Selected Computing Research Papers

Volume 4

June 2015

Dr. S. Kendal (editor)

Published by
the
University of Sunderland

Edited, typeset and printed by
Dr. S Kendal
University of Sunderland
David Goldman Informatics Centre
St Peters Campus
Sunderland
SR6 0DD

Tel: +44 191 515 2756
Fax: +44 191 515 2781

Contents Page

A Critical Study of Current Natural Language Processing Methods for the Semantic Web

Lee Bodak

Abstract

The emergence of semantic web service orientated architectures has inspired various aspects of research into Natural Language Processing methods. Many of these methods aim to increase the recall accuracy and precision of query responses from web services. This paper considers three such methods; Keyword Clustering, Short Text Queries and Keyword Discovery, and proceeds to evaluate and compare each of them. Conclusions show that a combination of two of these methods would provide the most efficient NLP method for web semantic discovery.

1 Introduction

In recent years, there have been great advancements in how technology processes the natural language. Natural Language Processing (NLP) methods are present in all aspects of today's technology, allowing more complex interactions between humans and computing devices. However, "NLP is a large area of research and application, with numerous research problems and approaches" (Crowston et.al 2012).

Workman and Stoddart (2012) explain how NLP data retrieval suffers from a lack of data validity due to misrepresented Natural Language (NL) queries, as well as a slow processing speed in the retrieval of query results. Additional research into data retrieval is being carried out by Maxwell and Schafer (2010).

A lack of robustness persists in the implementation of NLP in web applications, and research is being carried out to improve the capabilities and performance of these web apps through NLP principles (Sateli et al. 2013).

Sivagar and Chaitanya (2014) focused their research in web based NLP, which aims to improve the accuracy and validity of responses generated from user inputs. Additional web based NLP research is being carried out by Shafi and Ali (2012).

This survey paper will take a critical look at current issues present in semantic web NLP and evaluate three proposed methods by researchers in order to reach scientific conclusions.

2 Web Semantics & NLP

The semantic web enables users to find and share information more easily. The implementation of NLP in web semantics is currently being researched in various forms including:

- Keyword Clustering
- Semantic Similarity in Short Texts
- Keyword Discovery Process

2.1 Semantic Web Service Discovery Framework – Keyword Clustering

Gunasri and Kanagaraj (2014) aimed to improve the reliability and recall performance of responses generated though NL queries when searching for web services. They focused their research on keyword clustering by implementing the Semantic web service discovery framework (SWSD).

Two algorithms were created in order to test the feasibility of keyword clustering with the SWSD. The first algorithm, finding cluster terms, works by taking a keyword parameter from the NL input and clustering it together with results that contain said keyword. The second algorithm, semantic matching, uses a linear combination to combine similar aspects of each component in the request and adding a weight (1 or 0) in order to rank the response.

Tests were carried out with these algorithms using 20 types of user queries matched with 30 types of web services. Each query was matched with at least one web service.

A graph was produced which shows the performance and accuracy of matching web services, some exact and some slight matches, and comparing the use of clustering techniques alongside standalone NL (see figure 1 below).

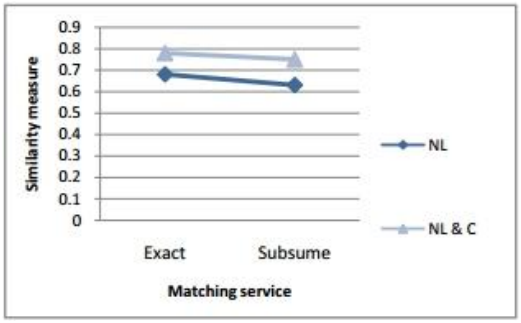


Figure 1 - Graph of Results - NL & NL with Clustering (Gunasri and Kanagaraj 2014)

Claims where made that compared with related service discovery methods, clustering based NLP grants the highest precision and recall and allows the most optimization of web service discovery.

The methodology presents a strong consideration of the implications of each service description language and how they may affect the framework, given their capabilities and limitations, before concluding which to use. The research that followed presented a clear understanding as to what they wanted to achieve and how they were going to do it; specifying how the algorithms they will be using will aid in monitoring the impact of keyword clustering opposed to an alternative method.

This presented a strong body of research which forms the foundation of the testing. The algorithm's formulas are based on earlier research into lexical keyword selection (Wu and Palmer 1994). The testing methods demonstrate good variation by taking a suitable amount of alternative user and web service types; 20 and 30 respectively, thereby using enough test data to produce reputable and repeatable results.

However, as the testing was both carried out and documented by the researchers themselves, opposed to an impartial body, the potential for bias in both the tests and results does exist. The graphs produced do accurately represent the results, yet due to the potential bias present in the testing, the graphs lose scientific merit.

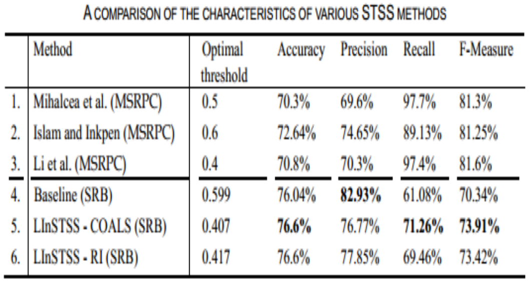
The NLP method demonstrated in this research shows improvements to recall accuracy against standard NL queries, yet the conclusions reached do not correlate with the testing demonstrated, as only one method was tested, yet the claims made state that this method provides the highest recall accuracy of all methods; therefore the conclusion can be made that this claim is not justified as further testing against multiple types of NLP methods is required before this claim is could be considered valid.

2.2 Language Independent Semantic Similarity in Short Texts

Furlan et al. (2013) produced research to improve how short text semantic queries are processed for highly inflectional languages, in this case, Siberian, as a lack of available resources outside of English are available. Current methods were analyzed and a new system called the Language Independent Short Text Semantic Similarity (LInSTSS) was proposed, based off a pre-existing statistical similarity method, developed by Mihalcea et al. (2006) and improved upon by Islam and Inkpen (2008).

The system consisted of two known algorithms; COALS and RI. They justify their choice by stating COALS achieves more consistent accuracy and RI as it is suitable for processing larger data sets. A paraphrase corpus (a group of sentences) in Serbian was produced, which they then ran through multiple matrixes against multiple web services, such as news headlines, which were then parsed into English and returned. These became sentence pairs and the foundation for testing.

To fully test the system, a larger sentence pair set called a Trading Data Set was produced. It consisted of 835 randomly selected sentence pairs, and was compared against a test data set, consisting of 359 set pairs. These sets where ran through the system in order to determine the accuracy of the resulting pars. A table of results was produced which compares the LInSTSS systems results against pre existing methods results (see figure 2 below).



A COMPARISON OF THE CHARACTERISTICS OF VARIOUS STSS METHODS

	Method	Optimal threshold	Accuracy	Precision	Recall	F-Measure
1.	Mihalcea et al. (MSRPC)	0.5	70.3%	69.6%	97.7%	81.3%
2.	Islam and Inkpen (MSRPC)	0.6	72.64%	74.65%	89.13%	81.25%
3.	Li et al. (MSRPC)	0.4	70.8%	70.3%	97.4%	81.6%
4.	Baseline (SRB)	0.599	76.04%	**82.93%**	61.08%	70.34%
5.	LInSTSS - COALS (SRB)	0.407	**76.6%**	76.77%	**71.26%**	**73.91%**
6.	LInSTSS - RI (SRB)	0.417	76.6%	77.85%	69.46%	73.42%

Figure 2 - Table of Results - LInSTSS accuracy compared to other methods (Furlan et al. 2013)

The claim was made that this approach to short text NLP generated the highest recorded accuracy, being just a few percent short of the maximal system accuracy at 78.27%. They also claim a significantly higher recall at the cost of a lower precision.

By using a pre-existing method (Mihalcea et. al 2006) and building upon it, we can determine that the methodology presented in this research is relevant and well developed. This previous method has high acclaim in the field, and has been previously adapted into further research by Islam and Inkpen (2008), so we know it is credible. The methodology also gained scientific merit by using a set of pre-existing results to justify their algorithm choice.

The tests they carried out were based on previous test results from earlier research, adapted to fit the sole criteria of this research, which further adheres to their relevance.

The quantity of data that was tested was substantial, involving 835 random selections of sentences. The use of random selection as well as high number of test data displays good science by ensuring that the results are both free of selection bias and are plentiful, allowing conclusions to be drawn.

The final results table includes results from a previous research project in order to compare, overall however this is redundant as the original results were from an experiment using the English language, whereas this experiment focused on Siberian, therefore the testing criteria would be different.

As the testing was carried out by Serbian researchers only, they would have a great understanding of the language being tested and therefore less prone to input errors in the test data, which could have lead to potential bias. This could have influenced the high recall value of the results as the system itself has not had to attempt to match errors in sentences that may appear with a user not fluent in Siberian.

The claims made are disputable due to the level of bias that may have been involved during the testing. The method itself provides an efficient way of processing NL, as longer text inputs are used just as much has standard keyword searching in the semantic web, and it requires no knowledge of a framework to implement and use.

Based on the claims of this research however we must conclude that these results depict information that is unreliable due to bias and they also compare against earlier results that are redundant.

2.3 Keyword Discovery Process – Web Services

Sangers et al. (2013) introduce a method to improve the accuracy of how users can discover web services linguistically, applying the SWSD framework and keyword matching NLP techniques. The SWSD engine approach is used which allows the searching of web service descriptions through defined keywords and filtering the results. The ontology language WSMO is used for this engine, allowing files to be parsed, read and written by an API. The engine will use 2 algorithms, sense matching and disambiguation.

Disambiguation allows words to be discovered and given an identifier based on a keyword. Sense matching takes the identified words from the disambiguation and produces a set of relevant web service results. The non – NLP lexical matching algorithm, Jaccard, was also included.

To test the engine, a repository of 35 WSMO web service descriptions was used. 61 test queries were performed against the repository, representing potential keywords a user may enter, and tested using both algorithms mentioned above. The 61 queries where split into 2 types, 33 represent preset web services and the remaining 28 represent non present web services. 2 sets where then produced, 40 queries used to obtain weights of the keyword matches in order to rank their relatedness and 21 testing the performance and accuracy. A total of 63 PR graphs were produced depicting the performance of similar queries, and a conclusive set of graphs was produced to show similarity in services (see figure 3 below).

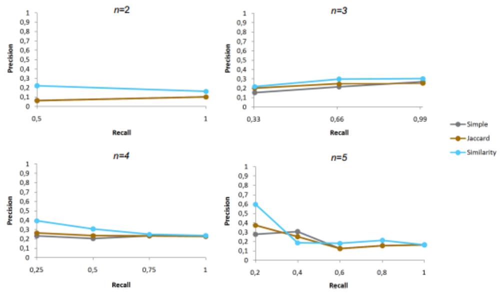


Figure 3 - Graphs for Discovery Of Similar Services (Sangers et al. 2013)

Multiple claims were made; in most cases Jaccard shows a higher precision for recall however all algorithms require the same precision for a full recall. Additionally, in view of the results shows in Figure 3, the claim was made that the similarity algorithm performs better for semantic discovery opposed to Jaccard.

Considering the justification of the ontology language choice, which was determined by a scientific comparison on their relevant strengths, as well as the scientific justification of the SWSD framework in regard to its usage and limited resources for keyword discovery methods, we can conclude that the methodologies presented in this research are scientifically accurate and relevant.

The testing performed included a moderate sized sample of data, with the pre defined descriptions being tested against 61 manual keyword sets. These tests appear scientifically sound as the keywords being tested are taken from a repository of the most common keywords used in web semantic searches, which ensures the results will be both accurate and relevant. Additionally, the tests were able to cover a multitude of variables. By splitting their keyword inputs into groups, they were able to test for recall accuracy, precision and weights of both algorithms against the same set of descriptions.

There was however the inclusion of a method that does not use NLP functionally in these tests, and while this was stated in the methodology, the results depict how the method compares to others, without mention to this non-NLP method. Consequently, these results may be flawed in that the NLP method itself requires additional assistance by non-NLP features to produce these results.

The graphs of results that were produced depicted very specific results from the tests; a total of 63 graphs were produced, which demonstrates the extent of testing involved. These graphs were summarized into averages from which claims where then made. These claims do indeed match the results generated, as a higher precision was reached by the pre-existing method Jaccard, however the conclusion can be made that the second claim which states the similarity method performs at a higher level is disputable due to the inclusion of a non NLP method during testing.

3 Contrasting Comparison of NLP Methods

The keyword cluster method boasts improved recall accuracy, thus resulting is more accurate responses for a user, as does the short text query method at 76%. The keyword clustering method however lacks the level of performance that the short text method provides, see Figure 2. Furthermore, the short text query method, since it does not rely on keyword filters, does not require the use and knowledge of a framework (SWSD) unlike the clustering method, and can therefore be deployed in a working environment with minimal effort opposed to the keyword filtering method.

Keyword clustering NLP does however provide a level of efficiency that the short text queries do not, see Figure 1. By ranking responses based on relevance, as well as combing multiple keyword inputs to pre-assigned responses based on predictions, users will experience a higher level of efficiency through prediction, whereas short text queries require a larger input and thus more data needs to be filtered before a response can be generated, resulting in a less efficient response method.

This however is very subjective as there are times when using longer input queries may be required to find more specific information, as well as the potential loss of accuracy in the predictions.

Sivagar and Chaitanya (2014) stress how a method of discovery should be created in a way that bridges the gap between NL keywords and a web service description.

Considering this, we can conclude that by combining the two methods into one that allows for longer input queries, but filters them through a clustered method and assigns rank-based predictive responses, we can create a refined NLP method that accentuates the positive recall accuracy of the keyword clustering method with the high performance of the short text queries and ultimately takes a step forward in bridging that gap.

4 Real World Implications of Applying NLP Methods

Considering how each of the three NLP methods function differently, we must also consider how their use would impact the real world. In view of a business environment, both the keyword cluster and keyword discovery method would require a programmer to have knowledge of the SWSD framework and its limitations, as well as knowledge of the ontology languages available.

By using either of these methods, a business or organization would restrict themselves to using only singular inputs to retrieve web service description data; however accuracy would increase due to the ranking and prediction methods they both implement.

For either of these NLP methods to function in the real world, a programmer would be required to understand additional concepts in order to implement them. This could create a new order of jobs involving teaching programmers this knowledge and allow them to adapt their own programming skills accordingly.

The short text query method would not require additional knowledge of frameworks to be implemented. However, as earlier discussed, this method is currently featured, predominantly for English NLP web discoveries, but alternative languages are without its resources. By implementing this method in the real world, all manner of businesses world would be able to adapt its functionality and increase both the precision and accuracy of their semantic web experience, potentially boosting clientele and revenue.

5 Conclusions

As we have summarized various NLP techniques, so to have we generated conclusions based on our findings. We have concluded that while each method brings forward advancements that aid in bridging the gap between natural language and web semantic descriptions, they also have their shortfalls.

Looking at the keyword clustering method, we have concluded that it does boast a high level of recall accuracy opposed to the standard natural language filtering technique, although further research is needed to discover how it fairs against other NLP methods.

The keyword discovery method results in high precision, however because the testing of this method involved a non-NLP method used to match the keywords, we can conclude that further research is required in order to advance the matching capabilities of the keyword discovery method.

Short text queries provide a high recall percentage and don’t require additional framework knowledge / engines for real world application. However, given the high potential of bias introduced in the experiments, we can conclude that further testing is required in order to obtain more scientifically accurate results.

Considering how these NLP methods function, we can conclude that as it stands, keyword clustering is the more efficient method due to its predictive indexing and ability to function as a NLP semantic discovery service. Conversely, recall and prediction is particularly higher in the short text query method. Furthermore, the short text query method does not require knowledge of a framework to function, so implementing it in the real world could be done with reduced costs and skill requirements.

Taking this into account, we can conclude that creating a combination of the two methods, we can create a functionally sound NLP method for the semantic web which can receive both short text and keyword queries, granting the flexibility of both inputs and the accuracy generated by sentence matching, as well as adapt a predictive indexing technique for the levels of efficiency found in keyword clusters.

References

Crowston, K Eileen, E Allen, H Robert, H., 2012, ‘Using natural language processing for qualitative data analysis.’ *International Journal of Social Research Methodology*, 15 (6), Pages: 523-543.

Furlan, B Batanovic, V Nikolic, B., 2013, ‘Semantic similarity of short texts in languages with a deficient natural language processing support.’ *Decision Support System*, 55, Pages: 710-719.

Gunasri, R Kanagaraj, R., 2014, ‘Natural Language Processing And Clustering Based Service Discovery’. *International journal of Scientific & Technology Research,* 3, Pages: 28-31.

Islam, A Inkpen, D., 2008, ‘Semantic Text Similarity Using Corpus-based Word Similarity and String Similarity'. *ACM Transactions on Knowledge Discovery from Data*, 2, Pages: 1-25.

Maxwell, T Schafer, B., 2010, 'Natural language processing and query expansion in legal information retrieval: Challenges and a response.' *International Review of Law, Computers & Technology*, 24, Pages: 63-72.

Mihalcea, R Corley, C Strapparava, C., 2006, 'Corpus-based and Knowledge-based Measures of Text Semantic Similarity'. *Proceedings of the National Conference on Artificial Intelligence*, 21, Pages: 775-780.

Sangers, J Frasincar, F Hogenboom, F Chepegin, V., 2013, 'Semantic Web service discovery using natural language processing techniques.' *Expert Systems with Applications*, 40, Pages: 4660-4671.

Sateli, B Cook, G White, R., 2013, 'Smarter Mobile Apps through Integrated Natural Language Processing Services.' *The 10th International Conference on Mobile Web Information Systems*, 8093, Pages: 187-202.

Shafi, J Ali, A., 2012, 'Defining Relations in Precisation of Natural Language Processing for Semantic Web'. *International Journal on Computer Science and Engineering*, 4, Pages: 723-727.

Sivagar, K Chaitanya, K., 2014, 'Dynamic Referencing of Web Services via Service Discovery and Natural Language Processing.' *International Journal of Computer Science & Information Technologies*, 5, Pages: 2019-2022.

Workman, E Stoddart, J., 2012, 'Rethinking information delivery: using a natural language processing application for point-of-care data discovery.' *Journal of the Medical Library Association*, 100, Pages: 113-120.

Wu, Z Palmer, M., 1994, 'Verbs semantics and lexical selection.' *Proceedings of the 32nd annual meeting on Association for Computational Linguistics*, 32, Pages: 133 - 138.

A Critical Evaluation on Current Wireless Wearable Sensors in Monitoring of Patients

Mmoloki Gogontle Gontse

Abstract

Commercially available wireless wearable sensors have become the core of remote patient monitoring. This paper describes a critical evaluation of current wireless wearable sensors in monitoring of ambulatory patients, the experiments and results of the prototypes evaluated and the claims and conclusions made using the comparisons. This paper gives recommendations on future work that is real world application of the proposed solutions evaluated in this paper.

1. Introduction

The current standard involving manual observation whereby vital signs are treated independently (Clifton et al. 2014) despite wearable patient monitors now being manufactured commercially, allowing the collection of continuous physiological data from ambulatory patients, high rates of (Hu 2011) undetected arterial fibrillations and sudden cardiac death are still being reported. A preventative measure (Hsu and Young 2014) can be put in place and can only be effective when atrial fibrillations are detected in the early stages. Normally this would require walking into the hospital for regular checks however the sporadic characteristic of cardiovascular diseases make it rather challenging in capturing the events. This calls for an un-obstructive, continuous monitoring of multiple parameters such as heart rate HR, body temperature, blood pressure (BP) and electrocardiogram (ECG) embedded in a daily wearable device. Reportedly available patient monitors are described as skin piercing by Tseng et al. (2014) causing pain and damage over long-term monitoring. Malhi and Mukhopadhyay (2012) argue the spiralling costs of hospitalisation thus propose a (Rehman et al., 2012) remotely continuous measurement of physiological parameters. Long-term monitoring requires for feedback from the unobtrusive wearables to maintain optimal health status. Atalay et. al. (2015) describes a high need for healthcare monitoring outside the hospital environment using wireless wearable devices. Pandian et. al. (2008) and Tseng et al. (2014) mention a wearable textile which can encapsulate multiple parameters and continuously collect and analyse a patient while Lee and Chung (2009) and Sardini et al. (2011) propose that a patient's current activity is also vital when monitoring ECG. Sardini and Serpelloni (2010) and Wong (2012) propose an ECG wearable device which communicates to a Health Cloud for doctors in a remote location while the wearable its self is worn by the patient in their everyday activities.

