Selected Computing Research Papers

Volume 3

June 2014

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

An Overview Investigation of Personalized Advertising to Improve the Privacy of the General User

Carl Marc Adams

Abstract

This research paper is to introduce the issues of privacy behind the campaigns of targeted and personalized advertising. Discoveries of the underlying problems will be made from a literature review. Methodologies and concepts of current personalised advertising campaigns will be identified and examined in order create a solution. The closing section of this paper concludes that businesses should take on the actions mentioned in order for everyone involved to benefit fairly from personalised advertising.

1 Introduction

As technology improves, many more new forms of personalised advertising are being used. While all tracking data of the general user, this is not always done correctly across these different forms. They are all based on tracking the behavior and actions of the user, especially while on the web. It is clear that our knowledge in data collection can be improved as commonly, the privacy of the user is invaded as the data is excessively collected. “After talking to his daughter the man discovered she was pregnant. Target had used sophisticated predictive analytics to determine that her previous buying patterns and behavior had indicated high probability of expecting a baby” (Greengard S. 2012). A father found out that his daughter was pregnant because of the personal advertising that she had been receiving from Target store; this is a prime example of privacy being invaded, for the daughter in this case. Another example, age, gender and income data are also often gathered “Nevertheless, they also are highly personal and potentially sensitive attributes that a consumer might not wish to share.” (William E et al. 2006).

So from the examples mentioned, it is clear that knowledge in privacy is lacking within the topic of personal advertising. Not accurately analyzing the data collected can keep these types of events occurring for the general user. However research has already been done on attempting to solve these problems. These consist of new methodologies to protect user’s data. “The capability of the technology to identify the personal characteristics of consumers is in potential conflict with the legitimate privacy rights of individuals.”(William E et al. 2006). An example of research concluding their findings by developing new technology for personalised advertising while keeping the users privacy from being invaded. Alternatively, concepts are created within the research that has been done, which will benefit further researchers on this topic. “This finding suggests that in evaluating how best to reach consumers through ads, managers should be aware of the multistage nature of consumers' decision processes and vary advertising content along these stages.” (Lambrecht A. 2013).

Towards this problem, this paper will conduct research of its own. This research will consist of viewing and evaluating the research of others who have attempted to resolve the issues of personalised advertising privacy for general users. By evaluating research that is already done, flaws in research can be found along with the creation of new ideas that can occur when combining methodologies and ideas of different research papers.

2 Consumer Perceptions

Hong W. et al. (2013) focus their research on Internet Privacy Concerns (IPC). Overall topic of personal information being gathered, stored, transmitted and published on the internet. Investigating how individuals perceive how their data is collected, stored and used. Hong W. et al. (2013) aim to identify alternative concepts as there has been little agreement previous literatures on this topic.

Four studies involving a total of nearly 4,000 users were conducted by Hong W. et al. (2013) to validate alternative models/concepts from those frameworks created by Multidimensional Development Theory (MDT). The main key dimensions this research looks at are collection, secondary usage, errors, improper access, control and awareness. The first study collected data from individuals using commercial websites, purposed to compare integrated concepts against two popular already existing concepts. Study two then cross validates findings from study one, using a government website instead of a commercial. Study three collected more data using commercial websites, however using revised wording in the survey, updated the concept of privacy concerns. Study four again cross validates using a government website, with the updated concept and revised wording. Each study had their own new group of around 950 users each to provide an input to the surveys.

Results were discovered once Study 1 and 2 were conducted, these showed that there was a large difference between government and commercial websites on how they collect data. "With the differences ranging from 1.26 to 1.83. Comparing the means of the dimensions in study one and study two, we found a much larger difference in the collection dimension" (Spangler W. et al. 2006). Previous research shown that there should be very little difference between the two however that was not the case this time. Study three used the revised worded survey and concept, compared to the earlier studies, the means of the statistical data returned of the collection and other dimensions were now within a closer range unlike study one and two, a range of -0.28 to 0.30. Study four cross validated this and the results of that study present results that were expected "ranging from -0.15 to 0.60" (Spangler W. et al. 2006). Confirming the results of study three. The key dimensions split into six separate dimensions allows closer study. The overall study provides an evaluation method for their privacy contexts of their websites or policies of their business. Guidelines that can be used for further research of privacy concerns. Conceptualizations of IPC were validated, as a result this research has contributed to building a better understanding of conceptualization of IPC.

Hong W. et al. (2013) paper is very recent and significant research for this literature review. A very strong input. Especially as the research included four empirical studies. Empirical studies are very reliable and accurate experiments. With the use of so many users (4,000), this would suggest a large range of different people were used. As the studies were split into four surveys, the last two being reworded. This allowed great allowance of comparison of the information returned from these surveys. Very excellent testability. Details of each survey was greatly explained, allowing other researchers to potentially reproduce the same research methods. Furthermore within the paper Hong W. et al. (2013) dedicated a section providing guidance on continuing the research, this shown great reliability as the results could be used for further research. Overall Hong W. et al. (2013) greatly contributed towards a better understanding of the conceptualization of Internet Privacy Concerns and provided a modified instrument that can be used for further research.

Spangler W. et al. (2006) explain what little users/viewers are capable of doing to prevent themselves from having their privacy invaded through television services such as TiVo. Specifically the Opt in and Opt out routes for viewers. Very little viewers understand any of this concept of having their data being gathered and being able to opt out of it, therefore very little have chosen this route. Limitations and regulations need to be in place to stop these services and businesses attempting to gather highly personal data to begin with. Spangler W. et al (2006) focus on the use of data mining techniques used to generate profiles for viewers using a specific television service. It has been identified that this service gathers highly personal information of those viewers, crossing the line of privacy.

