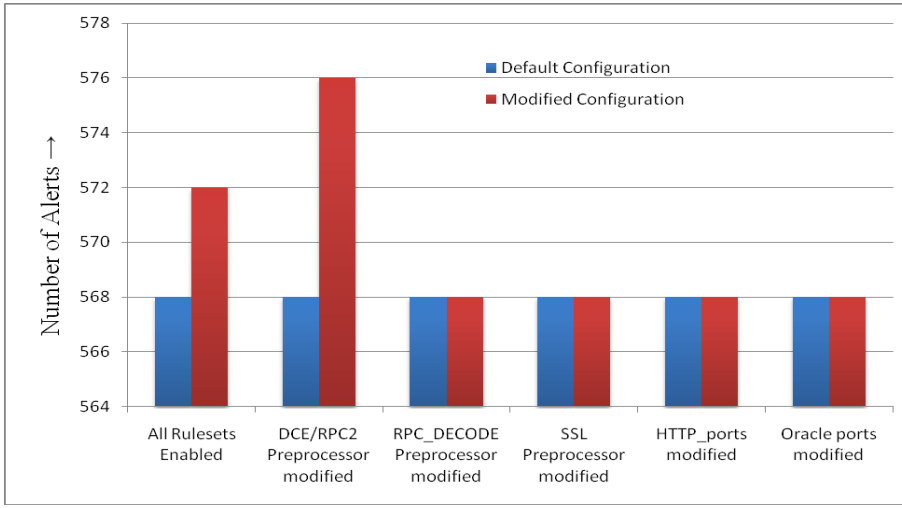


Figure 1: Comparison of alerts flagged with Snort's default configurations v/s all modifications done

As seen in the above figure, Snort's default configuration flagged only 568 alerts. However, when all the rulesets present in Snort's configuration were enabled (modification 1), it led Snort to flag 572 alerts; indicating an improvement in Snort's performance. Furthermore, modifications made to DCE/RPC2 preprocessor (modification 2) bettered Snort's performance all the more; total number of alerts triggered being 576. But, by far, outstanding and most encouraging results have been accrued by modifications done to stream5 preprocessor (modification 7); success of which can be accredited to Richard Bejtlich. Here, the total number of alerts showed a phenomenal increase to a staggering 2756, because of which results of stream5 preprocessor modification are not displayed in the above graph as it is beyond its scale. Therefore, the two most effective modifications established by means of this research are stream5 preprocessor (modification 7) and DCE/RPC2 preprocessor (modification 2).

Besides, the above graph also shows that there have been some modifications which have not affected Snort's performance at all; keeping the number of alerts same as in

Snort's default configuration. The modifications which have flagged 568 alerts, same as the default configuration are:

- RPC_decode preprocessor (modification 3)
- SSL preprocessor (modification 4)
- HTTP_ports (modification 5)
- Oracle_ports (modification 6)

Nonetheless, as also mentioned in the previous chapter, it should be carefully noted that in spite of the fact that these modifications have not enhanced Snort's capabilities of detecting evasion attacks specific to these datasets, they could prove to be of utmost significance in live commercial environments; especially due to ever evolving techniques of evading Intrusion Detection Systems.

The core reason behind the improved detection in Snort can be accredited to the highly significant modifications made to the default configuration of Snort. For instance, stream5 preprocessor modification flagged a total of 2756 alerts compared to 568 alerts in the default configuration. To be more precise, the dataset 'CVE-2003-0533-EvasionTCPSegment3-SMBDecoyWrites5 SMBResourceSegment33.pcap' flagged a mere 5 alerts in the default configuration whereas, after the modifications the same dataset flagged a staggering 1950 alerts. This is because, as a consequence of the modification, Snort was able to detect the most characteristic evasion technique 'Fragmentation Overlap'. Snort's default configuration was unable to detect this evasion technique because the default configuration uses the keyword 'policy_first' meaning that Snort will favour the first overlapped segment and the 'overlap_limit' is set to zero by default meaning that there is no limit to the number of overlapping packets per session. Hence, the default configuration does not inspect the contents of overlapping packets and simply considers the first of the overlapping packets. However, the modified configuration performs with flying colours and flags tremendous number of alerts because the keyword 'policy_first' is disabled (commented-out) plus the 'overlap_limit' is set to 1 which limits the number of overlapping packets per session to one. Therefore, nothing goes undetected and Snort scrutinises each and every packet overlap.

In spite of all the achievements of the experiments conducted, there were a few limitations of the research. Due to time constraints, the research was unable to deeply analyse the aspect of false positives. Also, an in-depth analysis of the contents and characteristics of the packets in the datasets could not be performed. Thus could have shed more light on the behaviour of Snort under different configurations and the legitimacy of the alerts generated.

5 Conclusion, Recommendations & Future

The aim of the research to improve detection capabilities and performance of Snort can said to be accomplished because the research has demonstrated awareness of intrusion detection technologies as well as IDS evasion techniques; designed and implemented tests that investigated the evasion resilience of Snort. Most importantly,

the research has meticulously tested and validated that the modifications made to Snort's default configuration file indeed proved to be beneficial by increasing the total number of alerts triggered.

According to the findings of this research, Snort would exhibit its maximum performance and would be most effective as well as effective in tackling evasion attempts provided all the rulesets are enabled along with all the preprocessors, suggested in the test results in previous chapter, are modified. The evidence of this is that Snort recorded the maximum number of alerts (2768) when it was run with this combined modification (Rulesets + Preprocessor).

Specific recommendations of this paper would be to preferably set 'Overlap_limit' to 1. This way it would become almost impossible to use 'fragmentation overlap' as an evasion technique to bypass Snort's detection, since Snort would monitor even a single overlapping TCP segment. Hence, nothing goes undetected. Moreover, all the mentioned changes in configuration should be adopted in order to stay at par with advancing evasion techniques; enable greater detection functionality and improve Snort's performance.

However, there are still a few stones left to be turned. One of the key areas for examination by the new researcher would be to delve into the phenomena of false positives. There could be an outside chance of the additional alerts triggered due to changes in Snort's default configuration, being false positives. Harmless enough, false positives could be a real nuisance as they bring down Snort's performance considerably.

6 References

ALRobia, I. (2010). "Evading IDS Detection: An extensive research about Snort IDS ability to detect Nikto evasion techniques", Masters Dissertation, University of Plymouth, UK.

Anderson, J.P. (1980), "Computer Threat Monitoring and Surveillance", http://seclab.cs.ucdavis.edu/projects/history/CD/ande80.pdf, (Accessed on 30 January 2011)

Antievasion Web Site (2010), "Technical details of the first 23 AETs and pcap files", http://www.antievasion.com/principles/principles/part-3, (Accessed 01 April 2011)

Bejtlich, R. (2007), "Snort's Stream5 and TCP overlapping fragments", http://searchsecuritychannel.techtarget.com/tip/Snorts-Stream5-and-TCP-overlapping-fragments?ShortReg=1&mboxConv=searchSecurityChannel_RegActivate_Submit&, (Accessed 16 July 2011)

Ester, J. (2011), "New Rule Pack and check your Snort.conf", http://blog.snort.org/2011/01/new-rule-pack-and-check-your-snortconf_04.html, (Accessed 22 July 2011)

Holland, T. (2004), "Understanding IPS and IDS", http://www.sans.org/reading_room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth_1381, (Accessed 23 November 2010)

Kelley, B. (2006), “Databases, Infrastructure and Security”, http://www.sqlservercentral.com/blogs/brian_kelley/archive/2006/05.aspx, (Accessed 25 November 2010)

Magalhaes, R. (2006), “Host-Based IDS vs Network-Based IDS (Part 1)”, http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html, (Accessed 25 November 2010)

Roesch, M. (1999), “Snort – Lightweight Intrusion Detection for Networks”, http://www.usenix.org/event/lisa99/full_papers/roesch/roesch.pdf, (Accessed 29 January 2011)

Rowland, C. “Intrusion Detection System”. United States Patent (Patent No. US 6,405,318 B1, 11 Jun 2002), http://www.google.com/patents?hl=en&lr=&vid=USPAT6405318&id=9-sLAAAAEBAJ&oi=fnd&dq=18.%09Rowland,+C.+%E2%80%9CIntrusion+Detection+System%E2%80%9D&printsec=abstract#v=onepage&q&f=false, (Accessed 24 November 2010)

Sourcefire Web Site (2009), “Snort® Threat Prevention Components”, http://www.imerja.com/files/file/White_Papers/Sourcefire/Snort%20Threat%20Prevention.pdf, (Accessed 19 July 2011)

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

Wireless VoIP Performance Analysis

A.Karawita and L.Sun

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

Abstract

During the past few years we have been seeing an increasing popularity of Wireless VoIP (Voice over IP) services, mostly due to the increasing availability of the software driven smartphones running Google Android and Apple iOS, where VoIP applications can be downloaded and installed on to the mobile device and then simply start using it similar to how you would have done in front of a computer. However there are still many major challenges with regard to quality that need to be overcome in order to offer customer an excellent service. In this paper we provide a detailed analysis on the performance of Skype's SILK speech codec. We setup a wireless VoIP test bed on an Android driven mobile platform and investigate the impact of packet-loss and background traffic, on the performance of SILK. We used recommended speech samples from the ITU-T database, and three different experiments were conducted. We used data extraction and reporting tools, to measure and evaluate the network performance parameters such as jitter, inter-arrival time, packet loss, and variation of bit rate on all these experiments. A relationship between packet loss vs. jitter and inter arrival time were seen. With increasing levels of packet loss jitter and inter-arrival time were affected badly. It was seen for 5% and 10% packet loss jitter can be tolerated as shown by the MOS score of 4.44 and 3.88 respectively. Informal subjective quality measurements showed SILK was able to tolerate packet loss of up to 10% before it showed signs of degradation. We believe that this study can be helpful for the research community who are currently doing performance analysis on SILK.

Keywords

Wireless VoIP, Android, SILK speech codec, Jitter, Inter- arrival, Bit rate, User perceived quality, MOS, PESQ.

1 Introduction

Traditionally Voice over Internet Protocol (VoIP) were transmitted via wired networks, but gaining rapid success to the telecommunication industry are Wireless LAN based VoIP technologies, popularly known as VoWLAN, that are emerging and at its early infancy, are expected to be the future of wireless communications. The popularity is due to the low deployment costs, ability of being more scalable and easy access to wireless hot-spots. In VoIP the quality of speech are notably the most important Quality of Service (QoS) requirements that govern end to end communication of this technology (Yamamoto and Beerends, 1997). VoIP transmits voice traffic via packet switched networks and packets get routed through the best and most efficient paths, virtual connections are setup for the duration of the call, between the caller and receiver, which gets terminated when one party hangs up.

Since SILK is a relatively new open source voice codec, there has not been much talk about it in the research community, however many publications consider the user perceived quality of Skype. Hence in the following we give an overview of some of the interesting work that has been done with regards to Skype and SILK. In Schlosser et al (2010), they provided a detail analysis on SILK speech codec and compare it to its predecessor iLBC and GSM, using objective quality measurements based on PESQ. They conducted experiments with bulk and random packet loss, applying error patters directly to the encoded VoIP frames. Their results show SILK performs well in all of these conditions. Other results showed if loss is applied to shorter speech samples the degradation is more. In Ramo and Toukomaa (2010), their research they consider three relatively new open source speech codecs, SILK, CELT and Broad Voice and compare with G.718 and some of the other ITU-T standardized speech codecs. Their results indicate SILK codec was the best performing codec compared to the rest, which received high MOS scores. Also how SILK was able to achieve different bit rates and change bit rate on frame by frame basics was look at. Other publications tried to compare Skype and MSN, and experiment were done with regard to packet loss, NAT scenarios; cross traffic and available bandwidth to come to a conclusion which VoIP application performs better (Chiang et al, 2006). According to Chen et al (2009), on their experiment on jitter buffer behaviour on Skype they mention that Skype's playout buffer remains within the range of 250 and 350ms, and does not adjust the buffer size according to the magnitude of the jitter.

The main objectives of this research paper are to (1) investigate the impact of packet loss and background traffic on the performance of SILK codec, and analyse key network performance parameters such as jitter, inter-arrival time, bit rate and packet loss. (2) To evaluate the performance of the recently published open source Skype SILK codec on two Android driven Smart Phones, and measuring the user perceived quality between the SILK sender and the receiver using informal subjective tests and objective measurements using PESQ.
The paper is structured as follows. In section 2, the testbed architecture and experimental setup is described. The results and discussion of the experiments would be presented in section 3. Finally we draw conclusions and future work in section 4.

2 Testbed Architecture and Experimental Setup

The figure 1 below illustrates a schematic diagram of the wireless testbed which would be setup to conduct all of the scheduled experiments that include measurement based experiments and subjective, objective based tests.

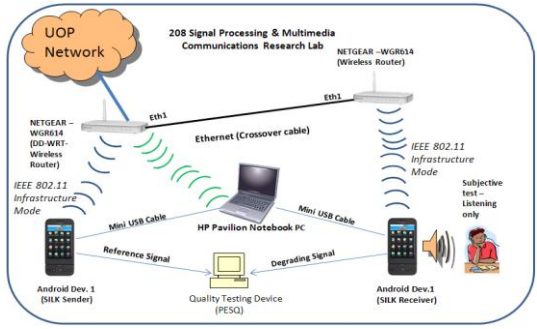


Figure 1: Testbed Architecture

2.1 Speech samples

As a clear guidance ITU-T P.862 should be referred when considering the selection of a reference speech signal. The recommended length of the reference signal for PESQ tests should be between 8 and 30 seconds, this includes any silence before after and between utterances (ITU-T, P.862). The ITU-T recommended reference speech samples can be obtained from the (ITU-T P.50).The converted .wav speech samples need to be sampled at 8000Hz and copied to the SD card of the SILK sender. A section of code was modified in the original SILK sender which will now read the wav files directly from the SD card of the phone (sender side).The degrading signal was captured to conduct objective quality measurements using PESQ, and the packets transmitted over the network were captured for network performance analysis. There were certain limitations that came up when capturing the degraded signal; eventually a voice recorder was used to capture the degrading signal from the speaker of the receiver. This may have some impact on recorded speech signal quality.

2.2 Measurement based experiments

TCPDUMP was used to collect voice packets under different packet loss rates at SILK sender and SILK receiver; these captured data would then be analysed using AWK scripts to calculate the performance parameters, which include, inter-arrival time of packets, jitter, packet loss and variation of bit rates. Three experiments were carried out. In the first experiment we would be introducing packet loss of 0%, 5%, 10%, 20%30% and 40% at a time for the duration of the call. In the second experiment, Gilbert model was used to simulate unconditional loss probability of 0%, 40%, 5%, 25%, 10% 0%, 30% interchanging every 10 seconds. In the third experiment, two streaming applications on both SILK sender and receiver would be played in the background along with SILK call simultaneously. NetEm was used to simulate packet-loss for these experiments except the third.

2.3 Objective and Subjective Testing Method

Objective measurements were conducted to measure end-to-end speech quality using PESQ. Packet loss would be simulated similar to the way subjective tests were carried out. Due to the limitations in the recording mechanism, it was expected that

the MOS scores given by PESQ should be far less compared to the subjective scores. Hence, in this case it wouldn't be practical to benchmark PESQ against the subjective score, as mapping would be accurately distributed. The listening-only tests were carried out as an informal subjective test that is the experiments were conducted on a non-sound proof research lab and following the guidelines that was recommended by the ITU-T P.800 – Methods for Subjective Determination of Transmission Quality (ITU-T P.800, 1996).

3 Experimental results and Discussion

In this section we present and discuss the results from measurement based experiments and the overall subjective and objective assessments. The results would be discussed experiment wise.

In experiment 1 we used different packet loss levels of 0%, 5%, 10%, 20%, 30% and 40%. Under 0% packet loss conditions, the average inter arrival time was 20.63ms and during periods of silence we observed the inter arrival times was reduced to 9.999ms as the DTX feature was enabled, that reacts by sending equal size bytes in quick succession until the speech parts are encoded (Rao and Toukomaa, 2010). When packet loss is increased for 0% to 5%, SILK was able to maintain the average inter arrival time, to about 20 to 21ms. But as the packet loss rate increased to 10%, it was clear that the inter arrival time was increasing steadily and when the packet loss rates reached 40%, the average inter arrival time was well above 40ms, which was quite high. This too meant the jitter was getting added up and speech frames that arrive later than the length of the jitter buffer can be discarded, which meant further packet loss. We examined the relationship of inter arrival time and packet loss illustrated in the figure 2. It shows the inter-arrival time from 40% packet loss, and the points plotted reflect the times the packet loss has occurred. As seen most of packet loss can be seen when Inter arrival time is more than 30ms. Most of the spikes that have inter arrival time of more than 100ms, was due to packet loss which can be clearly seen. Also looking closely we are able to observe packet loss occurring during periods of silence, below 10ms; this certainly would not have a significant effect on the quality of speech. The location of loss within the speech was looked at (Sun et al, 2001) and it highlighted unvoiced signals have no impact on overall quality. We can also assume when packet arrive having a high inter-arrival time, and it is more than the time of the jitter buffer, there is a high chance that these packets can also be discarded, shown by almost every tall spike.

When packloss starts to increase, the levels of jitter values starts to increase significantly as seen in the figure 3, which shows jitter for packetloss of 0% (bottom line), 20% (middle line) and 40% (above line) . Looking at 0% packet loss the line is fairly flat, apart from two few spikes due to the delay in loading and playing the speech from the phone memory, comparatively the lines for 20% and 40% bounces all over the place, and spikes fluctuates rapidly,which indicates there is high jitter on the call and as a result a lower MOS is expected. The average jitter levels for 40% packet loss was close to 35ms which is quite high, compared to the 25ms Jitter for 20% packet loss. We also saw the jitter level for 5% and 10% packet loss can be can be tolerated upto some extent as user perceived quality was not effected significantly shown by the higher MOS scores.

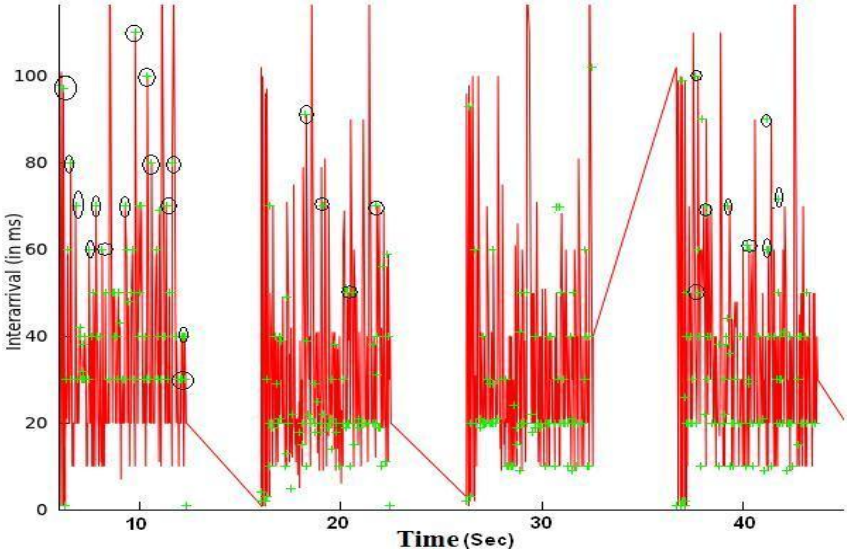


Figure 2: Inter-arrival vs Packet loss

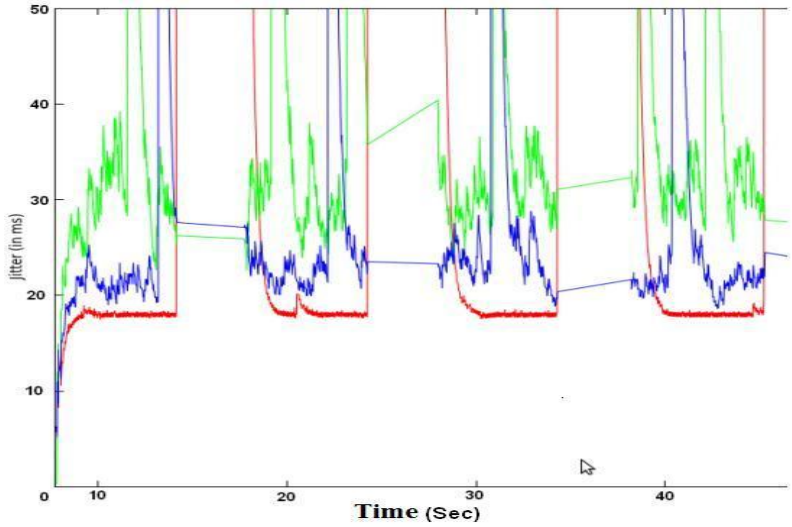


Figure 3: Jitter vs Packet loss

In experiment 2 we hope to understand the effects of random packet loss happening during different time intervals of the call , rather than a constant rate in experiement 1. One of the important result from this experiment was to understand the relationship between packet loss and jitter. Figure 4 illustrates the jitter line after 110 sec on to the call, as seen the line is really messy, with scattered spikes bounching throughout the graph, this leads to loosing the smoothness in a call, with annoying distortions at the receiver. The points marked in the jitter line indicates the time packet loss has occurred. With increasing levels of packet loss, we are able to see

jitter is starting to increase and all the packets that were loss were being scattered across the areas of high jitter. Also it can be seen when jitter is very high, it can contribute to a higher loss as shown above. As the packets are randomly dropped by the router, the packets that arrive later than playback can also be dropped (Yamamoto and Beerends, 1997).