The structure of the paper consists of: current wearable's which presents and evaluates implementations of a wearable in monitoring of patients. Experiments undertaken and discussions describing the evaluation process and the results of the experiments will also be addressed. Lastly the paper concludes on the current wearables mentioned in the previous section.

2. Current Wearables

In this section, four (4) technical proposals by different authors which aim to achieve the same goal are presented and evaluated. The experiments carried out to justify the proposed solutions and their results will be used as the evaluation criterion of each of the technical proposals.

2.1. Smart Vests

Tseng et al. (2014) describes an implementation of a wearable device with multiple parameters being continuously collected and transmitted wirelessly to a gateway for analysis and presentation of the data. The wearable consists of an ECG acquisition device, a mobile phone platform and a health care server (Tseng et al. 2014). Because the wearable is a vest, comfort and convenience for extended monitoring in daily life are the major design consideration. Tseng et al. (2014) proposes an improvement in comfort-ability by using dry foam ECG electrodes to come into contact with the skin as compared to traditional wet electrodes that required conductive gel and were reported to be penetrating through the skin causing high cases of discomfort. Figure 1 illustrates a prototype of the vest. The proposed vest continuously acquires the users ECG signal and communicates it via Bluetooth to a mobile phone platform. The program in the mobile phone then transmits an average heart rate (HR) using a short message service (SMS) every 2 hours to a healthcare server. In the case of abnormal HR, the program sends immediately to the healthcare server. Embedded in the SMS is global positioning system information (GPS), contact details, message time, SMSC number, message body and raw abnormal ECG data (Tseng et al. 2014).

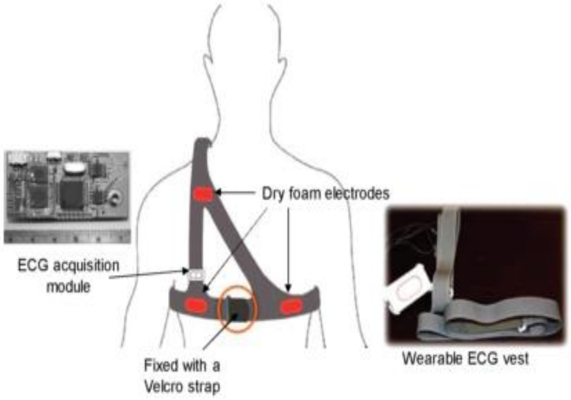


Figure 1 Proposed dry foam ECG monitoring wearable (Tseng et al. 2014).

For a greater battery life, Tseng et al. (2014) proposes an 1100mah battery to boost a life of up to 33 hours. To test the prototype Tseng et al. (2014) used the conventional wet ECG electrodes to record sets of ECG data. These sets were used to generate the simulated human ECG signals to correlate between signals measured by the dry foam against those by wet electrodes. The correlation is of a high 99.51% (Tseng et al. 2014). Tseng et al. (2014) then produced a clinical study with a sample of 20 patients with atrial fibrillations. The standard of the experiment design adhered to the American National Standard for ambulatory ECG analysers (ANSI/AAMI EC38–1994) (Tseng et al. 2014).

Tseng et al. (2014) concludes that the dry foam electrode adapts to the skin even under motion its stable thus it provides a potential for routine and repetitive measurement of the heart rate. In the experiments Tseng et al. (2014) follow national standards to ensure that it works to the best ability required. The sample size of the experiment is described allowing for other researchers to be able to do the experiment and validate its claims.

2.2. Smart Shirts

Sardini et al. (2011) emphasize that as much as observing electrocardiogram (ECG) just like the smart vest, the current physical activity is required to be able to assess the hearts condition and current activity being performed using three-axis accelerometer signals. The combination of the ECG and accelerometer take the design of the T- shirt to allow for mobility and comfort for continuous collection and analysis of the patient. The design also allows for communication in a wireless network. Sardini et. al. (2011) claim that their prototype is fully non-invasive with none of its sensors coming into direct contact with the skin. Once the sensor records physiological parameters, the signals are conditioned by amplification and filtering for digitization for the reading device to be able to transmit them to a wireless device. The wearable T-shirt is embedded with compact rechargeable batteries

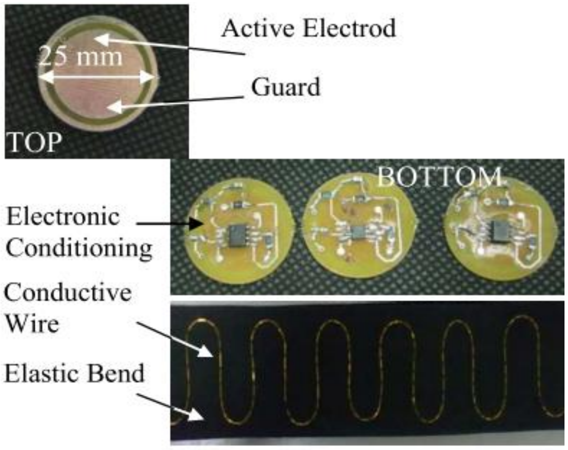


Figure 2 Illustrates the active electrodes (Sardini et al. 2011)

Figure 2 illustrates the electrodes on the fabric of the T-shirt however figure 3 illustrates the placement of the electrodes on the prototype. The third electrode is a reference electrode which is intended to minimize voltage (Sardini et al. 2011).

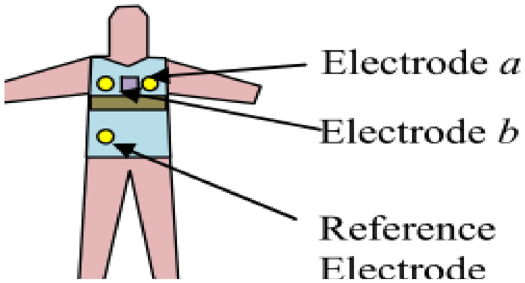


Figure 3 Placement of electrodes on the T-shirt (Sardini et al. 2011)

For the experiment, Sardini et al. (2011) describes a data acquisition device with rechargeable batteries and is of compact size. A wireless module is used to transmit data to a mobile phone or a personal computer and is controlled. Experiment results show that the wearable proposed is completely non-invasive.

The experiment details have been fully given by Sardini et. al. (2011). The results of the experiments can be trusted and can be said to be reliable as the same experiment can be carried out again in order to attain the same results as in the experiment.

A shirt is a piece of clothing so the proposal does not address issues of washing, getting torn and worn out. So in the future, issues pertaining the above issues not addressed in the proposal should surely be addressed. The claim made by Sardini et. al. (2011) suggests that the shirt should be non-invasive has been proven valid as per the experiment and the experiment results.

2.3. Chest Belt

Another garment worn within basic clothing of a patient is a belt that runs across the chest embedded with (Sardini and Serpelloni 2010) a circuit board, two skin electrodes, a body temperature sensor, an accelerometer for movements and fall detection and a respiratory sensor. Sardini and Serpelloni (2010) claim to develop a wearable for an unconscious and extended monitoring of vital signs of the user.

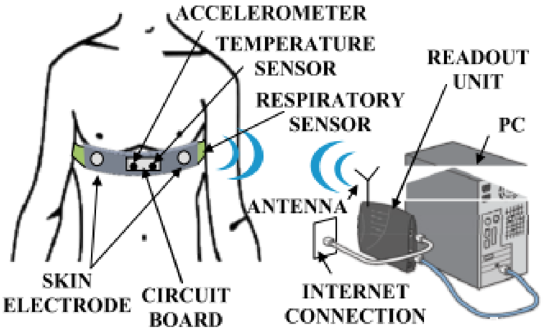


Figure 4 This diagram shows the wireless chest belt transmitting to a portable readout unit (Sardini and Serpelloni 2010).

The placement of the belt horizontally across the chest as illustrated on figure 4 allows for easy capturing of respiratory data due to rib cage movements over time. The two skin electrodes record electrical potential between two points of the body and display the heart's electrical activity (ECG) versus time. The patient's activity is tracked by the use of the accelerometer during normal day to day activities such as walking and Sardini and Serpelloni (2010) also present in their results cases were falls are also recorded by the accelerometer.

The communication is done through a wireless module. The proposed wearable is embedded with a microcontroller to establish communication channels with the readout unit and in cases of were the proposed wearable is not being used it alternates it between sleep and wake up modes (Sardini and Serpelloni 2010). The data recorded from the sensors is transmitted to the readout unit after being amplified and filtered for optimal digitization. A remote location which receives and analyses the psychological parameters generates automatic alarms and transmits the records to the internet

Sardini and Serpelloni (2010) suggests that preliminary experimental results tested conditioning of each sensor. The results of this experiment show that the proposed chest belt suggested by (Sardini and Serpelloni 2010) showed sensitivity in the axis which is good for responsiveness of the device.

In the conclusions, Sardini and Serpelloni (2010) experimental results illustrate cardio-respiratory signals, the heartbeats, the respiratory cycles and the patient activities such as walking and running can be obtained clearly by the device. However none of the experimental results show any use of the device by human subjects but a simple test of each sensor. On the other hand the author concludes that the wearable is safe to be used for telemedicine diagnosis and home care management yet no real subjects actually used the wearable to ensure it is of a higher quality than those in the conventional health monitors which can only be located in health care centres.

The experiment results are not reliable as they do not describe fully how the experiment was carried out and the experiment was never really tested on human beings or simulated using international standards to ensure that it is a practical wearable device

2.4. Wrist strap

Malhi and Mukhopadhyay (2012) propose a simple wrist strap connected to a finger ring as displayed in figure 5, to monitor multiple ambulatory physical parameters such as heart beat per minute (BPM), body temperature and fall detection. The strap on is embedded with temperature sensor, heart rate sensor and a two-axis accelerometer for impact on both axis(Malhi and Mukhopadhyay 2012). Because battery is and has always been a concern for wearable devices, operational amplifiers of low-power were used for low battery consumption by the Zigbee-Based wrist wrap (Malhi and Mukhopadhyay 2012). The main aim of the proposed wearable device was to develop a wearable device that needed not a panic button as observed with products already available in the market as stated by Malhi and Mukhopadhyay (2012) in their preliminary analysis. They argue that in cases of emergencies, the users are often unconscious and unable to press the panic button to remotely call for help.

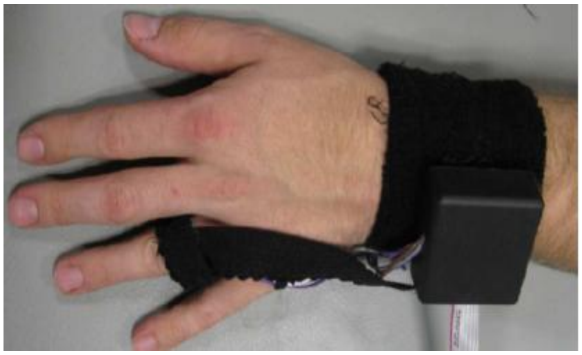


Figure 5 Zigbee-Based Wrist strap prototype connected to a finger ring (Malhi and Mukhopadhyay 2012).

Malhi and Mukhopadhyay (2012) tested the sensors of the prototype separately for easier analysis and understanding. With respect to the temperature sensor, it is placed inside the wrist strap in such a way that it comes into contact with the skin of the user allowing for temperature of the surface of the skin to be recorded. The skin temperature is at an estimated 5.1 Degrees Celsius less than that of the body temperature when measured by a general practitioner at the ear. Malhi and Mukhopadhyay (2012) suggest that it is not a requirement for their prototype to get the exact body temperature thus this method of using a less accurate reading was acceptable however set thresholds of temperature were to be monitored to be able to set off the alarm. Many females and males were selected according to Malhi and Mukhopadhyay (2012) as sample size of the experiment.

Malhi and Mukhopadhyay (2012) designed an inexpensive and simple heart rate sensor which recorded the heartbeat of a user per minute. The sensor measures blood volume as the amount of absorbed near-infrared spectroscopy (NIR) light changed with the flow of blood. It uses a low wavelength in which only the haemoglobin is the only tissue which absorbs it. This sensor was located at the finger ring to record the heartbeat per minute. The sensor signals the heartbeat which is then amplified, filtered and analysed (Malhi and Mukhopadhyay 2012). To record impact of falls the accelerometer was tested with walking, sitting, standing, writing and a simulation of the user falling (Malhi and Mukhopadhyay 2012). Malhi and Mukhopadhyay (2012) suggest that the results were highly accurate and detected falls very well. Malhi and Mukhopadhyay (2012) tested the RF transmission range at 30 meters through obstacles such as walls. During this test, a 9 volt battery was used to power up the developed prototype.

In the conclusion Malhi and Mukhopadhyay (2012) mention that the prototype was successfully developed and tested and it provided a panic button which can be used under an emergency situation. Malhi and Mukhopadhyay (2012) claim that their proposed wrist strap will be enabled with the ability to report an abnormal heartbeat, temperature and fall without pressing of a panic button yet in their conclusions they mention their system still requires a panic button in the case of an emergency. This contradicts their main aim of the removal of the button. They do not elaborate on what emergency the panic button will be reporting that the system itself does not already record. So there is still room for improvement; to make the wearable device completely button-less.

When carrying out their experiments, no human tests were carried out, no different activities such as walking, sleeping, running were monitored using the proposed wrist strap to ensure that each of the sensors and which combined, can recognise variable changes in the skin temperature, the heart rate and any falls during such activities. Without these experiments it cannot be concluded that the proposed wrist strap actually works for human users.

3. Conclusions

This work provides a detailed analysis of current wearables to monitor patients such as a wrist strap, a belt that runs across the belt, a vest and a T-shirt. Various factors were observed such as skin and body temperature, heart beat rate and blood pressure. The major design considerations were the ability of the wearable to be able to monitor remotely, be comfortable enough to be worn in everyday life, easy to use and report to the user and health facilities. Generally the current research was outstanding however the experiments did not reveal enough on the usability factor of the wearable. The most of the experiments did not consider the human subject for the testing. Individually each sensor in a wearable performed very well illustrating good sensitivity. As a recommendation proposed wearable devices should always be tested out on human beings to ensure that indeed the wearables work and are effective. Also when testing the wearables the sensors should be tested at the same time whilst attached to the wearable to ensure not only the microprocessor is capable of parallel running the retrieval of signals and also to ensure that the results accurately recognise and report an variation of a health state.

Once the sensors start working simultaneously, the power consumption will be obviously higher than when testing with that of one sensor thus as a recommendation it can be suggested that a larger power capacity whilst maintaining a miniaturized size of the battery pack. This will ensure that the wearable is un-obstructive to the human user which is a key component in the design stages of a wearable device. The software of the mobile platforms must also be tested for usability to ensure that each and every users with no respect to age and literacy must be able to use and understand with ease.

References

Atalay, O., Kennon, W. & Demirok, E., 2015. ‘Weft-Knitted Strain Sensor for Monitoring Respiratory Rate and Its Electro-mechanical Modelling’. *IEEE Sensors Journal*, vol. 15, no. 1, pp.110–122.

Clifton, D., Clifton, L. & Pimentel, M., 2014. ‘Predictive Monitoring of Mobile Patients by Combining Clinical Observations with Data from Wearable Sensors’. *IEEE Journal of Biomedical and Health Informatics*, vol.18, no.3, pp.722–30.

Hsu, Y.-P. & Young, D.J., 2014. ‘Skin-Coupled Personal Wearable Ambulatory Pulse Wave Velocity Monitoring System Using Microelectromechanical Sensors’. *IEEE Sensors Journal*, vol.14, no.10, pp.3490–3497.

Hu, S., Shao, Z. & Tan, J., 2011. ‘A real-time cardiac arrhythmia classification system with wearable electrocardiogram’. *Body Sensor Networks (BSN)*, 2011, pp.119–124.

Lee, Y.-D. & Chung, W.-Y., 2009. ‘Wireless sensor network based wearable smart shirt for ubiquitous health and activity monitoring’. *Sensors and Actuators B: Chemical*, vol. 140, no. 2, pp.390–395.

Malhi, K., & Mukhopadhyay, S. (2012). ‘A Zigbee-based wearable physiological parameters monitoring system’. *Sensors Journal*, vol.*12*, no.3, 423–430.

Pandian, P. S., Mohanavelu, K., Safeer, K. P., Kotresh, T. M., Shakunthala, D. T., Gopal P., Padaki, V. C., 2008. ‘Smart Vest: wearable multi-parameter remote physiological monitoring system’. *Medical engineering & physics*, vol. 30, no.4, pp.466–77.

Rehman, A., Mustafa, M., Javaid, N., Qasim, U., Khan, Z.A., 2014. ‘Analytical Survey of Wearable Sensors’. In *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*. IEEE, pp. 408–413

Sardini, E. & Serpelloni, M., 2010. ‘Instrumented wearable belt for wireless health monitoring’. *Procedia Engineering*, vol. 5, pp.580–583.

Sardini, E., Serpelloni, M. & Ometto, M., 2011. ‘Multi-parameters wireless shirt for physiological monitoring’. In *2011 IEEE International Symposium on Medical Measurements and Applications*. IEEE, pp. 316–321.

Tseng, K. C., Lin, B., Liao, L., Wang, Y.,Wang, Y., 2014. ‘Development of a Wearable Mobile Electrocardiogram Monitoring System by Using Novel Dry Foam Electrodes’. *IEEE Systems Journal*, vol.8, no.3, pp.900–906.

Wong, D.L.T., 2012. ‘A wearable wireless ECG sensor with real-time QRS detection for continuous cardiac monitoring’. In *2012 IEEE Biomedical Circuits and Systems Conference (BioCAS)*. IEEE, pp. 112–115.

Evaluation on Research targeted towards Worm Viruses and Detection Methods

Adam Keith

Abstract

Worm viruses are a threat to both computers and their users, which have resulted in people proposing and developing various worm detection methods. This research paper focuses on various detection methods that exist today or have been proposed, ranging from early stage worm detection, host based methods, simulation worm-detection and varying scan rates and techniques. The paper will evaluate the methods and experiments done during development, what results were acquired and what the authors claim. The reason why this paper evaluates these methods is so it can provide insight on how reliable the methods are.

1 Introduction

One of the biggest threats to computers is worm viruses. An example of their type is polymorphic worms which combine self-replicating and rapid spreading worm characteristics, making them difficult to catch (Bayoglu et al, 2012). For a while, worms have proven to be a huge security threat to the Internet and being able to counter them and have complete defence against them has proven to be difficult, as they continuously evolve (Yu et al, 2011). There are many different ways to detect and prevent worms from infection, though some ways are not especially effective. Constant quarantine strategy can be a good defensive measure against worms, but its reliability in imperfect intrusion detection systems is deemed poor (Yao, et al 2012).

This research paper will critically evaluate various methods of worm detection, such as Early Stage Worm Detection, Host Based Methods, Simulation Worm-Detection and Varying Scan Techniques and Rates. These methods will be evaluated by their intentions, experiments, results and claims.

After each paper is analysed, they will receive an evaluation based on how in-depth the research was, whether the results were genuine or biased and to determine if the authors' methods are capable of being used in the real world.

2 Detecting Worms at an Early Stage

The following section will look into the worm detection method by Chen and Ranka (2005) that intends to detect worms as early as possible.

Chen and Ranka (2005) developed a worm detection method called Worm-Virus Early Warning System (WEW), because they believe that the need for such a method is essential.
The authors put the focus of their method experimentation on TCP-based worms, due to limited scope and they also state that they discover infected systems by using random scanning (Chen and Ranka, 2005).