Spangler W. et al. (2006) aim to create a data mining module prototype that creates accurate data of viewers without conflicting with legitimate privacy rights of those viewers. Spangler W. et al. (2006) overall conduct a comparison between the capabilities between their prototype (VPM) and the used technology of the service in topic. This will in turn allow them to determine whether the service is truly gathering data that viewers don't wish to have gathered. Additionally Spangler W. et al. (2006) look at viewers perceptions of privacy violation. Findings of Spangler W. et al. (2006) basically show that the less accurate the data mining technology, the more viewers must receive the personalised ads. "100 male teenagers in affluent households, and if the profiling model is 70% accurate in classifying members of this group, the PVR or service provider would have to create a pool of 143 households"(Spangler W. et al. 2006). Additionally Spangler W. et al. (2006) shed light on how consumer's negative reaction to these inaccurate ads will affect marketing statistics. Therefore companies should prevent violations and to compensate consumers suitably when violation occurs.

Spangler W. et al. (2006)'s research focuses very strongly on the topic of viewer profiling. Which relates to this literature review suitably as it still fits in with the topic collecting user data without informing the user. Covering many concepts and ideas, Spangler W. et al. (2006) compare a variety of possible solutions already out there for consumers. Comparison of a created prototype and other current methods, results were shown of just how many users would receive personal ads compared to how many user's data was collected. However the experiment that was conducted has barely been explained in detail. There is no mention of how many users were involved or how they were involved. The statistical data provided though was from research done into a PVR service provider, not the prototype. So this data is still valid, however the use of the prototype has been non-existent in this research making the reliability questionable.

Rapp J. et al. (2009)'s research aims to examine the subject of consumer's privacy and policies surrounding this area. Concerns are identified within the literature, discovering the tensions between advertisers and consumer interests. This will provide a better understanding and direction on how to move forward. Rapp J. et al. (2009) conduct literature review of many papers, covering various things from advertising basing on mailing. Internet advertisements such as click ad banners, search/behaviour data mining and finally neuromarketing which consists of potential future brain scanners that pick up responses and preferences. But most importantly Rapp J. et al. (2009) examined the responses of consumers that these literatures had conducted their experiments with. Results showed that fears were continuously raised by consumers of what companies actually do with collected information and who actually has access. More importantly, that websites should inform consumers of data collection so users become generally more aware. This should not only be a website owner's responsibility but users should gain knowledge and awareness of privacy issues in general. Information has great value, businesses are taking this information without compensating the user/consumer. This shows there is no fairness, no trading or transaction. There may be no way of producing a policy or overall regulation for this issue however the best thing consumers can do now is to become aware of these issues and protect themselves the best way they can until negotiations can be made with all parties and agreement can be made on regulation and legislation.

Rapp J. et al. (2009)'s literature review very much relates to the problem at hand. Specifically the area of internet privacy, for this research paper it provides some very strong points and evaluations of how cookies are used along with other methods such as data mining to collect user data. Referencing from very valid research papers, these claims were proven. Number of papers were reviewed specifically for the internet section and a table was provided with descriptions and recommendations from each paper. These allowed easy identification of significant issues and their partnered recommendations. These recommendations can then be focused on and compared effectively. There was no question of the validity of this information. This allowed Rapp J. et al. (2009) to conclude that users must be informed by website owners of data collection with additional personal awareness that consumers must already have.

An overall summary of the papers covering the perceptions of consumers has been very constructive in this literature review. A number of things have been discovered. One of the points discovered is that consumers have worrying lack of awareness of their data being collected secretly. As mentioned "few fully understand the widespread access and use by marketers and advertisers. Part of the problem is a true lack of interest in reading lengthy disclosure warnings" (Rapp J. et al. 2009). A more important point though, users that are aware of privacy issues believe they have very little control of their personal data, of who can collect and use it. "Specifically, online consumers deem control an important aspect of their interaction or information exchange with websites, but they do not consider themselves to have much control over" (Hong W. et al 2013) and "Nevertheless, a majority of America is concerned they have lost control over personal information, fears businesses mishandle these data, and believes current legislation does not provide sufficient protection."(Rapp J. et al. 2009) confirm this.

3 Data Mining

Hwang S. et al. (2008) aim their research at identifying the strong relationships between types of customers and the genres of products that often that appear in a transaction database, to be used to generate a list of new potential customers for a new released product. With the use of synthetic data, comparisons of performance using the algorithms Hwang S. et al. (2008) made after discovering the association rules. Then Hwang S. et al. (2008) can determine how well these new rules work in the operation of promoting new books. These rules can then be used on promotions on many various items. Results were found within Hwang S. et al. (2006)'s research. The experiments demonstrated that target marketing using relationship rules were very effective when trying to promote new books. Using a hierarchy system to classify the books and customers to be linked to. "58% and 71% of Chinese books issued to a patron can be classified in a single category at the second and first levels of the hierarchy" (Hwang S. et al. 2006). This in other words means the customers' exhibit highly changed behaviour in the categories. This shows the success of the approach used in this research depends on the use of a product hierarchy. This can only be used on some types of products however others may need more analysis in order for it to remain effective.

Hwang S. et al. (2006)'s research bases on data mining techniques which is highly relative for this literature review. Little mention of consumer perceptions is mentioned, only methods of collecting data. The experiments conducted are easily reproducible as explanations of these are very detailed. Synthetic data was generated using a number of nodes set up in a hierarchy system with children to the root of the nodes. Overall creating a leaf hierarchy system with products assigned. Normalization was used to weigh the nodes and generate statistics on frequently selected products. The aim of this experiment was to create a new approach to mining GP association rules for targeted advertising of new products without associating transaction records, this was achieved. Providing a justification that the aims had been met and knowledge had been improved. Reliability is also found within Hwang S. et al. (2008)'s research as it is detailed on how to extend the research in several directions such as improving effectiveness of the influencing of the availability of a product or using the GP association rules to recommend new products to a given customer.