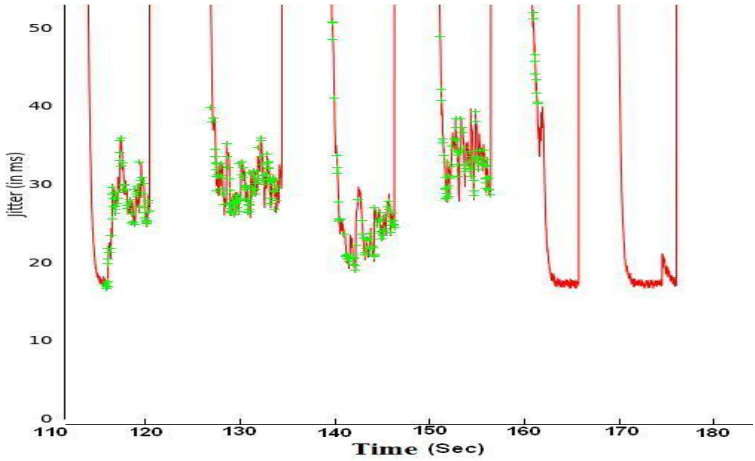


Figure 4: Jitter Vs. Packet loss (40%)

In experiment 3, the SILK encoder and decoder was experimented by introducting background traffic while the call was on progress. No packet loss was simulated for this experiment. Once the call is placed between the sender and receiver, a random video form youtube was being streamed and played at both sender and receiver. It was seen that that jitter was affected by background traffic.The impact of background traffic on voice quality was seen when Jitter was severely affected by background traffic and the bit rate drop below average when background traffic was been played and returned to the average bit rate once the video was finished playing, this is illustrated in figure 5. It was observed that http packets were overwhelming the UDP packets. And the SILK packets sent were severely interrupted and for short durations it was observed no SILK packets were sent at all, as a result the bit rate falls to as low as 9000 bits per second.

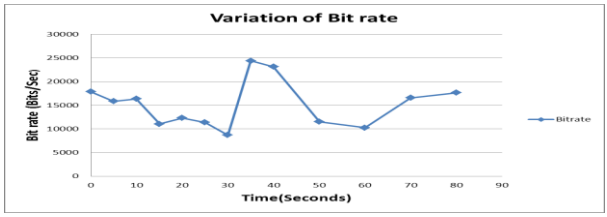


Figure 5: Variation of bit rate for background traffic

3.1 Subjective vs. Objective Quality Measurements

We assessed the user perceived speech quality for SILK codec using objecive and subjective measurements and tryed to understand if packet loss had an impact on the user perceived quality. Table 1 shows the summarized average MOS and PESQ scores for different levels of packet-loss.

Packet-Loss (%)	MOS	PESQ
0%	4.55	3.15
5%	4.44	3.08
10%	3.88	2.91
20%	2.87	2.56
30%	1.88	0.90
40%	1.12	-1.00 (Invalid Result)

Table 1: MOS vs. PESQ score

MOS scores gathered for different packet loss scenarios were recorded according to intelligibility and clarity of the user's audio quality perception. The MOS scores are very satisfying for 0% 5% and 10% packet-loss with 4.55, 4.44 and 3.88 respectively which is a very respectable score known as *communication quality*. But after the packet-loss levels are gradually increased to 20% and above the overall speech quality starts to gradually degrade. For 40% packet-loss 88% of the subjects rated as "Bad" as it was impossible to distinguish as to what sample was being played at the receiver.

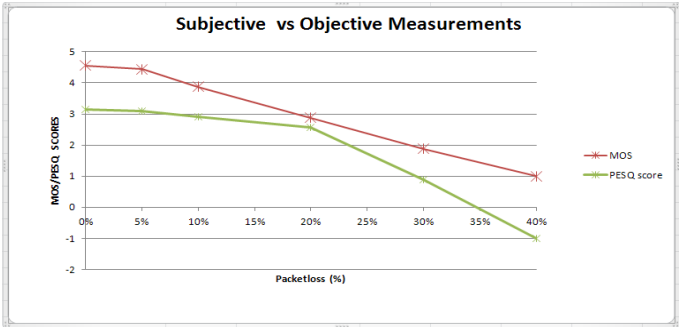


Figure 6: Subjective vs. Objective Measurements

The PESQ score of 3.15 can be viewed as a reference point for no-loss and with increasing levels of packet loss the PESQ scores start to fall gradually, and for 40% packet loss, the degraded signal could not be processed by PESQ. According to Schlosser (2010), SILK is able to achieve PESQ scores of 4.5 for 0% packet loss. Figure 6, illustrates the variation of both subjective and objective scores. The MOS (top) is linearly decreasing after 5% packet loss. At 5% packet-loss the overall speech quality, was hardly affected, but at 10% the MOS was still 3.88 which is still a good communication quality. In the case of PESQ (bottom) a linearly decrease is seen after 20% packet loss. From 0% to 20% packet-loss the difference in PESQ scores was only 0.59, which indicated the quality was quite well preserved compared to 0.67 in subjective tests. Therefore it was a clear indication that subjective results vary depending on

user expectations and personal opinions, but in objective measurements these are not part of the algorithm.

4 Conclusion and Future Work

In this research paper we studied the impact of packet loss on user perceived quality of Skype SILK codec. From the results obtained we found out SILK codec does extremely well in packet loss conditions of 5% to 10%, where a high MOS was seen. But after 10%, we observed the speech degraded very rapidly and when it came to 30%, the speech was almost impossible to understand. We studied the relationship between packet loss vs. inter arrival time and packet loss vs. jitter. In both cases we found, packet loss can be a major factor that can influence the values of Jitter and inter arrival time. When it came to jitter, we observed that with increasing levels of packet loss that was being simulated, it caused the jitter line to fluctuate very rapidly and all the packets that were loss were being scattered across the areas of high Jitter. For the case of inter-arrival time, it was observed when packet loss is increased from 0% to 10%. The inter arrival time for 20% packet loss was well above 20ms and at 40% packet loss the inter arrival time was close to 40ms at the receiving end. We also notice SILK initial started with a high bit rate, and after 15-20 seconds the average rate is achieved. The impact of background traffic on voice quality was seen when Jitter was severely affected by background traffic and the bit rate drop below average when background traffic was been played and returned to the average bit rate once the video was finished playing. In our future work, we will pursue measuring user perceived quality on different sampling rates, as SILK supports super wideband up to a sampling rate of 24Hz.

5 References

Chen, K.-T., Huang, C.-Y., Huang, P. & LEI, C.-L.(2009). Quantifying Skype user satisfaction. *In:* SIGCOMM '06 Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications 2006.

Chiang, W.-H., Xiao, W.-C. & Chou, C.-F. (2006). Performance Study of VoIP Applications:MSN vs. Skype.publication. *In:* MULTICOMM 2006 proceedings., 2006. MULTICOMM.

ITU-T (2001). Perceptual evaluation of speech quality (PESQ), an objective method for end-to-end speech quality assessment of narrowband telephone networks and speech codecs. *T Recommendation P.862, February 2001*

ITU-T (1996). Methods for objective and subjective assessment of quality. ITU-T Recommendation P.800,August 1996.

Raake, A. (2006). *Speech quality of VoIP: assessment and prediction*, John Wiley and Sons.

Ramo, A. & Toukomaa, H. (2010). Voice Quality Evaluation of Recent Open Source Codecs. *INTERSPEECH 2010.* Nokia Research Center, Tampere, Finland: INTERSPEECH 2010.

Schlosser, D., Jarschel, M., Burger, V. & Pries, R.(2010). Monitoring the User Perceived Quality of SILK-Based Voice Calls. *In:* Australasian Telecommunication Networks and Applications Conference 2010 Auckland, New Zealand. ATNAC.

Sun, L., Wade, G., Lines, B. M. & Ifeachor, E. C (2001) Impact of packet loss location on perceived speech quality. In: Proc. Internet Telephony Workshop (IPtel 2001), USA – New York.

Yamamoto, L. A. R. & Beerends, J. G. Y. 1997. Impact of network performanceparameters on the end-to-end perceived speech quality. *ExpertATM Traffic Symp., Mykonos, 1997* . Greece, Sep. 1997.

Performance Analysis of Video Call using Skype

K.K.Mathew and L.Sun

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

Abstract

Skype is one of the most popular VoIP applications nowadays. Skype's benefits, beyond its free and low costs, are said to include quality assurance (both audio and video) even in adverse network conditions, reliability and its easy set-up. This paper mainly concentrates on the video quality of the most popular VoIP application, Skype. The main aim of the research is to find out how Skype adapts to its video send bit rate in extreme network congestions and also to analyse its video performance in various network conditions. This involves in conducting a user behaviour analysis for Skype, which examines how users respond to the degradation of the video call quality, i.e. with regard to packet loss, to which extend users continue to disregard to the call quality before dropping the call. This paper also aims at rating what Skype's performance are in terms of Quality of Experience and Mean Opinion Score under various network conditions.

Keywords

Skype, video call, video quality, QoE, throughput, interarrival time, average payload size, PSNR, MOS

1 Introduction

With the advancements in the internet technology, both in the case of speed and efficiency lead to the introduction of many VoIP applications. Quality of the video becomes one of the main issues during sending the video over the network or the internet. With the increased popularity of the Skype there were many researches done on the quality of service provided by the Skype and all states that Skype has superior quality than all the other VoIP providers.

Skype is one of the most popular multi-network voice-over-IP (VoIP) telephony which uses the P2P technology (Hoßfeld and Binzenhöfer, 2007). User friendliness and high quality of services in which almost all the services are free of cost increases the popularity of Skype rapidly. Skype is a part of the famous file sharing system KaZaA which uses the concept of nodes, super nodes and servers. The Skype arranges the participants into super nodes and ordinary nodes. Super node is nothing but a node with some additional processing capabilities. The super nodes create an overlay network and the ordinary node select one super node from the network. The ordinary node then passes the queries through the super node on which they are associated (Zhang et al., 2010). Recent studies(De Cicco et al., 2011)on Skype video congestion experiment shows that Skype adapts in a good manner to the suddenly changing bandwidth and it tries to maintains the quality of the video in low

bandwidth conditions. Recent studies conducted by (Boyaci et al., 2009)on Skype congestion control mechanism states that Skype has the capacity to distinguish between the loss due to congestion and random loss of packets by analysing the packet delay. Skype come up with high quality audio and video communication even in adverse network conditions increase the interest of the researchers to study more about the Skype and its usage. Especially the researches become more curious about the studies that are related to the video call rather than the audio ones because of the Skype's amazing video quality in different network situations. There were relatively less studies conducted in the field of video quality of Skype.

The increased popularity and the use of proprietary protocols increased the interest of the researchers in the field of the Skype's communication. Many researches have been conducting on the quality of the Skype's communication and the behaviour of Skype on different network conditions. Apart from the others this research paper mainly aims in studying the effect of other applications (e.g. Torrent) on the performance of Skype. It mainly concentrates on the Quality of Experience (QoE) to the end user and how the Skype adapts its send bit rate in the case of network congestions were also discussed in this paper.

2 Testbed setup

The experimental setup consists of two PCs in which one act as the transmitter and the other act as the receiver. Both the PCs have Skype installed in it. Apart from the two PCs with the configurations mentioned above the experimental testbed consists two Linux based routers. PC1 act as the sender and PC2 acts as the receiver and both the routers are connected to the internet. The following figure 1 shows the experimental testbed.

Figure 1: Testbed setup for the experiment.

3 Experiments and Results

The video traffic was generated with the help of Splitcam which injects video file to the transmitter and send to the receiver. This technique helps to inject the standard video file to the Skype interface. All the experiments were performed with standard CIF video sequences with a resolution of 352X288 and a frame rate of 25 fps. All the experiments done using the testbed specified in the figure 1 are used to measure the

metrics like throughput, interarrival time, average payload size, PSNR and the subjective quality metric MOS based on the data captured in Wireshark. Apart from that this section also deals with how Skype distributes the individual payload size in the case of network congestion occurs.

3.1 Experiment 1

In this experiment packetloss was introduced at the router interface starting from 0 percentage i.e. no packet loss and moving up to 20 percentage. The values obtained for the throughput, inter arrival time, data rate send, PSNR and MOS are represented in the following figure 2.

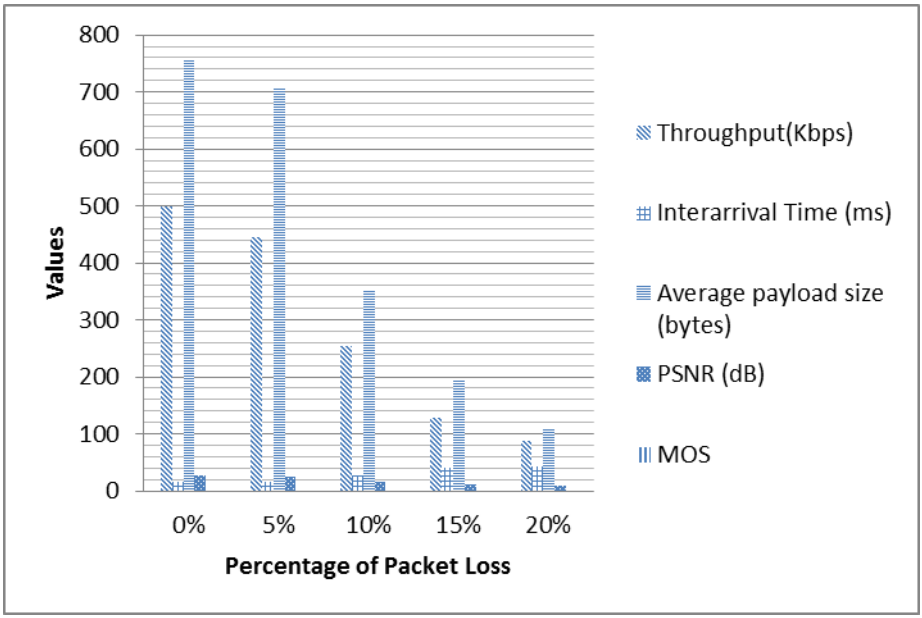


Figure 2: Interarrival, throughput values obtained in packet loss

From the figure 2, it is noticed that when there is an increase rate of packet loss Skype decreases the throughput since throughput is the average rate of the data send from the transmitter to the receiver in the communication path. It is also observed that the throughput reaches a minimum level at high percentage of packet loss (e.g. at 20%) and at this level Skype can't able to make the video communication but still it maintains the call due to its adaptation mechanism. It is also observed that there is a gradual increase in the value of the interarrival time with the rise in the packet loss rate. Since interarrival time is the amount of time between two successive packets delivered from the sender to the receiver. With the increased level of packet loss the Skype increases the interarrival time of the packet sending and this resulted in the degradation in the quality of the call. The next observation is on the payload size and how it varies with the increasing packet loss rate. It seems that with the increasing packet loss rate the average payload size decreases. It is also observed that the value of the MOS score goes down with the values of the PSNR. When the rate of packet

loss is lesser the values of the PSNR and the MOS are higher but with the increase in the packet loss causes both the values to fall down.

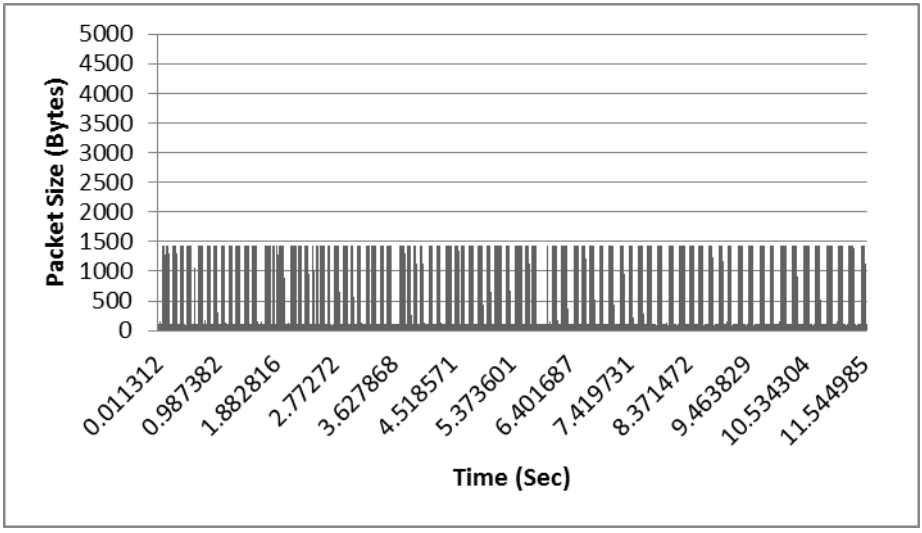


Figure 3: Packet distribution in the case of no packet loss

From the figures 3 is the packet distribution in the case where there is no packet loss. It clearly shows uniformity in the packet size distribution which means that almost an equal size is maintained in the distribution of the packet size and it doesn't maintain this uniformity in distribution in the case of higher packet losses. From figure 2 we can also observe that the average payload size decreases with increase in the packet loss rate. This makes the conclusion that when the packet loss become higher the distribution of the packet size decrease in a non- uniform manner.

3.2 Experiment 2

Switching the packet loss at constant intervals will become one of the suitable ways to understand the behaviour of the Skype in the fluctuating network environment. Because in the real world the network environment is always deals with changes.

In this experiment certain amount of packet loss is introduced in the router interface for a constant interval of time and checks how it affects the quality of the video. From the figure 4 it is observed that when the throughput is high in the case of low ranges (during the beginning stages for e.g. 0-5%) of packet loss switching and after every switching the consecutive rise and fall in the values of the throughput. But the case of interarrival time and average payload size are different there is a gradual and continuously increasing rate of the Interarrival time with the high rate of the packetloss changes. Apart from that the value of the average payload size fluctuates when then rate of the packet loss increases at constant interval of time. It seems that the value of the PSNR decreases with the increase in the packetloss and reaches the minimum at high level of packet loss similarly it is also observed that MOS values are going down with the increase in the packet loss.

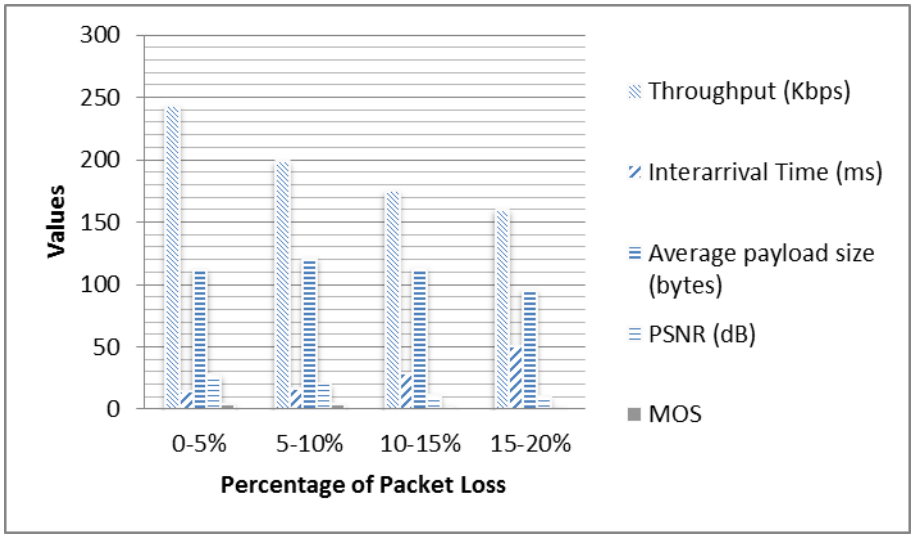


Figure 4: Behaviour of the Skype traffic in changing network conditions

In the case of individual packet size distribution it seems that the packet size is almost similar and it size of the packet is less. But when the packet loss range increases it is observed that the size of the packet increases and decreases drastically at regular time intervals. The figure 4 given above shows the general behaviour of the packet distribution when there is a packet switching occurs. When the packet loss switching range is very less the size of the individual packets distributed are small in size and when the packet loss range increases the size of the individual packets increases drastically at regular interval of time.

3.3 Experiment 3

The experiment also aims at finding out the behaviour of the Skype when two peer to peer applications work at the same time. Since torrents are the most popular applications which uses high amount of bandwidth and use the peer-to-peer technology for communication. The experiment also focuses in finding out the effect of other application (e.g. normal direct download) in the video quality of Skype.

In the case of the effect of the peer-to-peer download application in the quality of Skype is discussed in this section. In this experiment, the allocation of bandwidth in torrent was set to high, medium, low and tests the behaviour of the Skype. In this experiment it is observed that the Skype cannot load the video many times but it still maintains the call without the video. The values obtained for the throughput, interarrival time, data rate send, PSNR and MOS are represented in the following figure 5.

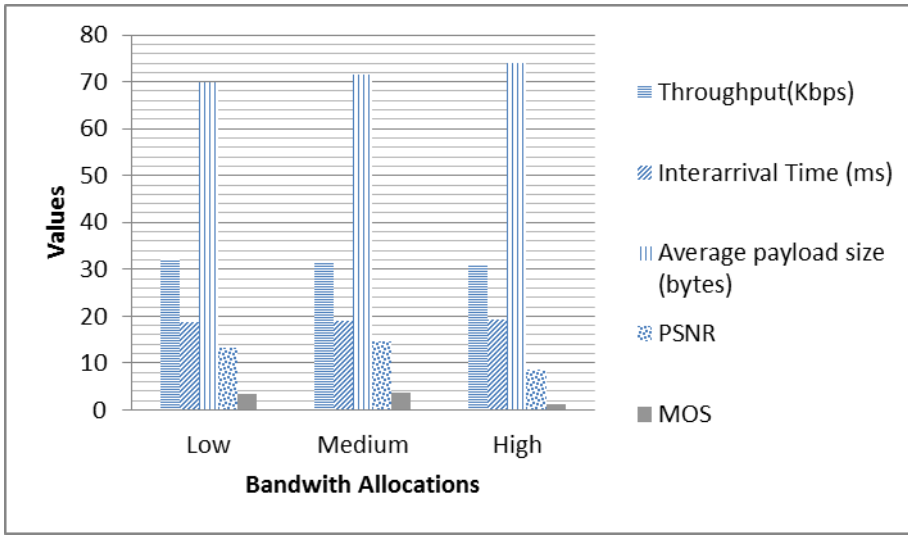


Figure 5: Skype performance in accordance with the bandwidth allocation in torrent

From figure 5 it seems that the value of the throughput decreases from low bandwidth allocation to the high bandwidth allocation. Since Skype cannot able to load the video due to the torrent traffic the values like throughput specified here are for the audio. In the case of low bandwidth allocation in the torrent interface, it seems that the throughput has got high value. This clearly reveals that fact that with the increase in the bandwidth usage of another peer-to-peer application, Skype reduces the throughput rate. From the figure 5 it is observed that the value of the Interarrival time increases slightly when the bandwidth allocation but it is not a massive increase. Similarly from the figure we can see that the values of the average payload size are also increased slightly. In the case of the MOS values obtained and the PSNR it seems that the MOS value going down with increasing bandwidth usage similarly the PSNR value also decreases with increasing bandwidth usage.