To test the method, they compared normal user activity with worm infected user activity by analysing the respective hosts. Chen and Ranka (2005) found that a normal user accesses a server by its domain name and gets resolved for an IP address via the domain name system (DNS) and found that if the domain name cannot be resolved there will be no TCP connection. However, they also found that a worm attempted TCP connections to random addresses and produced a lot of connection failures (Chen and Ranka, 2005). Their experiment showed that over 99.6% of connections made to random addresses at their chosen Internet protocol service port failed and also found that the percentage will be higher for unpopular services (Chen and Ranka, 2005). Chen and Ranka (2005) state they found that a worm infected host will have a high rate of failed connections in comparison to a non-infected user who will have a lower rate, due to corruption.

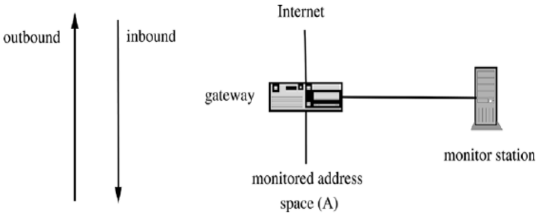


Figure 1 WEW Sampling Internet Scan Activities Chen and Ranka (2005)

During the testing, they deployed the method into the gateway of a large network enterprise, along a set of default parameters. Using diagrams of the system sensitivity and the actual number of infections detected, the authors showed how it works when deployed into the gateway, through simulation and algebraic expressions. But, it is not stated which enterprise network was used.

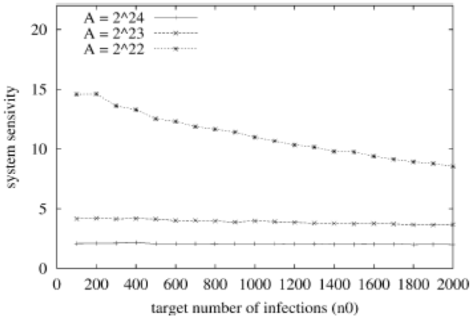


Figure 2 System Sensitivity Chen and Ranka (2005)

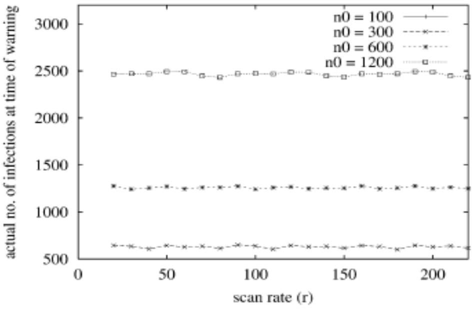


Figure 3 Actual Number of Infections Chen and Ranka (2005)

Chen and Ranka (2005) claim that with seeing the differences in behaviour, they can distinguish normal users from worm-infected hosts and the method being a valuable component that sets up the defence measures needed and reveal information on hosts that need to be fixed. They also claim that it works well for large enterprise networks, but not with small enterprise networks, due to space size, but they state that the method could work with small enterprises if they link together.

While the amount of research and test results look promising, the authors not mentioning where the new method was deployed, not mentioning many method limitations and not confirming that it had been tested in the real world may make the results seem biased. However, the results of their tests can let the authors continue with the research and see if the method is capable of working in the real world. Furthermore, they had also used mathematical calculations and diagrams which can lessen the potential bias.

3 Host Based Methods

The following section will look into the worm detection method by Chen, et al (2014) that intends to detect host-based worms.

Chen, et al (2014) developed a new host-based worm detection solution called WormTerminator, possessing the ability to find and contain Internet worms quickly and let non-infected traffic through. They developed the new method alongside a virtual machine that duplicates the host operating system and puts it alongside the original, intending to divert any outgoing traffic and show patterns of worm propagation (Chen, et al 2014).

To test it, the authors created and deployed a prototype of their new method into a custom made network with its own host and used the Linux/Slapper worm to see how it would work against it, by stopping the worm from connecting to server ports and executing exploit procedures. Every time the worm virus was released into the network, the method was timed to see how fast it could stop the worm. After conducting the same test of releasing the Linux/Slapper worm into the network ten times, the authors found that the method can disconnect the network as the worm was about to start and then have it captured (Chen, et al 2014).

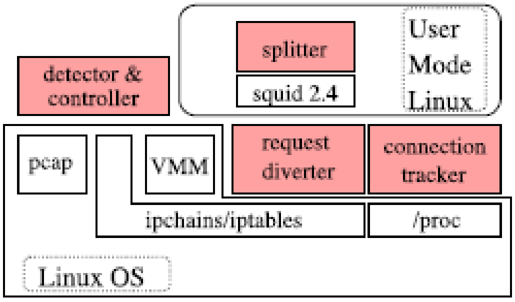
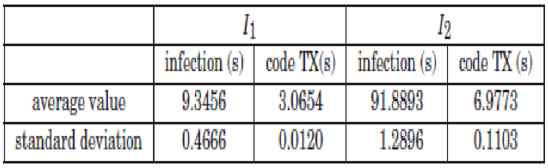


Figure 4 WormTerminator prototype implementation Chen, et al (2014)



	I_1		I_2	
	infection (s)	code TX(s)	infection (s)	code TX (s)
average value	9.3456	3.0654	91.8893	6.9773
standard deviation	0.4666	0.0120	1.2896	0.1103

Table 1 Slapper: Infection and Code Transmission Time Chen, et al (2014)

Chen, et al (2014) claim that with the real-time experiments, they were able to confirm that the method can contain fast worms without blocking normal traffic, as they were able to implement a prototype in Linux and saw how effective it was against Linux/Slapper. However, they also claim that there are limitations in the method, such as there being a high chance that a fast worm will always target a set of host vulnerabilities, but if a worm targets a set of different host vulnerabilities, the method may not be effective, if the implementation was straightforward.

The amount of research and testing done towards this experimentation seems to be well thought out, as they had managed to test the method ten times, thus ensuring that the method is free from any faults. The diagrams and tables showing the results of the method working against the Linux/Slapper worm show that they were willing to see what would happen if they tried to use their method in the real world. This means that the host-based method could work in the real world, even if they mentioned that there are limitations with it being a host-based method and may not perform as well.

4 Worm Detection via Simulation

This section looks into research that had been done on worm detection via simulation, intending to both detect and analyse worms. This research had been done by both Nicol (2008) and Zou et al (2007).

Nicol (2008) developed a new model of preferential random scanning to find out the sensitivity of worm propagation speed to the distribution of vulnerable hosts through the network via simulation. Nicol (2008) also proposed and studied two optimisations, from a fluid-based simulation of scanning traffic through a backbone network to help detect problems. Zou et al (2007) had created and presented a simulation model for email worms that analyses the behaviours of users, checking time and the likeliness of an infected attachment being opened. The reason for that is that email worms have been reported to nearly bringing the whole Internet system down (Park et al, 2007). Zou et al (2007) also use simulation to compare worms on different topologies to see how much damage they cause, depending on the topology.

Nicol (2008) tested their simulation/worm scan method by using “Preferential Scanning”. With this technique, they developed a two-tier model to observe the impact on variance of the initial distribution of vulnerable hosts (Nicol, 2008). In order to prove the reliability of the technique and to determine how the speed of the viruses can affect vulnerable hosts and networks, the author simulated a worm with Code-Red vII-like parameters (Nicol, 2008). The Code-Red virus was said to have infected more than 350,000 computers in less than 14 hours by exploits (Yu et al 2010). Zou et al (2007) tested their email worm propagation simulation model by having it capture an email worm propagation scenario. The results showed the model can reveal that the differences between email worms and scanning worms are that email worms depend on human interaction in order to execute.

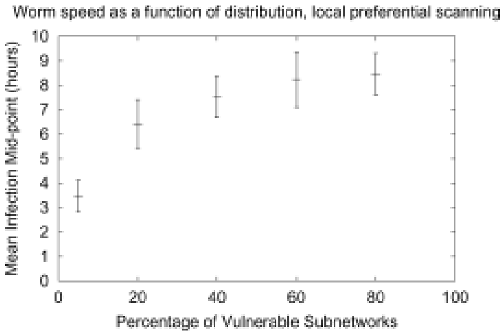


Figure 5 Sensitivity to numbers of infectable subnetworks Nicol (2008)

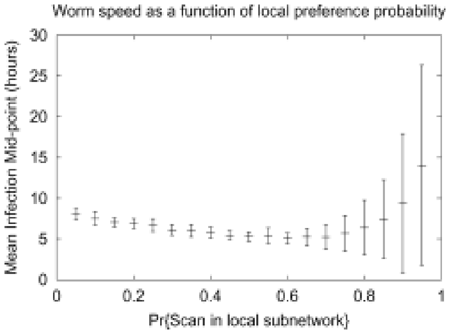


Figure 6 Sensitivity to local preference probability Nicol (2008)

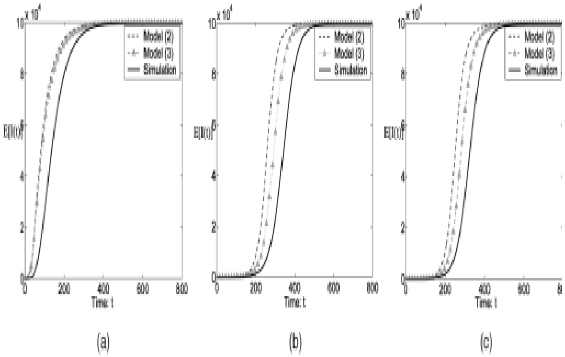


Figure 7 Effect of the distribution of e-mail checking time T,. (a) Power law topology. (b) Small-world topology. (c) Random graph topology Zou, et al (2007)

After testing the method, Nicol (2008) claims that the simulation of large-scale worms is an important tool for evaluating defences. They back up their claims with algebraic equations, along with diagrams of how the method performs in certain circumstances. Zou et al (2007) claim that they are capable of achieving an effective defence model by showing how different a worm's behaviour is, depending on which topology is used. However, they also added that their method needs more work, as they had only relied on simulations of worm propagation and previous topological epidemic models haven't been accurate, due to email worms not sending out random scanning.

$$\frac{N}{i(S_0 - i)\lambda_s} \times i \times \lambda_s = \frac{N}{S_0 - i}.$$

Figure 8 Algebraic Equation Nicol (2008)

The research that was done by Nicol (2008) puts a lot of focus on worms for their method, especially with the use of logical diagrams and algebraic equations to back up their claims and how it has potential of working in the real world. While diagrams and equations were used throughout the paper, the author did not mention any problems occurring during the experimentation and that can make the final results not seem thorough. Zou et al (2007) had also put a lot of in-depth research in worm detection via simulation, as they had explored the information of how the simulation model can propagate worms. They also took the limitations into consideration and had stated that more work would be needed in order to make it completely reliable, meaning that they are willing to improve it, before using it for real.

5 Varying Scan Techniques and Rates

The following section will look into the worm detection methods that involve the Techniques and Rates of Varying Scans by Yu et al (2011) and Xia et al (2006).

A new worm-detection scheme called the attack-target Distribution Entropy-based Dynamic detection scheme (DED detection) was designed by Yu et al (2011). The authors also intended to compare their method with other methods using real-world internet traces as background scan traffic. Xia et al (2006) had created and proposed their own detection method, Victim Number Based Algorithm. The authors claim that with their method, they are to detect worm events before at least 2% of susceptible hosts become infected.

Yu et al (2011) demonstrated their scheme's performance with other detection schemes on detecting both the VSR worm and the PRS worm. To set up the simulation, the authors used real-world Internet traffic traces for traffic that hadn't been infected. After the authors had set up a 15 days trace on a certain date for the scheme, with no worm attacks being reported, they acquired the statistical profile of traffic traces, giving them the mean value and standard deviation of traffic rates (Yu et al, 2011). To validate the results, Yu et al (2011) tested the scheme on different dates fifteen times. The experimentation Xia et al (2006) had conducted involved designing algorithms in order to detect anomalies, as they claim that if there are many addresses sending scan packets to addresses and services that are dead, within a short space of time, there's a high chance that is a worm attack. The results of their experiments were that the worm starts infecting at 3:00 am and the authors were able to detect the worm events at 5:43 am, after infecting less than only 0.83% of susceptible hosts, as it was performing a routable scan.

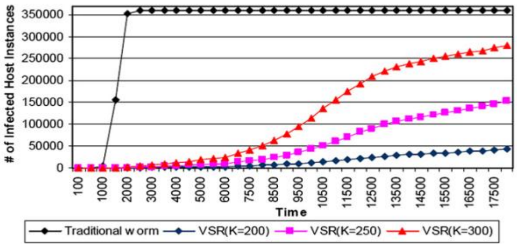


Figure 9 Infection ratio for different VSR worms Yu et al (2011)

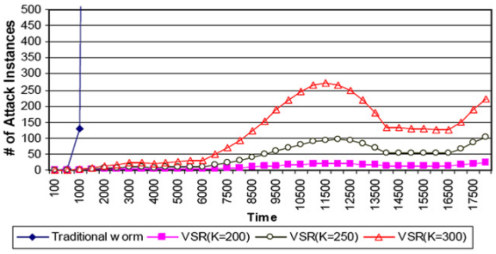
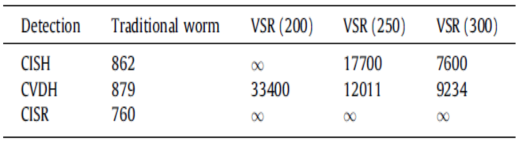
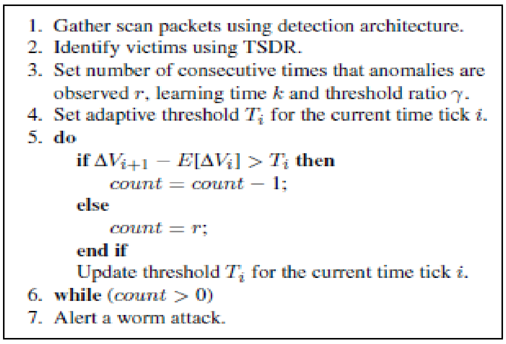


Figure 10 The number of observed worm instances for different VSR worms Yu et al (2011)



Detection	Traditional worm	VSR (200)	VSR (250)	VSR (300)
CISH	862	∞	17700	7600
CVDH	879	33400	12011	9234
CISR	760	∞	∞	∞

Table 2 Detection time (DT) of some existing detection schemes Yu et al (2011)



```
1. Gather scan packets using detection architecture.
2. Identify victims using TSDR.
3. Set number of consecutive times that anomalies are
   observed $r$, learning time $k$ and threshold ratio $\gamma$.
4. Set adaptive threshold $T_i$ for the current time tick $i$.
5. do
       if $\Delta V_{i+1} - E[\Delta V_i] > T_i$ then
           $count = count - 1$;
       else
           $count = r$;
       end if
       Update threshold $T_i$ for the current time tick $i$.
6. while $(count > 0)$
7. Alert a worm attack.
```

Figure 11 Victim Number Based Algorithm for worm detection Xia, et al (2006)

Once the tests were done, Yu et al (2011) claim that their detection scheme is capable of distinguishing worm scan traffic and non-worm scan traffic and that their results demonstrate how effective it is at detecting VSR worms and PRS worms. Xia et al (2006) claim their method's simplicity and effectiveness make it highly practical to implement, as it can use parameters to indicate worm attacks. However, they also state some issues with it, such as the difficulty of deploying Internet monitoring components and implementation costs, to which they state more work must be done for the resources.

The research done towards virus detection by Yu et al (2011) is in-depth, as it analyses both VSR worms and PRS worms, to prove that there are worms with varying scan rate, which was needed for their scheme. As for the method working in the real-world, the authors stated that they had used real-world Internet traffic traces for their tests. This means that while their general area may need more research, their method does have real world potential. Xia et al (2006)'s research in various worm detection architectures, techniques and algorithms possess specific details on their functionality, showing that they have considered how they work in order to provide for their algorithm. Algebraic calculations are present in the paper, which makes their results logical and credible, due to using mathematics. The method however is not ready to work in the real world, due to more research being needed in the areas of expenses and component compatibility.

6 Conclusions

At the present time, there is no method guaranteed to completely protect systems from worms, meaning they can only be used as system protectors with certain limitations. The administrator/technician in charge of the network method would need to ensure that the method is fully up-to-date and can detect incoming worms.

The research papers that have been analysed and evaluated have proven to be interesting as they show that there is potential towards creating various worm detection methods that can protect a computer network in many different ways.

The research done towards the Worm Virus Early Warning System by Chen and Ranka (2005) shows that a lot of theory, logic and information regarding the type of gateway were applied. While the analysis, calculations and simulation done towards their method generated some good results, it would still need to be confirmed that it was tested in the real world, in order to see how it would work against a real worm. If the method was tested in the real world, it may prove to have potential at detecting worms early.

Also, the research that was done towards the Host-based Worm Virus System by Chen et al (2014) shows a lot of experimentation done towards the method. This was proven by them doing a real time method test, in which they put a prototype of their new method against Linux/Slapper. If they were willing to deploy this method into the real world, then it does have potential of being considered useful, though more research must be done on how the method could stop worms from infecting any host.

The research done on Worm Detection via Simulation by both Nicol (2008) and Zou et al (2007) show a lot of real world potential, with the use of logical diagrams and algebraic equations to back up their claims on the methods' functionality. If the authors of the respective papers decide to fully analyse the faults of their methods and do more tests and modifications, their methods could be useful in the real world.

The research that had been done on Varying Scan Techniques and Rates by Yu et al (2011) and Xia et al (2006) specifically analyses various worm scan rates for their techniques. Yu et al (2011)'s method using real-world Internet traffic traces for testing give it high potential of working in the real world, despite it needing some improvements. This means that while their method may need more research, their method does have real world potential. Xia et al (2006)'s research on general worms and anomalies gives their algorithm real world potential as well, as long as more research is done on expenses and implementation.

While all of the methods and research presented in this paper need more work to be used in the real world for real, out of the methods that were analysed in this research paper, the Host Based Method is the most detailed of how the development process went, how much potential it has of detecting worms and stopping the hosts and servers from getting infected.

References

Bayoglu B. and Sogukpinar I., 2012, 'Graph based signature classes for detecting polymorphic worms via content analysis', *Computer Networks,* Volume 56, Issue 2, pages 832-844.

Chen S., Liu L., Wang X., Zhang X. and Zhang Z., 2014, 'A Host-Based Approach for Unknown Fast-Spreading Worm Detection and Containment', *Journal ACM Transactions on Autonomous and Adaptive Systems (TAAS) – Special Section on Best Papers from SEAMS 2012,* Volume 8, Issue 4, pages 21.1-21.18.

Chen S. G. and Ranka S., 2005, 'Detecting Internet worms at early stage', *IEEE Journal on Selected Areas in Communications,* Volume 23, Issue 10, pages 2003-2012.

Nicol D., 2008, 'Efficient Simulation of Internet Worms', *ACM Trans Model Comput simul,* Volume 18, Issue 2, pages 5:1-5:32.

Park I., Sharman R., Rao H. and Upadhyaya S., 2007, 'Short term and Total Life Impact analysis of email worms in computer systems', *Decision Support Systems*, Volume 43, Issue 3, pages 827-841.

Xia J., Vangala S., Wu J., Gao L. and Kwiat K., 2006, ‘Effective worm detection for various scan techniques’ *Journal of Computer Security*, Volume 14, Pages 359-387.

Yao Y., Guo L., Guo H., Yu G., Gao F. and Tong X., 2011, Pulse quarantine strategy of internet worm propagation: Modeling and analysis, Computers and Electrical Engineering, Volume 38, pages 1047-1061.

Yu W., Wang X., Champion A., Xuan D. and Lee D., 2011, ‘On detecting active worms with varying scan rate’, *Computer Communications*, Volume 34, Issue 11, pages 1269-1282.

Yu W., Zhang N., Fu X. and Zhao W., 2010, ‘Self-Disciplinary Worms and Countermeasures: Modeling and Analysis, *IEEE Transactions on Parallel and Distributed Systems*, Volume 21, Issue 10, pages 1501-1514.