4 Conclusions

As mentioned in the summary of Consumer's Perceptions section, it has been discovered there is a commonly mentioned lack of consumer awareness of how their data is being collected and used. However within this literature research there has been a methodology found that would be beneficial. "For these reasons, most ecommerce companies have established privacy policies and communicated those policies in public forums, most commonly on their Web sites" (Spangler W. et al. 2006). This is an example of what businesses can do in order to inform the consumer of what the business does with a user's data. If the consumer is informed thoroughly enough, they will be capable of making decisions on how to protect their data. Another methodology found is Hwang S. et al (2008)'s hierarchy system, although not specifically relating to the core issue, the concept of targeting advertisements to consumers without collecting highly personal data using the hierarchy system is incredibly encouraging as the data collected is not potentially damaging for the consumer. These methodologies mentioned would benefit both consumers and businesses. Ultimately from this literature review, it is certain that businesses and advertisers are very capable of and must do more to “anticipate and prevent violations” (Spangler W. et al 2006), and to compensate consumers fairly in order to prevent negative reaction towards their business. It is now known that consumers are extremely uninformed in this area and businesses are taking advantage of this. Businesses must take responsibility and provide the consumer easy access to information about how their data is being used.

References

Greengard S., 2012, ‘Advertising Gets Personal,’ *Communications of the ACM* Vol. 55, No.8, pp. 18-20.

Hwang S. Yang W., 2008, ‘Discovering Generalized Profile-Association Rules for the Targeted Advertising of New Products,’ *INFORMS Journal on Computing* Vol. 20, No 1, pp. 34-45.

Hong W. Thong J., 2013, ‘Internet Privacy Concerns – An Integrated Conceptualization and Four Empirical Studies,’ *MS Quarterly* Vol. 37, No. 1, pp. 275-298.

Lambrecht A. Tucker C., 2013, ‘When Does Retargeting Work Information Specificity in Online Advertising,’ *Journal of Marketing Research* Vol. L, pp. 561-576.

Rapp J. Hill R. Gaines J. Wilson R., 2009, ‘Advertising and Consumer Privacy,’ *Journal of Advertising* Vol. 39, No. 4, pp. 51-61.

Spangler W. Hartzel K. Gal – Or M., 2006, ‘Addressable Advertising and Viewer Profiling,’ *Communications of the ACM* Vol. 49, No 5, pp. 119-123.

A Critical Analysis and Evaluation of Current Computing Research Aimed At Enhancing Facial Recognition Systems Performance

Obruche Orugbo Emueakporavwa

Abstract

Human facial recognition system is one of the imperative areas of research that is advancing, several techniques is been introduce to improve facial recognition system performance. This paper analysed, compared and evaluated three different techniques used to enhance facial recognition systems performance, these includes fusing global and local Gabor features, Curvelete transform for 3D facial identification and ROI selection strategy. Evaluation proves that combining two of the most successful Curvelet-Transform for 3D Face Identification and Facial Expression Action Unit Detection Techniques gives enhanced performance than either alone. It also presents real world application of the techniques and some future work has been recommended.

1. Introduction

In recent times there has been advancement in facial recognition system performance.

Biometrics makes automated use of the unique personal features to establish identity, among adopted biometrics, facial recognition is certainly the most popular one due to a wide variety of possible application such as security.

There is need to improve the techniques use in computer vision, in which facial recognition is most extensively applied (Esan et al., 2013).

According to Devi & Bajaj (2010) using colour of human skin as a criterion for capturing face which encompasses sophisticated pattern recognition techniques is faster than accessing other features. Islam et al. (2012) argued that the issue of machine facial recognition is still a demanding task in pattern recognition and computer vision. On the other hand Krasimir et al., (2013) reported that 2D face recognition techniques have issues that are associated with captures of a human face. According to Lumei & Sato (2013) the complete circle of facial expression starts from a neutral to an obvious facial expression, although this paper aims at enhancing facial recognition system performance.

This survey paper critically analyse and compare research papers from different researchers on different possible methods with proving results of the claims made to enhancing facial recognition system performance, Conclusions will be made through out the paper and will all be drawn together at the end.

2. Face Recognition Using Global and Local Gabor Features

Achieving efficient face recognition system performance as Nazari & Moni (2013) claims a new face recognition algorithm using feature selection based on fusing global and local Gabor wavelet features. The proposed algorithm has been evaluated on standard ORL database containing 400 Gray-scale images, where each individual has ten pictures. The average recognition rate was evaluated using KNN and Multi-class SVM for random sets of pictures (shown in Table I and Table II).

Face Recognition Methods	**Average Recognition Rate**			
	d=4	*d=5*	*d=6*	*d=7*
Global Gabor features	78.9%	79.8%	81.9%	82.2%
Fusing G-	84.9	86.72	89.1	89.8

2DFLD [12]				
Our proposed method	88.6%	89.9%	90.5%	91.8%

TABLE I: Comparison between Global Gabor face recognition, G-2DFLD feature fusion face recognition [12], and our proposed method in term of average recognition rate with different values for d. KNN classifier is used.

Face Recognition Methods	**Average Recognition Rate**			
	d=4	*d=5*	*d=6*	*d=7*
Global Gabor features	88.6%	89.4%	95.5%	90.9%
Fusing G-2DFLD [12]	92.8	96.71	99.1	98.7
Our proposed method	97.8%	98.2%	98.8%	99.5%

TABLE II: Comparison between Global Gabor face recognition, G-2DFLD feature fusion face recognition [12], and our proposed method in term of average recognition rate with different values for d. Multi-SVM classifier is used.

The proposed techniques out performs the G2-DFLD with recognition rate of 88.6% and 97.8% respectively, this shows an increase in average recognition rate compared with the G2-DFLD.

This research is well thought out and set up, their testing is of a very high standard, because it makes use of train and test dataset on a standard ORL database covering wide range of appearance which includes race and gender, The result is also in accordance with the claims of the researcher because the experiment was conducted in such a way to ensure that variables are minimized where possible and the training set images were randomly selected with all images sizes of 112x92 pixels. This ensures that the experiment was unbiased and can actually be repeated. However, the experiment was only carried on frontal face images this proves that the techniques will have low recognition rate for images that are non-frontal or facing sideways.

Another issue was that the experiment did not state the time it takes the system to identify a possible match. Although the system may be accurate but the timing is important if the method will be applied in automated systems and the techniques happens to be slow that will be a major setback. Also the database uses Gray scale images to makes its comparison this shows that images has to be converted to Gray-scale before comparison and facial recognition can be identify.