From the figure 6 it is observed that for direct download applications throughput is increasing slightly and the case of interarrival time and average payload size also getting increased with advancement in the download. The values of the PSNR are high when compared to the values obtained for the peer-to-peer applications. The values of the MOS are high when compared to the peer-to-peer applications reveals the fact that the quality of the Skype video call does not affected by the direct download options where the was a degradation in the quality of the video call in the case of peer-to-peer applications.

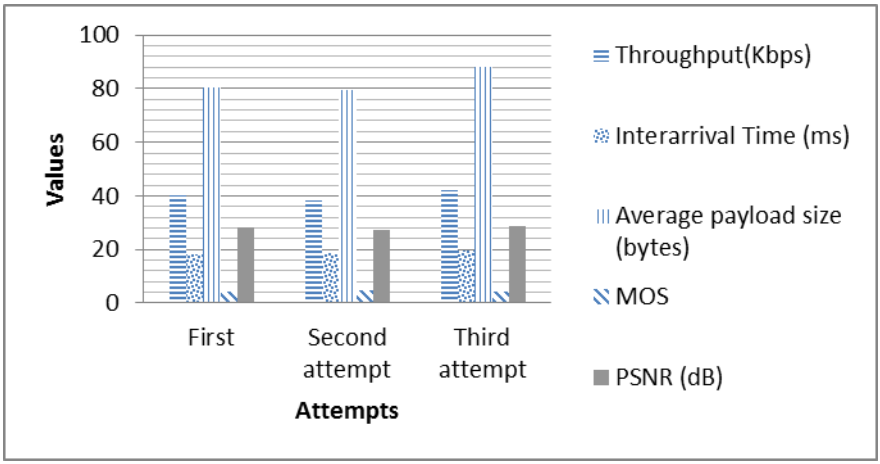


Figure 6: Skype performance in accordance with the direct download options.

4 Conclusion

Quality of the communication is one of the most important concerns in the field of telecommunications especially in the field of VoIP communication. Most of them were looking for an application that provides high quality service to the customers with the less usage of the network resources such as bandwidth and all. During the early stages the service providers were compete themselves with themselves to developing a high quality service with less usage of the network parameters. Most of the resulted products were good in some way but none of them were perfect. But the evolution of the Skype with their proprietary technology changes the entire concept of the VoIP telecommunication.

In this paper, the studies were conducted on the video quality of Skype in different network situations and the experience of the users. Analysis on the performance of the video quality of Skype under different situations made the conclusion that the quality of the video goes down when there is large amount of network distortion but still Skype tries to adjust the video quality to certain extent but it drops the video when the disturbance in the network is very high but it never drops the call. From the results and observations made it has found that the Skype struggles well to maintain the video quality when another bandwidth intensive application is competing at the same time. It also reveals the fact that the when multiple bandwidth intensive applications compete together, the video quality experienced by the end user will be worse. From the end users point of view that is calculated with the help of the subjective tests made performance of the Skype is better in conditions where the network conditions are average and sometimes below average. But at the same time the quality of the video goes really bad at the situations where there is any other application competing for the bandwidth but at the same time it tries to maintain the call without dropping it in almost all the situations even if it drops the video. This thesis figures out the performance of the Skype video on different network situations and concludes that Skype performs well in video quality except in the cases where there is multiple peer-to-peer applications work together.

5 Future work

There were many studies conducted on the quality of video in VoIP systems. But most of the studies conducted in simulated or in experimental setups. Future work would concentrate in answering the following questions of the video quality of VoIP applications especially the Skype. Since Skype adapts well in most of the worst situations in a network environment, we would concentrate more on the real time communication between two hosts in different portions of the globe. How the communication happens in the situations of sudden changes in network? How Skype adapts and maintain the quality of the video when communicating with countries with variation in available bandwidth?

In the current communication system limited availability of the bandwidth will become a great problem in most of the developing countries especially in remote areas where using dial up connections and this is still a problem in using the video communication. Future work also covers a study about the performance of Skype video quality in low bandwidth situations**.**

6 Reference

Boyaci, O., Forte, A. G. & Schulzrinne, H. Year. Performance of Video-Chat Applications under Congestion. *In:* Multimedia, 2009. ISM '09. 11th IEEE International Symposium on multimedia, 14-16 Dec. 2009 2009. 213-218.

De Cicco, L., Mascolo, S. & Palmisano, V. 2011. Skype Video congestion control: An experimental investigation. *Computer Networks,* 55**,** 558-571.

Hoßfeld, T. & Binzenhöfer, A. 2007. Analysis of Skype VoIP traffic in UMTS: End-to-end QoS and QoE measurements. *Computer Networks,* 52**,** 650-666.

Zhang, D., Zheng, C., Zhang, H. & Yu, H. Year. Identification and Analysis of Skype Peer-to-Peer Traffic. *In:* Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on, 9-15 May 2010 2010. 200-206

Performance Analysis of Voice Call using Skype

M.Pradhan and L.Sun

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

Abstract

The purpose of this research is to investigate how Skype adapts its voice sender bitrate in reaction to network congestions and what Skype's performances are in terms of voice Quality of Experience (QoE) or Mean Opinion Score (MOS) under different network conditions. The voice quality of Skype was evaluated by setting up a VoIP testbed that allowed making voice calls between two Skype clients, each installed on a separate PC. The network conditions were altered as desired and sample speech files from the ITU-T P.50 database were used to play through Skype during a Skype-to-Skype voice call. The resulting audio was recorded along with the call traffic being captured. The audio quality of the recorded speech samples was then evaluated by using the PESQ algorithm and the network parameters were calculated from the captured call traffic using Awk scripts. The results obtained showed that the voice quality of Skype deteriorates with increasing amounts of packet loss in the network. Further, the throughput values that were obtained indicated that Skype tends to reduce its send bitrate when it encounters packet loss in the network which could result in increased delay. The values obtained for the interarrival times indicated that the packet interarrival time increases with increasing packet loss and this could lead to increase in the mouth-to-ear delay. Finally, the jitter values obtained were found to be well within the acceptable limit for VoIP and thus it could be concluded that jitter does not have much effect on the audio quality of Skype.

Keywords

VoIP, Skype, voice quality, PESQ, throughput, interarrival, jitter

1 Introduction

VoIP (Voice over Internet Protocol) is a form of voice communication that utilizes audio data in order to transmit voice signals to the end user. Over the last few years, VoIP has emerged as one of the most vital technologies in the world of communication and is providing stiff competition to the traditional telephone lines due to its lower cost and richer features (Kazemitabar et al. 2010).

Skype is one of the most popular VoIP applications that are freely available on the web today. Skype allows users to make voice and video calls over the internet and also provides instant messaging (IM) services. Skype makes use of a proprietary protocol known as the Skype protocol and its operation is based on P2P (Peer-to-peer) technology while other VoIP clients make use of the traditional client-server architecture. Skype call traffic is generally transmitted in the form of UDP (User Datagram Protocol) packets over IP networks. The payload of the UDP packets is compressed and encrypted, thus securing the call data (Speidel and Eimann, 2010).

Existing research on Skype has indicated that Skype provides better voice/video quality in adverse and changing network conditions as compared to its other VoIP competitors. Menezes Filho et al. (2005) analysed and compared Google Talk, MSN Messenger, Skype and Yahoo Messenger using Ethereal software to capture the packets for each. From their study they concluded that Skype was the best software for having a VoIP conversation, providing better voice quality with less phonetic loss since it had the highest speed of them all for transmitting information.

Adopting a measurement-based approach, Chiang et al. (2006) performed a quantitative evaluation of both MSN and Skype. The results obtained indicated that Skype's overall throughput showed an up to 47% improvement over that of MSN and its MOS score showed an over 50% improvement over that of MSN. Also, the variance of interarrival time in Skype was found to be very low.

Ahmed and Shaon (2009) analysed the various performance aspects of three widely used VoIP applications – Skype, GTalk (Google Talk) and Gizmo. Although under ideal conditions it was found that the performance of all three applications was similar, when the network parameters were changed, Skype exhibited better adaptation quality than the other two.

Skype's superior voice quality is possibly due to its supposed built-in adaptation/control mechanism which enables it to adapt its voice/video sender bitrate automatically in order to ease network congestion. However, due to Skype's proprietary nature, details of how this adaptation/control mechanism works are still unknown and needs to be investigated.

A proper understanding of the mechanisms that Skype utilizes in order to provide good voice/video quality in difficult network conditions may help in contributing towards the improvement of other VoIP applications available to the users. For this purpose, the effect of the different network parameters on the perceived voice quality of Skype will have to be studied and investigated in detail. Also, further research in this direction may result in further improving the overall quality of voice/video that can be made available to the users by VoIP providers including Skype.

The goal of this research is to investigate and analyse the performance of voice quality of Skype under different network conditions by setting up a VoIP testbed, conducting voice calls between two Skype clients installed on two separate PC's, collecting the call traffic and analysing it. The PESQ (Perceptual Evaluation of Speech Quality) algorithm will be used to evaluate the speech quality since it is one of the most widely used tools in the industry for objective measurement of voice quality. The network parameters such as throughput, interarrival time and jitter will be calculated using Awk scripts.

The rest of the paper is structured as follows. In Section 2, the setup of the VoIP testbed is provided along with the description of the experiments performed using the testbed platform. The results of the experiments conducted are presented and discussed in Section 3. Finally, Section 4 concludes the paper and suggests some future investigations.

2 VoIP testbed platform and the experimental scenarios

In this section we present the VoIP testbed that was setup along with the experiments that were carried out using the testbed platform.

2.1 The testbed setup

Figure 1 illustrates a diagram of the VoIP testbed that was setup in order to perform the various experiments as part of this research.

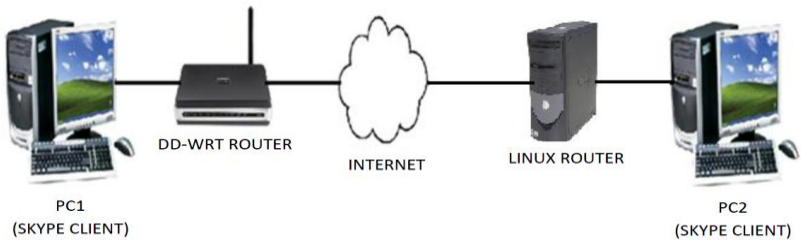


Figure 1: VoIP Testbed Architecture

The main components of the VoIP testbed are the two local PC's – PC1 and PC2, and the DD-WRT wireless router. Besides that we have the Linux router. On PC1, the software applications that were installed and utilized were OPTICOM Opera v3.5, Skype 5.3, Wireshark (Version 1.6) and Windows Media Player 11 (WMP) while on PC2, the software applications that were installed and utilized were Audacity (Version 1.2.6) and Skype 5.3.

The DD-WRT router is a NETGEAR wireless router that has the DD-WRT (Linux-based firmware) installed on it. The DD-WRT router was used in the experiments to modify network conditions such as introducing packet loss with the help of Linux commands like "tc" and "netem". It connected PC1 to the internet via cables. The Linux router is a Linux machine that has Ubuntu installed on it and is configured to act as a router. It connected PC2 to the internet via cables.

2.2 Design and Methodology for the experiments

Two major experiments were conducted as part of this research using the testbed platform that is described in 2.1. The methodology and the procedure for both the experiments is the same except for the use of a different reference speech sample file to be played through Skype for each. A reference speech file of significantly longer length was used in performing the second experiment. The following sub-sections will explain the way in which both the experiments were performed.

2.2.1 Selection of speech samples

Speech samples from the ITU-T P.50 database were used for all the objective voice quality tests that were performed. The P.50 database consists of several speech

samples available in different languages and all in the "WAV" file format. For each language, there are 16 speech samples of which 8 are male voices and 8 are female voices. The language that was selected for the experiments performed as part of this research was British English and only the first three files in female voice were used since the gender was not under consideration. The sample rate for the "wav" files was converted to 8000 Hz using Audacity and the files were saved again.

For Experiment 1, the B_eng_f1.wav speech file was selected to be played through Skype. The length of this speech file is 7.2 seconds, the sample rate is 8000 Hz and the audio is in female voice. The speech file consists of three sentences separated by a few seconds of silence. For Experiment 2, three sample speech files, namely, B_eng_f1.wav, B_eng_f2.wav and the B_eng_f3.wav were combined using Audacity to form a single reference speech file of length 21.745 seconds. This reference speech file has a sample rate of 8000 Hz and consists of 9 sentences spoken three at a time in three different female voices, all of which are separated by a few seconds of silence.

2.2.2 Introduction of Packet Loss

In order to introduce packet loss into the network, it was required to gain access to the DD-WRT router and this was done by using the 'telnet' command on the 'default gateway' for PC1. Next, packet loss was introduced at the network interface that connects PC1 to the DD-WRT router by using the Linux command 'tc'. The following command was used to introduce new packet loss or to change the amount of packet loss that was already introduced:

tc qdisc add/change dev eth0 root netem loss%

'Netem' provides network emulation functionality and is controlled by the 'tc' command. The amount of packet loss to be introduced is specified by the 'loss%' (The Linux Foundation, 2009). In both the experiments, 6 different amounts of packet loss (0%, 5%, 10%, 15%, 20% and 25%) were introduced into the network using the 'tc' command and further tests were conducted with regards to the voice quality of Skype and the estimation and calculation of the throughput, interarrival time and jitter in Skype for each amount of packet loss introduced.

2.2.3 Evaluation of voice quality using PESQ

In order to evaluate the voice quality of Skype, a sample reference speech file was selected to be played through Skype. A different reference speech file was used for Experiment 1 and Experiment 2 as was discussed in 2.2.1. At first, the desired amount of packet loss was introduced into the network. Then packet capture was started on Wireshark on PC1 and a Skype-to-Skype voice call was conducted from PC1 to PC2. This call was answered on PC2 and the 'record' button was hit on Audacity on PC2.

Next, the reference speech file was played in WMP on PC1. Once the file had finished playing - the recording was stopped in Audacity, the voice call was ended and packet capture was stopped in Wireshark. The sound recorded in Audacity and

the packets captured in Wireshark were saved in their respective default file formats. This process was carried out 3 times for each amount of packet loss introduced into the network and all the sound files and pcap files were saved.

Now, each of the recorded sound files was edited in Audacity to conform to the waveform and length of the original reference speech file and was exported in "wav" file format. Next, each of these "wav" files was used one by one along with the original reference speech file in OPTICOM's Opera software and the PESQ algorithm was run. The PESQ results obtained are presented in Section 3.

2.2.4 Evaluation of throughput, interarrival time and jitter

Awk scripts were designed for the evaluation of the throughput, interarrival time and the jitter in Skype. Ubuntu 11.04 was installed on a laptop and 'tcpdump' command was used in the Terminal to extract the data from each pcap file in text format. Next, the Awk scripts were run in the Terminal to calculate the throughput, interarrival time and jitter for each pcap file and the results obtained are shown in Section 3.

The Awk script for calculating the throughput was based on the understanding that the throughput was the total amount of data sent in the form of UDP packets by Skype on PC1 to Skype on PC2 during the total time duration of the voice call. The script was also used to evaluate the average payload size for each pcap file. The Awk script for calculating the interarrival time was based on the evaluation of the time difference between the arrivals of two successive packets at the destination. The Awk script for calculating jitter was based on the following formula (Toncar, 2010):

$$J(i) = J(i-1) + (|D(i-1, i)| - J(i-1)) / 16$$

The jitter "J(i)" after every i-th packet that was received, was estimated by calculating the change of interarrival time and dividing it by 16 in order to reduce the noise as well as to reduce the influence of large random changes (Toncar, 2010). The value thus obtained was then added to the jitter value for the previous packet i.e. "J(i-1)". The jitter was evaluated over the entire duration of each voice call that was conducted, which lasted around 60 seconds.

3 Experimental results

3.1 PESQ results

The average PESQ MOS scores obtained from both the experiments are displayed in Figure 2. The results obtained indicate that the voice quality of Skype deteriorates when there is packet loss in the network. The more the amount of packet loss in the network, the more is the degradation in quality of the voice signal. The PESQ results obtained from Experiment 2 are found to be more accurate in terms of the clearly visible decreasing trend of the PESQ scores with respect to increase in packet loss in the network.

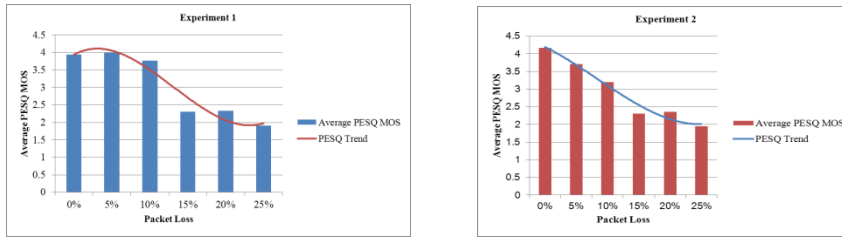


Figure 2: Average PESQ MOS scores obtained from Experiments 1 & 2

3.2 Throughput results

The results for the average throughput of Skype obtained from both the experiments are displayed in Figure 3. These results indicate that Skype's throughput decreases with the presence of increasing amounts of packet loss in the network. This means that Skype reduces the amount of data it sends when it encounters packet loss. The throughput was evaluated in terms of 'kilobits per second' (kbps). The results obtained for the average payload size of the packets sent by Skype indicate that initially, though Skype reduces its voice sender bitrate with increasing packet loss, it transmits the audio packets with increased payload to compensate for the missed data. However, it is observed that when the packet loss is at 15% or more, the payload size gets reduced significantly and this needs to be further investigated.

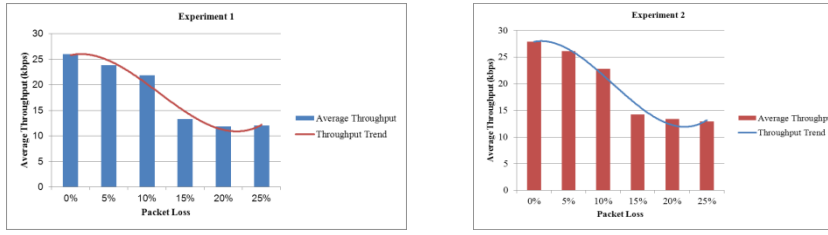


Figure 3: Average Throughput values obtained from Experiments 1 & 2

3.3 Interarrival time results

The results for the average packet interarrival times obtained from Experiment 1 and Experiment 2 are represented in Figure 4.

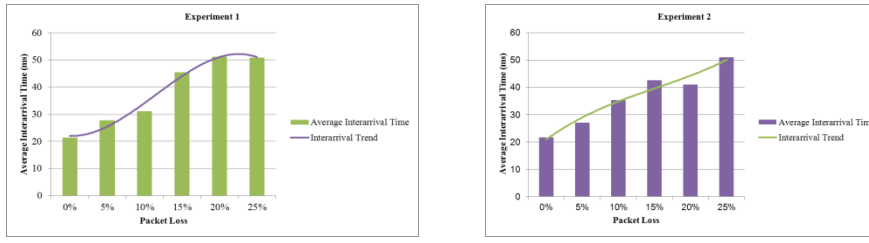


Figure 4: Average Interarrival Time values obtained from Experiments 1 & 2

The above results clearly indicate that the packet interarrival time increases consistently with increase in packet loss in the network and a similar trend was observed in the results obtained from both the experiments. This is because when a packet is lost and does not arrive at the destination, the interarrival time continues to add up until the next packet arrives successfully. The interarrival time was evaluated in terms of 'milliseconds' (ms).

3.4 Jitter results

The results for the average jitter values obtained from Experiment 1 and Experiment 2 are represented in Figure 5.

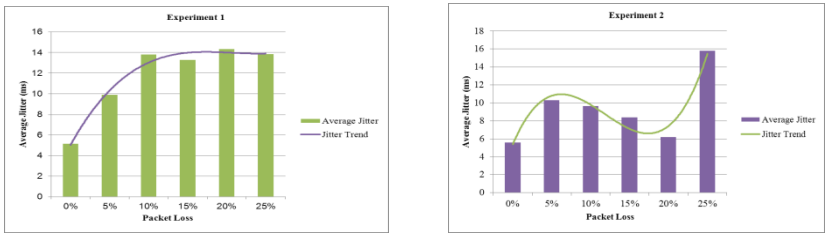


Figure 5: Average Jitter values obtained from Experiments 1 & 2

Although the jitter results obtained from Experiment 1 show a slight increasing trend with increase in packet loss in the network, no particular increasing or decreasing trend is observed in the jitter results obtained from Experiment 2 as can be seen in Figure 5. The interarrival time was evaluated in terms of 'milliseconds' (ms). Overall, the jitter values obtained from both the experiments indicate that the voice quality of Skype is not affected much due to jitter as jitter of up to 25 ms is deemed to be acceptable (irockasterisk, 2011).

4 Conclusions and future work

This paper investigated the voice quality of Skype. The main goal of the study was to analyse the behaviour of Skype in different network conditions and to observe how its voice quality was affected in these conditions. For both the experiments conducted, the PESQ MOS scores obtained indicate that the voice quality of Skype tends to deteriorate with increasing amounts of packet loss present in the network. Skype is able to provide decent to average voice quality up until 10% packet loss present in the network. But once the packet loss is at 15% or more the voice quality is affected badly with lots of noticeable gaps in the audio.

The throughput values of Skype that were evaluated under the presence of different amounts of packet loss indicate that Skype tends to reduce its send bitrate when it encounters packet loss and this could lead to increased delay. On investigating the payload size of the packets sent by Skype in different packet loss conditions, it is observed that initially, though Skype reduces its send bitrate with increasing packet loss, it transmits the audio packets with increased payload to compensate for the

missed data. However, it is observed that when the packet loss is at 15%, the payload size gets reduced significantly and this needs to be further investigated.

The values for the packet interarrival times obtained from both the experiments clearly indicate that the packet interarrival time increases consistently with increase in packet loss in the network and this could lead to increase in the mouth-to-ear delay, thus affecting the voice quality of Skype that is experienced by the end-user. The jitter values obtained from both the experiments are fairly inconsistent, especially those obtained from Experiment 2. However, the values obtained are well within the acceptable jitter value for VoIP (25 ms) and this indicates that jitter does not have much effect on the quality of voice in Skype.