Zou C., Towsley D. and Gong W., 2007, ‘Modeling and simulation study of the propagation and defense of internet e-mail worms’, *IEEE Transactions on Dependable and Secure Computing*, Volume 4, Issue 2, pages 105-118.

Evaluation of Security Techniques in Cloud Storage Systems

Aone Maenge

Abstract

Cloud storage is one of the technologies that are dominant in today's IT Era. Several techniques have been developed to provide better performance and security on data stored in cloud storage systems. Therefore, this research paper is focusing on analyzing, comparing and evaluating techniques in place to combat security threats in cloud storage systems. It focuses on revocable multi-authority ciphertext-policy attribute based encryption (MA CP-ABE) technique, Third party auditor (TPA) technique and Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage technique. Based on evaluation of these techniques, recommendations are made regarding which is the most current suitable technique to secure data in cloud storage systems.

1 Introduction

As cloud storage systems are in public domain, data stored in them are exposed to a lot of security threats such as unauthorized access, denial of service, security key management to mention but a few. Li et. al. (2013) indicated that, one major concern is the issue of whether data owners could actually have a control on how they share their sensitive information stored on third party servers which are not trusted. Wang et. al. (2011) articulated that, sometimes cloud service providers can intentionally remove data files in cloud storage that are not often accessed by clients. This means that the integrity and availability of data stored on untrusted servers are not guaranteed.

The other security problems that are encountered on cloud storage that impede its wide adoption is that, sharing of specific information or data by data owner can sometimes be difficult and it can also expose sensitive data to people who were not supposed to view it. Hur and Noh (2011) indicated that, this happens when attribute based encryption does not have capabilities of attribute and user revocation.

The other security threat on cloud storage is the issue of tying secret keys together to user's global identifier from many different authorities in attempt to escape collusion attack and this can results to user's privacy being compromised. Han et. al. (2012) indicated that, it is possible for multiple authorities to work together to trace the user through his/her Global identifier (GID), by getting his/her attributes and then impersonate him/her. Hur (2013) articulated that one other problem is that, key generation centers can decipher every encrypted data sent to certain users by creating their attribute keys. It is clear that security in cloud storage systems is indeed a major concern.

Research has been done to address security issues mentioned above. Yang and Jia (2014) proposed a scheme claimed to revoke data access for multi authority in cloud storage systems. Wang et. al. (2013) proposed a scheme claimed to be secure by supporting privacy preserving public auditing in cloud storage systems. Chu et. al. (2014) also proposed a scheme claimed to securely aggregate a number of secret keys for sharing data in cloud storage. This proposed solutions above claim to address issues of performance and security by ensuring integrity, privacy, confidentiality and availability of data stored in cloud storage systems.

Therefore, the purpose of this paper is to look at the most current research papers focusing on the schemes mentioned above for combating security threats on cloud storage systems. Critical evaluation of the proposed techniques/schemes is done to determine the most suitable technique that perform better and secure data stored in cloud storage system.

2 Revocable Multi-authority ciphertext-policy attribute based encryption (MA CP-ABE) technique

Yang and Jia (2014) carried out a research on revocable multi-authority ciphertext-policy attribute based encryption (MA CP-ABE) which focuses on addressing security issues on cloud storage systems by ensuring both forward security and backward security. Yang and Jia (2014) articulated that, on backward security the withdrawn user would not be able to decrypt any new ciphertext that needs the withdrawn attribute to decrypt. Yang and Jia (2014) also stressed that, on forward security the user who just joined would be able to decrypt the previously published ciphertext, if it has sufficient attributes. With this scheme, it is not necessary for the server to be fully trusted as each attribute authority is responsible for the enforcement of key update not the server.

Attribute revocation method is used which have three major components, namely Update Key Generation, Secret Key Update by Non-Revoked Users and Ciphertext Update by Cloud Server.

When the attribute is withdrawn from the user, the corresponding attribute authority runs the algorithm called update key generation (UKeyGen) to compute the update keys (Yang and Jia 2014). Yang and Jia (2014) state that, "upon receiving the update key the user (Non-Revoked User) then update his/her secret key by running the new secret key update algorithm". When accepting an update key from the authority, cloud server updates the encrypted data associated with the attribute that has been revoked, it does this by running the ciphertext update algorithm. With this three components, backward security and forward security is guaranteed.

Experiment has been conducted to test computation efficiency on proposed scheme against Ruj's DACC scheme. Yang and Jia (2014) articulated that Linux system was used to implement both schemes. Intel Core 2 Duo CPU with a speed of 3.16GHz and 4.00 GB RAM were used. Version 0.5.12 of the pairing-Based Cryptography (PBC) library was used to deploy both schemes. Yang and Jia (2014) indicated that symmetric elliptic curve was used, with 512-bit base field size and the embedding degree was 2. The simulation results on Fig. 1 are the average of 20 tests.

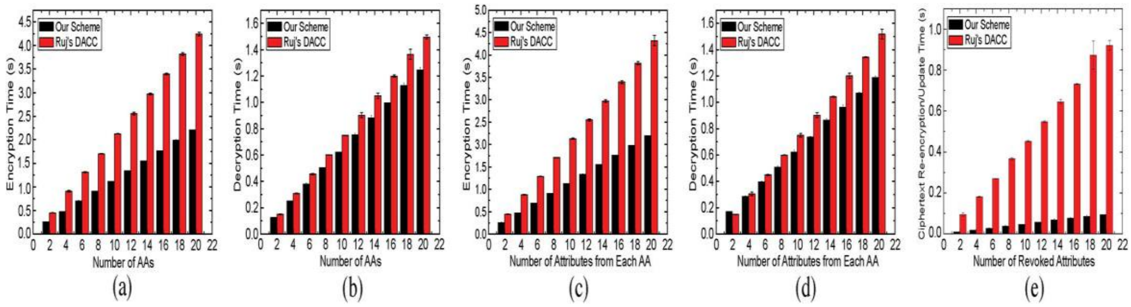


Fig 1. This diagram shows Comparison of Computation Time. (a) Encryption. (b) Decryption. (c) Encryption. (d) Decryption. (e) Re-encryption (Yang and Jia, 2014).

In conclusion, the authors' scheme had less encryption and decryption time as compared to Ruj's DACC scheme. This means that the computation time of the author's scheme is more desirable.

Based on what the authors of the proposed method have presented, there are still remaining questions as they claimed that their proposed scheme can achieve both forward security and backward security. However, they did not show experiments in their paper and there are no results presented on security part of their method to prove that indeed the scheme can achieve forward security and backward security. The authors only showed the algorithms of their proposed solution and concluded by emphasizing that their scheme can achieve both forward security and backward security the same as Wang et. al. (2013) did, by presenting algorithms of their method.

The authors gave details on what resources they have used to carry out their experiments on time computation or performance of the scheme. They also presented their results well, but still this is questionable as the authors tested their scheme against only one scheme which is Ruj's DACC scheme and tests were only conducted on Linux system whereas there are many other systems that the scheme could have been tested on to get reasonable results. This is not enough as it is difficult to tell on how the scheme perform as compared to other schemes and on different systems.

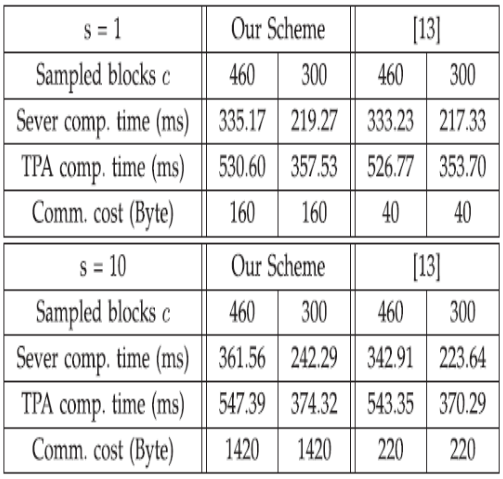
To conclude this, experiments need to be done on revocation attribute method and present the results and show how it does against other proposed schemes in terms of performance and security on many other different systems, the same as (Schnjakin and Meinel 2013) did on their experiments, using more than one system to test their scheme, so that a concrete conclusion can be made.

3 Third party auditor (TPA) Technique

Wang et. al. (2013) proposed a third party auditor scheme which its main goal is to ensure that privacy preserving public auditing is possible on cloud data storage. The scheme has five (5) major components that guarantees its safety and performance, namely public auditability, storage correctness, privacy preserving, batch auditing and lightweight.

Public auditability, this component allow third party auditor to examine the properness of data on cloud that is on request without getting a replica of the entire data or resulting to extra online problems to users of the cloud. Storage correctness, ensures that there are no cheats on cloud server that will be able to pass the third party auditor's audit without keeping a complete data of the user (Wang et. al. 2013). Privacy preserving, this ensures that the third party auditor cannot get data content of the user from the information that was collected when auditing process toke place. Batch auditing, enable third party auditor with secure and effective auditing capability to deal with many auditing delegation from many different users at the same time (Wang et. al. 2013). Lightweight, is the component that allow third party auditor to carry out auditing with the smallest amount of communication and computation overhead.

Experiments were conducted to test the performance of privacy preserving protocol and batch auditing method. Wang et. al. (2013) state that third party auditing/user side process was deployed on the workstation that had an Intel Core 2 processor with a speed of 1.86 GHz, 2.048 GB of RAM and a 7,200 RPM Western Digital 250 GB Serial ATA drive. To further describe the experimental environment, the authors indicated that on the implementation side of the cloud server process, the Amazon Elastic Computing Cloud (EC2) was used with a large instance type, which had 4 EC2 Compute Units, 7.5 GB memory, and 850 GB instance storage. All algorithms were deployed using C language and the authors' code used Pairing-Based Cryptography (PBC) library version 0.4.21. The experiment used an MNT elliptic curve, with 159 bits base field size and entrenching degree 6. All the simulation results are the average of 20 tests (Wang et. al., 2013)

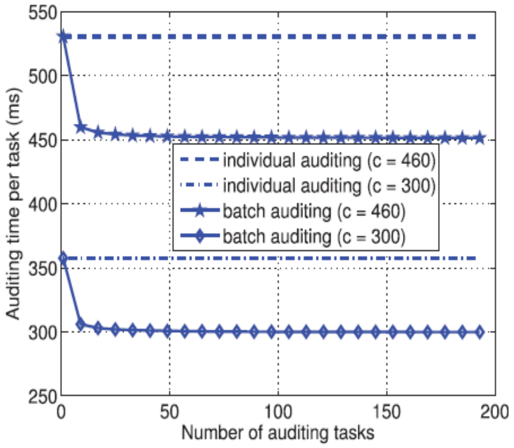


s = 1	Our Scheme		[13]	
Sampled blocks *c*	460	300	460	300
Sever comp. time (ms)	335.17	219.27	333.23	217.33
TPA comp. time (ms)	530.60	357.53	526.77	353.70
Comm. cost (Byte)	160	160	40	40

s = 10	Our Scheme		[13]	
Sampled blocks *c*	460	300	460	300
Sever comp. time (ms)	361.56	242.29	342.91	223.64
TPA comp. time (ms)	547.39	374.32	543.35	370.29
Comm. cost (Byte)	1420	1420	220	220

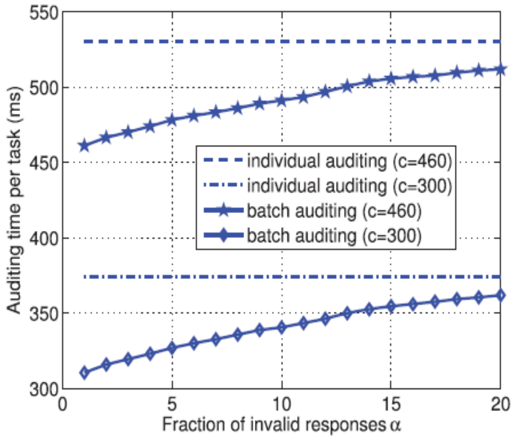
Table 1 Privacy-Preserving Protocol (Wang et al. 2013)

Table 1 shows performance of the authors' scheme "under different number of sample blocks" (Wang et. al. 2013).



Graph 1 Batch Auditing Method (Wang et. al. 2013)

Graph 1 shows a "comparison on auditing time between batch and individual auditing" (Wang et. al. 2013).



Graph 2 Batch Auditing Method (Wang et. al. 2013)

Graph 2 shows the difference between batch and individual auditing when 256 portion of responses are not valid: for each task auditing time represent overall auditing time divided by tasks number.

In conclusion, Batch auditing decreased the third party auditor's computation cost, as over fifteen percent of task auditing time were saved. The scheme can remove offline guessing attacks with the cost of slight greater communication and computation overhead.

It is clear that the authors of the proposed scheme did not perform any experiment on security aspect of their scheme specifically on storage correctness, privacy-preserving and batch auditing methods as they are the major one concern with making sure that data stored in cloud server is secure. The authors did not show security results of their methods. They only provided equations and algorithms for storage correctness, privacy-preserving and batch auditing methods and they concluded by emphasizing that their methods is secure based on equations and algorithms they came up with. Algorithms are well presented to indicate how the methods can provide security. The methods on the side of security is still questionable as experiments needs to be carried out to get full prove of whether the methods can provide security the authors of this research are claiming.

The authors described the experimental set up well for testing the performance of their proposed methods. They also showed the results of their tested methods. The experiments and results presented are for privacy preserving and batch auditing methods, other components of the scheme are not tested. Therefore, it is not confirmed in the authors' paper on how those components perform as there are contributing to the general performance of the scheme. Experiments need to be conducted on untested components of the scheme.

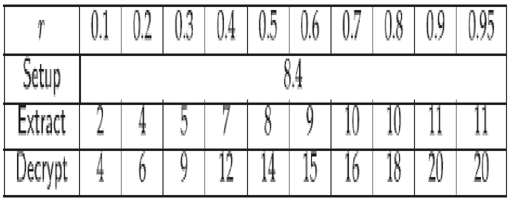
Looking at table 1 which presented the results of two schemes one supporting privacy-preserving (authors scheme) and the one not supporting privacy preserving, experiments also need to be conducted to test authors scheme against schemes that support privacy preserving so that a solid, fair judgment and conclusion can be made on the performance of their scheme.

4 Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage

Chu et. al. (2014) proposed public-key cryptosystem scheme which its main aim is to allow one to combine any number of secret keys to produce a single key for easy selections of ciphertext set in cloud storage and let files which are outside the set to remain confidential. As to make sure that this scheme achieve what it designed for, five polynomial-time algorithms were created, namely setup, KeyGen, Encrypt, Extract and lastly Decrypt.

Setup algorithm is executed by owner of the data to establish the public system parameters, thereafter, data owner also execute KeyGen algorithm to generate public or master secret key pair. At this stage anyone who want to encrypt data can do so, by running encrypt algorithm and decide what ciphertext class associated with the data to be encrypted. Chu et. al. (2014) states that, “the data owner can use the master-secret key to generate an aggregate decryption key for a set of ciphertext classes via Extract”. “Finally Decrypt algorithm is executed by delegatee who received an aggregate key generated by Extract” (Chu et. al. 2014).

To understand how the scheme is performing, experiment was conducted on Setup, KeyGen, Encrypt, Extract, and Decrypt polynomial-time algorithms. Chu et. al. (2014) state that, “pairing-based cryptography (PBC) Library version 0.4.18 for underlying elliptic-curve group and pairing operations were used”. “The test machine was sun ultrasparc IIIi system with dual CPU (1,002 MHz) running Solaris, each with 2-GB RAM” (Chu et. al., 2014).



r	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	0.95
Setup	8.4									
Extract	2	4	5	7	8	9	10	10	11	11
Decrypt	4	6	9	12	14	15	16	18	20	20

Table 2 (Chu et. al., 2014)

Table 2 shows performance of some scheme’s components with different delegation ratio.

In conclusion, the execution time of setup, KeyGen and Encrypt are not dependent on delegation ratio, therefore in experiment KeyGen toke 3.3 milliseconds whereas encrypt toke 6.8 milliseconds. The scheme dealt with 65 536 ciphertext classes and are adequate for fine grained data sharing in many situations.

The authors of this proposed scheme have well-articulated on how they carried out the performance experiment of the scheme by stating the resources they have used. They tested all the components of the scheme as they indicated on their paper and presented the results of those components, being Setup, KeyGen, Encrypt, Extract and Decrypt. Even if they authors did well on other areas of the scheme there are questions which remained unanswered as the results presented by authors are only of the proposed scheme. It is still not confirmed in the paper of this authors on how the proposed scheme perform against other schemes as there are no other schemes results presented in the paper for comparison like (Yang and Jia 2014) did, to test their scheme against Ruj’s DACC scheme for comparison even though it is not enough to test a scheme against only one scheme.

Like research by Yang and Jia (2014) and research by Wang et. al. (2013) illustrated that their results are of the average of 20 tests, it is not confirmed in this authors paper on how many times did the authors repeated their experiment to ensure reliability of the results.

For a concrete conclusion about this method/scheme to be made, more experiments need to be carried to show its performance against other existing proposed schemes. As the authors indicated that only delegatee who received aggregate key can decrypt an encrypted data, it was expected for security experiment on the scheme to have been done, and therefore, experiments are required to be done on security aspect of this scheme and tested against other schemes.

5 Conclusions

In this paper the most current research papers on security techniques on cloud storage systems have been thoroughly looked into and evaluated. Both security and performance of the techniques were evaluated. Even though, all the research on security aspect of the schemes were more theoretical, all the schemes presented algorithms well to illustrates on how the schemes can protect data stored in cloud storage systems. Experiments need to be conducted on all the research evaluated in this paper to implement security algorithms proposed to prove claims made by authors.

On performance aspect of the schemes the research evaluated in this paper have selectively illustrated on how components of the schemes perform. Only research by Chu et. al. (2014)

presented the results of all components of the scheme. Attribute revocable method proposed by Yang and Jia (2014) clearly showed that its computation time for encrypting and decrypting data is a desirable one compared Ruj's DACC method. On research done by Wang et. al. (2013), batch auditing proposed illustrated that it can achieve less computation time as compared to individual auditing method with that is more preferable. On research done by Chu et. al. (2014) it is difficult to draw a conclusion as the scheme is not tested against other schemes for comparison. Therefore, tests and results are needed of the proposed scheme against other schemes.

On research evaluated in this paper it is difficult to draw a solid conclusion on which of the presented research can provide a better security because no experiments have been conducted to implement security algorithms proposed. Performance tests of all the research was carried out with some resources of different versions and different schemes had different components tested, with that it is difficult to draw a concrete conclusion on which of the three schemes has a better computation time.

As mentioned earlier more experiments are needed on all the research evaluated in this research paper, but based on what the research have presented different research could be integrated to form a solid security technique and also achieve better performance. Research by Yang and Jia (2014) and Wang et. al. (2013) could be put together to achieve security and performance required in cloud storage systems.

References

Chu C-k, Chow S.S.M, T-zeng W-G, Zhou J and Deng R.H, 2014, 'Key-Aggregation Cryptosystem for Scalable Data Sharing in Cloud Storage', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25 Issue 2, Page 468-475.

Han J, Susilo W, Mu Y and Yan J, 2012, 'Privacy- Preserving Decentralized Key-Policy Attribute-Based Encryption', *IEEE Transactions on Parallel and Distributed Systems,* Vol. 23 Issue 11, Page 2150.

Hur J, 2013,'Improving Security and Efficiency in Attribute-Based Data Sharing', *IEEE Transactions on Knowledge and Data Engineering,* Vol. 25 Issue 10, Page 2271.

Hur J and Noh D.K, 2011, 'Attribute-Based Access Control with Efficient Revocable in Data Outsourcing Systems', *IEEE Transactions on Parallel and Distributed Systems,* Vol. 22 Issue 7 Page 1214.

Li M, Yu S, Zheng Y, Ren K and Lou W, 2013, 'Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption', *IEEE Transactions on Parallel and Distributed Systems,* Vol. 24 Issue 1 page 131.