However, a database where images have their natural look and not Gray scale images to evaluate the new method would have been preferable for this technique since real life images are not Gray-scale.

Therefore the results clearly shows that more research is needed to be done to improve the techniques by including non-frontal images in the database also it should state the time for the system to identify a possible match.

2.1 Curvelet-Transform for 3D Face Identification

An experiment was performed on the FRGC v2 dataset, which is partitioned into training and a validation set containing 4007 and 466 3D images were selected, one per person under neutral expression. The remaining images 3541 were divided into 1944 neutral images and non-neutral expression of 1597 images (Elaiwat et al., 2013)

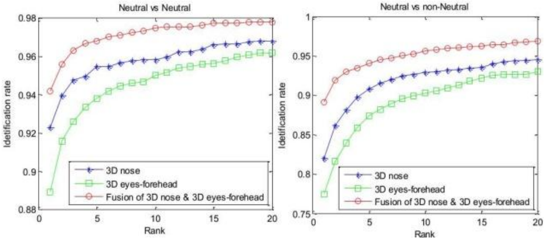


Figure III: Identification results for 2D faces (Elaiwat et al., 2013)

Figure III shows the experimental outcome obtained from 3D faces, Curvelet features of 3D nose zone has 92.3% identification rate while non-neutral expression of 82%. Figure IV shows the identification outcome for curvelet features of 2D faces expression of 77.9% neutral, 80% non-neutral and 85.44% for 2D nose, forehead and fusion of nose and eyes-forehead.

The outcomes with neutral and non-neutral facial expressions identification rates are 63.8%, 64.5% and 76.58% for 2D nose, 2D eyes-forehead and fusion between nose and eyes-forehead respectively.

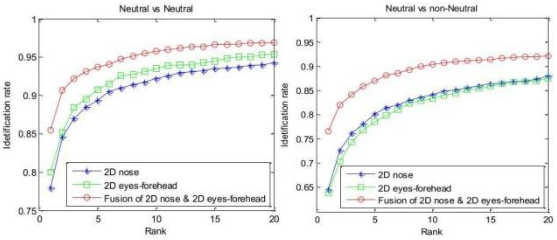
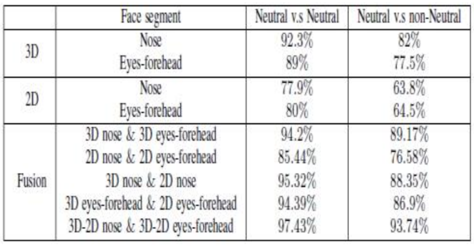
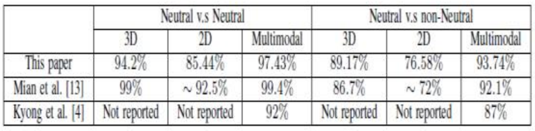


Figure IV: Identification results for 3D faces
(Elaiwat et al., 2013)

The graph shows that the Curvelet features based on 3D data attain improve facial identification rates than 2D data in both neutral and non-neutral cases.



	Face segment	Neutral v.s Neutral	Neutral v.s non-Neutral
3D	Nose	92.3%	82%
	Eyes-forehead	89%	77.5%
2D	Nose	77.9%	63.8%
	Eyes-forehead	80%	64.5%
Fusion	3D nose & 3D eyes-forehead	94.2%	89.17%
	2D nose & 2D eyes-forehead	85.44%	76.58%
	3D nose & 2D nose	95.32%	88.35%
	3D eyes-forehead & 2D eyes-forehead	94.39%	86.9%
	3D-2D nose & 3D-2D eyes-forehead	97.43%	93.74%



	Neutral v.s Neutral			Neutral v.s non-Neutral		
	3D	2D	Multimodal	3D	2D	Multimodal
This paper	94.2%	85.44%	97.43%	89.17%	76.58%	93.74%
Mian et al. [13]	99%	~ 92.5%	99.4%	86.7%	~ 72%	92.1%
Kyong et al. [4]	Not reported	Not reported	92%	Not reported	Not reported	87%

Table III and IV: Shows Identification rate results and Performance comparison using the FRGCv2 dataset, respectively.
(Elaiwat et al., 2013)

This result shows that the Curvelet features based on 3D data achieve better identification rates than 2D data in both neutral and non-neutral cases.

The techniques proves to be efficient especially in its ability to detect curves and lines, which characterize the human face, although the techniques proves to be accurate buts positioning of vector muscles into correct positions is very tasking. However, the experiment does not state if manual trial and error had be done to efficiently place object in an optimal position.

The experiment also shows that the images in the database in which the experiment was tested on have limited pose variations, this may have considerable effects on the outcome of the experiment. Therefore, the database in which the experiment was tested on is supposed to have large varying head orientation of subject that varies from 90 degree to 45 degree rotation and lighting as well as variations of background, distance and aging as this is common in a real world scenario.

Therefore, the techniques requires extensive computation when simulating large numbers of deformations with 3D lattices, this tends to be a setback in the proposed techniques as facial recognition system needs speed for optimal performance.

2.2 Facial Expression Action Unit Detection

Selection for the 17 AUs as shown in figure V, the upper levels AU1, 2, 3, 4, 5 have negligible dependency on the middle or lower face regions and hence upper face region of a size 32 x 32 was selected. The experimental results shows that AU10, 20 have high tendency of misinterpretations with AU12, 23, 28 and hence the whole face is selected as their ROIs with a bit of trade-off on their performance.

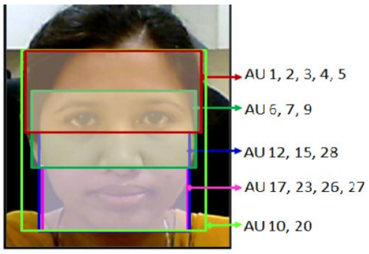


Figure V: ROI proposed strategy
(Velusamy et al., 2013)

The analysis and results of the proposed ROI scheme are present in figure (VI) below.