Overall, it is observed that Experiment 2 provides more substantial, clear and accurate results than Experiment 1 and at the same time helps to verify some of the results obtained from Experiment 1, thus justifying the use of a longer sample speech file in Experiment 2. In future, we would like to conduct research with regards to limiting the bandwidth of the network and then evaluating the voice quality of Skype as well as investigating the TCP-friendliness of Skype with background TCP traffic.

5 References

Ahmed, A.S. and Shaon, R.H. (2009) Evaluation of Popular VoIP Services. Adaptive Science & Technology [e-journal], 58-63. Available through: IEEE Xplore [Accessed 11 August 2011].

Chiang, W., Xiao, W. and Chou, C. (2006) A Performance Study of VoIP Applications: MSN vs. Skype. [online] Available at: http://multicomm.polito.it/proc_multicomm06_3.pdf [Accessed 10 August 2011].

irockasterisk (2011) VoIP quality: culprits and thresholds. [online] Available at: http://irockasterisk.blogspot.com/2011/06/voip-quality-culprits-and-thresholds.html [Accessed 27 August 2011].

Kazemitabar, H., Ahmed, S., Nisar, K., Said, A.B. and Hasbullah, H.B. (2010) A Survey on Voice over IP over Wireless LANs. [online] Available at: http://www.waset.org/journals/waset/v71/v71-63.pdf [Accessed 17 August 2011].

Menezes Filho, L.C.A., da Costa, M.L., Belem, R.L. and Arruda Filho, E.J.M. (2005) Performance and Quality of Service on Free Softwares for VoIP. [online] Available at: http://www3.iesam-pa.edu.br/ojs/index.php/TELECOM/article/viewFile/636/522 [Accessed 10 August 2011].

Speidel, U. and Eimann, R. (2010) How well does Skype compress its call data? [online] Available at: http://busy-byte.de/~raimund/documents/publications/ICAIT_2010_Paper.pdf [Accessed 8 August 2011].

The Linux Foundation (2009) netem. [online] Available at: http://www.linuxfoundation.org/collaborate/workgroups/networking/netem [Accessed 23 August 2011].

Toncar, V. (2010) VoIP Basics: About Jitter. [online] Available at: http://toncar.cz/Tutorials/VoIP/VoIP_Basics_Jitter.html [Accessed 26 August 2011].

E-Security Awareness among Developing Nations

N.B.S.Ramar and S.Atkinson

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

Abstract

The growth in the internet and its technologies has been increasing over the past few years. Especially, across all the cities in India there has been a tremendous growth in technology. At the same time the threats which are faced by today's internet users is also increasing. Many new types of threats are emerging each day and users are facing a difficult time dealing with the threats. There has to be much awareness created among the user from the basic knowledge of installing an antivirus program to configuring one.
This research will be looking at users' awareness among the internet security and their knowledge towards them. The aim of the research is to analyse the current security threats on the market and find how users' consider internet security. The research was carried using a survey which contained 22 questions about security threats they have come across, security technologies they use and to what extent they are aware about security policies.
The results of the research shows us that, the level of awareness among individuals who use internet are comparatively low, with many users' being a victim to online attacks. But if we consider on an average they have showed improvement comparing to the previous results done by some researches. The research will provide recommendations on how to improve security when accessing the internet.

Keyword

Internet Security, Awareness, Security Threats, Security Policy, Security Management.

1 Introduction

From the beginning of internet, it is used for many things and there is always a risk of malicious attacks. Now everything relies on internet and the security of internet is considered as one of the important issue. Today more than half the people of India who use internet are not aware of the security issues. The survey conducted by Pune cyber-crime division and Tech forum reveals that almost 50% of college students are unaware of security measures which have to be taken. They use the same password. Their antivirus is a free version which has only minimal features. The government conducted an awareness program in 2008 and the results of the program were that people have not taken computer security seriously. In 2009 the same survey showed no improvement among people (Indian Express, 2009).

This project is about the security related risks involved in using internet among various groups of people in India, the purpose of the project is to find the awareness among the people using computers, their knowledge about security products and

different types of threats. I used a questionnaire which was sent to a certain number of people and their responses are collected. The responses are then analysed and explained. Finally, the solutions to the problem, today's people are facing will be discussed.

2 Background

There has been many research conducted by organisation and government officials about the use of security and the awareness among people. However, if users are not familiar with security tools they will not use it. It might even scare them instead of letting them use it. During 1999 there were only less than 1% internet users in India, whereas now it is more than 52 million internet users in India. It is an increase of more than twice of people using internet (Google, 2008).

Since the rapid growth of internet, the risk of security has also increased. Now computers are used in all fields from booking railway tickets to issue of drivers licence. People can benefit from the online internet facilities. The number of users who use internet on a daily basis is more than 25 million (One India, 2008).

The survey conducted by IMRB (Indian Market research Bureau) and commissioned by VeriSign over 5,000 internet users from 10 cities in India advises that more and more users are concerned about security nowadays. The survey results states that more than 90% of survey respondents have come across some of the issues today's online users are facing. Such as phishing, key logging and identity theft. And the most worrying part is most of them are unsure about how to combat the problems.

The results of the survey states that 60% of users have access to internet in a frequent basis i.e. at least more than 4 times a week. 44% of users shop the internet online with 53% using social networking sites like (Facebook, Orkut and LinkedIn) and blogging. The unawareness of users is that almost 38% of the users are using the same password everywhere. Only 11% of the respondents look for authenticity (Padlock) which would be shown at the bottom right end of the page. More than 80% of the users are not worried about secure websites (https :). The results of the survey suggest that people want to be safe online when using internet, but they are unaware of the process of how to keep them safe. Although users are not worried about secure sites, almost 84% would like to use two state authentications. The process of two state authentications is a user uses his login details such as user name and password with another form of authentication like a token which could include a secure code only the user can access, or like a code sent to the user's mobile phone which could be used to authenticate.

3 Research methodology

3.1 Introduction

In this we will discuss about different methods that are available for conducting this research. The method used in the research to get fair results is also discussed in this chapter. There are different methods that could be used for the research, but the

method (Qualitative and Quantitative) which is used in this research could give better results.

3.2 Why Survey

The need for survey is to get a better idea about the awareness among people. Many organisations use surveys to find some answers to a set of questions. The survey is mainly used to find out about the people's views and their interests. The survey data can be used to make certain decisions.

3.2.1 Four main reasons for conducting surveys

1. How people think about security and its technologies.
2. The opportunity to deliberate important topics with the target population.
3. The objective data is used to make important decisions. Using the data collected from the survey we can do what is important and leave the other things.
4. With the help of surveys we can compare it with the previous attitudes of people and use it to change for the future (Why Survey, 2005).

3.3 Research Plan

This research is divided into few parts, which are as follows:

- Gathering knowledge about the people's attitudes towards security.
- Finding about the security aspects by literature review.
- Framing the questions to get a better response from the users.
- Reaching the target population using certain methods.
- Finding about the latest technology and analysing it to recommend to users.

3.4 Data sampling

Data sampling is done in order to reduce the cost and fasten the data collection. It is not necessary to survey the whole population. For this research data sampling is done over questionnaire to various backgrounds of people. In order to get a more precise idea about obtained data we need to analyse properly the obtained quantitative data (Oakley, 1999).

3.5 Survey Questionnaires

The questions for the survey were intended for the general internet users. The general issues were considered for closed end. Considering the qualitative analysis, preferences is a part of both open and closed end and it is basically not possible to do without preferences. This analysis for the research will include the preferred results based on the closed end and the responses acquired (Bryman, 1995).

3.6 Targeting the survey respondents

The main important part of the research is targeting your respondents. The survey respondents were selected randomly from a set of people who are at least basic computer users.

3.7 Questionnaires

The issues related to computer users were taken into consideration, and the literature review with other previous data's are all considered before framing the questions. The questions are framed so that the target population (i.e. general users) should understand and answer the questions. The questionnaire has different set of questions which will give an idea about the basic level of security knowledge among the users.

3.8 Target Population

The respondents which we select should be the actual persons we need for this research. The selection of target population is an important task. If the wrong target population has been chosen then the results will be a biased result. In order to get an unbiased result, the target population should be carefully selected. In this research the target population is the general computer users from India who are in the age group between 18 and over. This includes working people, college students and retired people.

3.9 Limitations of Research

Since the research is done about the awareness among people in India, there are few difficulties which I came across.

- The Target Population (i.e. users) are in India. So the data collection was quiet hard. But since I had Contacts in India I was able to collect the data.
- The questionnaire which was framed has to be accurate. Even though it may not show an accurate numerical data, it will show the clear picture of the research.

4 Analysis

The results of the survey reveals that on the average nearly 40% of the respondents are not aware of certain security threats and they have never know about certain security features. Some users' lack of knowledge towards using their passwords and keeping their antivirus up to date is a major concern. Even though the figures show a worrying factor still lot of users have responded by saying they use antivirus/ internet security software. Many other questions the answers were of not up to the level of securing their computers when they are online. So majority of them need awareness towards their use of security features.

5 Discussion

This chapter will discuss and elaborate the results of the previous chapter. The questions were framed in order for all the participants to answer with the best of their knowledge. Since the survey is not a compulsory one, users can withdraw at any time if they want to. So we can assume that they provided honest answers to all the questions. The questionnaire was posted as an online survey and the link was sent to all the participants via email. The main aim of this research is to study the awareness among people in India who use internet. The previous researches done by Government of India and other sources have been used as guidance in framing the questions. This result will help us to understand the users' approach towards security. We might think that some respondents from a background have a large impact and some will have less impact on the survey. Nevertheless, the survey will consider each and every individuals own difficulties and awareness about security and its features. Each and every user may have a different problem when it comes to securing their computer.

6 Recommendation

The recommendations will be based on the survey results obtained. After explaining about the security awareness about users' and why they are not aware of the security features. This part will recommend some of the solutions to the problems faced by users'. Even after all the necessary tools and software available in the market, people are still not familiar with the products. Although users' are not aware of these threats and issues it is also the responsibility of Internet service provider, Email service provider and the software vendors to advice users' how to use the security. If the companies don't instruct the people then the process of better security will not be attained. Since without the help from software vendors it is impossible to create awareness among users' we use two methods of recommendations. One is for the end users' and the other is for software designers.

6.1 End user awareness

The answers from the survey reveal that end users are aware of certain things such as *How concerned are you about the security* majority of them said very concerned which showed us that they care for the protection of their computers from threats but at the same time only one fourth of them said they update their antivirus daily. So we need to educate them the basic security protection method like how to configure an antivirus/ internet security for good protection and how to update the antivirus regularly. We need to show them with good examples and pictures in a way even a beginner user should be able to use security. The first priority after buying a new computer should be properly securing their computer with antivirus. We need to educate them about security in schools. Most of the schools in India have computer science as a main subject with Mathematics, Science and English. But they only learn about how to use computer, word processing and email but not about how to secure their computers. This should be included in their curriculum. It is clear from the survey that nearly 40% of them are not aware of the following Spam, Malware/Spyware, Phishing and worms. People need to be educated about all the types of threats in the internet. Whether they have been a victim or not they should

know about all types of threats and the ways to avoid them and protect themselves. If they are aware of all the threats then there is less chance that they will be a victim of such threats.

6.2 Software designer's job

The software designer's, ISP's and ESP's should contribute more towards educating their users'. Software designers' should consider the beginners and design their software so that anyone could be able to use with little or no knowledge. ISP's should include security advice and guidance booklet for all the users'. They should inform the customers about the best security tools available in the market. More money has to be spent towards educating the users'. Since broadband usage is just beginning in most parts of the India it is better to educate the users' before they start using their computers for the first time. ESP's should educate them about the spam messages received and what action should be taken. If there is a suspicious website the customer should be able to contact someone to talk to about the issue. Also the password selection guidelines should be provided to the customers. ESP's and ISP's should not allow customers to select a low level password. They should only allow the password to be created if it contains two alphabets with one capital letter and the other small, one number and a special symbol. If the combination of all is selected then it should be a strong password.

7 Conclusion

The research started by explaining the level of awareness among the users'. The efforts taken by the users' and the companies have been discussed. Still the users' lack some of the basic awareness. The aim and objective of the research is also discussed.

This is then followed by literature review where we studied about the previous researches and why there is lack of awareness. And also the major threats are discussed in the literature review.

The methodology was discussed with the types of methods used in this research which is qualitative and quantitative. The research is carried out in a survey manner where the survey participants are selected from various cities in India. The survey was done through an online link sent to participants over email.

Results were then analyses and discussed in the following chapters. The exact problems faced by people and their awareness are analyzed using qualitative methods. Some of the results were same compared to the previous researches done by other people where there is no improvement even after the awareness programs. At the same time some of the results showed us that people are changing over and time and realizing the threats.

We can conclude by saying it is mainly the users' responsibility to keep them safe from active threats and protecting them online. However, the designers also have to do their part so that we can have a better secured and protected internet. Finally, it is hoped that this research aim and objectives were met. The main aim was to find the

awareness among the people in India who use internet and computer. The possible recommendations were also provided in this research.

8 Future Works

As we can see from the past researches and compare it with this research there is some improvement. By educating the users and testing their awareness from time to time could improve the chance of security awareness. This research should continue until we get the response from all the users' that they have secured their computers and protected them online. Until then this research should continue to achieve its ultimate goal which is each and every users' computer should be secured. The research had some limitations, there is no face to face interview conducted in this research. Also this research has quantitative questions which were explained in a qualitative way. The future research should be face to face with more qualitative questions.

9 References

Bryman, A. (1995), *Quality and Quantity in Social Research*, Urwin Hyman ltd., London, U.K. ISBN: 0-04445-132-6

Google (2008) *Google public data* [WWW] Available from: http://www.google.com/publicdata?ds=wb-wdi&met=it_net_user&idim=country:IND&dl=en&hl=en&q=number+of+internet+users+india#met=it_net_user&idim=country:IND [Accessed 06/11/2010]

Indian Express (2009) *Low awareness about cyber security among youth* [WWW] Available from: http://www.indianexpress.com/news/half-the-wifi-connections-in-city-unsafe-says-survey/555553/ [Accessed 05/11/2010]

Oakley.A, (1999), *Critical Issues in Social Research – Power and Prejudice*, ed. Hood.E, Mayalland.B, Oliver.S, Open University Press, Philadephia, USA. ISBN: 0-33520-870-3

One India (2008) *49 million internet users in India* [WWW] Available from: http://news.oneindia.in/2008/05/29/35-million-regular-internet-users-india.html [Accessed 21/01/2010]

Why Survey? (2005) *why is it important to survey?* [WWW]Available from: http://knowledge-base.supersurvey.com/survey-goals.html [Accessed 14/11/2010]

Section 5

Robotics

Optimization and Dynamic Stabilisation of Bipedal Gait

D.Caçador and G.Bugmann

Centre for Robotics and Neural Systems, Plymouth University, Plymouth, UK

Abstract

This research study aspires to optimize and dynamically stabilize the cyclic gait generator currently in use by the University of Plymouth humanoid robot in international competitions such as FIRA – Federation of International Robot-soccer Association.
Firstly, it tries to find the most stable gait algorithm, reproducing the theoretical and practical feet trajectory shapes obtained. The gaits developed and the ones currently being used are evaluated for their maximum stride lengths achievable and for their natural ability to recover from instabilities, where it is found that the Half-Circular and the New gaits outperform the other three gaits tested.
Finally, a dynamic stabilization methodology is developed that attempts to correct the robot forward-backwards oscillations when walking unstably. The methodology developed is tested using an automatic instability procedure that creates forwards-backwards oscillations and IMU readings of the X-axis acceleration are provided showing the successful robot stabilization after destabilization. Also standard deviations are calculated and show that the Half gaits although the best they are the ones that benefit the less from the dynamic stabilization.

Keywords

Cyclic Gait Generator, Dynamic Stabilization, Optimization.

1 Introduction

Biped locomotion although mastered by humans is still in present days one of the hardest types of locomotion to mimic effectively in robots. Despite the somewhat rapid development of sophisticated prototypes, the development of controlling algorithms has still a long way to go before efficient bipedal gait control can be implemented, Siciliano, et al (2008).

The system developed by Gibbons, P. et al, 2009, at the University of Plymouth uses a cyclic approach to the generation of the feet trajectory. The algorithm attempts to generate a circular feet trajectory which has a given height and length that can be changed on the fly. The circular trajectory is divided in any multiple of 8 as intended by the user and for each new foot position, the inverse kinematics take care of calculating all leg servo angles. However, there is no control integrated, it works as an open-loop system.

Several biped locomotion control methods have been suggested throughout the many studies conducted so far. The “active control methods” category was mentioned by Kajita, et al. (2003), Nakanishi, et al. (2003) and Sugihara, et al. (2004) as a tracking control methodology in which the problem of bipedal locomotion gets separated into the trajectory (or pattern) design and the stabilization (or compensation) controller.

Some methods of control use “dynamic filtering” in order to convert an input trajectory into a dynamically stable and consistent trajectory. Nakamura, et al. and Yamane, et al. (2000) suggest a system using a dynamic filtering method able to interactively generate motions for a humanoid robot. By allowing the filter to use only temporal-local information, they are able to respond to the interaction between the robot and the environment, varying the reference trajectory according to a kinematic combination of motions.

Ultimately, this project will try to deliver an optimized gait generation algorithm with a dynamic stability control system. The trajectory based gait generation will rely on offline generated trajectories, which are augmented with the model predictive approach stability control that takes into account the data received from the IMU and computes in real time the optimal robot movement that generate a stable gait.

2 Gait Generator Optimization

2.1 Current Gaits

The gait generator started as being a circular trajectory gait. The user would only have to define what would be the stride height, the stride length, the number of poses in which the trajectory would be divided and the number of ticks per pose for the required gait. Firstly, in order to get familiar with the actual output of the gait, a pen was attached to the right foot of the robot and the algorithm run at several speeds and step sizes. Figures 1 shows the obtained shapes.

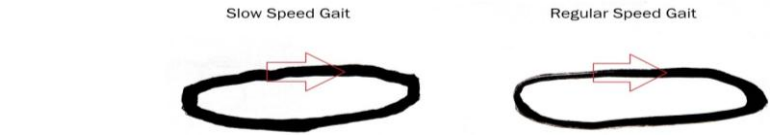


Figure 1: Foot trajectory drawn by the circular gait. On the left the robot is set to 80 poses per cycle and 3 ticks per pose, while on the right to 24 poses per cycle and 3 ticks per pose. Stride length is 20 and stride height is 10.

Another gait already developed at the robotics club was a triangular shaped gait. This gait was inspired by the concept of horizontal ground speed matching. By bringing the foot in a forward to backwards motion before the contact with the ground, one would minimize some of the ground reaction force peaks that introduce instability to the walking gait. Figures 2 shows the output trajectory shapes of the right foot of the robot running the gait at several different speeds and strides.

Figure 2: Foot trajectory drawn by the Triangular gait. On the left the robot is set to 80 poses per cycle and 3 ticks per pose, while on the right to 24 poses per cycle and 3 ticks per pose. Stride length is 20 and stride height is 10.

Analysing the images, one observes that there is a big discrepancy on the trajectory shape when the trajectory is run at faster speeds. In order to explore the cause of these disparities, a test was done with the gait, where both the angle transmitted to the servo and the servo current angle were stored and plotted, as seen in figure 3, below.

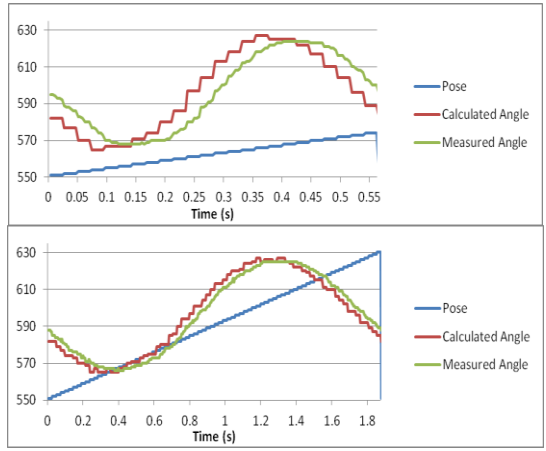


Figure 3: Right foot servo angle sent and measured, at regular gait speed (top graph) and at a slower gait speed (bottom graph). One X-axis unit represent a full gait cycle.

Closer analysis shows that the disparity between servo angle sent and measured can reach up to 3 poses. However, one pose disparity is expected because the servo upon receiving a command from the controller would take time to reach the requested angle. This delay explains the odd shapes seen in figure 2 on the right. If one looks attentively, it can be observed that the side of the triangle has a curved corner as the foot was on its way to the vertices of the triangle when it received another command to start move downwards. When moved slowly, these disparities in the gait trajectory disappear, as seen in figure 3 on the left.

2.2 New Gaits

The first approach taken to optimize the gait trajectories was to minimize hip movement on the stance leg. This would bring the gait closer to the natural human gait which is very efficient and very low power consuming. In order to do that, the

gait algorithm was changed so that a constant hip height relative to the floor could be maintained. It was implemented in both the circular and triangular gaits. These new gaits were named the half circle and half triangle gaits respectively. Figures 4 and 5 are the foot trajectories drawn by those gaits respectively.

Figure 4: Foot trajectory drawn by the Half-Circular gait. On the left the robot is set to 80 poses per cycle and 3 ticks per pose, while on the right to 24 poses per cycle and 3 ticks per pose. Stride length is 20 and stride height is 10.

Figure 5: Foot trajectory drawn by the Half-Triangular gait. On the left the robot is set to 80 poses per cycle and 3 ticks per pose, while on the right to 24 poses per cycle and 3 ticks per pose. Stride length is 20 and stride height is 10.

After observing some stability improvement over the existing gaits, it was time to incorporate all concepts in one gait generator. This gait trajectory would have both vertical and horizontal ground speed matching; however the horizontal speed matching occurs only at the moment of contact between the flying foot and the ground. Also, the new gait has a round shape when the stance foot is starting the flight phase of the cycle, in order to raise it quickly, minimizing the chances of dragging the foot on the floor. Figure 6 is the trajectory drawn by the new gait.

Figure 6: Foot trajectory drawn by the New gait. On the left the robot is set to 80 poses per cycle and 3 ticks per pose, while on the right to 24 poses per cycle and 3 ticks per pose. Stride length is 20 and stride height is 10.

As can be observed, the vertical ground speed matching is achieved by contracting the leg (i.e. raising the foot by) a fraction of the total stride height of the gait. This prevents violent ground reaction force impulses at the moment the stance feet are switched, inherently minimizing the instabilities created at this crucial phase of the gait.