Schnjakin M and Meinel C, 2013, 'Scrutinizing the State of Cloud Storage with Cloud-RAID: A Secure and Reliable Storage above the Clouds', *IEEE International Conference on Cloud Computing*, Vol. 6, Pages. 310 – 317.

Wang C, Chow S. S.M, Wang Q, Ren K and Lou W, 2013, 'Privacy- Preserving Public Auditing for Secure Cloud Storage', *IEEE Transactions on Computers,* Vol. 62 Issue 2, Pages 362-372.

Wang Q, Wang C, Ren K, Luo W and Li J, 2011, 'Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22 Issue 5, Page 847.

Yang K and Jia X, 2014, 'Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage', *IEEE Transactions on Parallel and Distributed Systems,* Vol. 25 Issue 7, Pages. 1735-1744.

An Evaluation of Current Power Management Techniques Used In Mobile Devices

Gabriel Tshepho Masabata

Abstract

Mobile devices currently depend on measures such as smart batteries to deal with power-hungry resources running on them. Several techniques are being introduced that can be used to better manage power in the mobile devices. This paper focuses on the analysis, comparison and evaluation of three different techniques used to manage power consumption in mobile devices, these include: thermal management techniques, energy measurements and models and energy aware OS. Basing on the evaluation, one technique that outperformed the rest was be presented and recommended for further research.

1 Introduction

Currently mobile devices are quickly becoming the most frequent means by which people connect with family, friends and the World Wide Web. Devices such as smart phones and cellular phones help in doing so. They come equipped with many resources that demand high power to run.

According to Benjamin et. al. (2010) each device has a user anticipated power lifespan. By being able to prolong the device battery life, people can perform more tasks with their devices (Benjamin et. al. 2010). Power management is necessary as the current power-saving techniques are tailored based on device capabilities (Chan et. al. 2013). Depending on how the user uses the device, battery life is therefore directly impacted.

Some users may simply use their device for applications like Bluetooth, Wi-Fi and Mobile Hotspots that place different energy demands on the device (Abousaleh et. al. 2014). However with all the convergence of these applications on the devices, the capacity of batteries cannot keep up as power demands incease rapidly. Other limitations are brought forth by the devices processing and storage capabilities becoming increasingly powerful (Chan et. al. 2013). This too demands tremendous power from the device batteries.

Depending on the nework the device is connected to (3G, GSM or WiFi), energy consumption occures basing on which of the network requires more power (Carroll and Heiser 2012). In this era of pervasive computing, most mobile devices now use smartphones which have power-hungry applications that demand a certain amount power to operate.

This paper looks into research currently being undertaken into using power management techniques to reduce power consumption in mobile devices. Techniques such as energy aware thermal management techniques will be looked into. The paper will critically assess the conclusions reached from a number of research papers already written. With the evidence and scientific methods used in mind, the conclusions will be correlated. This is to reach a personal conclusion basing on the knowledge gained.

2 Literature Review: Power Management Techniques

The manner in which mobile devices consume energy can quickly sap their limited battery resources. A variety of research papers have been analyzed and key topics have also been highlighted that are relevant in the field of power management.

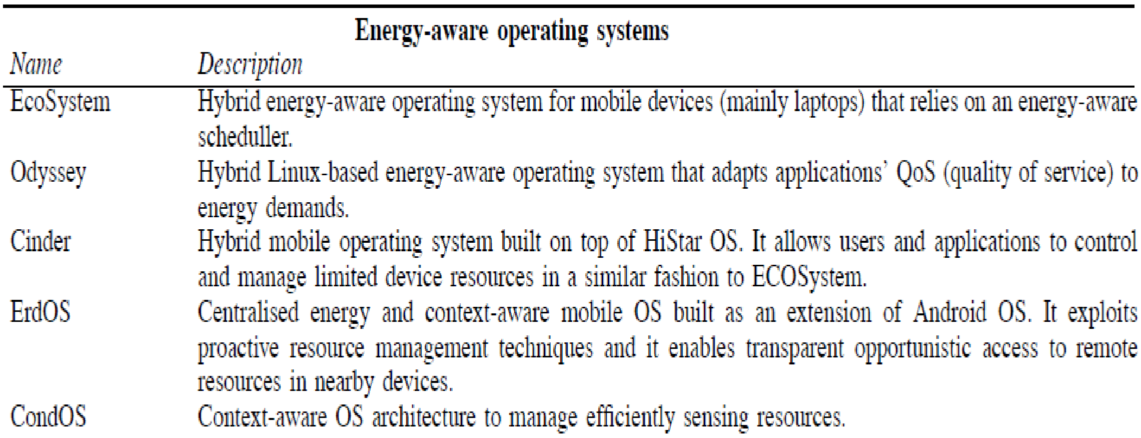
2.1 Energy Aware Operating Systems (OS): Hybrid OS

Energy efficiency in mobile devices still raises the main question of who is to be responsible for power management, the applications, OS or both. Rodriguez and Crowcroft (2012) claim that the right answer is both, but then suggests that this can be done at the OS level. In this research paper by Rodriguez and Crowcroft (2012), the intention of the investigation was to reduce power consumption by merging energy management techniques and device resources. The authors claim that this will be done by leveraging coaction between applications and OS as most of the research about power saving in mobile devices only looks at handling individual parts expeditiously rather than from an overall OS viewpoint.

Roy et. al. (2011) also stated that efficient power management can be achieved by first understanding how the user requires resources from the mobile device. Rodriguez and Crowcroft (2012) added that the key interest in energy aware OS is fuelled by the power restrictions of current mobile devices as applications now require more power to function hence reducing battery life to minimum operation time. Roy et. al. (2011) further claims that resource and energy management being done solely at the OS can present some scalability issues and with that in consideration, they proposed a hybrid solution.

Roy et. al. (2011) stated in their research paper that their proposed hybrid solution of integrating the applications and OS is possible with the use of systems that follow a hybrid approach. The research provided good insight about the systems tested during the experiments, however experiments never displayed the actual testing of the systems; EcoSystem, Odyssey, Cinder, ErdOS and CondoOs. Their OS testing techniques was never conducted on any other system other than the specified five, and so there is questionable evidence to conclude this testing technique as competent (Roy et. al. 2011).

Rodriguez and Crowcroft (2012) further states that new energy management tools, resource profilers and schedulers will have to be developed to support the software-level energy management



Energy-aware operating systems	
Name	*Description*
EcoSystem	Hybrid energy-aware operating system for mobile devices (mainly laptops) that relies on an energy-aware scheduller.
Odyssey	Hybrid Linux-based energy-aware operating system that adapts applications' QoS (quality of service) to energy demands.
Cinder	Hybrid mobile operating system built on top of HiStar OS. It allows users and applications to control and manage limited device resources in a similar fashion to ECOSystem.
ErdOS	Centralised energy and context-aware mobile OS built as an extension of Android OS. It exploits proactive resource management techniques and it enables transparent opportunistic access to remote resources in nearby devices.
CondOS	Context-aware OS architecture to manage efficiently sensing resources.

Table 1 Descriptions of Energy-aware operating systems (Rodriguez and Crowcroft 2012)

Results clearly show that EcoSystem, Odyssey and Cinder are Hybrid OS which means that the claims made about merging the mobiles application and the OS has been confirmed.

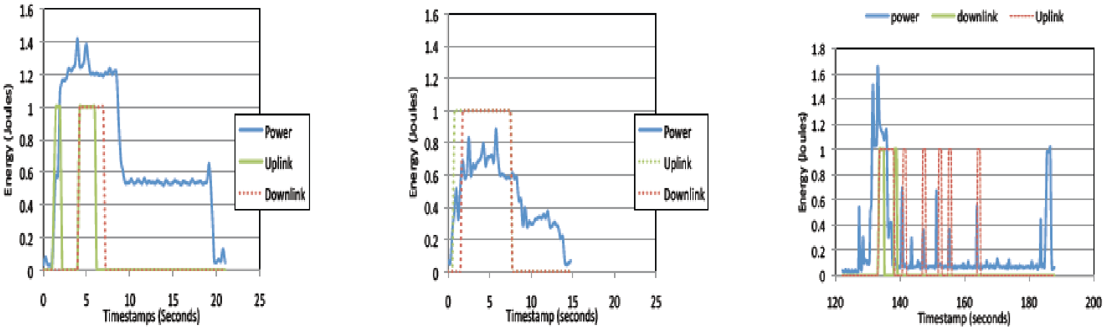
The authours concluded that the use of hybrid OS can significantly help better manage power consumption. However, the scalability issues that will arise outweigh the advantages of implementing the technique (Rodriguez and Crowcroft 2012).

2.2 Energy Measurement and Models

According to Carroll and Heiser (2012), morden smartphone hardware designers have integrated power saving features to enable hardware parts to regulate their power usage based on requested funtionality and performance.. This paper by Carroll and Heiser (2012) investigates how energy models can be used for design that would help manage power consumption in mobile devices. This technique tries to measure and record the manner in which mobile devices utilize energy under situations such are data transmission, resource utilization and power profiles such as WiFi connectivity.

Knowledge gained from the models help developers design devices with features that can regulate power usage such as functionality that allows users to select a preferd power profile, hence extending battery life (Carroll and Heiser 2012). The first test/ experiment carried out by Carroll and Heiser (2012) was basing on how energy consumption in joules of three power profiles, namely power, uplink and downlink for WiFi, GSM and 3G networks compared and which comsumed the most power.

The authors claimed that WiFi would be the network that has power profiles that consume the most energy and was correct as the results supported this claims. The test lasted for 2.5 hours as a controlled lab experiment. This was the avarege time the three identical mobile devices could all perform at their maximum capacity across the three networks (Carroll and Heiser 2012).



(a) 3G: Power Profile - 50K

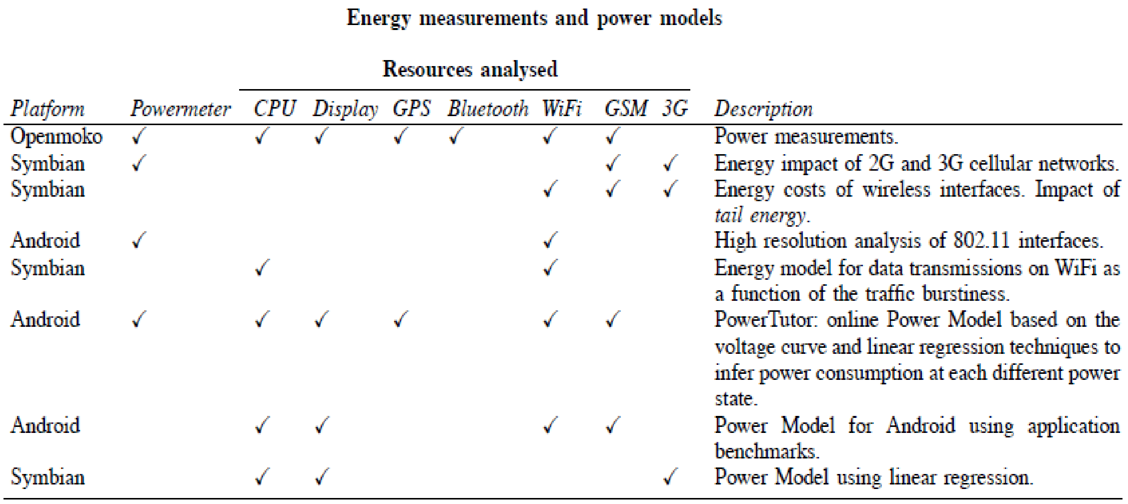
(b) GSM: Power Profile - 50K

(c) Wifi: Power Profile - 50K

Figure 1 Results of Power profiles for Power, Uplink and Downlink of 3G(a), GSM(b) and Wifi networks(c) with energy set to 50K (Carroll and Heiser 2012)

A second experiment carried out by Caroll and Heiser (2012) presented findings of how Android, Symbian and Openmoko Neo Freeruner phone (2.5G) consumed power using specified mobile’s resources. However the manner in which the findings were presented failed to clearly show any models and how the measurements were done.

According to Zhang et. al. (2010) experiments on the Openmoko yeilded positive results after using a external high resolution power meter to show that display and GSM are the most energy intense component. The findings from the Openmoko test were corroborated with the power usage of a Nexus One and HTC Dream (Table 2) (Zhang et. al. 2010)



Energy measurements and power models

		Resources analysed							
Platform	*Powermeter*	*CPU*	*Display*	*GPS*	*Bluetooth*	*WiFi*	*GSM*	*3G*	*Description*
Openmoko	✓	✓	✓	✓	✓	✓	✓		Power measurements.
Symbian	✓						✓	✓	Energy impact of 2G and 3G cellular networks.
Symbian						✓	✓	✓	Energy costs of wireless interfaces. Impact of *tail energy*.
Android	✓					✓			High resolution analysis of 802.11 interfaces.
Symbian		✓				✓			Energy model for data transmissions on WiFi as a function of the traffic burstiness.
Android	✓	✓	✓	✓		✓	✓		PowerTutor: online Power Model based on the voltage curve and linear regression techniques to infer power consumption at each different power state.
Android		✓	✓			✓	✓		Power Model for Android using application benchmarks.
Symbian		✓	✓					✓	Power Model using linear regression.

Table 2 Energy measurements and power models (Carroll and Heiser 2012)

The experiments continues by the authors modeling four usage profiles (WiFi+SA, WiFi, GSM and 3G) and simulating the energy consumed by the profiles each day based on transfer of different data sizes (Figure 2). Both 3G and GSM consumed more energy as data transmission continued.

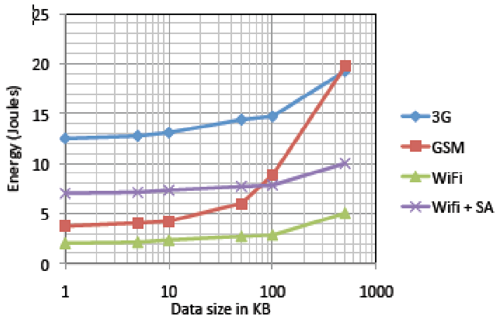


Figure 2 Graphic result of Data size in KB against Energy in Joules (Carroll and Heiser 2012)

The authours concluded that the use of energy management and models to gather data on how energy is utilized can help provide information on which mobile resouces uses more power. The information can the help manage power consumption in the devices (Carroll and Heiser 2012).

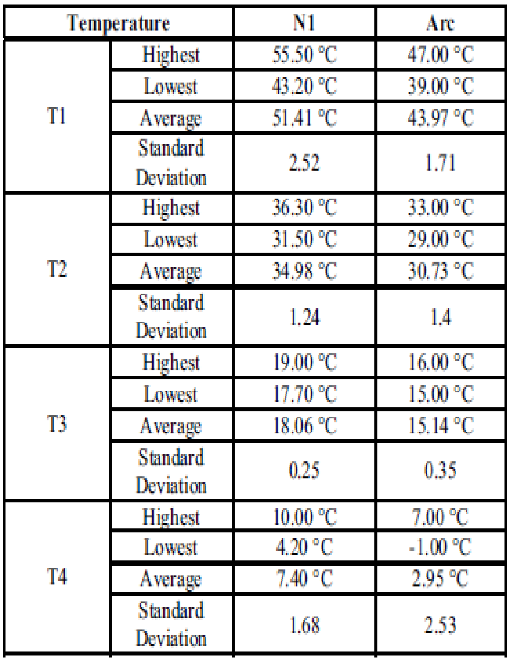
2.3 Thermal Management Techniques

The ultimate goal of energy management in most mobile devices that use rechargeable batteries is to maximize the lifetime of the device (Jung et. al. 2012). In their research paper, Jung et. al. (2012) investigates how energy consumption in mobile devices relates to the functioning temperature of the devices and how power can be managed using knowledge gained. Devices require thermal management techniques to efficiently manage their energy and improve reliability in the process (Brooks and Martonosi 2013).

The work conducted by Mulas et. al. (2008) on the thermal management techniques was significant as it provided insight on how this techniques are used as ways of reducing power consumption in the device systems. The claims made by Jung et. al. (2012) that using thermal management techniques in the mobile devices can prolong battery lifespan were good as experiments conducted proven the claims.

Jung et. al. (2012) conducted an experiment based on the assumption that energy efficiency can be achieved through low system temperature. The conditions of the experiments were set as two Android Smartphones, Nexus One (NI) and Xperia Arc (Arc) were selected for the test equiped with voltage sensors, temperature sensors and current sensore. The author assignied devices the same level of workload with varying operating temeperatures.

Each experiment began with both the smartphones having 80% of their battery capacity remeining and ends it when the system turns off. Experiment failed to state justification for doing so. The experimental environment was used to control the systems temperature.



Temperature		N1	Arc
T1	Highest	55.50 °C	47.00 °C
	Lowest	43.20 °C	39.00 °C
	Average	51.41 °C	43.97 °C
	Standard Deviation	2.52	1.71
T2	Highest	36.30 °C	33.00 °C
	Lowest	31.50 °C	29.00 °C
	Average	34.98 °C	30.73 °C
	Standard Deviation	1.24	1.4
T3	Highest	19.00 °C	16.00 °C
	Lowest	17.70 °C	15.00 °C
	Average	18.06 °C	15.14 °C
	Standard Deviation	0.25	0.35
T4	Highest	10.00 °C	7.00 °C
	Lowest	4.20 °C	-1.00 °C
	Average	7.40 °C	2.95 °C
	Standard Deviation	1.68	2.53

Table 3 Temperature sets used for the experiment on N1 and Arc (Jung et. al. 2012)

System Lifetime: Basing on the results below, Jung et. al. (2012) concludes that battery lifespan does not simply increase as temperature rises or falls. Results show that Arc lasts longer in all the tests than N1.

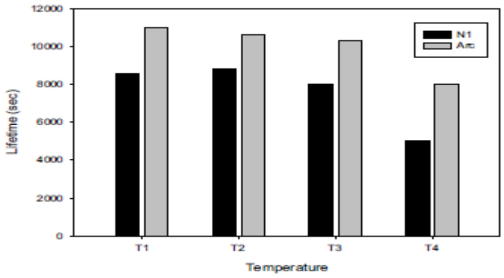


Figure 3 Available lifetime in each temperature set for N1 and Arc (Jung et. al. 2012)

Power Consumption: Basing on the results below, the research states that the N1 and Arc uses more energy when functioning under high temperatures. Results show that N1 consumes more power in all the tests than Arc (Figure 4).

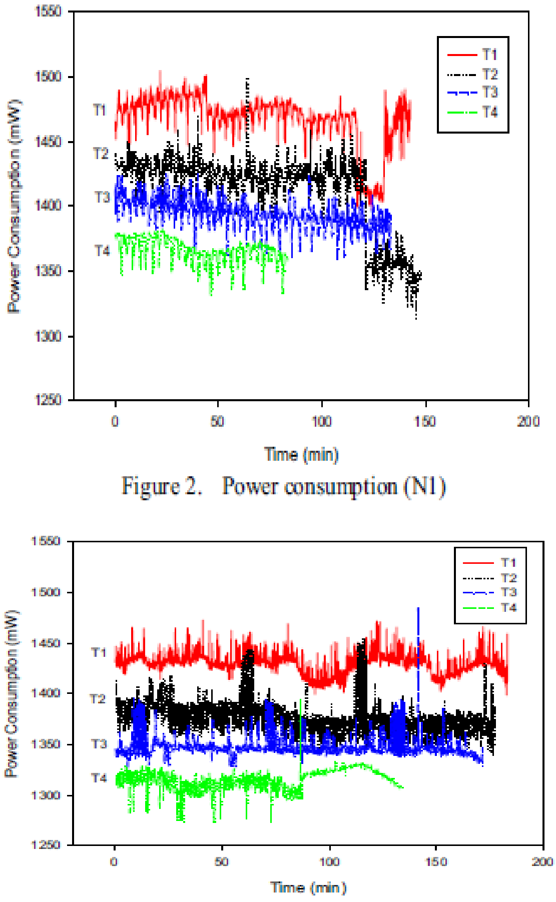


Figure 2. Power consumption (N1)

Figure 3. Power consumption (Arc)

Figure 4 Power consumption levels of N1 and Arc (Jung et. al. 2012)

Available Energy: Basing on the results below, the total energy rises as temperature increases. Results show that Arc has more available energy than N1 in all tests.