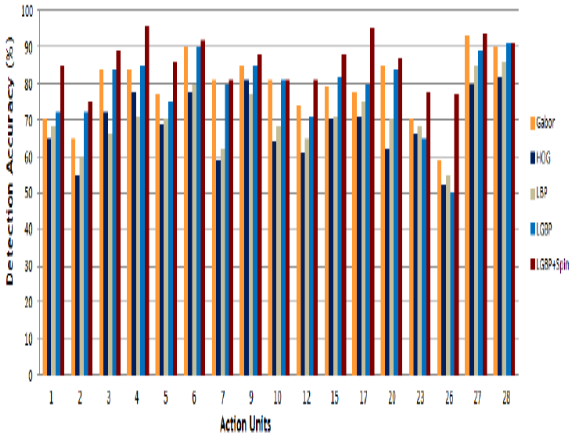


Figure VI: Performance comparison chart
(Velusamy et., al, 2013)

Table V shows the result of whole face based and the proposed ROI base scheme on a base system using LGBP feature and SVM classifier.

AU	Whole	ROI
4	0.55	0.79
5	0.62	0.81
9	0.44	0.66
12	0.71	0.83
12	0.71	0.83
12	0.71	0.83
27	0.56	0.78
Avg	*57.60*	*77.40*

Table V: Results of WHOLE & ROI based methods
(Velusamy et al. 2013)

AU	LGBP[8]	Ours
1	72	89
4	85	95
5	77	86
12	69	83
17	80	96
23	65	78
26	50	77
Avg	*71.14*	*86.28*

Table VI: Comparison of features detection accuracy
(Velusamy et al., 2013)

The results present in figure VI show that the proposed spin support based description results in an improved detection accuracy of 92.3% for the 17 AUs on standard databases. As shown in table VI, the proposed system achieves as high as 15.14% of table V (Velusamy et al., 2013)

The experiment show an increase in accuracy using the constructive training techniques compared with the LGBP.

The experiment used realistic data captured by mobile devices and surveillance cameras with wide range of illumination variations, ethnic variations, and camera angles and all image sizes was crop to 96x96 pixel which was tested on multiple and internal database and the experiment are conducted in a way to ensure that variables and discrepancies are minimized where possible to avoid biasness. This gives credibility that the experiment can be repeated for further verification of the experimental result.

Another issue with this technique is that it could suffer from time lag involved in querying database and there were no experiments to represent timing.

Also the experiment was limited to non-basic emotions such as agony and delight, Furthermore the techniques will be misled if objects are wearing spectacles because the experiment did not test images with object wearing spectacles, as a result of this limitation, there will be wrong reading of the action unit and this might lead to a false detection of objects.

To improve this technique, further research needs to be carried out to improve the performance of the system to include emotions like agony and delight and also enable it to detect faces with spectacles and to further improve the accuracy, speed and overall performance of the system.

3. Application of Methods

As digital image tends to increase massively on the internet and the use of digital videos in databases, facial recognition system has become a major part of most content based image retrieval systems (CBIR). Facial recognition techniques can be applied in biometric system identification, video conferencing, image indexing, video databases and intelligent human computer interfaces.

Facial expressions Action unit detection (Velusamy et al., 2013) can be applied in video conferencing systems to automatically control the focus of the camera on the current speaker using motion detection and facial analysis detection.

Curvelet-Transform for 3D Face Identification (Elaiwat et al., 2013) can be used for 3D character facial expression animation studio production, adverts and gaming and can improve human-computer interaction when applied to mobile application.

Facial recognition technique Using Global and Local Gabor Features (Nazari and Moni, 2013) can also be used for authentication and access control in Automated Teller Machine where the system compares the given individual to other individuals in the database and gives a ranked list of matches.

However facial recognition should be used alongside with other security measures like PIN authentication in the cases of ATM systems and not as stand-alone security measures for user authentication (Peter et al. 2011)

4. Comparison of Facial Recognition Techniques

This survey paper has looked at different approaches to synthesize facial recognition performance, validity claims made by the researcher aim to add significance knowledge to the science community.

Research by (Nazari and Moni, 2013) and (Elaiwat et al., 2013) shows that (Elaiwat et al., 2013) has low error rate than (Nazari and Moni, 2013) but their computation is more complex, it uses geometric curves and lines and provides better images reconstruction and recognition compare with (Nazari and Moni, 2013) images recognition using selection based on fusing global and local Gabor wavelet features.

The proposed technique using global and local gabor features (Nazari and Moni, 2013) is robust and faster but (Elaiwat et al., 2013) is superior in terms of recognition rate.

While facial expression action unit detection techniques (Velusamy et al. 2013) shows a higher recognition rate and computation time because it uses action unit detection of the object forehead, eyes, nose and mouth. However, it is limited to images with spectacles.

The limitation observed during the comparison is that each method or techniques uses different database.

Although facial expressions occur during conversation, none of the cited techniques did consider this possibility, this indicate the need for future work to be done with regard to advance implementation facial gestures. Apart from the above started weaknesses, there are concerned with the database set being used, as the image set of disgust is smaller compare to that of fear.

All the above methods are appearance based methods using statistical or probabilistic analysis of images to recognise faces. Humans are identifying one person from another by analysing the difference in features of each person.

Although all three techniques claims shown that their results and performance are database dependent, selected step and choice of good parameter sets, together with the robustness issue should be taken up for further study.

5. Conclusions

To enhance facial recognition system performance several different kinds of techniques should be used together. Combining two of the most successful Curvelet-Transform for 3D Face Identification and Facial Expression Action Unit Detection techniques gives enhanced performance than either alone: they are complimentary in the sense that Facial expression action unit detection captures small appearance details while Curvelet-Transform encode facial recognition over a wider range of scales.

Both features are advance techniques so it is beneficial to use Facial expression action unit detection to reduce the dimensionality prior to normalization and integration.

Finally, for the enhancement of facial recognition system performance, current methods have to be improved with concern to accuracy and robustness in natural environment.