3 Imbalance Detection

In normal circumstances, the robot will walk forwards or backwards maintaining a certain pitch angle predefined by the user. The imbalance detection system exploits this predictability and attempts to detect when this value differs from prediction. Firstly, a relation between the tilt set to the robot and the X-axis acceleration was experimentally measured to be as the following:

$$Target\_Acceleration = 0.4149 * Tilt + 10.088 \quad (1)$$

Then, the imbalance detection algorithm takes the value of acceleration retrieved from this relation and calculates the difference to the current detected acceleration. The gait is deemed unstable as a direct proportionality to the absolute value of this difference. Figure 7 shows the difference in the X-axis measured acceleration between a stable gait and an instable one. One can observe that when a gait is stable the X-axis acceleration hardly changes as the robot torso is kept upright at the defined tilt. However, if a robot is oscillating back and forth, the accelerometer is sensitive enough to detect this undesired movement before it escalates until the robot fall.

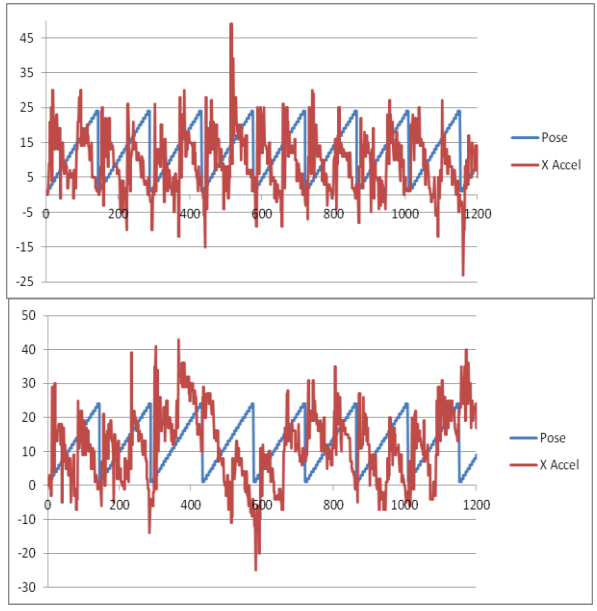


Figure 7: X-axis acceleration of a stable walking robot on the left and an unstable one on the right.

Comparing both figures, one observes that when the robot is walking after being affected by an external disturbance, the X-axis acceleration value will start oscillating until the robot falls or is gradually attenuated.

4 Stability Control Method and Tuning

If an imbalance is detected in the robot gait, one needs a control strategy in order to stabilize it. The approach taken considers the X-axis acceleration difference calculated during the imbalance detection as a measure of how instable is the gait at the moment that the IMU was read. When the robot is inclined forwards, if the gait trajectory was allowed to run as usual, the flying foot would encounter the ground earlier than expected making the robot trip on its own feet. Also, the foot would no longer be parallel to the floor making it reach the floor even earlier.

The stabilization algorithm takes the difference between the current acceleration measured by the IMU and the equivalent acceleration to the tilt currently setup of the robot. This is accomplished by adding a certain slope to the right side of the trajectory shape proportional to the acceleration differences. The slope correction is calculated once for each foot every gait cycle. The right foot slope is calculated at the ¾ of the gait cycle pose and ¼ for the left foot. This starts the correction while the foot is well in the air. Figure 8 illustrates this effect on the feet trajectory.

The corrected stride height is calculated as a function of the current stride length. There is also a Gain tuning variable that is multiplied to the acceleration difference that is used to control the correction slope according to the stride length and height setup parameters. The equation below represents the complete update of the vertical coordinate of the foot position:

$$YFootPos_{corrected} = YFootPos_{original} + Gain * (XAccel_{measured} - XAccel_{target}) * (XFootPos_{original} - XOffsetPos) \quad (2)$$

Where, $YFootPos_{\_original}$ and $XFootPos_{\_original}$ are the coordinates of the foot position calculated by the gait generator; $XAccel_{\_measured}$ is the IMU X-axis acceleration data; $XAccel_{\_target}$ is the target X-axis acceleration calculated for the setup tilt at correction moment; XOffsetPos is just an offset to the X position of the foot setup by the user.

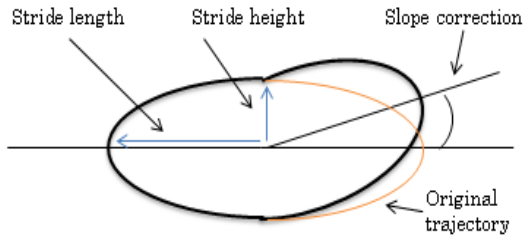


Figure 8: Circular trajectory with imbalance correction slope. Stride length on both sides of the trajectory shape is kept the same, only the stride height is changed.

The feet angle is then corrected according to the slope of the corrected trajectory. The best value to send was found to be the same as the correction stride height added to the original one.

5 Evaluation

The first test performed consisted on having the robots starting from a still position, steadily increase their walking speed and perform 15 steps, finally reducing its speed and coming to a halt. This procedure was repeated several times increasing the size of the stride length each time and was performed in both forward and backwards walking directions. The objective was to observe when the robot failed to finish the run. To be considered a successful run the robot had to run each experiment twice.

The second test was performed in order to assess the capability of each of the gaits to recover from disturbances. The robot was setup to walk forward at a fixed setup of 10 stride length and 10 stride height, 24 poses and 3 ticks per pose. In its path a small obstacle was placed in the floor in the direction of the right foot. The height of the obstacle was gradually increased. If the robot recovers from the instabilities produced be the obstacle, it would be considered a successful run. Figure 9 below demonstrates the obtained results for both tests.

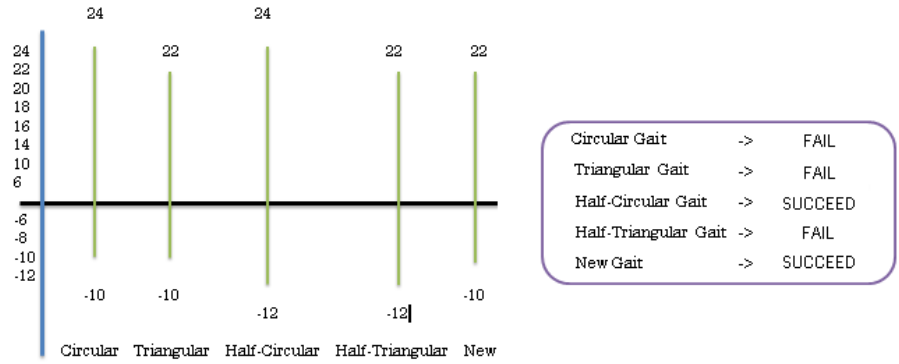


Figure 9: Gait algorithms speed and stability tests, left and right respectively.

The results from the speed and stability experiments show that although some improvements were visible, no gait was considerably better than the others. However, on the second stability experiment, both the Half-Circular and the New gaits were able to walk past a 5 mm obstacle after stepping on top of it.

Afterwards, an experiment was devised in order to evaluate the effectiveness of the stability control algorithm. This consisted in having the robot walk with every gait at a fixed 10 stride length and 10 stride length. These values were used because every gait can stably walk at those speeds and also because the algorithm needs to be optimized for each value of step length. The test consisted in having the robot steadily increase its stride length up to the required value of 10 and then perform 8 gait cycles (i.e. 16 steps) and at the beginning of the third cycle, the Tilt value is

increased by 20 and after 1 pose would be set back to its original Tilt value. This action induces a similar disturbance regardless of the gait algorithm used.

IMU data was recorded in order to observe the transition from stable to instable walk and back again to stable. In Figures 10 to 14 one can observe the experimental results, where the top and bottom graphs on each figure are the results without and with the dynamic stability algorithm respectively. Also, the standard deviations of the data sets presented were calculated and are displayed in Figure 15.

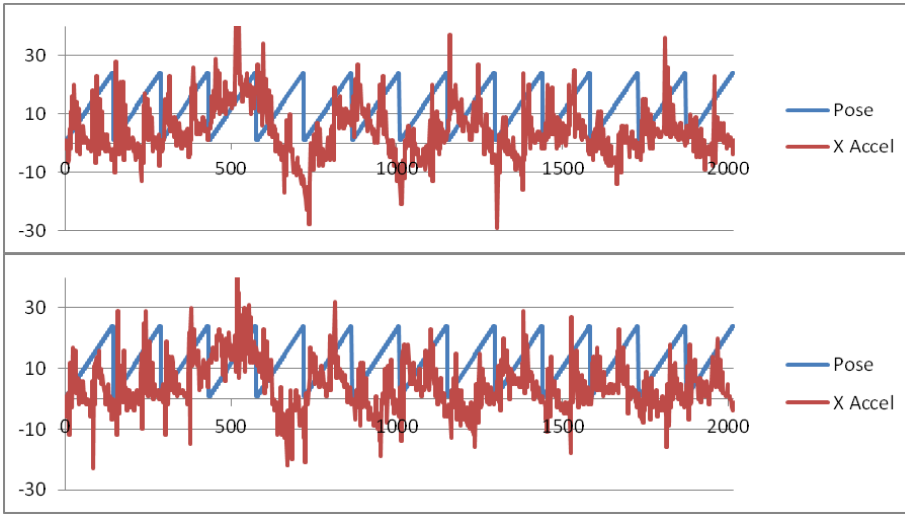


Figure 10: Stability control experimental results for the Circular Gait. Top and bottom graphs represent the IMU reading without and with the dynamic stabilization respectively.

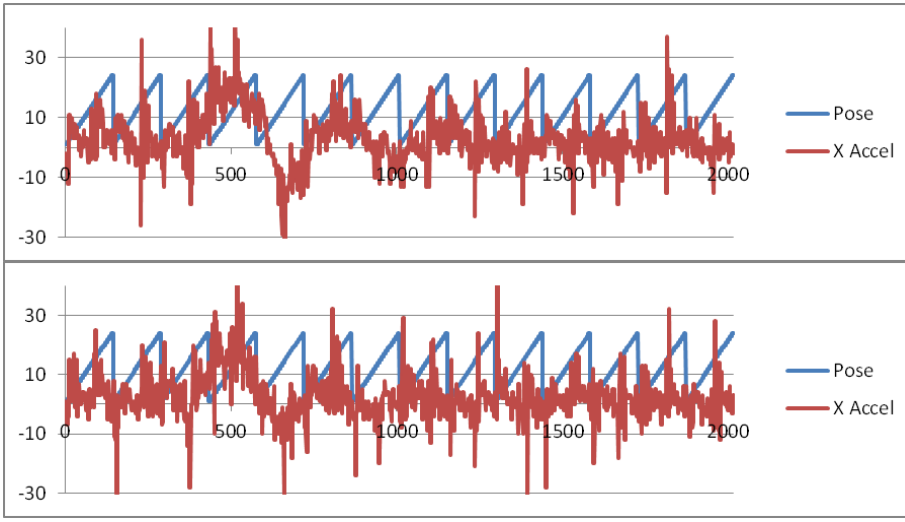


Figure 11: Stability control experimental results for the Triangular Gait. Top and bottom graphs represent the IMU reading without and with the dynamic stabilization respectively.

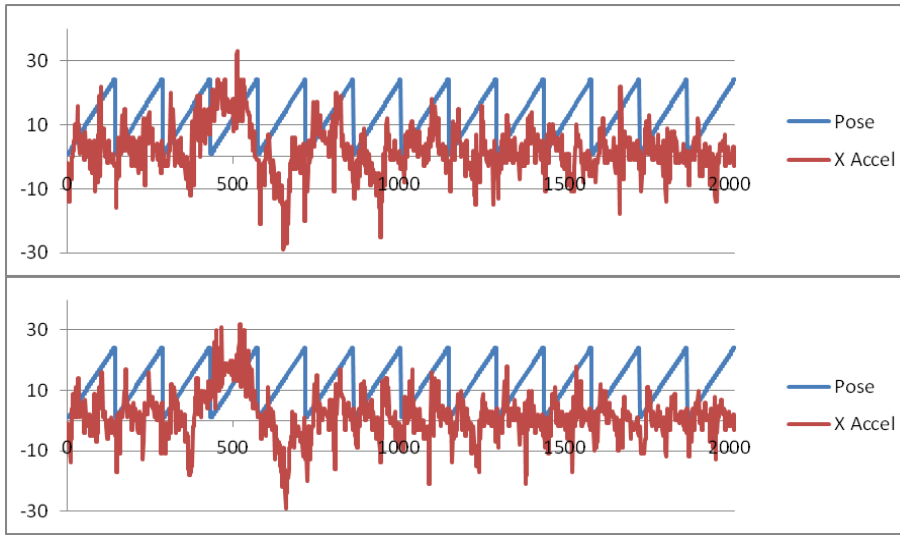


Figure 12: Stability control experimental results for the Half-Circular Gait. Top and bottom graphs represent the IMU reading without and with the dynamic stabilization respectively.

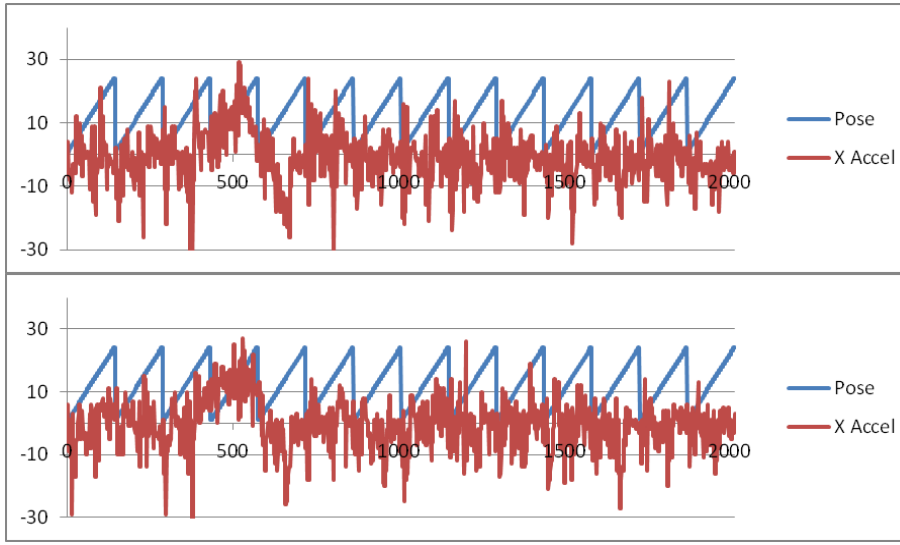


Figure 13: Stability control experimental results for the Half-Triangular Gait. Top and bottom graphs represent the IMU reading without and with the dynamic stabilization respectively.

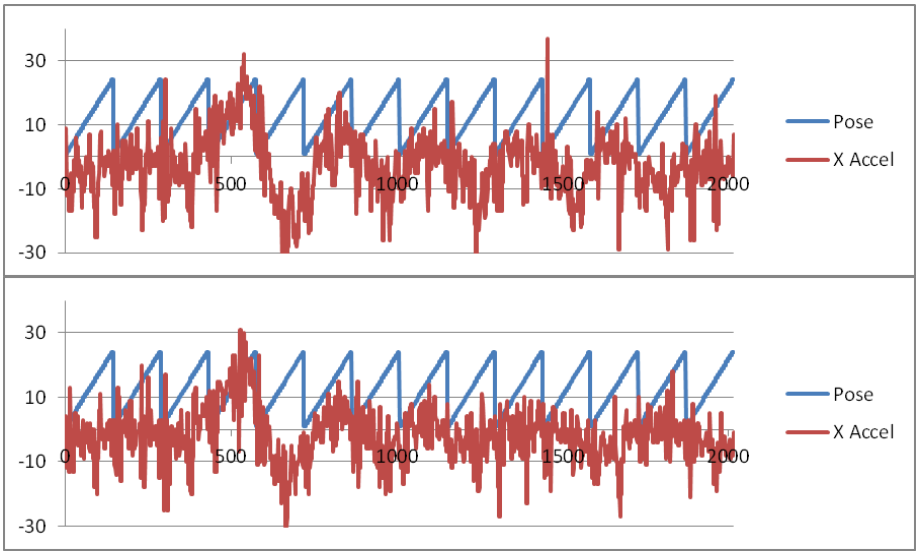


Figure 14: Stability control experimental results for the New Gait. Top and bottom graphs represent the IMU reading without and with the dynamic stabilization respectively.

Gaits	Standard Deviation	Without Dynamic Stabilization	With Dynamic Stabilization
Circular		8.779	7.597
Triangular		7.686	7.186
Half-Circular		6.879	6.486
Half-Triangular		7.560	7.315
New		9.385	7.419

Figure 15: Standard deviations obtained for corresponding data sets for all gaits

6 Conclusion and Future Direction

Several gait generators were developed, each based on a different natural stabilization concept. There was already a gait based on horizontal ground speed matching, then the vertical ground speed matching was implemented and also the gait with constant hip height.

The results of the optimization process allow one to conclude the newer gait feet trajectories, although not improving the maximum stride length achieved, they produce cleaner ground reaction force readings and allow for a better recovery from instability while stepping over a small obstacle.

On the dynamically gait stabilization, an algorithm was developed that took the difference between intended inclination and measured inclination, changing the slope of the right side of the feet trajectory. This is able to compensate for the reduced

distance between the flying leg and the ground caused by the extra robot inclination. The algorithm is also able to correct the angle of the feet that is about to touch the ground. It was found that this algorithm is able to stabilize the robot after being destabilized. This was observed both in the graph comparisons between X-axis acceleration readings with and without the dynamic stabilization algorithm and confirmed with the standard deviations calculated on those IMU readings. The standard deviations show an improvement on all gaits by using the dynamic stabilization, where the Circular and the New gait benefit the most.

Future developments can include a further exploration of the ground speed matching concept. Currently, the support leg has a fixed timing for the lowest hip height, which could be improved by shifting it earlier or later in the foot trajectory cycle in order to slow down the robot fall quickly and then slowly raise it back before the time to switch support legs for the next step.

Furthermore, I envisage that an update to the dynamic stabilization algorithm could be done in the future. This would concern the tuning gain, which is currently optimized for a gait setup of 10 stride length and 10 stride height. The update would make this a dynamic gait that would change accordingly to the optimized value for any gait setup in use.

7 References

Gibbons, P, Mason, M. Vicente, A., Bugmann, G. and Culverhouse, P. Optimization of Dynamic Gait for Bipedal Robots (2009), Proceedings of 4th Workshop of Humanoid Soccer Robots IEEE Humanoids 2009.

Kajita, S., Kanehiro, F., Kaneko, K., Fujiwara, K., Harada, K., Yokoi, K., et al. (2003). Biped walking pattern generation by using preview control of zero-moment point. Paper presented at the IEEE International Conference on Robotics and Automation (ICRA '03).

Nakanishi, J., Morimoto, J., Endo, G., Schaal, S., & Kawato, M. (2003, 27 - 31 October). Learning from demonstration and adaptation of biped locomotion with dynamical movement primitives. Paper presented at the IEEE/RSJ Int'l Conference on Intelligent Robots and Systems (IROS '03). Las Vegas, USA.

Siciliano, B., Oussama Khatib, O. (2008). Springer Handbook of Robotics. Springer, ISBN 978-3-540-23957-4.

Sugihara, T. (2004). Mobility enhancement control of humanoid robot based on reaction force manipulation via whole body motion. Unpublished PhD Thesis, University of Tokyo, Tokyo.

Yamane, K., & Nakamura, Y. (2000). Dynamics filter - concept and implementation of online motion generator for human figures. Paper presented at the IEEE International Conference on Robotics and Automation (ICRA '00).

Huro Cup Vision System

P.Eastham and P.Culverhouse

School of Computing and Mathematics, Plymouth University, Plymouth, UK

Abstract

The purpose of this report is to provide an investigation into the development of efficient embedded C++ based vision systems for use on a humanoid robot which will be partaking in the FIRA Huro Cup. The main objective is to develop a mono camera based vision system capable of obstacle recognition and avoidance.

Keywords

Vision; HuroCup; Bioloid; Navigation

1 Introduction

Currently vision is a key area of research in field of robotics with many areas being investigated from teams around the world. The primary reason for this interest is that human beings use eyes as the main perception for most tasks they undertake, and as such if robots are able to exist usefully within human environments it would make sense that robots make full use of visual information. Ideally robots should be able to navigate around environments and its changing aspects without the need of adding special landmarks for them to use, this unfortunately is still a long way off.

The aim of this project is to implement an efficient vision system for FIRA's Huro Cup events for use on a low powered embedded system. The project will build upon existing code in order to implement improved efficiency and reliability throughout the existing vision systems as well as detail the design of algorithms for the HuroCup obstacle run event.

This research paper will lay out the implementation of the code looking at the core parts of the code which are the base platform and obstacle run event. The obstacle run event will further break down the requirements into four key areas, obstacle detection, mapping, route planning and finally localization.

At the end of the paper a full documentation of testing will be undertaken followed by a conclusion that will round up the paper by summing up the feasibility of the designs and put forward any further work needed to improve upon the algorithms.

2 Implementation

As part of the project the existing launch pad "Prog" was rebuilt to allow for easier implementation of the new obstacle run event however although the code was

completely re-written a lot of the theory could be kept in place from the existing code.

"Prog_v2" is based on the original "Prog" written by Martin Mason, Guido Bugmann, and Nicolas Michel. Originally developed for robot football "Prog" was written in C using OpenCV 2.0 libraries, it was later adapted into a launch pad for

The aim of the re-write to streamline the code and allow for a simplified interface, include the addition of global functions for regularly used code and the inclusion of extra features such as undistort used in the obstacle run event.

2.1 Image Capture

At the core of the vision system is a robust colour range system that is based on a HSV colour space. The colour recognition allows for a number of separate objects to be stored, having a max and min value range for each Hue, saturation and value parts. This range based system allows for most colours to be tuned in such a way that light issues such as shadows can be overcome.

For some events such as obstacle run measurements are needed to be taken from the scene, for these cases it is important that any camera distortion is removed as shown in Figure .

OpenCV provides functions that can be used to calibrate the camera such as Chessboard corners calibration, once this is done the intrinsic and distortion matrix can be stored for later use. Performance is further be increased by generating an Undistort map from the matrices before instigating the main loop.