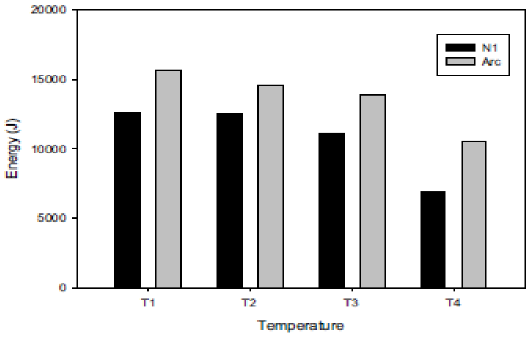


Figure 5 Energy consumed for N1 and Arc (Jung et. al. 2012)

The authours concluded that the device temperature does indeed affect how power is consumed. Devices using thermal manage techniques better manage power consumption and lasts longer battery wise (Jung et. al. 2012).

3 Critical Evaluation

The claim about merging resources and energy management to reduce energy consumption in mobile devices has been carefully examined by Roy et. al. (2011) to produce evidence that it can be achieved. Rodriguez and Crowcroft (2012) did a good review by stating why there is a need for energy awareness in mobile OS. However even with scalability problems that could arise due to reliance on the OS, Roy et. al. (2011) was able to suggest a solution (hybrid OS) that overcomes this issue. Authors could have looked into multi-hybrid OS that allows a device to run more than one OS.

The method used to confirm the applicability of Energy-aware OS in the findings shared by Roy et. al. (2011) do indeed state that a hybrid Energy-aware OS can be used to merge applications and OS in the mobile devices. The hybrid solution does expeditiously handle resources and ultimately accomplish power savings by reducing energy consumption (Roy et. al. 2011).

The findings presented by Rodriguez and Crowcroft (2012) do show positive results as three hybrid systems are described however the results fail to show how the hybrid systems where tested. As claimed by Rodriguez and Crowcroft (2012), new energy management tools, resource profilers and schedulers would have to be developed to support the software level energy management as they are required.

On the other hand methods used to confirm the applicability of Energy Measurement and Models in mobiles hansets has a strong base as experiments executed by Carroll and Heiser (2012), do indeed show that energy models can be used to test various power profiles. The findings from the models allows designers and developers to observationally estimate the power usage of different power profiles using the measurement results (Carroll and Heiser 2012).

Results from Figure 1 show that for 3G and WiFi, the power profile that consumes the most energy in the shortest time intervals is mobile power. Only in GSM does both Uplink and Downlink power profiles consume higher energy than Power. Claims made by Carroll and Heiser (2012) were proven to be accurate.

The comparison of how resources consume energy in different platforms was excellent as the results displayed which platform consumes the most power (Table 2). However Carroll and Heiser (2012) failed to explain why they selected the used values to model profiles/ resource. Other platforms such Roy et. al. (2011) proposed hybrid solutions could have been considered for experimentation to further gather energy consumption measurements and models.
Carroll and Heiser (2012) did an excellent job in using various testing factors such as energy consumption of transfers of different data sizes (Fig 3) and Power profiles of 3G, GSM and Wifi networks (Figure 1) to show their impact on consumption of energy on the mobile devices.

After analysing the research methodology used by Jung et. al. (2012) regarding device temperature and battery lifetime, this technique has been validated with a series of experiments and comparisons to similar techniques by other authors. Jung et. al. (2012) used a good testing strategy to evaluate the importance of thermal management in mobile devices as mostly positive results were gathered form it. However the experiment failed to consider the possibility that testing devices of the same platform (Android) can affect the overall results as different platforms require different electrical capacity to function. Additional testing is reqiured to validate wherethere platforms have any effect on the results.

Both results and the authors from Figurre 4 experiments by Jung et. al. (2012) suggests that the mobile device lifetime does not simply last longer basing on the temperature reading. From the graph it is clear that Arc has a longer lifetime than N1. In regards to power consumption, results show that the devices actually use more power when the temperature is high, further emphasising the importance of thermal management in the devices as claimed by Brooks and Martonosi (2013).

Compared to the other two techniques, Jung et al. (2012) used an good method of gathering and presenting the results for available energy after all the four tests were conducted. In their research, Mulas et. al. (2008) supported assumptions made by Zhou et. al. (2012) suggesting that the reason why energy in devices rises as temperature increases is because as the temperature grows, the output voltage and battery capacity increases. Overall, the experiment and analysis presented by the authors were justified and addressed the issue at hand (power management).

4 Recommendations

Using hybrid OS is good in that power management is handled solely at the OS level. Developers could also use multi-hybrid OS that utilizes more than one OS in the same device enabling users to be able to, by choice use the one they find power conservative.

The use of energy management and models could be implemented as a device testing method rather than a power management technique as results gathered could be used to design other power management technique.

Recommendations also include the use of thermal management techniques for future use in mobile devices as a power management technique as most devices also require temperature regulation to also manage power consumption.

5 Conclusions

Power management is one of the most important features any mobile device should have and effectively utilize. The power management technique that is easy to use and emplement is the most helpful one. After evaluating a few power management technique, it is clearly evident that the use of thermal management techniques suggested by Jung et. al. (2012) helps in better managing power consumption in mobile devices. It can be concluded by stating that temperature regulation in mobile devices to better manage power usage is the one of the most important features required in power hungry mobile device designs.

Alternatively techniques such as the use of hybrid OS and energy models do prove applicable but lack support from other authors that carried out simillar research that could support the proven claims and assumptions. Energy aware OS technique presented by Rodriguez and Crowcroft (2012) is not a viable method since further developments would need to be done in order for the device to support the merging on top of needing a hybrid OS and tested OS are not well known/used OS such as Blackberry OS.

A technique that would use the mobile device hardware to thermally manage system lifetime, power consumption and available energy based on preference would be very helpful for the users as battery life would be extended.

References

Abousaleh M., Yarish d., Arora D., Neville S. W., and Darcie t.e. 2014, 'Determining Per-mode Battery Usage within Non-trivial Mobile Device Apps', Victoria, Pages 202-209.

Benjamin R. M., John P. D., Randolph C. M., and Joseph G. T., 2010, 'Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices', Virginia, Pages 52-60.

Brooks D. and Martonosi M., 2013 'Dynamic Thermal management for High Performance Microprocessors', *In proc. of the 7th international symposium on high-performance computer architecture (hpca)*, Monterrey, Mexico, Pages 171-182.

Carri W. C., Nicholas B., and Singh J. P., 2013, 'Network-assisted Mobile Computing with Optimal Uplink Query Processing', *IEEE transactions on mobile computing*, Vol. 12, No. 6, Pages 1065-1068.

Carroll A. and Heiser G., 2012, 'An Analysis of Power Consumption in a Smartphone', *In proceedings of the 2010 usenix conference on usenix annual technical conference*, Berkeley, Pages 21–21.

Jung W., Kim D., and Cha H., 2012 'Observing Thermal Characteristics of Energy-Aware Mobile devices', *2012 IEEE international conference on embedded and real-time computing systems and applications*, Yonsei University, Seoul, Korea, Pages 465-468.

Mulas F., Pittau m., Buttu m., carta S., Acquaviva A., Benini L., Atienza D., and

Micheli G. D., 2008, 'Thermal Balancing Policy for Streaming Computing on Multiprocessor Architectures', *In proc. of the design, automation and test in europe conference and exhibition, munich*, Germany, Pages 734–739.

Roy A., Rumble S. M., Stutsman R., Levis P., Mazi`eres D., and Zeldovich n., 2011, 'Energy Management in Mobile Devices with the Cinder Operating System', *Proceedings of the sixth conference on computer systems*, New York, Pages 139–152.

Vallina-roDriguez N. and Crowcroft J., 2012, 'Energy Management Techniques in Modern Mobile Handsets', *IEEE communications surveys & tutorials*, Vol. ii, No. 12, Pages 1-20.

Zhang L., Tiwana B., Qian Z., Wang z., Dick R. P., Mao Z. M., and Yang L., 2010, 'Accurate Online Power Estimation and Automatic Battery Behavior Based Power Model Generation for Smartphones', *In proceedings of the eighth ieee/acm/ifip international conference on hardware/software codesign and system synthesis 2010*, New York, NY, USA: acm, Pages 105–114.

Zhou x., Xu y., Du Y., Zhang Y., and Yang J., 2012, 'Thermal Management for 3D Processors via Task Scheduling', *In proc. of the 37th international conference on parallel processing (icpp)*, Portland, OR, USA, Pages 115-122.

An Evaluation Of Current Wide Area Network Cyber Attack Detection Methods Aimed At Improving Computer Security

Hayley Roberts

Abstract

Cyber attacks on wide area networks are the most common attack on computer systems advancing so rapidly that more research is needed to keep data secure. This paper describes an evaluation of current research aimed at solving a problem with cyber attack detection within wide area networks. Methods of cyber attack detection and how effective they are at dealing with and detecting such attacks on computer systems are compared. This is in order to determine the most effective method for cyber attack detection within wide area networks. Recommendations are made regarding the best method to use for improving computer security in this field by analyzing, comparing and evaluating different research recently carried out in recent years. Overall this paper concludes what actions both individuals and companies should take in order for everyone to benefit fairly from detection methods for use on wide area networks to improve computer security.

1 Introduction

Computers and technology form a part of our daily lives and without it the world would no longer function. With technology advancing ever so quickly and cyber attackers finding more ways to hack into systems and steal information, the demand for a Cyberattack Detection System (CDS) which is capable of improving security is on the increase. Cyber attackers always seem to be one step ahead of any software which claims to stop intruders on networks, and if new technology does become available it is not long before the cyber attackers have found a way around it. Filshtinskiy (2013) conducted an experiment of how quickly cyber attackers could enter a system once a new detection system had been added. He claims that attackers *"can race ahead of the pack, figuring out how to steal from somewhere before anyone realised"*.

1.1 Limitations Of Cyber Detection Systems

Current knowledge is always very limited when it comes to CDSs as cyber attackers develop new technology to enter systems and networks unlawfully on a daily basis. This *"presents a challenging problem because it must be addressed in a rapidly developing environment"* (Thaw D, 2013) which we do not have the knowledge to achieve. Cyber attackers target Wide Area Networks (WANs) to access information on websites such as credit card details and a recent study suggests that there is *"not enough technology available at this point in time to completely stop these types of attacks"* (Edwards C, 2014) or to detect them. More research is needed into this specific area to help detect and stop cyber attacks on WAN to improve security.

1.2 Research Being Conducted

This is in order to determine the most effective method for cyber attack detection within WANs a literature review of current knowledge will be accessed. The main reason for this research will be to make recommendations regarding the best method to use for improving computer security in this field by analyzing, comparing and evaluating different research recently carried out in recent years to push our current boundaries of knowledge. Décary-Hétu and Dupont (2012) conducted a study and stated that we can help the world by providing a *"promising research method in conjunction with more traditional cyber attack practices in order to realise a detection systems potential"*. Researchers such as Sanders and Hannem (2012), Holt et. al. (2012), and Holt and Bossier

(2012[i] and 2012[ii]) conducted studies on CDS in general however these do not focus on the key aspects of WANs and so are irrelevant in this area of research. Once research into this security issue is looked into then it could help push more research into other cyber attack related areas.

2 Security Vulnerabilities

There are many security vulnerabilities when it comes to a WAN. One way to help prevent these security issues is to ensure that a good CDS is actively running on the network. Both individuals and business that use any type of network needs to consider certain things when security of data and systems are under threat. Common things to consider include:

- The amount of time a cyber attacker is willing to spend on a targeted network could result in whether or not they are successful in entering the system.
- Deciding whether to defend against major attacks, minor attacks, or both types of attacks at the same time.
- A type of system which is capable of deterring cyber attackers and stopping the majority of attacks coming in.

2.1 Cyber Attackers Time And Effort

Cremonini and Nizov-Tsev (2012) conducted an experiment into cyber attack investigation regarding the risks and benefits of a new CDS within WANs. Their research took a group of attackers spending a specific amount of time and effort on discovering defenders characteristics. Experiments were done in a real life environment against multiple systems with three different defense levels of basic, standard and advanced. Cremonini and Nizov-Tsev (2012) got five attackers with a set amount of time to hack into one hundred different systems with ten defenders monitoring the systems. No defender was told when their system would be attacked or for how long for, their job was to monitor the CDS on the WAN to determine if their system was successful or if the attackers gained entry without their knowledge.

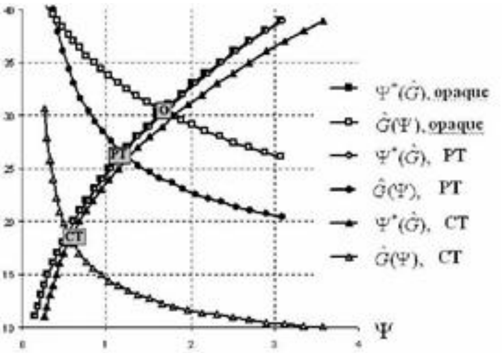


Figure 1 - Best Response Correspondences By Attackers And Defenders (Cremonini And Nizov-Tsev, 2012)

The researchers Cremonini and Nizov-Tsev (2012) claimed that *"the amount of effort an attacker will make regarding the wide area network would determine the outcome of the cyber attack detection system success"*. The researchers also concluded and determined that defenders who decided to make a security investment had far fewer successful cyber attacks than those without and even just having the protection in place deterred some attacks. These claims can be shown in Figure 1. This was the case as results showed that the best WAN CDS response corresponded with how much effort an attacker was willing to put into the attack on the WAN. Cremonini and Nizov-Tsev (2012) results mean that even with the three different levels of CDS the cyber attackers could still gain access to the system both detected and undetected; which can be seen in Figure 2. These results indicate that cyber technology is not as good at detecting cyber attacks as first thought as they still can gain access to the system depending on the time spend trying to access it.

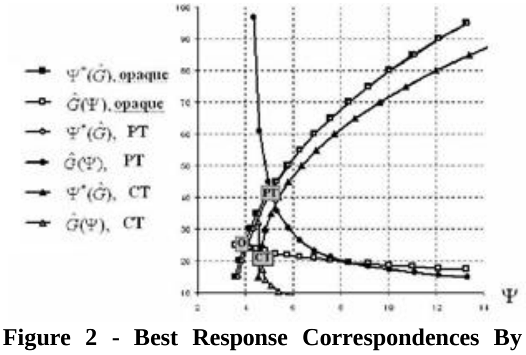


Figure 2 - Best Response Correspondences By Attackers And Defenders (Cremonini And Nizov-Tsev, 2012)

There experiments were carried out ensuring reliable data however the experiments Cremonini and Nizov-Tsev (2012) did failed to consider the possibility of different WAN settings or devices used. Some devices and networks may have their own built in security detection software and therefore additional testing is required before we can be sure of the validity of these claims. Cremonini and Nizov-Tsev (2012) should have carried out testing in the same conditions and environment on a set WAN to ensure that all the CDS testing was valid and fair.

2.2 Defend Against Minor Or Major?

Herley (2014) conducted research into the best strategy for dealing with cyber attacks. The research carried out examined whether or not all attacks should be blocked or if a CDS should focus more on immediate threats. This is due to previous research conducted by Lusthaus (2012) who stated that many cyber attacks pass through WANs on a daily basis and CDSs cannot cope with the amount of traffic resulting in the possibility of both minor and major attacks getting through into the system undetected. Herley (2014) conducted laboratory tests into how effective five different CDSs were at dealing with all incoming cyber attacks while trying to defend and prevent them all. Herley (2014) then repeated the tests with the same five CDSs but focusing on major cyber attacks first before dealing with the minor attacks. All the experiments were conducted on the same specification WAN network to ensure validity.

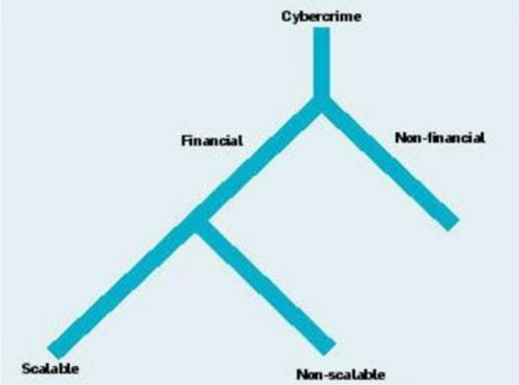


Figure 3 - Dividing Attacks As Financial And Non-Financial. Financial Attacks Are Further Divided Into Scalable And Non-Scalable (Herley, 2014)

Herley (2014) claimed that if a CDS focused primarily on aggressive major attacks then a WAN would overall be more protected from cyber attackers. Whilst research was being carried out the conclusion that scalable cybercrime with a financial implication were the cause of the majority of the major cyber attacks; this can be seen in Figure 3. Results showed a significant increase in security on the WANs were a CDS focused on the major attacks. By the end of the research Herley (2014) concluded that this was because *"with major threats cancelled out a cyber attack detection system can easily deal with minor attacks"*. This was proved correct as the time taken to deal with the major attacks and then the minor attacks at a later time proved far more effective than dealing with all the attacks at once; this can be seen in Figure 4.

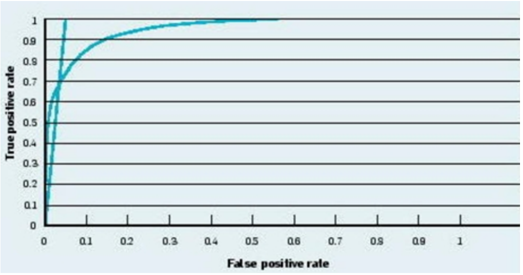


Figure 4 - Time Taken To Deal With Major And Minor Attacks Together Verses Dealing With Them Separately (Herley, 2014)

The research was carried out in a controlled environment with the same specification types of software and hardware for the WAN. The results show sufficient evidence and it does justify the claims made. If the research was to be repeated the same results should be shown. However Herley (2014) solves only part of a problem with security issues in WANs regarding CDSs.

2.3 Stopping Cyber Attacks Altogether

Dey et. al. (2012) was another researcher who did a study into effective methods of cyber detection. Research was carried out using twenty-five real life businesses all with various different WANs and used five ethical hackers to try and gain access to the system. Dey et. al. (2012) monitored how effective each system was at finding and detecting the attacks on the network. All hackers had set types of hacks to perform on each system and each hacker did five systems each. The study itself was to *"calculate if one type of cyber detection had a higher success rate at securing the threat of attacks on a wide area network than another"* (Dey et. al., 2012).

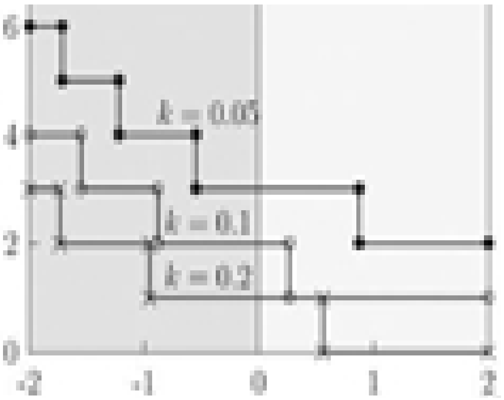


Figure 5 - Wide Area Network Security Drops Over Time When Attacked By A Cyber Attacker (Dey et. al., 2012)

Dey et. al. (2012) claimed that the results showed that no matter what protection is in place a cyber attacker will eventually gain access to a WAN system if given enough time to do so. Results did show this, and all of the CDSs which were tested showed a drop in security after time had passed since the attack begun; this can be seen in Figure 5 and in Figure 6. Both Dey et. al. (2012) and Cremonini and Nizov-Tsev (2012) have claimed that a cyber attacker can gain access to any system if given the right amount of time to do so.