References

Devi M. S. and Bajaj P., 2010, ‘Active Facial Tracking’, *3rd International Conference on Emerging Trends in Engineering and Technology (ICETET)*, Vol. 5, pp. 91 – 95.

Elaiwat S. Boussaid F, Bennamoun M, El-Sallam A., 2013, ‘3D face identification using Curvelet transform’, *1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Vol. 4, pp. 1 – 6.

Esan O. A. Ngwira, S. M. Osunmakinde I.O., 2013, ‘Bimodal biometrics for financial infrastructure security’, *2^nd^ conference on Information Security for South Africa*, Vol. 1, pp. 1 – 8.

Islam M. R. Toufiq R. Rahman M. F., 2012, ‘Appearance and shape based facial recognition system using PCA and HMM’, *7th International Conference on Electrical & Computer Engineering (ICECE)*, Vol. 1, pp. 1 – 4

Kar S. Hiremath S. Joshi D.G. Chadda V. K. Bajpai, A., 2006, ‘A Multi-Algorithmic Face Recognition System’, *Advanced Computing and Communications*, Vol. 3, pp. 321 – 326

Krasimir T. Manolova Agata Paliy Ihor, 2013, ‘Comparative Analysis of 3D Face Recognition Algorithms Using Range Image and Curvatur Based Representations’, *7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, Vol. 1, pp. 394 – 398

Lumei Su Sato Y., 2013, ‘Early facial expression recognition using early RankBoost’, *10th IEEE International Conference and Workshops on Automatic Face Gesture and Recognition (FG)*, Vol. 4, pp. 1 - 7

Mliki H. Fourati N. Smaoui S. Hammami M. , 2013, ‘Automatic Facial Expression Recognition System’, *ACS International Conference on Computer Systems and Applications (AICCSA)*, Vol. 1, pp. 1 – 4

Nazari S. Moin M. S., 2013, ‘Face recognition using global and local Gabor features’, 2013 *21st Iranian Conference on Electrical Engineering (ICEE)*,Vol. 3, pp. 1 – 4

Peter K. J. Nagarajan G. Glory G. Devi V. Arguman S. Kannan K., 2011, ‘Improving ATM security via face recognition’, *3rd International Conference on Electronics Computer Technology (ICECT)*, Vol. 6, pp. 373 – 376

Shenoy A. Davey N. Frank R., 2013, ‘Recognizing facial expressions:Computational models and humans’, *13th UK Workshop on Computational Intelligence (UKCI)*,Vol. 1, pp. 191 – 198

Velusamy S. Gopalakrishnan V. Anand B. Moogi P. Pandey B., 2013, ‘Improved feature representation for robust facial action unit detection’, *IEEE Consumer Communications and Networking Conference (CCNC)*, Vol. 1, pp. 681 - 684

A Critical Evaluation of Current Research into Wireless Network Hotspot Security.

Anthony Holt

Abstract

With more and more companies providing internet access through public wireless hotspots in more places than ever before it is vital that security systems are developed and implemented to protect naive users from the dangers of their use. This paper explores research into the threats that the public expose themselves to when they connect, knowingly or otherwise, to a public wireless hotspot. The paper concludes with a critical evaluation of research; proposing and exploring solutions hoping to safeguard users.

1 Introduction

Access to the internet through the use of public wireless hotspots is becoming more and more a part of everyday life (Aime et al. 2007). With higher demand on wireless hotspots by users who are often ignorant to security needs, comes a greater need for security (Choi et al. 2011).

Current research demonstrates some of the threats and security implications that surround the use of seemingly safe public wireless access points by the general population. (Chenoweth et al. 2010; fahmy et al. 2012)

Although it has been mentioned in the past that "Achieving a truly secure connection at a public wireless hotspot is an impossible proposition" (Potter B, 2006). There are several pieces of work which suggest possible solutions to reducing wireless hotspot security concerns such as Matos et al. (2012) and Leon (2008) to name a couple.

This survey paper will take a look into current issues which public wireless hotspot users face and the solutions which propose to solve them. The aim of this research paper is to evaluate current research into improving the security of Public Wireless hotspots.

2 Security Vulnerabilities

Aime et al. (2007) highlight general issues underpinning the use of WiFi and by extension, public wireless access which are still present to this day. The research aims to explain about how wireless is inherently unreliable, that it is simple to disrupt access to services or even the entire access point and ultimately that to their knowledge "No current practical or theoretical framework handles WiFi dependability issues." (Aime et al. 2007). The research explains how identity and statistical traffic analysis is possible even without compromising any present network security including WEP and 802.11i (WPA2). The research also goes on to describe other attacks including Jamming, locating mobile nodes, hijacking, energy draining and issues surrounding shared channel usage. It is mentioned that in the upper layers of the OSI model, often applications can reveal personal information which attackers can use to "profile and track potential victims" (Aime et al. 2007). The article goes on to describe some lab experiments which were conducted in order to identify how real the threats that have been outlined are using off the shelf hardware and open source software.

Although the research describes open source software and easy to obtain hardware, the specifics of neither are explained and as such the lab results are not repeatable. After introducing the vulnerabilities the research explained that a key question is raised: “How real are the threats we’ve outlined?” and suggested that they will answer this question with attack tools they have built in their labs. The research explains that it was successful in exploiting the vulnerabilities suggested during the study but no data is available in the research paper to back up the claims that this is true. It is understandable that there is only so much space available for publication and that the researchers may have aimed to include as much detail of their findings but without any provided data, or even explanations of how the attacks were conducted in the six pages published, it is difficult to justify the claims.

Bicacki & Tavil (2008) detail 15 currently known and in most cases tested WiFi denial of service methods (Table 1). Their research includes 15 countermeasures which can mitigate against the disruption caused by the attacks and known drawbacks to each of the measures which were proposed (Table 2). They go on to propose a suite of security extensions which they hope are to be implemented into the 802.11 standard.

This is a highly comprehensive article which brings together a wide range of research into one document. The suggestions for multiple countermeasures are listed however their effectiveness are not tested within this research. The researchers move on to conclude that they have developed a suite of proposed security extensions which will more or less mitigate against all of the attacks discussed throughout the research. Although the security measures proposed depicted in (figure 1) are described in detail by the researchers, they do accept the limitations of their suggestions by listing eight significant questions which need to be resolved before their extensions would be feasible.