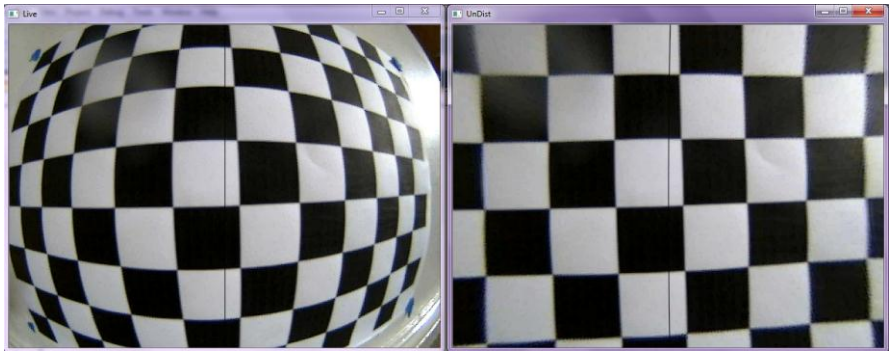


Figure 1: Pre and Post camera calibration

2.2 Obstacle run

For the robot to navigate a field of obstacles and successfully complete the obstacle run event, a number of key problems must be overcome. These can be broken down into Vision, mapping, planning, and finally localizing.

Obstacle Detection – the obstacle detection code is the section that analyses the scene seen through the robots camera in order to pick out the various types of obstacles that the robot may encounter.

Mapping – the mapping sections role is to convert the detected objects into an overhead map which can then be stored for use in the localization process.

Route Planning – route planning is used to locate gaps wide enough for the robot and then plot the most direct route to the goal using the information given.

Localization – Finally the localization routine is used to keep track of the robots position as it moves.

The following section will look at the techniques used in each section detailing the assumptions that must be made as well as the method of implantation.

2.2.1 Obstacle detection

As the obstacle event uses bold primary colours for all the obstacles a colour based object detection system was implemented to provide a robust detection method specifically designed for detecting the obstacles.

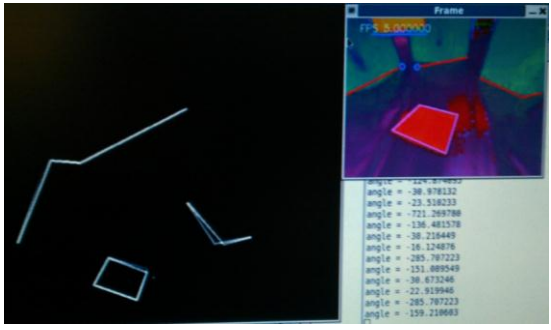


Figure 2: Obstacle detection and mapping

Once likely obstacles are found a range of techniques are used to build a list of points capable of representing the scene as demonstrated in **Error! Reference source not found.**

The wall obstacles will make up the bulk of the map and can be assumed to fall into the following assumptions:-

i. A wall will be on the ground (pitch).
ii. Multiple walls may overlap in the scene.
iii. A wall may be at any angle.

Find contours
Check blob size
Simplify contours
Remove near vertical lines
Check patch above each line point is the wall
Check patch below each line point is the pitch

The hole obstacle is represented by a shape lying flat on the ground, the hole colour is also used to make the sides of the course, the following assumptions can be made:-

i. All sides of the hole will be on the ground (pitch).
ii. A 2d shape that can be represented by a polygon

Find contours
Check blob size
Simplify contours
Check enough of the corner points have some pitch colour

The gate obstacle is a piece of card linking two wall obstacles creating a doorway that the robot could crawl through. The assumptions made are:-

i. The gate is always above two wall obstacles

Find contours
Check blob size
Check wall below bottom corners of object
Find all wall points below
Create point pairs

2.2.2 Mapping

The technique used to convert the detected objects into a map was a form of direct measurement in which the camera height from the ground and angle must be kept constant in order for accurate results to be generated. A transform matrix is used to convert it from the cameras X-Y co-ordinate to the world's X-Z plane (Figure 3).

Figure 3: visual representation of Pre and Post perspective transformation

2.2.3 Route Planning

The route planning was implemented using a grassfire algorithm (Yong et al, 1992) that was optimised by only looking at paths that head from the top of the map to the target at the bottom, ignoring the possibilities of heading back away from the target.

As the robot is not a point mass, the first step of the route planner is to dilate the obstacle line map to take account of the robots width (**Error! Reference source not found.** 4a).The burn process then takes place from the position of the robot to the bottom of the screen (fig 4b). After the main burn takes place a trace back algorithm then generates a path from the grassfire map fig 4c), a number of possible behaviours were experimented with all of which followed the minimum values of the neighbours. The behaviour finally selected used a order of preference to determine the next neighbour to chose, this provided a balance between a reduced number of corners whilst keeping an efficient path.

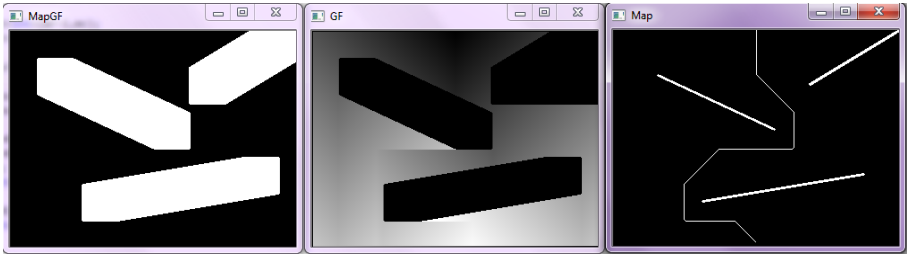


Figure 4: Three stages of the Grassfire algorithm

Due to the nature of the visual information only a minimal map can be created from any one position as it is possibility that some obstacles will be obscured by others. Due to this only the first step of the generated route is used before the mapping algorithm is run again. And a new route is built

2.2.4 Localization

The localization stage of the obstacle run makes use of a Monte-Carlo algorithm (Rofer & Jungel, 2003; Malis & Vargas, 2007) to steer the robot down the requested path and maintain pose awareness allowing for the goal to be reached. For it to work

the obstacle detection system is again used to build a list of obstacles which can then be compared against the map to determine the robots position.

To simplify the computation the navigation is split into two parts, the local navigation is carried out by the Monte-Carlo based on the mapped scene, for the duration of a single step of the route. The global navigation is stored as an offset from the robots start position which is updated based on the change of poses during each local navigation phase.

The Monte-Carlo algorithm can be split into three core parts:-

Update movement phase takes the robots predicted motion and uses it to update each particle with added noise.

Update sensor compares the angles of the map points from the robots position with each of the particles; the closer the match the more probability of the particle is increased.

Re-sample reallocates the particles primarily in regions of high probability.

3 Results

Unfortunately the obstacle run was never fully integrated, as a result testing will look the individual parts that make up the system, and asses the feasibility of the system as a whole based on the performance these parts.

3.1 Obstacle detection

The colour based obstacle detection was shown to work, successfully recognising all three types of obstacle, wall, gate and hole in a range of pitch setups. Unfortunately issues caused by shadows and other lighting issues have proved to be problem in certain test situations. These issues could cause the object to appear as a different size or orientation when mapped, in extreme situations the obstacle could disappear altogether.

For the wall obstacles the detection system was able to distinguish overlapping objects as well as angled ones, however as the wall obstacles use near vertical lines to separate the overlapping obstacles some occasions exist when a wall obstacle is not picked up as it is perceived as to near vertical to be included.

The speed of the code allowed the rapid use of algorithm allowing some of the visual flaws to be overcome by collecting multiple scenes worth of visual data.

Get thresholds	*7ms*
Get Objects	*15 – 50ms*

3.2 Mapping

The Mapping stage was greatly simplified by the use of the perspective transformation which efficiently transformed the view scene into a top down map using minimal processing time. As the map is generated as point pairs the maps were versatile to the various types of obstacles as well as taking up minimal memory.

Perspective Transform *1ms*

The only drawback of this method for generating the map was the angle of the head must be precisely known which unfortunately is difficult to accomplice whilst the robot is moving.

3.3 Route Planning

As can be seen in Figure 5 the route planner was both able to distinguish the gaps large enough for the robot to pass through and then plot the best route through as well as create and error state should no path exist. Despite working well enough for the task at hand a number of issues still remained.

Firstly the output path generated was always based on 45 degree turns, which although generally gave acceptable routes would in some situations lead to very small segments.

Despite not being a huge problem as the routine only runs occasionally the timing could be drastically reduced by choosing a more sensible map size. Currently the map is 320 x 240 pixels which was primarily chosen for the view size.

Grassfire Routine *250 – 400ms*

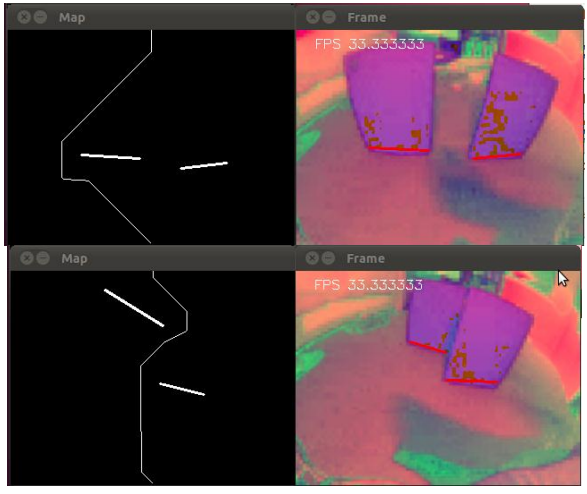


Figure 5: Examples of the route planning tests

3.4 Localisation

On the whole the localization implementation was not very successful and the algorithm failed to reliably find the robots position. Testing was done using static values and the kidnapped robot test. By integrating odometry the reliability of the localisation should increase significantly as the robot always starts in a known position after mapping the scene.

Testing during the development process using a simplified update sensor routine proved the core principal of the Monte-Carlo system worked well. The test simply increased the probabilities for particles within a small area of the pitch. After a short period all the high probability particles had migrated to the specified area. As the core of the Mote-Carlo worked the fault fell with the update Sensor phase of the Monte-Carlo. The reason for the lack of reliability may be to do with a lack of information being used to compare positions. The comparison has no knowledge of what object type the point belong and mealy uses the angle from its position to the mapped point.

4 Conclusion

The aim of the project was to build upon existing code to improve reliability and efficiency of the Huro Cup vision systems as well as develop new algorithms for the obstacle run event.

The update process went well improving both the reliability as well as the operating speed of the vision systems, leading to world records in the 2011 Huro Cup sprint and marathon events. On top of improving the functional abilities of the code the re-build also allowed for a much faster calibration process, making it easier for fine tuning to be done in the heat of competition. The final advantage that the re-build achieved that should not be overlooked is cleaning up the code and structuring it in easy to read fashion with common utilities wrapped into global functions, that can allow future students to build upon and add future events.

Whilst elements of the program worked well it is unfortunate that the obstacle run event was never fully completed, looking at each part however shows a range of useful techniques that could be expanded upon to finalize the obstacle run event code. The first part the colour based obstacle detection was shown to work, successfully recognising all three types of obstacle, wall, gate and hole in a range of pitch setups. Unfortunately issues caused by shadows and other lighting issues have proved to be problem in certain test situations. The perspective transformation also proved an efficient method of converting the visual data into a map of the obstacles, reducing the need for additional calculations. And finally the route planner could successfully generate the optimal route and is capable of distinguishing gaps that are large enough regardless of the orientation of the gap. The Localisation unfortunately proved unreliable tests reveal that the fault falls with the update Sensor phase of the Monte-Carlo and is due to not enough of the visual information being used to compare the scene as obstacle type is not taken account of.

5 References

FIRA. (2011, June). Retrieved from www.FIRA.net

Malis, E., & Vargas, M. (2007). *Deeper understanding of the homography decomposition for vision-based control.* INRIA.

Rofer, T., & Jungel, M. (2003). Vision-Based Fast and Reative Monte-Carlo Localization. *Robotics and Automation (ICRA-2003).* Taipei.

WillowGarage. (2011, May). *OpenCV Documentation*. Retrieved from http://opencv.willowgarage.com/documentation/

Yong, K., Hwang, & Narendra, A. (1992). A Potential Field Approach to Path Planning. *Robotics and Automation Volume 8* .

ICub Simulation: The Modi Experiment

B.Gaschignard and A.Cangelosi

School of Computing and Mathematics, Plymouth University, Plymouth, UK

Abstract

This document presents a summary of the work done for the MSc Project. The purpose was to re-create the "modi" experiment. It gathers most of researches made, explanation of problems met and algorithm programmed in the purpose to re-create the "modi" experiment by using a humanoid robot, the iCub robot. It also explains behaviour expected and actions finally observed by the achievement of the experiment by using the iCub simulator and Aquila, a graphical user interface which provides to communicate in an easiest way with robot simulated. Finally, results will be discussed; comparisons will be done to try to extract what have been concluded at the end of the realisation of the modi experiment.

Keywords

Humanoid robot; neural network; movement detection

1 Introduction

Nowadays, communications are more and more important. With the technologies available today, the number of data exchanges each day does not stop to increase. Because people get used to communicate through natural way by using senses like the view and the hearing, robot has to be adapted with these types of communication. Humanoid robot proposes solution to communicate with the user due to voice recognition. The point is they have to be able to learn by themselves for their experiences.

The aim of the project is to re-create the modi experiment. The experiment is very similar to a situation of language learning for a child. The purpose is to teach a word to the robot. This word is associated with an object. For doing that, the system is based on a neural network algorithm. This type of algorithm allows system to learn from its sensors and situation it has to face.

2 Background

The project aim is to reproduce the 'Modi' experiment with the simulation software of the iCub. The iCub is humanoid robot designed with a size of a 3.5 years old child. He was created in 2004 to support different project. It is the support of cognitive science researches and artificial intelligent experiment. The 'Modi' experiment is clearly explained by researchers and professors from the University of Plymouth. "Two different objects [are showed] in turn, one consistently presented on the left, and the other consistently presented on the right. Following two presentations of each object, the child's attention is drawn to one of the now empty

presentation locations and the linguistic label “modi” is presented. Finally the children are presented with both objects in a new location and asked; “can you find me the modi”.” (A. F. Morse); The purpose of this project is to recreate this experiment with the iCub simulator.

The system is constituted by three main parts. The first part corresponds to the vision motion detection algorithm. Secondly, there is the voice recognition part of the system. The third and last part is the neural network side of the project.

2.1 Motion detection and tracking

The motion detection will be done when the robot keeps a static posture. Motion cannot be directly observed but can be perceived by detection of intensity changes. “Motion detection algorithms are often based on the differencing operation of image intensities between each frame and background image.” (Remagnino, 2001). The idea is to calculate differences of parameters’ values of pixel between two consecutives images. Then, a threshold will be used to avoid detection of noise. The appropriateness of the threshold’s value chosen directly influences the reliability of the algorithm. Gaussian and Laplacian models can also be used to reach this purpose. Those methods consider that the texture of background is difference enough from texture of moving objects to let motion detection. Other researchers focus on models which detect movement by “measuring the amount of texture change”. As they explain, “we measure the amount of texture change and classify it into two categories: moving and stationary objects. The […] situation in which the background texture and the texture of moving objects are similar illustrates a typical situation in which the proposed approach outperforms any background modelling method.” (workshop, 2001).

The detection of movement will let to keep the iCub attention on an object. Then, the iCub will have to follow movements of this object.

2.2 Speech recognition

The purpose of speech recognition is to analyse a sentence said by a human. The translation must allow obtaining a text corresponding with the words pronounced by the user of the system. This is possible due to signal processing and artificial intelligent methods. The sentence is recorded within a numeric format, then, the voice recognition software categorizes phonemes according probabilistic model. Then, according to a statistic model, word are recognise.

The paper about the “modi” experiment proposes to use the open source CMU Sphinx library for this part of the software. (A. F. Morse).

2.3 Neural Network

The system will use a neural network algorithm. “Artificial Neural Network refers to computing systems whose central theme is borrowed from the analogy of the biological neural networks.” (Mehrotra, Mohan, & Ranka, 1997). Indeed, the idea is to re-create the neural network structure of an animal or a human nervous system.

The biological inspiration comes from the fact that we use neurons are simple computational device. All those devices are connecting between themselves thereby creating an artificial neural network. Each of those units has several inputs come from neighbours or external sources. They use them to compute an output signal which is then propagated to others devices. Each connection has a weight characteristic which also affects the behaviour of the neural network. Due to the fact that each node can compute in the same time, neural network are parallel computational models.

One of the main appeals of using a Neural Networks is its ability to learn. Indeed, a system which has the possibility to learn by itself from training and experiment might be able to achieve much more complex task that a basic system could do. (Saad, 1998).

The Second main appeal in Neural Network algorithms is their generalisations abilities. "The far more interesting quality definitely is the generalization capability, i.e. the ability that the network produce the desired output given previously unseen input data" (Lavrac, Wrobel, & European conference on machine, 1995). It means that the Neural Networks system must be able to compute and produce reasonable outputs for unknowing input.

2.4 Self-Organisation map

In the field of neural network system, they are Self-Organisation map algorithms. They belong to unsupervised learning categories of neural networks. Just the input is used in the algorithm to learn without any set output goals. Usually, they create a two-dimensional representation of the input. The main advantage of using this kind of algorithm is that "the self-organizing map (SOM) is a neural network model that is capable of projecting high-dimensional data onto a low-dimensional array."(Obermayer & Sejnowski, 2001). Another advantage of this low dimensional projection is that it can be easily represented by a colour map. This map is also called Kohonen map in referring of the Finnish professor and academician who made several researches in neural network algorithm

"In the pure form, the SOM defines an "elastic net" of points (parameters, reference, or codebook vectors) that are fitted to the input signal space to approximate its density function in an ordered way. The main application of the SOM are thus in visualization of complex data in a two-dimensional display, and creation of abstraction like in many clustering techniques." (Kohonen, 2001). The other characteristic of SOM is that activity of nodes resulting of an input vector will affect the map. Indeed, the winning node, which has the highest activity, will have its weights changed but also weights of neighbourhood nodes.

2.5 Hebbian learning

In the "modi" experiment, the self-organisation map algorithm is complete by the Hebbian learning method. It is a similar idea that the neighbourhood function. Information contains by two different maps can be gathering in one other matrix with the Hebbian learning. The important idea is that Daniel Hebb "stated that the

information can be in synaptic weights." (Gupta, Jin, & Homma, 2003). In the "modi" experiment, maps which contain main information in their weights will be associated or merge to let the connection of key data.>

3 Software implemented

3.1 The simulator

Because the purchase of a real iCub robot is an important financial invest, a simulator have also been developed. This simulator, called iCub simulator, have been used. To control this simulator, Aquila, an open-source project which has been developed by Martin Peniak and Anthony Morse, is also used.

3.1.1 Graphical User interface

The graphical tool offers a wide type of command to use the iCub simulator. For this experiment, a new tab was created and had to gather all the important command in a same frame. This tool presents several elements belongings to three categories. The first one brings together elements which give some information about the state of the system. They are active elements. The second one is constituted by action button. These buttons create an event when the user clicks on one of them. Each button is associated with a specific function which its call at each button event. The last category corresponds with buttons which have much more a passive impact in the progress of the algorithm because their activation does not lead to a call function. Usually, they are used to set a variable, action a flag or change the value of a parameter.

3.2 Algorithms

3.2.1 Movement detection

The movement detection is the first part of the algorithm. ICub's cameras contently scan the landscape and give a frame of what the iCub is looking. The idea is to compare the new image just captured with the former one. Head and eyes of the robot are fixed. So if a pixel have its colour changed, that means that something has moved in front of the iCub. To detect changes of pixel's colour, the difference of values of each RGB's pixel component between the two images recorded are computing. Theoretically, if this difference is null, the colour of the pixel has not changed and we can conclude that anything have moved. In practical cases, there are some noises due to luminosity's changes or because the iCub moved a little bit. A threshold has to be applied to delete noise. Then, a small pixel's colour change will not be recorded but object's movements will be detected.

The problem with this algorithm is that as soon as the iCub start to move either his head or even just one part of its body, the image's frame recorded will completely be changed. The all image will then detect movements. This movement detection is not wrong because the iCub is moving. But if we want to track an object and if this object is not fixed, another algorithm need to be developed. Indeed, the movement of

the object moving in the same time that the iCub is moving will be detected but in a fog a movement's detection.

There are two solutions possible to track an object moving. They are both based on detecting the colour of the object. As soon as an object is detected, the colour of this object is saved. Then, two options are proposed. Either this colour can be used to filter this image to obtain a new image. This new image is made just made just by black and white pixel. Black pixels contain the information of the movement. Or it can be used to find the coordinates of the object in the new frame.

In my case, I decided to scan all pixels and compare each RGB values with RGB values of the objects detected. When I have founded it, I have the coordinates of one side of the moving object. I can then track it.

3.2.2 Speech recognition

The speech recognition part of the system has not been implemented. However, most of elements necessary to control the speech recognition part of the system have been integrated in the graphic user interface.

3.2.3 Self-Organisation Mapping

As already explain above in this thesis, the neural network part of the system is the key part in the implementation of the software. As in speech recognition, in the field of neural network, several libraries are available to set up quickly a neural network algorithm. None of these libraries have been us for the project. All neural networks function has been again completely implemented.

In the software, the base of neural network is constituted by two first self-organisation maps. One is used for the colour detected and the other is used the posture of the iCub. Both colour map and posture map, also called body map, works on the same principle. In a first time, they are trained with input vector data. In a second time, they are used to find the modi. For the colour map, input vectors corresponded with the colour parameters of the pixel pointed. Concerning the posture map, they are usually four values, corresponding to data needed to describe robot's posture.

Two other matrixes are used in the system. They are the result of the Hebbian learning between the colour map and the body map for one of them, and between the body map and the word map.

4 Results

4.1 Capture the attention of the robot.

The motion detection and the tracking part of the project let the robot to obtain numeric colour information that we need to match with a word. With the graphical user interface, an object is put in a moving state in order to be detected. The program

saved corner's coordinates of the rectangle corresponding of the area in which the object has moved. This rectangle is drawn on a frame to observe the delimitation of the image's area which has change. The point is that the matrix representing the image captured is refreshing each T second. During this time, the object can move more or less. If the movement is not so important, we can consider that, by saving coordinates matching with the center of the square detected, we saved coordinates of the center of the object moving. But, for instance, what happened if a cube move vertically up to three times it height during a T time. The middle of the rectangle drawn will point not on this object but on the background.