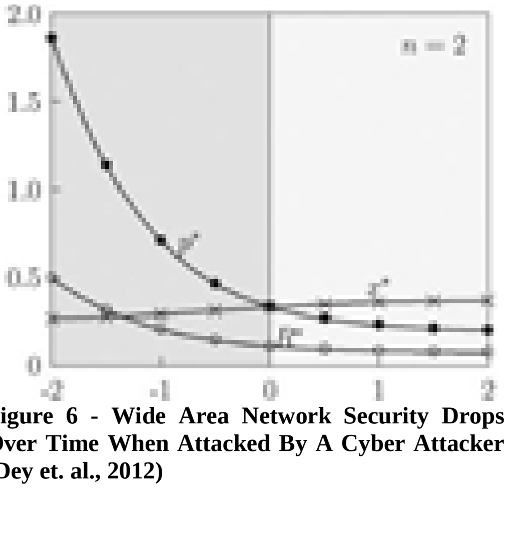


Figure 6 - Wide Area Network Security Drops Over Time When Attacked By A Cyber Attacker (Dey et. al., 2012)

Dey et. al. (2012) concluded that *"all cyber attackers will be able to gain access to any system and no cyber attack detection system will be able to defend all types of attacks"*. Although there is sufficient evidence to show that a cyber attackers can gain access to the five systems tested as long as they are given as much time as required, the results do not give any evidence that a CDS cannot stop all attacks. This is not what Dey et. al. (2012) were conducting research into and therefore their conclusion that no system can stop all types of cyber attacks is invalid. There actual tests also did not take into account that all of the WAN systems were different and also did not indicate that they checked to make sure that the ability of the hackers were the same. These two things could have had a huge impact on the results and therefore their research does have flaws in its validity.

3 Security Solutions

Solutions proposed by all researchers have their place in helping to prevent cyber attacks and increase security on a WAN. Both Cremonini and Nizov-Tsev (2012), and Dey et. al. (2012) looked at similar causes and solutions to improving security. Both can to the conclusion that cyber attacks will stop at nothing to gain access to a WAN and no CDS will be able to stop them eventually entering the system. This is all down to the time and effort (Cremonini and Nizov-Tsev, 2012) an attacker is willing to spend on a target. If an attacker spends enough time on that targets then no amount or type of CDS is going to be able to prevent it (Dey et. al., 2012). However true this may be a solution may be possible by ensuring that the CDS that is running on a network is fighting against the right types of attacks to ensure security is improved.

Herley (2014) determined that major attacks should be dealt with first and stated that *"major attacks should always take priority over minor attacks"*. By first ensuring that major attacks are dealt with the minor attacks can then be dealt with at great ease. A CDS that focuses on both types of attacks at once struggles to keep all attacks at bay and yet a CDS that focuses on the major attacks first deals with all attacks far quicker. By dealing with the attacks in a timely manner the CDS can help deter cyber attacks causing the attackers to try elsewhere, hopefully on another network. If all businesses and individuals using WANs adopted this approach to their own networks then there would be far fewer successful attacks on systems across the world.

4 Conclusions

The literature review conducted related well to the problem at hand and all the researches use their results well to drive their argument. All researches describe their experimental work and results even if some did not describe their tests in enough detail to ensure complete validity of the data presented. All research which looked into the current WAN and the use of CDSs aimed at improving computer security helped towards making final conclusions and recommendations regarding network security related issues.

There are many security issues regarding CDSs on WANs and all researches have shown a contribution to knowledge. Cremonini and Nizov-Tsev (2012) determined that a cyber attacker can gain access to a WAN despite the CDS in place given the time and effort they put into an attack. Herley (2014) determined that major attacks should be dealt with first, and Dey et. al. (2012) determined that all CDSs at this present moment in time cannot stop all attacks on a network.

This research has proved that cyber attacks on WANs are the most common attack on computer systems advancing so rapidly that more research is needed to keep data secure. The current research aimed at solving a problem with cyber attack detection within WANs cannot completely solve all problems with the security issues. Methods of cyber attack detection and how effective they are at dealing with and detecting such attacks on computer systems are beginning to be understood. The most effective method for cyber attack detection within WANs would indicate that the method proposed by Herley (2014) would be best at this present moment in time. These recommendations are made due to the researcher's evidence for improving computer security in this field by analyzing, comparing and evaluating different types of CDSs.

Both individuals and companies should implement a CDS that will deal with major threats before attempting to deal with the minor threats which are less likely to cause security flaws in the system. This will help increase security on WANs however will not solve all the problems relating to CDSs on WANs. Improving this one area of weakness will benefit everyone using a WAN by contributing to eliminating major threats from networks.

References

Cremonini, M. Nizov-Tsev, D. 2012. 'Risks And Benefits Of Signaling Information System Characteristics To Strategic Attackers'. *Journal Of Management Information Systems*. 26 (3), p241-274.

Décary-Hétu, D. Dupont, B. 2012. 'The Social Network Of Hackers'. *Global Crime*. 13 (3), 160-175.

Dey, D. Lahiri, A, Zhang, G. 2012. 'Hacker Behavior, Network Effects, and the Security Software Market'. *Journal Of Management Information Systems*. 29 (2), p77-108.

Edwards, C. 2014. 'Researchers Probe Security Through Obscurity'. *Communications Of The ACM*. 57 (8), p11-13.

Filshtinskiy, S. 2013. 'Cyber Crime, Cyber Weapons, Cyber Wars: Is There Too Much of It In The Air?'. *Communications Of The ACM*. 56 (6), p28-30.

Herley, C. 2014. 'Security, Cyber Crime, And Scale'. *Communications Of The ACM*. 57 (9), p64-71.

Holt, T. Bossier, A. 2012[i]. 'Police Perceptions Of Computer Crimes In Two Southeastern Cities: An Examination from The Viewpoint Of Patrol Officers'. *American Journal Of Criminal Justice*. 37 (3), p396-412.

Holt, T. Bossier, A. 2012[ii]. 'Predictors Of Patrol Officer Interest In Cyber Crime Training And Investigation In Selected United States Police

Departments'. *Cyber Psychology, Behavior And Social Networking*. 15 (9), p464-472.

Holt, T. Bossler, A. May, D. 2012. 'Low Self Control, Deviant Peer Associations, And Juvenile Cyber Deviance'. *American Journal Of Criminal Justice*. 37 (3), p378-395.

Lusthaus, J. 2012. 'Trust In The World Of Cyber Crime'. *Global Crime*. 13 (2), p71-94.

Sanders, C. Hannem, S. 2012. 'Policing 'The Risky': Technology And Surveillance in Everyday Patrol Work'. *Canadian Review Of Sociology*. 49 (4), p389-410.

Thaw, D. 2013. 'Criminalizing Hacking, Not Dating: Reconstructing The CFAA Intent Requirement'. *Journal Of Criminal Law And Criminology*. 103 (3), p907-948.

Current EMG Pattern Recognition Research Aimed At Improving Upper Limb Prosthesis Control

Molly Sturman

Abstract

Research into the application of electromyogram (EMG) pattern recognition is showing that it is essential in the intuitive and natural control of upper limb prosthetics; however, clinically it is not often used due to its limitations. In this paper, the methodology of three different pattern recognition classification methods will be compared, evaluated and analysed, these include: single LDA classification, simultaneous parallel approach and conditional parallel approach. The purpose is to investigate the advantages and disadvantages of each of the approaches. Recommendations will be made from the results for further research and comparisons regarding the uses of each technique and their real life application.

1 Introduction

The application of electromyogram (EMG) pattern recognition in the control of upper limb prosthesis has been a popular topic of research over the last five years. However, it is not clinically used due to its limited dexterity (Scheme, 2011) and EMG recordings can become unreliable over time (Zhang et. al. 2013) making the limbs not suitable for everyday situations. Hargrove, L J et. al. (2013) conducted research into increasing the number of EMG channels to improve the accuracy of the pattern recognition system without needing more electrodes. Amsuss et. al. (2014), Scheme (2011) and Zhang et. al. (2013) provide research into making prosthesis more clinically viable and allowing the user more intuitive control.

EMG pattern recognition could offer the user more control of the prosthesis, including allowing them to gain more movement and control of the force they put into their movements, as it will learn how the EMG changes depending on the user's intent (Khokhar, Z et. al. 2010).

This research paper will focus on studies that have been carried out on using EMG pattern recognition to improve upper limb prosthetics. The paper will discuss different classification strategies, results of the research and critically evaluate the strength of the outcome. Conclusions will be made throughout the paper regarding how each method will affect the prosthesis and then finally summarized at the end. A literature review was undertaken which consisted of 12 papers. The primary object of these papers was improving the dexterity of upper limb prosthesis. This paper uses the research of those that focused on improving the pattern recognition and artificial intelligence by looking at the classification errors and processing time.

2 Background

There are three types of pattern recognition methods which will be evaluated, and these shall be referred to as single LDA classification, simultaneous parallel classification and conditional parallel classification.

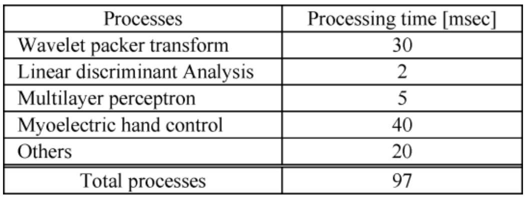
Young, A et. al. (2013) explains that with the conditional parallel approach each classifier makes an assumption that a discrete motion is active. The parallel approach also makes an assumption: "a set of features characterizing the EMG signals repeatedly describes a state of muscle activation and maps it to one degree of freedom" (Wurth, S M, Hargrove, L J 2013). However, both studies show that this assumption may not always be correct. On the other hand, Single Linear Discriminant Analysis does not rely on any assumptions or previous knowledge.

3 Linear Discriminant Analysis

Chu, J et. al. (2007) conducted a study comparing a Linear Discriminant Analysis (LDA) approach to three other feature projection methods - Principal Components Analysis (PCA), Non Linear Discriminant Analysis (NLDA) and Self-Organizing Feature Map (SOFM) - to try to determine whether this was a useful method in classification accuracy in a short time span. It was initially decided that the processing time should be less than 300ms with a 125ms window increment to avoid delays.

The study focused on nine types of hand motions, using four surface electrodes to measure the EMG signals. The hand motions assessed were: “flexion and extension of the wrist, radial and ulnar flexion of the wrist, pronation and supination of the wrist, opening and grasping of the fingers, and relaxation.” (Chu, J et. al 2007). The study was conducted in twenty sessions per participant using ten participants. The motions were randomly ordered in each session and the participants were asked to perform them for five seconds each.

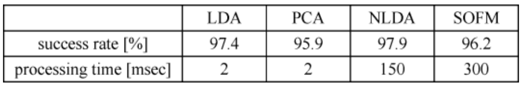
The results table Fig. 1 shows the processing time to the millisecond of the different processes and the total processing time for the movement to be completed. The total processing time was 97ms which met the requirements and proved no obvious delay to the user.



Processes	Processing time [msec]
Wavelet packer transform	30
Linear discriminant Analysis	2
Multilayer perceptron	5
Myoelectric hand control	40
Others	20
Total processes	97

Fig. 1 Average Processing Time For Real Time Pattern Recognition (Chu, J et. al. 2007)

Fig. 2 shows the classification success rate percentage and the processing time for LDA, PCA, NLDA and SOFM. Whereas the NLDA has the highest success rate, the processing time was significantly higher than the LDA, which had only a 0.5% difference in the success rate. Due to the processing time of the NLDA the conclusion was drawn that the LDA performed better, as the NLDA did not meet the requirements of the processing time being less than 125ms window increment.



	LDA	PCA	NLDA	SOFM
success rate [%]	97.4	95.9	97.9	96.2
processing time [msec]	2	2	150	300

Fig. 2 Average Values of MLP Classification Success Rate and Processing Time (Chu, J et. al. 2007)

The research was focused and carried out well. The paper explains the method used well and has quite a thorough description. The motions assessed were relevant and commonly used, and the order of the movements was randomised. However, there was no reference in the paper as to how the motions were randomised.

The study concludes that the LDA method gave the user the ability to operate the prosthetic with a high success rate and a low processing time. The results confirm that the LDA meets both of these requirements, with a processing time of 2ms, leaving the total processing time as 97ms, which is well within the requirements. This reflects the conclusion that the LDA method, in an experimental setting, was the most appropriate method in this test.

Real life application, however, is a limitation of this study as the study concludes that more research will need to be done to make it more appropriate. The study was conducted assuming that the EMG signals came from a ‘static contraction in a steady-state motion and fixed movement velocity in a transient-state motion’ (Chu, J et. al. 2007). This means that the study is difficult to apply to everyday tasks for an individual and therefore, requires further research.

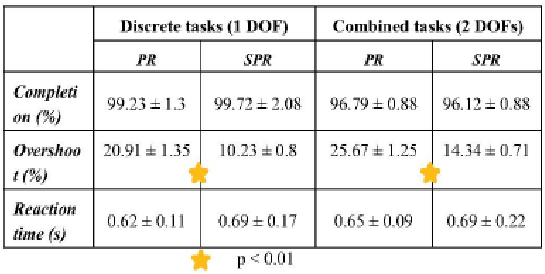
The method used by Chu, J et. al. (2007) compared the LDA method to three other methods. Hu, H et. al. (2012), on the other hand, compared the study to five extended LDA methods, which could be used as further research into the area, although some of the classification methods do overlap. The types of LDA methods studied by Hu, H et. al. (2012) may help to further the research by Chu, J et. al. (2007) to improve its real life application.

4 Simultaneous Parallel Approach

Wurth, S M, Hargrove, L J (2013) used on a strategy with two simultaneous parallel classifiers to create a more natural and intuitive upper limb prosthesis operation. This was compared to a sequential method to assess the advantages of simultaneous pattern recognition for prosthetics.

The study was tested on eight right handed people aged between 23 and 30. Six surface electrodes were placed equidistant around the forearm on the subjects. A real time single LDA was used as classification for the output into one of the motion classes to test the sequential pattern recognition. For simultaneous pattern recognition, two parallel classifiers were used; one for each degree on freedom. The difference between the sequential pattern recognition and the simultaneous pattern recognition was assessed with control strategy, target type and session as fixed factors and the participant classified as a random factor.

Fig. 3 show both of the methods tested for both discrete and combined tasks and rated on completion, overshoot and reaction time. The paper states that the results reflect the initial hypothesis that a simultaneous pattern recognition system will be more appropriate when participating in combined tasks.



	Discrete tasks (1 DOF)		Combined tasks (2 DOFs)	
	PR	*SPR*	*PR*	*SPR*
Completion (%)	99.23 ± 1.3	99.72 ± 2.08	96.79 ± 0.88	96.12 ± 0.88
Overshoot (%)	20.91 ± 1.35 ★	10.23 ± 0.8	25.67 ± 1.25 ★	14.34 ± 0.71
Reaction time (s)	0.62 ± 0.11	0.69 ± 0.17	0.65 ± 0.09	0.69 ± 0.22

★ $p < 0.01$

Fig. 3 Results showing the difference between simultaneous pattern recognition (SPR) as opposed to sequential pattern recognition (PR) in both discrete and combined tasks. (Wurth, S M, Hargrove, L J 2013)

The research by Wurth, S M, Hargrove, L J (2013) was explained thoroughly and conducted well.

These results show that there is potential for simultaneous pattern recognition to be a useful and appropriate method for multi - functional upper limb prosthesis. However, other methods would provide a much quicker reaction time and this is essential in creating an intuitive prosthetic.

Young, A et. al. (2012), used an alternative hierarchal approach which was based upon using a parallel approach. This took a similar approach but built on it to create a more complex method that provided low classification errors.

They conclude that whilst the research is a good basis for further studies, it did not necessarily show that the simultaneous parallel approach was a more appropriate method than a sequential method. This conclusion is representative of the results and the limits to the research that was conducted.

5 Conditional Parallel Approach

Young, A et. al. (2013), proposed a method known as the conditional parallel approach. It is an extension of a parallel approach which uses two simultaneous classifiers. They compared this to a regular parallel method and the LDA method to determine whether their method was an improvement on other methods for improving the degrees of freedom in upper limb prosthesis.

The study was conducted on three male non-amputee subjects and three female non-amputee subjects as well as two above elbow (trans-humeral) amputees who had undergone TMR surgery. All of the partakers were seated, un-restrained and were not given any feedback throughout the experiment. There were six pairs of electrodes places equidistant from one another around the circumference of the upper forearm for the non-amputee subjects and eight pairs of electrodes placed on the biceps and triceps for the amputee subjects.

Four degree of freedom classifications tests were carried out for the three classification strategies on the participants. The performance of the classification strategies was evaluated by the percent of incorrect classifications. Comparisons were made with classification error as the response variable, and the fixed factors as the classifier strategy, degree of freedom configuration and the number of channels. The participant was classified as a random factor.

The results in Fig. 4 show that for both two and three degree of freedom configurations the LDA and conditional parallel method performed significantly better than the parallel method. The conditional parallel performed a lot better than a single LDA classifier with a two degree of freedom configuration and slightly better using a three degrees of freedom configuration.

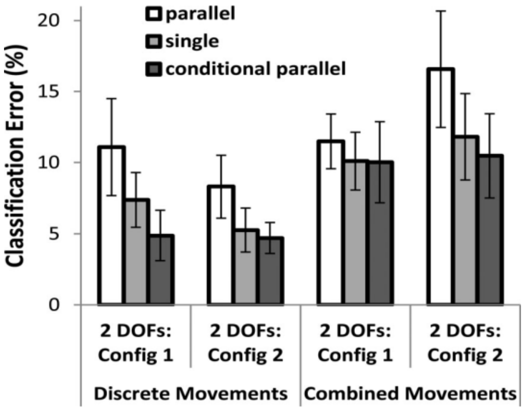


Fig. 4 Classification Errors for the three different methods for the varying degrees of freedom. "Configuration 1 is wrist and hand DOFs and configuration 2 is rotation and hand DOFs. Results are shown for six channels of EMG and are an average of six subjects. Error bars show ± 1 standard error of the mean." (Young, A et. al. 2013).

The research conducted by Young, A et. al. (2013) was a well thought out and in depth approach. The study was tested on both amputee and non – amputee participants which helps to confirm that the method will be applicable in the real world. The participants were all treated the same, ensuring that the results were not affected by position of the subject. as the amputee subjects had undergone TMR surgery, the placement of the electrodes was appropriate

This study did not test online control; however, there have been many other studies, such as Hargrove, L J et. al. (2011), which gives evidence of a strong correlation between online controllability and classification accuracy.

The conclusions drawn in this paper show that the conditional parallel approach is aimed at trans-radial amputees, although future research could look into using similar techniques for TMR subjects also. The paper also states that the research could be used to develop a deeper look into using simultaneous pattern recognition and the conclusion that a conditional parallel approach has few classification errors than the parallel approach appears to be justified.

6 Comparison of Pattern Recognition Techniques

The research evaluated throughout this paper all had an aim to improve upper limb prosthesis using EMG pattern recognition. The methods all had advantages and limitations stated in their conclusions and results allowing comparisons to be made for a recommendation for the most appropriate method.

The conditional parallel approach had advantages of low classification errors, as the results by Young, A et. al. (2013) show that they had lower errors in both discrete and combined movements. This is a significant advantage as low classification errors will provide fewer problems for the user.

LDA does also have a low classification error, shown both by Young, A et. al. (2013) and Chu, J et. al. (2007), although not as low as the conditional parallel approach. It does, however, have a very quick processing time which will provide a more intuitive prosthesis for the user. Research into methods extending from LDA and improving the real life application may make it a more suitable option, however.

The research by Wurth, S M, Hargrove, L J (2013) showed that, whilst simultaneous pattern recognition had advantages of high completion percentage and lower overshoot percentage over sequential pattern recognition in combined motions, there was the disadvantage of it having a slower performance in the discrete motions, whilst being equally efficient otherwise. The simultaneous approach is inferior to the other methods analysed as it shows no significant or consistent advantages in improving upper limb prosthesis.

The results all show that all three methods analysed have limitations, such as real life application or online control, which require further study to allow fully intuitive results.