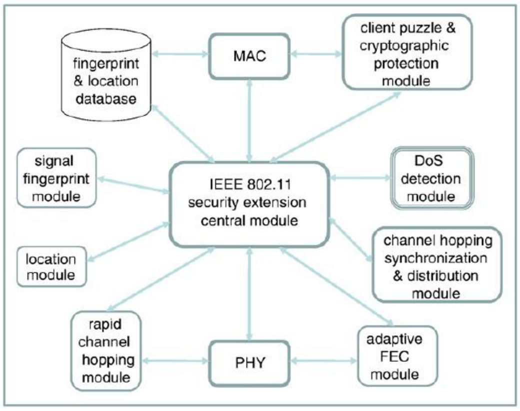
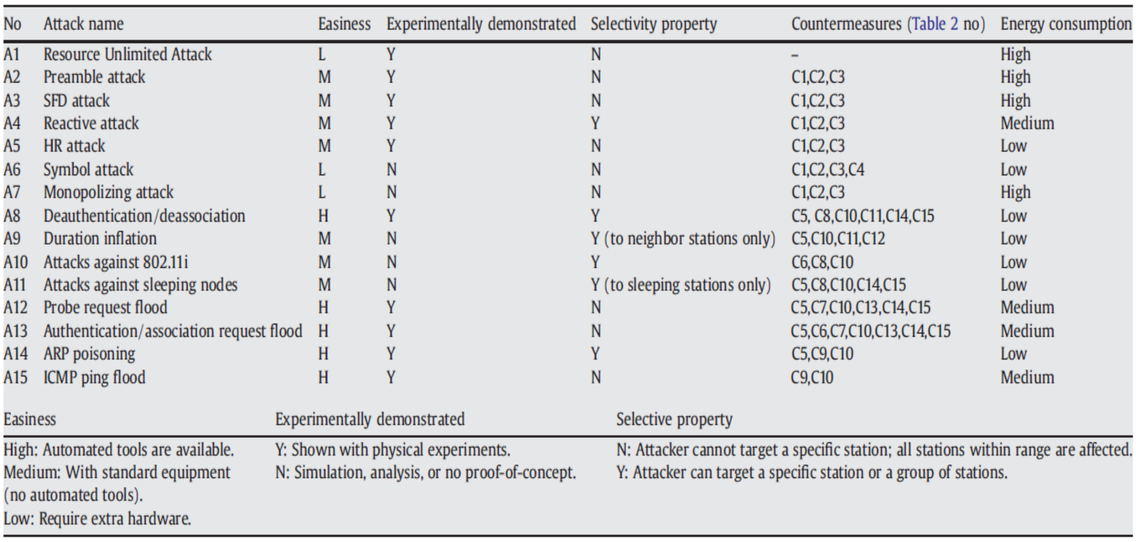

fingerprint & location database
MAC
client puzzle & cryptographic protection module
signal fingerprint module
IEEE 802.11 security extension central module
DoS detection module
channel hopping synchronization & distribution module
location module
rapid channel hopping module
PHY
adaptive FEC module

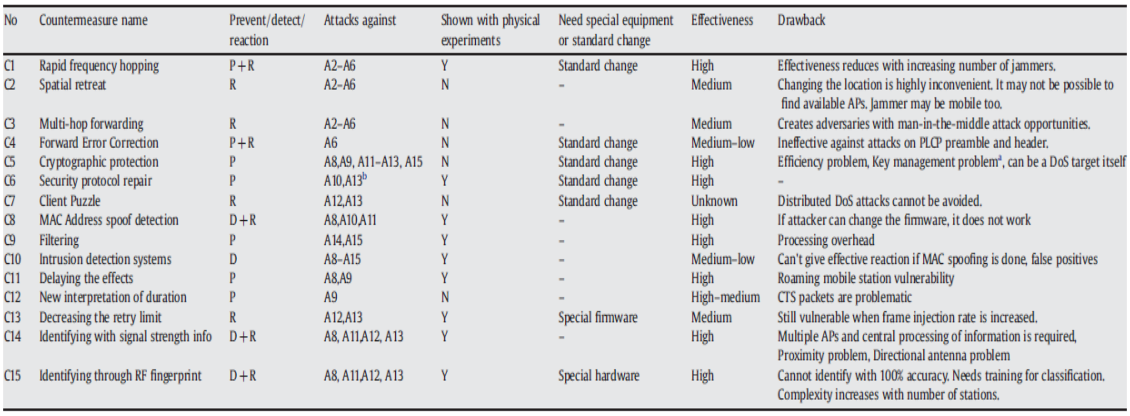
Figure 1 Proposed security measures



No	Attack name	Easiness	Experimentally demonstrated	Selectivity property	Countermeasures (Table 2 no)	Energy consumption
A1	Resource Unlimited Attack	L	Y	N	–	High
A2	Preamble attack	M	Y	N	C1,C2,C3	High
A3	SFD attack	M	Y	N	C1,C2,C3	High
A4	Reactive attack	M	Y	Y	C1,C2,C3	Medium
A5	HR attack	M	Y	N	C1,C2,C3	Low
A6	Symbol attack	L	N	N	C1,C2,C3,C4	Low
A7	Monopolizing attack	L	N	N	C1,C2,C3	High
A8	Deauthentication/deassociation	H	Y	Y	C5, C8,C10,C11,C14,C15	Low
A9	Duration inflation	M	N	Y (to neighbor stations only)	C5,C10,C11,C12	Low
A10	Attacks against 802.11i	M	N	Y	C6,C8,C10	Low
A11	Attacks against sleeping nodes	M	N	Y (to sleeping stations only)	C5,C8,C10,C14,C15	Low
A12	Probe request flood	H	Y	N	C5,C7,C10,C13,C14,C15	Medium
A13	Authentication/association request flood	H	Y	N	C5,C6,C7,C10,C13,C14,C15	Medium
A14	ARP poisoning	H	Y	Y	C5,C9,C10	Low
A15	ICMP ping flood	H	Y	N	C9,C10	Medium

Easiness	Experimentally demonstrated	Selective property
High: Automated tools are available. Medium: With standard equipment (no automated tools). Low: Require extra hardware.	Y: Shown with physical experiments. N: Simulation, analysis, or no proof-of-concept.	N: Attacker cannot target a specific station; all stations within range are affected. Y: Attacker can target a specific station or a group of stations.