To avoid this error, a modification can be done in the program. The delta time use to refresh the image can be reduced. But the processing of the program will be heavier because the computing to refresh image and detect movement will be done more often. It will consume much more time and get the algorithm slow. Another solution is to save the background in a matrix. The new image is compare with the background matrix to see if an object is appeared. If this object was also detected at the same place in the former matrix representing the image captured, it means that the object is static. Otherwise, the object is moving and his colour can be saved. As usually, new problems appear when the robot is moving and the background don't match anymore with the real background that the iCub is observing.

Once the object has been detected, the robot can track it with his head and eyes with an algorithm based on the RGB colour model. In order to do that, the coordinate of the up left corner of the object moving are saved. The difference between coordinates of the central point and coordinates of the point found is calculated. It lets to know how much the robot need to move its head and its eyes to put the object in the center of its field of vision. When an object is animated and when the robot tries to track the object, a delay can be observed. Indeed, the moving object is never perfectly situated in the middle of the image because the robot is still late. To correct this shift, a moving prediction algorithm could be used. But it is not the real purpose of the experiment now studying.

4.2 Training self-organisation map

As explain above in the thesis, the first task to do before using the self-organisation is to train them. To test the efficiency of the training part, a checkbox "test SOM" have been had the graphical user interface to give input vector data with randomly values. These randomly chosen values are intended to create a random environment which the system could be facing. Self-organisation maps are so trained with all of these different input vectors.

Then, charts are made to observe the evolution of maps. Below, several graph represent the evolution of the state of each map for each weight between the beginning of the experiment, when map are randomly set up, and the end of the experiment, when map have been train.

In figures above, we see that weight x of each node of the body map have been randomly initialized. The second picture represented the map at the end of the experiment. Data input values used to train the map have been randomly chosen between -50 and 50. Indeed, this is the range that the x position of the robot's head

can have. We can easily see that the map has self-organised according to the value that were given as input. Each node have a specific weight x value. All x value are represented on the training map because the z-axis scale start from -50 and end at 50.

4.3 The modi experiment

After having a look on how the neural network of the system works, it is interesting to see how the system behaves when the purpose is to recreate the modi experiment. The protocol followed to recreate the modi experiment is the following.

1. The object number 1 is showed to the iCub on the robot's left. Then the robot detects the movement and track the object.

2. The object number 2 is showed to the simulated robot on its right. The object 2 is animating and the robot detects the movement to track the object.

3. The robot attention is drawn to one side, either to its left or to its right. The users click on the button "that" to simulate the word "modi".

4. Both objects are presented in front of the robot, which is a new location for them. But they are shown on the same side than before. Then the users click on the button "Find" to find the modi.

The experiment has been made ten times in row. For each time, the system has been able to find the "modi". The high percentage of success in the result let say that the system is very accurate and efficient.

5 Conclusion

Through this project, the "modi" experiment has been recreated. The two main part of the project have been in one side, to program the moving detection and the tracking, and in another hand, to code the neural network algorithm of the system. During the implementation of the project, different solutions for each part of the project have been written and tested to try to find the most suitable solution to reach the goal. But several problems have been met and to figure out most of them, new solutions had to be put in place.

The recommendation that could be made for possible future project is to start by implementing a simple solution of neural networks. For instance, it could be more efficient to start to take one weight parameter to each node of the body map and the colour map. It could be to clearly understand how the neural networks system works and behaves. It is quite important when results of the Hebbian learning function start to be analysed.

This project has shown how, in learning language, the posture is used to associate a word with an object. It supports this idea that human memory used former and old memories to fix new knowledge. Here, the body posture has a central role in learning a new word. It allows the system to make the link between two situations lived but which firstly seems to have anything in common. Once again, this experiment shows us how human, and particularly in this case, children behaviours can inspired the

design of system. Researchers have to carry on working on human cognitive science to bring out new system more and more efficient.

6 References

A. F. Morse, T. B., A. Cangelosi, L. B. Smith. Thinking With Your Body: Modelling Spatial Biases in Categorization Using a Real Humanoid Robot.

Gupta, M. M., Jin, L., & Homma, N. (2003). Static and dynamic neural networks: from fundamentals to advanced theory: Wiley.

Kohonen, T. (2001). Self-organizing maps. Berlin; New York: Springer.

Lavrac, N., Wrobel, S., & European conference on machine, l. (1995). Machine learning ECML-95 : 8th European conference on machine learning Heraclion, Crete, Greece, April 25-27, 1995 : proceedings. Berlin [etc.]: Springer.

Mehrotra, K., Mohan, C. K., & Ranka, S. (1997). Elements of artificial neural networks: MIT Press.

Obermayer, K., & Sejnowski, T. J. (2001). Self-organizing map formation: foundations of neural computation: MIT Press.

Remagnino, P. (2001). Video-Based Surveillance Systems: Computer Vision and Distributed Processing: Kluwer Academic Publishers.

Saad, D. (1998). On-line learning in neural networks: Cambridge University Press.

Workshop, M. l. a. d. m. i. p. r. s. i. (2001). Machine learning and data mining in pattern recognition : second international workshop, MLDM 2001, Leipzig, Germany, July 25-27, 2001, proceedings. Springer: New York.

Optic Flow Computer Vision-Based SLAM Mapping

J.Johnson and P.Culverhouse

School of Computing and Mathematics, Plymouth University, Plymouth, UK

Abstract

The aim of the project is to implement an algorithm to detect loop closure for a robot navigating in an environment. Loop closure is the task in which the robot is able to identify a previously visited area. In order to identify a previously visited area the robot should extract salient features from the image and maintain a database of these salient features. Every time a new observation is made by the robot the database is queried to check for loop closure. While the robot is travelling the position of the robot should also be tracked on a map using Optic flow. Optic Flow is a measure of how far a feature identified in the first image shifted in the second image. This displacement of the feature between the frames will give a vector known as the optic flow vector. This vector is used to analyse the motion pattern of the robot and create a map based on the optic flow vectors. These two tasks are important part in the Simultaneous Localisation and Mapping algorithms. The algorithm developed will add mapping capability to the competition robots.

Keywords

SLAM, SURF, Loop Closure, Optic Flow, OpenCV, Odometry, localisation, mapping.

1 Introduction

Human cognition and interaction with the environment has always inspired the robotic engineers over the past years. Vast amount of research are done to make robots and machines more interactive. As time goes by the machines started to interact and behave more closer to the humans. For example many of the primitive robotic systems were based on wheeled platform. These robotic systems are ideal for navigating on flat surface and is restricted to flat surfaces. But as the terrain gets complex, researchers and engineers took inspiration from the quadruped and Bipedal locomotion.

Modern day computers are capable of performing highly complex mathematical calculations and other sophisticated simulations within fraction of seconds. But on the other hand in a human perspective we can perform task like walking, running, grabbing an object, recognising faces etc. even as a part of our reflex action. But at the same time robots find them difficult for even stabilise itself and walk. This is mainly because the microprocessors which is the processing brain of the robots executes program sequentially line by line. But in case of human our brain is capable of simultaneously processing all our sensory inputs. The modern day alternative is using FPGA based processing where parallel task can be run at the same time and much faster.

The algorithm developed for this project adds mapping capability to the competition robot. The algorithm is also able to tackle the loop closure problem which exists in SLAM (Simultaneous Localisation and Mapping). The robot is able to identify previously visited scenes by searching through the database of stored key points. This project is inspired by the paper published by Newman(Newman and Kin, 2005). The implemented algorithm is also able to map the location of the robot in real time on a map using the principles of optical flow. The overall basic flow diagram of the system is illustrated in figure 1 below.

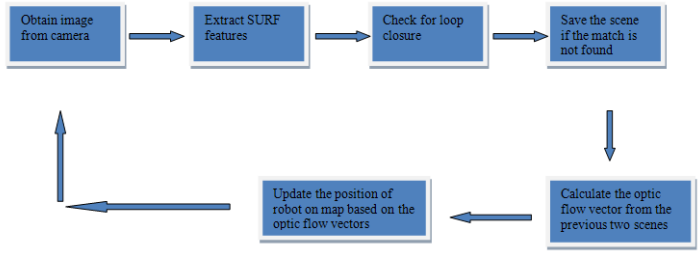


Figure 1: Overall block diagram of the implemented system

2 The existing system

The aim of the project is to improve the existing system implemented by Boimond Patrice (Boimond, 2010) . Boimond B (2010) developed a robust application using OpenSURF and OpenCV to detect loop closure and also avoid obstacle. OpenSURF is an open source library for detecting SURF features and was developed by Christopher Evans in 2009. The existing system captures a camera image and extract SURF features from it and stores it to an array of feature vectors. This process is repeated for three captures image.

From the surf descriptors of these three frames are matched to select only the robust features from the three images. A total of ten of the robust features is then chosen to from these three frames and is added to a floating point array. These ten robust features from the three images represent a scene. Now every time a new scene arrives the features are checked with the stored value in the array and would perform a nearest neighbour check and if the scene was not previously detected it will be added to a new location in the array and the scene index is increased. For an image size of 352x288 Boimond's code ran at a frame rate of here to four frames per seconds.

3 Loop Closure

Loop closure as described before is a problem which exist is SLAM where the robot has to identify a previously visited scene. Inorder to recognise the previously visited scenes the algorithm should be able to extract salient features from a scene. There are lots of method to extract features from an image like edge detector, corner detector, SIFT (Scale Invariant Feature Transform)(Lowe, 1999), SURF (Speeded Up Robust

Features)(Bay et al., 2006) etc. The important property of a feature descriptor is its repeatability. This means that the features have to be recognised again if the same scene is observed. The SIFT and SURF descriptors are two feature descriptors which satisfies the above requirements. The drawback of the SIFT method is that it uses 128 dimensional descriptor to describe a feature. This will increase the computational cost. Whereas SURF descriptors uses only a 64 dimension descriptor. SURF is computationally efficient and robust at the same time.

This property of the SURF features was the reason for choosing the SURF features. The image processing is done using OpenCV. It is an open source computer vision library originally developed by Intel in 1999. OpenCV version 2.0c was used for this project. The operating system used was LINUX Ubuntu 10.10.

OpenCV uses the function cvExtractSURF() is used to obtain the SURF descriptors from the image. After the execution of the function the descriptors and key points are stored in an OpenCV linked list data structure called the cvSeq. Once the descriptors and the key points are obtained the a nearest neighbour search is done using FLANN.

FLANN stands for Fast Library for Approximate Nearest Neighbour. FLANN is a library used for performing the approximate nearest neighbour search in a high dimensional space like a 64 element SURF descriptor spaces using various algorithms. A nearest neighbour search is an algorithm to find the closest point in a metric space. The SURF descriptors are used to compute the nearest neighbour check. The index of the successfully found descriptors between two scenes will be stored in a vector. A scene is identified if the FLANN algorithm identifies 40 points between two scenes. If a scene is found the program will report a loop closure. If it is a new scene then the descriptors are saved as an XML file and a floating point vector will maintain a time stamp of the detected scene. This time stamp can be used to check how long ago the scene was detected and also it helps to eliminate loop closure report for recent features. The typical time taken for OpenCV to extract features from an image is around 250mS. The maximum size observed by a saved descriptor XML file was around 16 KB. It is normally in the order of four to six KB.

4 Optic flow

Optic flow is a technique of motion detection, object segmentation, time to collision etc. Optic flow is a measure of the extent of changes of certain elements/features between two frames or it's the "*apparent motion of image Brightness*" (Bradski and Kaehler, 2008)(page 224). The concept of optic flow was first studied by James J Gibson in 1940. By computing the vectors that indicates the changes between the two frames the overall motion of the frame can be determined. Figure 2 below illustrates an example of optic flow, where a person moves his hand and the third image displaces the optic flow vectors which represents the displacement of the object between the first and second frame.

Figure 2: A simple example of optic flow, the third image represents the optic flow vectors (red lines)

The concept of optic flow can be easily visualised as a journey in a car. If a passenger looks forwards to the windscreen, the passenger will experience a flow of scenes. The objects closer to the road i.e. trees, fences and so on will appear to move backwards at a faster rate compared to a distant mountain or building. It can be noticed that as the car keep moving forwards everything in the vicinity of the passenger's field of vision will be moving outside. Objects that are on top appears to move upwards and points below will move more downwards , the points on right will move more to right and points to left will move further left in a nutshell the particles will move away from the centre of the field of vision. This point at the centre of the screen is called the focus of expansion or FOE figure 3.

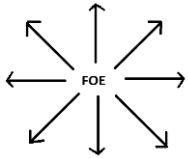


Figure 3: An illustration of focus of expansion, example of optic flow vectors for forward moving robot

The opposite of this phenomenon occurs when the car reverses. Then all the points in the frame appear to converge at the centre of the screen. But when the car takes a left turn then all the points in the frame appear to move to the right side as seen in figure4 below.

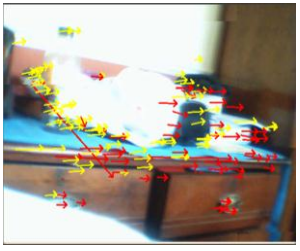


Figure 4: optic flow vectors pointing to right for a left turn

These are the basic assumption required from the optic flow vector to analyse the motion of a robot. The mapping is based on these two assumption:

a. The robot is travelling at a constant velocity.
b. The robot makes a turn at a constant rate and with a constant angle.

A SURF feature based optic flow is done between the two images. The direction and magnitude of the optic flow vector will give the information about the navigational property of the object. The robot is considered to move left only if the 90% of the optic flow vectors move to the right. This 90% optic flow assumption is done because even if the robot is moving forward or backwards the features on the side of the image will move more to the right or more to towards the left so that it will converge (moving forward situation) or diverge (moving backward situation) at the focus of expansion(FOE), but in this situations it is highly unlikely that the optic flow vectors will move in the same direction. So every time the robot acknowledges a right turn the angle of the robots position on the map is incremented by five degrees and the angle is decremented for a left turn.

To see if the robot is moving forward or backwards the angle of the vector is calculated using the *atan2()*. So if the robot is moving forwards the points below the FOE will move down this corresponds to a negative angle. So if the angle formed by the vector is negative then the robot is considered to move forwards. It is now obvious that if robot moves backwards the points below the FOE will move upwards making a positive angle. The position of the robot on the map is defined by the point *m1* and for a robot moving forward the position is updated as (*global_angle* is updated only when the robot turns):

*m1.x = m1.x + (y_average*sin(global_angle));*

*m1.y = m1.y -(y_average*cos(global_angle));*

for a reverse motion the points are updated as:

*m1.x = m1.x -(y_average*sin(global_angle));*

*m1.y = m1.y +(y_average*cos(global_angle));*

5 Observation

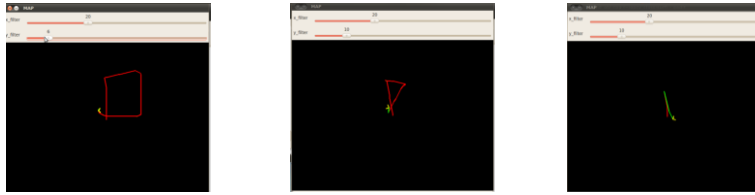


Figure 5: a- rectangular path, b- triangular path, c – to and fro in straight line

To test the algorithm the test platform used was a laptop mounted on a wheeled platform. The robot was taken for several course like a rectangular course, triangular

course and moving forward and backward in a straight line. The map created by the program is illusted in figure 5.a 5.b and 5.c

6 Discussion

It can be seen from the above figures that based on the assumption the mapping is done successfully by the robot based on the assumption of constant velocity and constant turn rate and turn angle. Basic filtering to avoid ambiguous mapping by a magnitude threshold. The robot will move only if the displacement of the optic flow vector is above the threshold value. The robot also report success loop closure for the above observations

The program can run at a rate of 7 to 10 frames per second only by performing the mapping. But when the loop closure part is implemented as the number of scenes in the memory increases the computation burden also increased. This is because the time taken to perform a nearest neighbour search will depend on how many scenes are stored and the number of descriptors in each scene.

The approach taken by Boimond (2010) saves the ten best descriptors from each scene, therefore this will reduce the computational burden. Since Boimond (2010) was using OpenSURF for performing loop closure and the code developed by the author was purely based on OpenCV, an optic flow algorithm was implemented on the program developed by Boimond(2010) using the openSURF. This algorithm can then be easily extended to perform the same mapping as the original code.

These are the naïve approach to solve the loop closure. In 2008 Newman(Cummins and Newman, 2008) developed an algorithm inspired by the bag of words feature matching technique and is called a FAB-MAP . This method is addressed as appearance based SLAM. The system is highly robust and can detect loop closure over a larger distance. According to (Cummins and Newman, 2009) the implemented system successfully detected loop closure over an area of 1000 Km. The efficiency of this algorithm is favourable reliable and fast and this is one of the major future development.

The competition robots use a wide angle camera and distortion is very common with a wide angle camera. In order to overcome this phenomenon the camera is calibrated using a chessboard. Upon calibrating the camera an intrinsic 3X3 camera matrix and a 5X1 distortion matrix is obtained. This is used to create an undistorted image. And this undistorted image was used to perform optic flow.

As discussed early the filtering of optic flow vector is done based on the magnitude threshold. An efficient method of filtering is by using kalman filter. It is an algorithm which is very efficient for system with noise and random nature. The kalman filter is able to estimate a close value the state depending upon the previous reading.

The Optic flow vectors were used to analyse how the robot navigated in an environment. But the odometry was not done completely from the optic flow vectors. It is possible to analyse how far the robot has travelled between the two frames based on the optic flow vectors. In order to understand how odometry can be

calculated a set of nine experiments was done. The optic flow vector is different at different distance. Although they all represents a same motion they are scaled by a factor. The factor increases with distance. Scale factor is the constant which is multiplied with the pixel values indicating the distance of the object from the camera, so that the actual distance will be obtained. Figure 6 indicates the observation of the first four experiments. It can be seen that the for a calibrated camera the scale factor increases linearly with the distance.

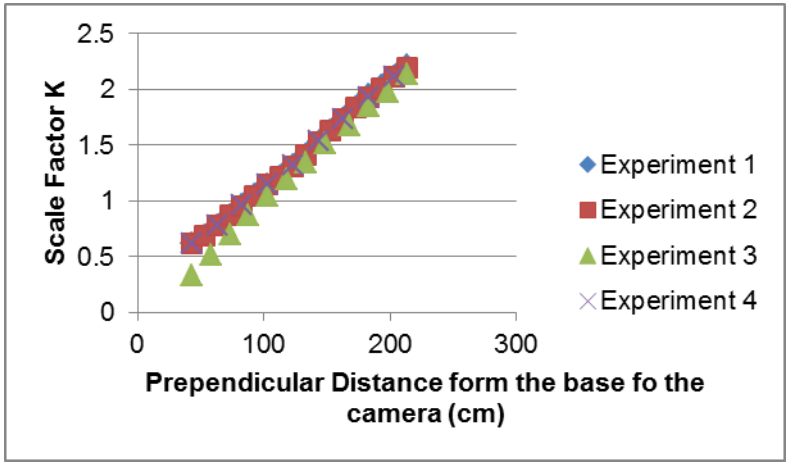


Figure 6: Experiments illustrating how the scale factor changes with distance

The BeagleBoard was also setup to run LINUX and was configured in such a way that it can be remotely accessed from a laptop through ssh.

7 Conclusion

A SURF featured based loop closure algorithm was successfully implemented using OpenCV on a laptop. The code written can be ported to the competition robot with minor changes to work on the BeagleBoard. The algorithm was also able to map the robot on a map based on the optic flow vectors. The system can be improved in future to improve the search method to detect loop closure using FAB-MAP (Cummins and Newman, 2008). The optic flow vectors also has to be precisely measured to obtain an accurate estimate of how fat the robot moved based on the optic flow vectors and from the observations of the experiments performed.

8 References

Bay, H., Ess, A., Tuytelaars, T. & Gool, L. V. 2006. SURF: Speeded-Up Robust Features *Lecture Notes in Computer Science,* 3951**,** 404-417.

Boimond P. 2010. *Plymouth Training Period report.* University of Plymouth.

Bradski, G. & Kaehler, A. 2008. *Learning OpenCV,* Sebastopol, O'Reilly Media Inc.

Cummins, M. & Newman, P. 2008. FAB-MAP: Probabilistic Localisation and Mapping in the Space of Appearance. *The International Journal of Robotics Research*.

Cummins, M. & Newman, P. 2009. Highly Scalable Appearance only SLAM- FAB-MAP 2.0.

Lowe, D. G. 1999. Object recognition from local scale-invariant features. *In:* Computer Vision, 1999. The Proceedings of the Seventh IEEE International Conference on, 1999. 1150-1157 vol.2.

Newman, P. & Kin, H. 2005. SLAM-Loop Closing with Visually Salient Features. *In:* Robotics and Automation, 2005. ICRA 2005. Proceedings of the 2005 IEEE International Conference on, 18-22 April 2005. 635-642.

Path Planning for Butler Bot using a Multiple-Timescale Histogram Grid

R.Merrison and G.Bugmann

Centre for Robotics and Neural Systems, Plymouth University, Plymouth, UK

Abstract

This report describes the development of a world representation and path planning system for use in an autonomous mobile robot that is designed to serve guests at social receptions held at the university. Existing approaches to this problem that are suitable for robots with limited sensors that operate in dynamic environments often make no attempt to utilize sensor data that is old or taken from parts of the map that are far away from the robot's current position. We present a system based on a histogram grid world representation that builds a map of the environment that stores both short-term and long-term data. The map is used with the A* algorithm to plan paths such that the short-term obstacle data is used to constrain the search to avoid obstacles and the long-term data is used to guide the algorithm into favouring parts of the map that are more likely to be free of moving obstacles. The system was tested using a simulated environment of similar size to the robot's intended environments and was found to produce good plans at high speed (tens of milliseconds per plan).

Keywords

Robotics, path planning, histogram grid, A*

1 Background

The Butler Bot (see figure 1) is one of the on-going projects that is being undertaken by the university's Robotics Club. The eventual aim of the project is to produce a robot that is capable of autonomously navigating around university receptions serving drinks and canapés to guests. Progress on the robot has been good: past and present students have created software that allows it to sense the weight of the items on its tray by analysing the oscillations of its body as it moves (Railhet et al., 2007); detect the locations of the people standing around it using facial recognition and stereo vision (Durand, 2010); localise itself in its environment using landmarks; and perform simple movement commands. One component that is still missing, however, is a system that allows the robot to build up a map of its environment and use this map to plan efficient paths to places the robot wishes to visit.