7 Conclusions

In this paper, pattern recognition methods of classification to improve upper limb prosthesis have been analysed and evaluated. A literature review has shown various ways that different researchers have attempted to improve the dexterity, control and intuitiveness of prosthetics.

A comparison of the research appears to prove that, although the parallel approach does have some advantages, both the conditional parallel and the LDA are superior methods to the parallel approach in terms of classification accuracy and processing time. This shows that in an effort to improve upper limb prosthesis the parallel approach would not currently be recommended.

From the research reviewed, the recommendation could be made that the conditional parallel approach will provide the lowest classification errors for both the discrete and combined movements which will be a positive argument for the user. Research should be conducted into using both the LDA method and the conditional parallel method to improve the processing time to create an upper limb prosthetic with full, immediate functionality.

References

Amsuss S, Goebel, P M, Jiang N, Graimann, B, Paredes, L, & Farina, D 2014, 'Self-Correcting Pattern Recognition System of Surface EMG Signals for Upper Limb Prosthesis Control', *IEEE Transactions on Biomedical Engineering,* Vol. 61, pages 1167 – 1176.

Chu, J, Moon, I, Lee, Y, Kim, S & Mun, M (2007), 'A Supervised Feature-Projection-Based Real-Time EMG Pattern Recognition for Multi-function Myoelectric Hand Control', *IEEE/ASME Transactions on Mechatronics,* Vol. 12, pages 282 – 290.

Hargrove, L J, Kuiken, T A, Lock, B A & Smith, L H 2011, 'Determining the Optimal Window Length for Pattern Recognition-Based Myoelectric Control: Balancing the Competing Effects of Classification Error and Controller Delay, *IEEE Transactions on Neural Systems and Rehabilitation Engineering,* Vol. 19, pages 186 – 192.

Hargrove, L J, Gajendran R, Tkach D C 2013, 'Crosspoint Switching of EMG Signals to Increase Number of Channels for Pattern Recognition Myoelectric Control', *6th Annual International IEEE EMBS Conference on Neural Engineering San Diego California,* 6 – 8 November, pages 259 – 262.

Hargrove, L & Wurth, S 2013, 'A Real Time Performance Assessment of Simultaneous Pattern Recognition Control for Multi-functional Upper Limb Prostheses', *6th Annual International IEEE EMBS Conference on Neural Engineering San Diego California,* 6 – 8 November, pages 851 – 854.

Hu, H, Limsakul, C & Phukpattaranont, P (2012), 'Application of Linear Discriminant Analysis in Dimensionality Reduction for Hand Motion Classification', *Measurement Science Review,* Vol. 12, pages 82 – 89.

Khokhar, Z, Menon, C & Xiao Z G, 2010, 'Surface EMG pattern recognition for real-time control of a wrist exoskeleton', *BioMedical Engineering Online 2010*, pages 1 – 17.

Scheme, E 2011, 'Electromyogram pattern recognition for control of powered upper-limb', *Journal of Rehabilitation Research & Development,* Vol. 48, pages 643-660.

Young, A J, Smith, L H, Rouse, E J, Hargrove, L J, 2012, 'A new hierarchical approach for simultaneous control of multi-joint powered prostheses', *The Fourth IEEE RAS/EMBS International Conference on Biomedical Robotics and Biomechatronics, Roma, Italy*. June 24-27, pages 514 -520.

Young, A J, Smith, L H, Rouse, E J, Hargrove, L J, 2013, 'Classification of Simultaneous Movements Using Surface EMG Pattern Recognition', *IEEE Transactions on*

BioMedical Engineering, Vol. 60, May, pages 1250 -1258.

Zhang X, Huang, H & Yang, Q, 2013, 'Real-Time Implementation of a Self-Recovery EMG Pattern Recognition Interface for Artificial Arms', *35th Annual International Conference of the IEEE EMBS Osaka Japan, 3 - 7* July, pages 5926 – 5929.

Positive and Negative: Effects Video Game Use Can Have on Personality Development

Shaun Watson

Abstract

Previous research has found that consistent video game use can have a string of effects on an individual in terms of personality, a large proportion of which cover the negative impacts. Research has shown that certain video games can increase cognitive abilities, increase social activities and influence various emotional personality traits such as aggression, joy and acceptance among various other emotions in adolescents particularly. The purpose of this article is to examine various aspects of personality development due to video game use and show both the positive and negative sides of these aspects. Considering both sides of this matter is important to maintain a well-balanced argument and in turn to produce useful recommendations and conclusions. Finally, to better understand the effects video games have on an individual's personality, it is vital to consider a range of aspects in relation to personality.

1 Introduction

In recent years video games have become a major part of almost all children's and adolescent's lives, with 97% playing for at least one hour a day in the United States (Granic, I et.al. 2013). A large proportion of the research done into the field of video games tends to focus on the negative impacts they have and what problems they cause and amplify such as the research done by (Markey, P.M and Markey, C.N 2010). Although this research is all valid and reasonable, a more balanced argument is needed which compares both negative and positive impacts of consistent video game use. In no way does this imply no research has been done into the positive side, research done by (Granic, I et.al. 2013), (Durkin, K et. al. 2013) and (Velez, J.A and Ewoldsen, D.R 2013) all show various positive elements of video game use. The aim of this paper is to place the positive side of "gaming" next to the negative side in terms of the effects it has on personality development mainly in adolescents and then compare the two sides with evidence to back up the arguments shown. This paper will focus strongly on the effects and changes that video games can have on personality in terms of skills, senses, abilities and traits of an individual. To conclude by offering some recommendations and backed up conclusions based on solid evidence. These recommendations will provide a basis for further research and possibly impact on design choices within future video games.

2 Aspects of Personality Development

The following research will be split up into four different sections which will account for the four aspects of personality development strongly linked to video game use: Cognitive, social, emotional and educational aspects. Although personality is a broad subject and could be split into many different categories, the four previously mentioned coincide with video game use.

2.1 Cognitive Effects

"Contrary to conventional beliefs that playing video games is intellectually lazy and sedating, it turns out that playing these games promotes a wide range of cognitive skills**"** (Granic, I et.al. 2013). The cognitive effects tend to be the most often considered effect of video game use; this is particularly true in terms of educational games. "From a psychological perspective, the potential of games to support and extend cognitive development is of particular interest." (Durkin, K et. al. 2013).

K. Durkin et. al. (2013) looked at various experiments that have been conducted which try to expose the cognitive changes due to video game use. One of these studies measured adolescents suffering from ADHD who were aged 6 to 12 and a comparison group of boys with TD, and were tasked with playing a relatively straight forward game, Point Blank and a slightly more complex one, Crash Bandicoot. Specifically, participants were tested in conditions where they had to maneuver a character along a route and not touch the side and in the latter, they had to do the same but also had to perform and action at a certain point (spin to destroy objects). Results of the former proved similar among both groups but the boys with ADHD performed poorly at the latter and kept performing the action at incorrect times. They concluded that working memory deficits in these children alter when confronted with different tasks.

The experiment could easily be recreated again if needed, although only a small group of boys, the results are reliable as the conditions were fair and accurate as all taking part in the experiment were under the exact same conditions and all participants were within a narrow age group therefore we can rely on this evidence. Overall this study shows that certain tasks in video games can have an effect on cognitive functions within the brain such as working memory and attention.

While it seems apparent that children become proficient at specific skills in video games, it appears that they generally keep video game play separate from other areas of life, so it is not clear whether these preferences and skills transfer to other contexts. (Hamlen, K.R 2013) This statement raises the question of why adolescents play video games and what is their motivation which in turn raises the question of why do people cheat at video games and what affect can cheating have on their personality as a result.

A study conducted was a qualitative study with three teenage boys. (Hamlen, K.R 2013) The data was collected via interviews with analysis, these interviews focused on the participant's background, details of the participant's background with cheat codes and participant's views on cheating in video games and academically. From this they concluded that those who choose to avoid the effort of completing the game tend to be those who are more likely to cheat in academics.

This experiment could not be done by anyone else as the questions that were asked in these interviews are unknown and it would strongly depend on the analysis of the individual (the interviewer). Although the topics of the questions are suitable as it is plausible that they could be used to see a correlation in cheating at video games and also in everyday life, this experiment can't be relied upon because of the lack of information given.

2.2 Social Aspects

The social side of video gaming is often overlooked by the press and general public. They tend to see video gaming as an antisocial pastime and link it strongly to loneliness and depression although there are some who see it as the complete opposite of this. Socializing is arguably the most important factor for the development of an individual's personality; interactions with others can define various characteristic through adolescence. Interactions can mold the opinions of a person and the outlook they have on various topics therefore can have an impact on personality. Social gaming refers to playing with other players either competitively or cooperatively, (Velez, J.A and Ewoldsen, D.R 2013)

An extensive study conducted that delved into the social side of gaming involved various experiments. One of which was very detailed and planned extensively. The experiment involved thirty six students (13 women, 23 men) who were randomly assigned to one of two game conditions (prosocial game vs neutral video game) the ages ranged from 19 to 43 years old. Tetris was used for the neutral video game and City Crisis was used for the pro social game. After participants played the game for 8 minutes, one of two experimenters left the room and informed a male confederate to enter in the role of a lonesome ex-boyfriend of the other experimenter. The actor was instructed to act very aggressive to the experimenter and get frustrated, as a measure of Prosocial behavior, it was measured if the participant intervened or not. The minimum requirement was that the participant spoke at all, if this occurred, the actor immediately left the room, if not then the other experimenter reenter and asks the actor to leave still in character.

Ten out of the 18 participants who played City Crisis intervened with the situation compared to only 4 out of the 18 who played Tetris meaning 56% of the participants in the prosocial video game condition helped, whereas only 22% in the neutral video game condition helped. They concluded from this that video games had an effect on the decision making process of the participant's and that playing a prosocial game increased the chances of compassionate behavior by up to three times. (Greitemeyer, T and Osswald, S 2010)

The study could very easily be recreated again with the information given; all conditions involved were very thorough and detailed. The students were randomly assigned and there was also a mixture in gender among the participants. The participant was completely unaware of what was about to happen in the experiment and they were given a questionnaire at the end to mask the real experiment. None of the participant's had any suspicions that the harassment scenario was not real. Therefore this study is perfectly valid and can be relied upon.

2.3 Emotional Aspects

Playing video games can have various different effects on an adolescent; one of these effects can be emotional effects. Emotions play a huge role in the development of personality, emotional tendencies can influence decision making and how others react and interact with an individual (e.g. if an individual is prone to anger) which can alter behavior.

The most controversial emotion that video games are accused of incurring is aggression. Various studies have been done looking into this accusation, such as (Willoughby T et. al. 2011), (Fraser A.M 2012) and (Espinosa P and Clemente M 2013) which show the correlation between video game use and aggressive tendencies.

A study which conducted an online survey involving 790 undergraduate students (547 women and 243 men) and which varied in ethnicity and marital status about various emotional related issues in correlation to gaming. The measurements for the study were violent video gaming, empathic concern and prosocial behavior. The actual online survey required a recruitment code to access it therefore no outside data was being collected, all participants were required to obtain consent otherwise they were unable to start the questionnaire. From this study, they concluded that males play significantly more violent video games than females and due to this females show much higher empathic concern than males and also much higher levels of prosocial behavior towards others. (Fraser A.M 2012)

Although this study included a larger ratio of women to men, it doesn't have any impact on the results. The study focused on vital topics of research which would ensure results that were useful for example they used the correlation between violent video games and the tendencies of a participant in terms of empathic concern and prosocial behavior. Although an online study, the participants were chosen from a select few universities and were briefed by their lectures on the study beforehand where they were given the recruitment code needed to access the survey therefore overall this study can be applied and counted as reliable.

A study conducted found that boys and girls who regularly played a mature rated video game were more likely to endorse four reasons to play: to compete and win, to relieve anger, modifying games and experimenting with games functionality (e.g. trying out different weapons/vehicles).

No extensive information about the study or the participant's is given, the method of the study is not enclosed so it would be impossible to recreate it in any way so although the conclusions of the study are solid and seem sensible, they can't be relied upon.

Tobias Greitemeyer (2013) conducted research to show that playing video games cooperatively increases empathic concern. Various studies were conducted within this research and various conclusions were reached as a result. Reported empathy differed across certain game conditions, exposure to violent video games resulted in a decreases in empathic concern and playing video games cooperatively resulted in an increase in empathic concern. (Greitemeyer T 2013)

2.4 Educational Aspects

“Video game play and the potential effects of game play on learning, achievement, and engagement have attracted psychologists, educational researchers, and learning scientists” (Evans M.A et. al. 2013) Learning and education are the key aspects of life that can define an individual and influence their personalities and alter how they develop. Research conducted by (Evans M.A et. al. 2013) and (Durkin, K et. al. 2013) have both looked into the effects video game use can have on education and learning.

Evans M.A et. al. (2013) used a game known as ‘The CandyFactory Game’ (CFG) in their research which was designed to accompany middle school students (aged 11 – 15) algebra readiness and emphasis on fractions. The CFG was created to enable students to physically enact their mental actions in terms of fractions. In the CFG students work their way through five levels that are designed to visually introduce them to the principles of fractions. As they progress, the CFG produces more complex scenarios therefore to complete the game students need to master the five fraction schemes which were: Whole, partitive unit, partitive, Iterative and reversible partitive. Students were accessed at the end of each level and rewarded based on the speed and accuracy they demonstrated.

The five levels enforced the students with different scenarios and ways of thinking. The purpose of the CFG is to measure the effectiveness video games can have on learning and what particular design features can improve an adolescents learning process. They concluded from this study that educational games can be beneficial in a variety of ways (e.g. allowing students to perform actions they are unable to perform in real life, competition, and reward systems).

This experiment focused entirely on the effectiveness of the game itself and little information is given about the group of participant’s other than an age range of 11 – 15 years old. No results of measurements are given other than conclusions that they reached because of the CFG. It is also noteworthy that this is just one game relating to fractions; therefore it is difficult to apply this study to actual video games not fully designed for academic purposes. Evans M.A et. al. (2013) do not claim to apply their conclusions to video games in general, they place emphasis on the fact that educational games could be beneficial for the learning process of an individual and not video games in general.

3 Discussion & Comparisons

After looking at various research, it is clear that certain theories are backed up by others and some theories don’t quite correlate to other findings therefore it is important to compare the implications of these theories.

The first aspect was the cognitive effects of video game use; we found that video game use can have an effect on working memory and attention and that these skills could be enhanced by consistent video game use to then be used in the real world. This would have an impact on the personality development of adolescents as it could potentially increase their general intelligence and problem solving abilities. The next focus was on cheating in video games, although the evidence found was unreliable, it is noteworthy to mention that cheating in video games could have a link to an individual cheating in other contexts which would have an effect on their personality as they would develop a habit of attempting to bypass any effort by cheating at any given task.

The second aspect looked at was the social effects of video game use; we looked at a study that studied the effect video games have on decision making. To put the study into the context of personality development, it shows that playing certain video games can have an effect on how an individual judges certain situations. Although this study was conducted on adults, it can also be applied to adolescents as decision making plays a huge role in growing up and can define the nature of a person. This could mean that consistent video game use could induce tendencies such as tolerance and compassion.

The third aspect looked at was the emotional effects of video game use, we looked at a study that measured the correlation between violent video games, empathic concern and prosocial behavior. This study shows that there is a correlation between certain aggressive tendencies and video game use (Violent video game use in particular) which raises the question; can the personality of an adolescent be influenced by certain video game use? This study shows that playing violent video games can show a reduction in empathic concern and a decrease in prosocial behavior. Adolescents are exposed to many different video games and many of which include violence of some nature. Although the participants of the previously described were between 18 and 29, there is no reason to believe that the effects would be any less significant on an adolescent.

On the other hand video games have often been found to allow individuals to vent their anger without consequence. (Olson C.K 2010) Video games can allow an adolescent to immerse themselves in unrealistic environment's which in turn can allow them to de stress and vent out their built up aggression where they know they are not going face any repercussions.

The final aspect looked at was education effects of video game use, we found that educational games designed specifically for use in an academic environment could be beneficial but we can't apply this to video games in general. It is difficult to apply the study we looked at to the matter of personality development. Although it would be acceptable to argue that educational games can have an impact on learning and therefore impact an adolescent's personality as a result. This is backed up by research such as (Durkin, K et. al. 2013) which looks into video games for adolescents with educational needs. Various educational needs are addressed in their research and various uses of video games to help these problems are well demonstrated such as video games to enhance the working memory of adolescent's suffering from ADHD.

4 Conclusions

By looking at the last decade in terms of 'Gaming' there has been a huge incline in its popularity and there is no reason to believe that its popularity won't continue to increase in the next decade therefore video games will continue to be prominent in a large majority of adolescents lives. After pulling together various pieces of research that cover a few positive and negative effects video games can have on personality development, we can conclude that like other media platforms (e.g. Books, Films, TV etc.) video games can have adverse effects on an adolescents personality and how they develop their unique personalities. Also, like other media platforms, it largely depends on what type of games they play. From our research we can conclude that playing violent video games consistently can result in a decrease in empathic concern and prosocial behavior although they allow an individual to vent their built up anger without consequence.

There are many aspects of the effects that video games can have on personality that we have not looked at in this research, we have only covered a very minute section of the potential research that could be conducted but the research covered is important as it exposes the fact that video games do have an effect on personality, positively and negatively.

Finally, we can see from this research that video game use can result in an increase in cognitive abilities, provide social interactions with others, provide emotional help and possibly an increase in academic performance which in turn could result in an adolescent becoming more motivated and intelligent and improve various life skills such as decision making and problem solving. On the other hand consistent video game use in certain types of games can result in emotional strains, less social interactions and poor academic performance which in turn could result in an adolescent becoming more depressed, secluded and distant.

References

Durkin K, Boyle J, Hunter S and Conti-Ramsden G, 2013, 'Video Games for Children and Adolescents with Special Educational Needs' *Zeitschrift Psychologie*, Vol. 221(2):79–89

Espinosa P and Clemente M ,2013, 'Self-transcendence and Self-oriented Perspective as Mediators between Video game Playing and Aggressive Behavior in Teenagers' *Journal of*

Community & Applied Social Psychology 23: 68 –80

Evans M.A, Norton A, Chang M, Deater-Deckard K and Balci O, 2013, ‘Youth and Video Games’ *Zeitschrift Psychologie*; Vol. 221(2):98–106

Fraser A.M, Padilla-Walker L.M, Coyne S.M, Nelson L.J and Stockdale L.A , 2012, ‘Associations between Violent Video Gaming, Empathic Concern, and Prosocial Behavior toward Strangers, Friends, and Family Members’ *J Youth Adolescence*, 41:636–649

Granic I, Lobel A and Rutger, C.M.E, 2013, ‘The Benefits of Playing Video Games’, *American Psychologist*

Greitemeyer T, 2013, ‘Playing Video Games Cooperatively Increases Empathic Concern’, *Social Psychology*; Vol. 44(6):408–413

Greitemeyer T and Osswald S, 2010, ‘Effects of Prosocial Video Games on Prosocial Behavior’, Journal of Personality and Social Psychology, Vol. 98, No. 2, 211–221

Hamlen K.R, 2013, ‘Understanding Children’s Choices and Cognition in Video Game Play’, *Zeitschrift Psychologie* ; Vol. 221(2):107–114

Markey P.M, and Markey C.N, 2010, ‘Vulnerability to Violent Video Games: A Review and Integration of Personality Research’, *Review of General Psychology*, Vol. 14, No. 2, 82–91

Olson C.K, 2010, ‘Children’s Motivations for Video Game Play in the Context of Normal Development’ *Review of General Psychology*, Vol. 14, No. 2, 180–187

Velez J.A and Ewoldsen D.R, 2013, ‘Helping Behaviors during Video Game Play’, *Journal of Media Psychology*, Vol.22 (4):190-200

Willoughby T, Adachi P.J.C and Good M , 2011, ‘A Longitudinal Study of the Association between Violent Video Game Play and Aggression among Adolescents’ *Developmental Psychology*, Vol. 48, No. 4, 1044–1057