An enormous amount of work has been published describing different approaches to robotic path planning. The planning problem for Butler Bot is particularly tricky as the robot's typical environment is likely to contain a large number of obstacles (people) that move in unpredictable ways. The sensors available to the robot for sensing its environment are also somewhat limited, comprising three IR range finders on the front of the robot with a range of around 90cm and an ultrasonic range finder with a slightly longer range.

Existing approaches to path planning in sensor-constrained robots in dynamic environments typically stick to only storing information about the world in a small area around the robot's current position. This is because it is impossible to keep an accurate map the environment outside of the range of the robot's sensors because it is constantly changing. One popular approach to this problem is the Vector Field Histogram (VFH), originally described by Borenstein and Koren (1991). The VFH approach divides the world into a histogram grid of evenly-sized cells. Every time the robot's sensors see an obstacle the value of the cell(s) in the grid that corresponds to the obstacle are incremented. Cells' values are also decremented at a regular interval to ensure that the world map remains up-to-date. When the robot wants to move in a particular direction it converts the nearby cells' obstacle counts into a circular (or polar) histogram with the robot at the centre. It then finds all of the "valleys" in this histogram that are wide enough for it the pass through and selects the one that most closely matches its desired movement direction. The basic VFH algorithm has seen a number of modifications (Ulrich and Borenstein, 1998; 2000) that attempt to deal with some its problems, but the emphasis is always on representing only the area near to the robot.

Figure 1: Butler Bot

2 Our approach

2.1 Multiple-timescale histogram grid

We believe that all sensor data gathered by the robot is valuable and worth storing permanently in some form. Dynamic environments tend to contain many static obstacles, such as walls, that have a big impact on path planning. Remembering the positions of such obstacles can allow the robot to plan long routes more efficiently. Even sensor data received about dynamic obstacles that have subsequently moved can be useful in the long-run as their distribution across the map can be used to identify the busy areas of the environment (such high thoroughfare central corridors) and quiet areas (such as unused side-rooms). This information can be used to plan

routes that avoid busy areas and hence minimize the chances of a dynamic obstacle being encountered.

Our approach was based on a histogram grid representation of the world that was similar to that used with the VFH algorithm. However, we chose to store two values for each cell. Both of these values represent the same thing, namely the proportion of sensor readings that have sampled the cell and indicated it contained an obstacle. However, one of the values was considered short-term and decayed to zero over time whilst the other did not decay and retained sensor information permanently. The short-term histogram values therefore stored information about the obstacles near to the robot that it had sensed recently, while over time the long-term values came to represent an obstacle density distribution across the map. Permanent obstacles such as walls have a value close to 1.0 in this map, whereas areas that contain dynamic obstacles have a value between 0.0 and 1.0 that indicates how crowded they generally are.

The grid-based representation of the world was used for more than just path planning in our Butler Bot control program. The robot also used it to remember the last time it had attempted to serve guests at each location in the map, allowing the higher-level action planning to operate on the same world representation as was used for path planning.

2.2 Path finding algorithm

A common way of finding paths in a grid-based representation of the world is the so-called "grassfire" (or "brushfire" or "bushfire") algorithm. This algorithm works by numbering cells. The starting position of the path is labelled zero. The non-obstacle neighbours of this cell are labelled 1; their neighbours are labelled 2, and so on until the goal cell is reached. A path can then be found by starting at the goal and repeatedly moving to the neighbouring cell with the lowest labelled value. This algorithm is sometimes also called the "wave-front" algorithm, as the values expand outwards from the starting position like a wave moving across the map, breaking around obstacles.

For graph-based, rather than grid-based, world maps the uniform-cost graph search algorithm can be used to find the shortest path from one node to another (Russell and Norvig, 2010, p.91). This algorithm works by starting at the initial node and maintaining a set of unexplored edges that lead from explored nodes. Each iteration of the algorithm explores the edge in this set that has the lowest total path cost. This repeats until an edge is explored that leads to a goal node. It is clear that this algorithm will always find the shortest possible path to the goal, because if a shorter path were to exist than the one that was found then this would have been explored first.

A simple transformation can be used to turn a grid-based map into a graph-based one. A node is created at the centre of each non-obstacle cell in the grid. These nodes are then linked to their adjacent nodes in either 4 or 8 directions. Path planning over the resulting graph using the uniform-cost algorithm is in fact equivalent to using the grassfire algorithm on the original grid-based map.

The disadvantage of both grassfire and uniform-cost is that they take a reasonably long time to execute. This is because they have no particular information about which direction they should be moving in in order to reach the goal; the wave-front expands evenly in all directions. The A* algorithm is a very popular graph search algorithm that is similar to uniform-cost except that it uses a heuristic function to guide its search through the graph. When used for path finding the absolute Euclidian distance between a node and the target node is a very effective heuristic that allows A* to find paths quickly.

Our approach used the A* algorithm to plan over a graph generated from the histogram grid. Nodes were created in the graph for all cells except those with a short-term obstacle confidence greater than a fixed threshold. This meant that the robot would not include any cells where an obstacle had been seen recently in its path finding process. The path costs of the edges leading out of some cell C to its neighbouring cells were calculated as the distance between the centre of the neighbouring cell and the centre of C, plus the long-term obstacle confidence of C multiplied by some constant scalar.

With this scheme the short-term memory (which is likely to be most reliable) acts as a hard block on the paths that can be found. The long-term memory, however, has a softer effect in that it simply encourages paths to be chosen that avoid areas of high obstacle confidence. It is not possible for an unfortunate set of observations of moving obstacles to cause the robot to get permanently walled in by imagined obstacles because only the short-term memory imposes hard limits on the paths that can be chosen and this memory fades as time goes by.

In practice it was necessary to make one small modification to the algorithm described here. The A* search was actually prevented from exploring any cells that were within a small distance of the cells that were marked as obstacles in the short-term memory. This was done so that the path planning took into account the size of the robot's body. By effectively "growing" obstacles in this way we can ensure that the robot keeps a safe distance away from them.

2.3 Testing Methodology

Unfortunately the real Butler Bot robot was not available for us to test our algorithm on. Instead, a simple simulator application that was developed as part of our project was used. This allowed the placement of arbitrary static and dynamic obstacles and simulated the robot's sensors in a reasonably basic fashion. A map was designed that consisted of four rooms, with a horizontal corridor separating the top two rooms from the bottom two (see figure 2 overleaf).

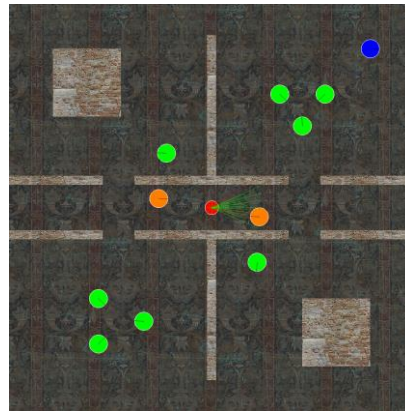


Figure 2: The test environment as shown in the simulator

This map has a connecting door between the top two rooms and another between the bottom two rooms. Additionally, two of the rooms have a large solid obstacle in their centre. The smaller circle in the centre of the image is the robot and the lines protruding from it are rays being cast to simulate its sensors. The two circles in the corridor near the robot are moving obstacles that continually walk backwards and forwards in the corridor, simulating a busy area. The circle in the very top right is the robot's tray refill area that is invisible to sensors. The remaining circles are static guests. Based on the size of the robot this environment represents a room of approximately 144m^2, which is roughly the size of some of the smaller reception areas available at the university. The size of each cell in the histogram grid was approximately 13cm x 13cm.

Testing consisted of repeatedly letting the robot explore the space starting with a blank histogram grid each time. The quality of the map that was produced and the paths that the robot chose to follow were examined.

Cell-based map representations have been criticised as being computationally inefficient (Thrun and Bücken, 1996) and so data was gathered about the time taken to perform path finding queries. The testing hardware was a laptop with an Intel T5750 Core 2 Duo 2.0GHz CPU with 3GB of RAM running Windows XP.

3 Results

Figure 3 below shows the robot's representation of the world that was built up after exploring the environment for around thirty minutes. The cells are shaded according to their long-term obstacle confidences. Blocking obstacles from the short-term histogram grid have been circled and a path that the robot has planned to a goal cell (marked with a *) is shown with arrows.

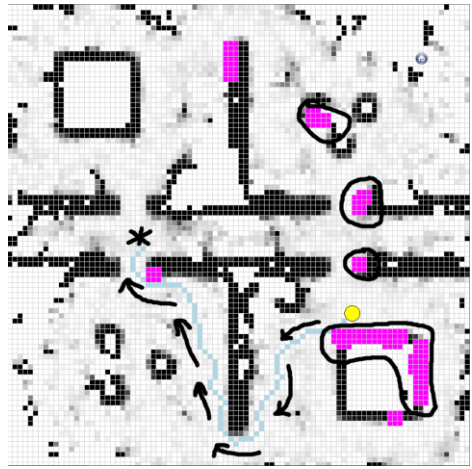


Figure 3: The robot's representation of the world after 30 minutes of exploration

Notice how the long-term histogram grid has produced a very accurate map of the static obstacles in the environment. It has also correctly identified that the central corridor is a relatively busy part of the map. As a result of this it can be seen that the path planner chose a longer route in order to avoid the corridor as much as possible.

Performance data was also good, with the average and maximum times taken for a single path finding query over the whole run equal to 3.3ms and 86ms respectively. This allows queries to be executed very often, allowing the robot to respond quickly to new sensor data. The memory required to store the map is estimated at approximately 415kB. The weakness of a cell-based approach to world representation is that the number of cells (and hence memory and CPU requirements) increases non-linearly as the dimensions of the world increase. However we have tested the system up to room sizes equivalent to $325m^2$ (the largest reception room size the university offers) and found performance to still be more than acceptable for real-time use.

4 Conclusions & Further Work

We have described a system for world representation and path planning that offers the advantages of both long-term global maps and short-term local maps. Our algorithm prevents dynamic obstacles from forming permanent barriers in the robot's memory by using long term obstacle data only as a guide to the path planning algorithm. Collisions with nearby obstacles that have been observed recently are prevented by using short-term decaying data to impose hard limits on path finding. Our experience was that for the typical kinds of environment that Butler Bot operates in a cell-based map of the world does not cause any problems in regard to CPU or memory usage. In our

Further work in this area should involve a closer examination of the effect that the system's variables have on the performance of the robot. The three variables that are

of most interest are: the rate at which cells in the short term memory decay; the obstacle confidence threshold for short-term memory cells becoming blocking obstacles; and the constant scalar that is used to convert the long-term cells' obstacle confidences into path costs.

5 References

Borenstein, J. and Koren, Y. (1991), "Potential field methods and their inherent limitations for mobile robot navigation", In: Proceedings of the 1991 IEEE International Conference on Robotics and Automation, Sacramento CA, USA, 9th-11th April 1991, Vol. 2, pp.1398-1404

Durand, J. (2010), "Face detection for Butler Bot", M.Sc. thesis, University of Plymouth

Railhet, S., Wolf, J., Adra, A., Kabbara, R., Deshmukh, S., Garghouti, M., Nash, G., Belpaeme, T., Culverhouse, P., Robinson, P., White, P. and Bugmann, G. (2007), "Sensor systems in a compliant geometry robot: Butler Bot", In: Proceedings of Taros '07, Aberystwyth, UK, pp.176-181

Russell, S. and Norvig, P. (2010), Artificial Intelligence: A Modern Approach, 3rd Edition, Pearson, New Jersey, ISBN: 978-0-13-207148-2

Thrun, S. and Bücken, A. (1996), "Integrating grid-based and topological maps for mobile robot navigation", In: AAAI (Association for the Advancement of Artificial Intelligence), In: Proceedings of the 13th National Conference on Artificial Intelligence, Portland OR, USA, August 1996

Ulrich, I. and Borenstein, J. (1998), "VFH+: Reliable Obstacle Avoidance for Fast Mobile Robots". In: Proceedings of the IEEE Conference on Robotics and Automation, Leuven, Belgium, 16th-20th May, 1998, Vol. 2, pp.1572-1577

Ulrich, I. and Borenstein, J. (2000), "VFH*: local obstacle avoidance with look-ahead verification", In: Proceedings of the IEEE Conference on Robotics and Automation, San Francisco CA, USA, 24th-28th April, 2000, Vol. 3, pp.1572-1577

Humanoid Robot Localisation

N.Michel and P.Culverhouse

Centre for Robotics and Neural Systems, Plymouth University, Plymouth, UK

Abstract

There are many existing localisation techniques that differ in complexity and efficiency, but they all have the same objective: give exploitable position information. Among the various method developed, the Monte Carlo localisation is one of the newest and most efficient way of finding a position of a robot. It is simulated and used here to localise a robot on a football pitch. Combining the data from its camera sensor with a particle filter aims to give the robot a situational awareness and enables better strategy capabilities.

Keywords

Localisation, SLAM, Markov, Monte Carlo, Kalman, particle filter, landmarks.

1 Introduction

The aim of this research was to develop a localisation algorithm for the football humanoid robot team at the University of Plymouth. The robot used is a modified version of the Bioloid kit from Robotis; the CM-5 has been replaced by a more powerful CM-700 and a beagleboard has been added to run the high level processing.

This paper presents the different methods available to implement a localisation algorithm on an autonomous robot; and gives a justification on the choice of the selected technique. Then it provides details about the steps the algorithm runs through. This section is divided into the simulation part and the embedded part. Then a discussion on the results and further possible improvement is made.

2 Localisation methods

The localisation method will depend on the mission to achieve and its specifications. There are different problems to face according to the choice of the technique used. Localisation method can be either relative or absolute, which means it is a relative or global problem solving. Its can also be differentiated by the type of detection, landmark or map based; and by the type of surrounding it will have to deal with, passive or active environment (Thrun *et al.* 2005).

The relative localisation method are sorted in two classes depending on the type of sensor used to collect data, the common point however is the lack of need for any kind of landmark. This kind of localisation is named *dead reckoning*. The first method, called odometry, is commonly used on wheeled robots, as it is a simple and cheap system (Negenborn 2003). It only requires wheel encoders and a kinematic model to estimate its own position. The counterpart is a low tolerance to difficult

grounds and to shocks. The second method called inertial navigation is currently in use in submarines (Brain). It relies on gyroscopes and accelerometers to track the position when moving. However there are disadvantages in relative localisation: firstly it needs to know its starting position, as it can only keep track of its location by following the movement of the system; secondly it accumulate error over time making this method inaccurate in long-term estimations.

Absolute localisation methods solve the global localisation problem. It can work without a prior knowledge of its initial position, can be landmark based or map based. Landmarks can be either passive or active, in case of passive landmarks the robot have to detect by itself the landmarks so is will be able to triangulate its position (Betke *et al.* 1995). In case of active landmark, called beacons, the robot only receives a signal and can perform either triangulation or a trilateration (Singhal 1997). The GPS is an example of localisation using beacon and performing trilateration. Map based methods work by extracting features from the environment and by processing a map that can be topological or geometric. This kind of method requires a lot of processing power and need more time than other absolute localisation techniques.

Simultaneous Localisation And Mapping technique, called SLAM, is used to create the map of its environment and localising itself at the same time (Nebot 2002). The great advantage of this method is the real autonomy of the robot, which does not need a prior knowledge of its surrounding. The disadvantage however is the complexity of such algorithms. The SLAM technique is one of the more challenging methods of localisation.

3 Implementation

3.1 Simulation

The simulation part displays a pitch and simulates a real robot and its estimated position, which is the result returned by the localisation algorithm. The user places the robot on the pitch then can control it by its speed and turn values.

The localisation algorithm is based on the Monte Carlo method. This is a particle filter updated each time the robot moves. The process runs through 3 steps: prediction phase, update phase and re-sampling phase.

A set of 1000 sample points, the particles, is placed in the initialisation phase with random coordinates and random orientations. A probability value is assigned at each point with the same normalized value: the some of theses value is equal to one.

The prediction step updates the coordinates of all points when the robot moves. Each point will then move the same distance the robot does but from their own position and with their own orientation.

The update phase does not change the position of the point but their probability value based on the value returned by the sensor. In this simulation it determines if the robot is standing on a line by only watching the colour of the pixel it is standing on. If it

detects it is on a line then all particles out of a line see their probability set to zero. The probability of the remaining point is increased in the same time in order to keep the sum equal to one.

The re-sampling phase move all the zero-probability points close to the non-zero-probability ones. Each time a point is moved its probability value is restored and the probability from all the other point is equally decreased to respect the normalization rule. 80% of the moved point is displaced near a high probability one. The point with the highest probability is the first one to attract particles, then the second one, etc… 20% of the moved point is replaced randomly on the pitch in order to solve the kidnapped robot problem.

3.2 Integration

A first difference with the simulation is the use of the visual input. The second one is the reset to zero probability of any point that get out of the pitch during the prediction phase. They will then be considered as false points and be moved during the re-sampling phase.

In order to proceed tests some new control functions have been added. A camera control mode allows the user to choose the right angle of the camera by changing the *pan* and *tilt* parameters. This is done by the arrows from the keyboard and controls the two servos of the head. The second feature is a robot controller function that allows the user to change the speed and the turn of the robot on the pitch by using the arrows from the keyboard. It works the same way as the simulation did by with the difference that pressing the left and right arrows doesn't change the angle but the angular speed. That does mean it will keep turning even the turn key has been pressed once; to stop turning it is possible to use either the right-shift key to reset the turn to zero or to press turn on the opposite other way.

4 Results

When the robot is replaced, we face the kidnapped robot problem. When re-sampling phase is active 20% of the moved points are randomly placed. However if there is not point with a zero-probability value there is no randomly placed points, as a consequence we have to wait until the robot sensor changes state to get a new re-sampling. For instance if the robot is on a line, the algorithm will have to wait until it gets out of the line to enable the re-sampling phase.

Due to the nature of a football pitch, we can expect symmetry problem while localising. However the simulation only rarely showed signs of this issue. The solution came from the use of integer values for the calculation of new coordinates; even if float are used for the sine and cosine at some point only integers are returned. This causes a lack of accuracy in the motion of the points within the simulation and slightly reduces the efficiency of the localisation algorithm, but it offered an unexpected and cheap solution to avoid the symmetry problem.

The robot may be subject to be manually repositioned, because of a fall, a failure of the video input, or it went out of the pitch, or any other reason. Because it needs to

be able to recover from such situation, it has to solve the kidnapped robot problem. Tests made proved it was able to recover, however the recovery speed highly depends on the number of particles. The price to pay for a fast recovery is slowest global performances of the localisation algorithm. Experiment made with 2000 points instead of 1000 showed a recovery at least twice as fast but with huge slowdowns when crossing lines due to massive re-sampling.

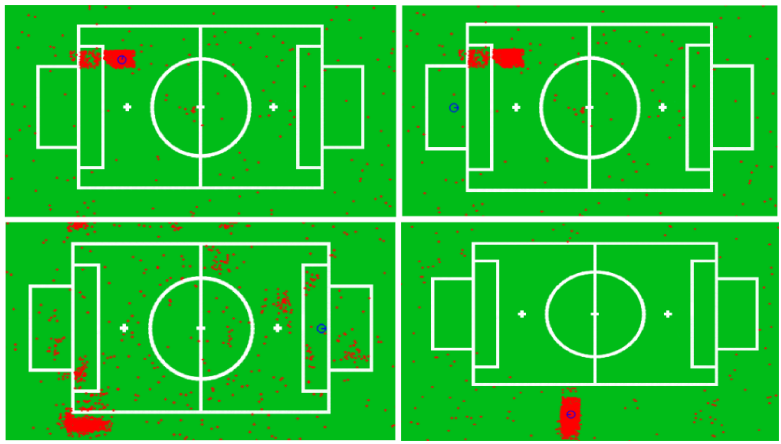


Figure 1: Kidnapped robot problem

Tests were made where the robot was localised (Figure 1, upper-left) then it was moved to another position. The localisation algorithm misplaces the robot (Figure 1, upper-right), but when it moves and cross whites lines particles positions are changed to random places within the re-sampling phase (Figure 1, lower-left). Then after some time the robot finds back its actual position (Figure 1, lower-right).

5 Conclusion

The primary objective, localise the robot, is completed, however reliability can still be improved. The Monte Carlo localisation is a good choice for the hardware capabilities provided. It is the good balance between the computational requirements and the quality of the results returned. With a better processor, it would be possible to increase the speed and accuracy of the localisation algorithm by processing a larger number of particles.

6 References

Betke, M., Gurvits, L. (1995) 'Mobile Robot Localization using Landmarks', Laboratory for Computer Sciences, Massachusetts Institute of Technology.

Brain, M., Freudenrich, C. 'How Submarines work', http://science.howstuffworks.com/transport/engines-equipment/submarine4.htm (Accessed 12th August 2011)

Nebot, E. (2002) 'Simultaneous Localization and Mapping: 2002 Summer School', Australian Centre for Field Robotics, the University of Sydney.

Negenborn, R. (2003) ‘Robot Localization and Kalman Filters: On finding your position in a noisy world’, Institute if Information and Computer Sciences, Utrecht University.

Singhal, A. (1997) ‘Issues in Autonomous Mobile Robot Navigation’, Computer Science Department, University of Rechester.

Thrun, S., Burgard, W., Fox, D. (2005) ‘Probabilistic Robotics’, MIT Press.

Author Index

Advances in Communications, Computing, Networks and Security

Volume 9

Edited by
Paul S Dowland & Steven M Furnell

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

The publications in this volume are based upon research projects that were undertaken during the 20010/11 academic year. A total of 24 papers are presented, covering many aspects of modern networking and communication technology, including security, mobility, coding schemes and quality measurement. The expanded topic coverage compared to earlier volumes in this series reflects the broadening of our range of MSc programmes. Specifically contributing programmes are: Communications Engineering and Signal Processing, Computer and Information Security, Computer Science, Computing, Network Systems Engineering, and Robotics.

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

RESEARCH WITH PLYMOUTH UNIVERSITY

ISBN 978-1-84102-320-5 90000
9 781841 023205