Table 1 Denial of service methods



No	Countermeasure name	Prevent/detect/ reaction	Attacks against	Shown with physical experiments	Need special equipment or standard change	Effectiveness	Drawback
C1	Rapid frequency hopping	P+R	A2–A6	Y	Standard change	High	Effectiveness reduces with increasing number of jammers.
C2	Spatial retreat	R	A2–A6	N	–	Medium	Changing the location is highly inconvenient. It may not be possible to find available APs. Jammer may be mobile too.
C3	Multi-hop forwarding	R	A2–A6	N	–	Medium	Creates adversaries with man-in-the-middle attack opportunities.
C4	Forward Error Correction	P+R	A6	N	Standard change	Medium–low	Ineffective against attacks on PLCP preamble and header.
C5	Cryptographic protection	P	A8,A9, A11–A13, A15	N	Standard change	High	Efficiency problem, Key management problem[a], can be a DoS target itself
C6	Security protocol repair	P	A10,A13[b]	Y	Standard change	High	–
C7	Client Puzzle	R	A12,A13	N	Standard change	Unknown	Distributed DoS attacks cannot be avoided.
C8	MAC Address spoof detection	D+R	A8,A10,A11	Y	–	High	If attacker can change the firmware, it does not work
C9	Filtering	P	A14,A15	Y	–	High	Processing overhead
C10	Intrusion detection systems	D	A8–A15	Y	–	Medium–low	Can't give effective reaction if MAC spoofing is done, false positives
C11	Delaying the effects	P	A8,A9	Y	–	High	Roaming mobile station vulnerability
C12	New interpretation of duration	P	A9	N	–	High–medium	CTS packets are problematic
C13	Decreasing the retry limit	R	A12,A13	Y	Special firmware	Medium	Still vulnerable when frame injection rate is increased.
C14	Identifying with signal strength info	D+R	A8, A11,A12, A13	Y	–	High	Multiple APs and central processing of information is required, Proximity problem, Directional antenna problem
C15	Identifying through RF fingerprint	D+R	A8, A11,A12, A13	Y	Special hardware	High	Cannot identify with 100% accuracy. Needs training for classification. Complexity increases with number of stations.

Table 2 Countermeasures

Potter (2006) outlines issues facing public wireless hotspots including Man In The Middle attacks and rogue access point attacks as depicted in (Figure 2). Potter explains that there are methods available in 802.11i which can be used to protect the user by authenticating with a RADIUS server but notes that a great deal of capital and effort are required to make this successful and even when these are both available, they are seldom implemented with aims to provide simpler access.

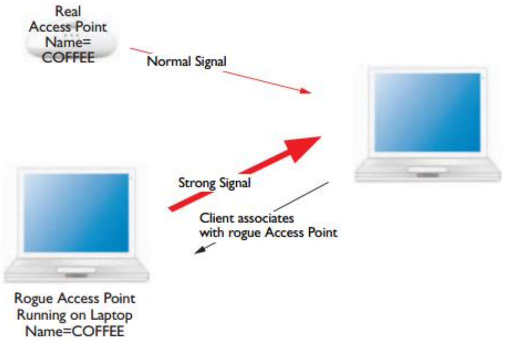


Figure 2 Man in the middle attack

Potter cleverly depicts the situation that some clients may have four year old laptops, some have a cutting edge Macbook pro and others may be running linux and that "there is no guarantee that any of these users will be able to support the most current wireless security." (Potter 2006)

Recent research by Fahmy et al. (2012) looks into some wireless security issues which could be faced by residents in Kampung which use a government run public wireless system which will soon approach 4000 wireless access points. A list of possible attacks are explained and testing is conducted in a laboratory in order to explore the reality of the attacks suggested. The research concludes that it lists only some of the potential issues that surround the Kampung wifi network and that these need to be addressed.

Fahmy et al. (2012) aim to "demonstrate the vulnerability of Kampung WiFi networks in order to amplify awareness". The research begins by describing the thousands of access points which are already in use by kampung residents and how more are being brought online. The research claims to have uncovered various security issues which will affect Kampung residents and goes on to simulate the attacks in a University College using 40 PCs and three laptops.

The researchers demonstrate security software which is able to recover email username-password combinations for their own email system. From these simulations the research makes unjustified claims that the paper has "demonstrated the possibility of wireless attacks to Kampung WiFi." As there has been no testing done using any Kampung WiFi equipment it is difficult to uphold Fahmy et al.'s hypothesis that user credentials would be so easily compromised. MIMOS who developed the Kampung WiFi Equipment may have deployed EAP with Transport Layer Security which would prevent the types of Man in the Middle attacks demonstrated by Fahmy et al. Research will need to be repeated using the same equipment and configurations used by actual Kampung WiFi equipment.

To help understand the extent that public users were revealing personal information whilst using public wireless hotspots Cheng et al. (2012) conducted a natural observation comprising of 20 airports across four countries. Their study aims to quantify privacy leakage and splits such leakage into five well described categories including Identity, Location, Financial, Social and Personal privacy. The research explains that privacy leakage does not just come from the users actions such as a website search, but also from the client device and advertisements which are displayed to the user whilst they are online. The results of their data collections are described in detail with various graphs and explanations. The research went on to conclude that "The results are quite alarming in the sense of the quantification of information that can be leaked while accessing public WiFi networks (without making much of an effort)." Cheng et al. (2012)

The methodology used demonstrates high levels of precision and rigor. The research is highly repeatable as Cheng et al. (2012) have included details of how the study was completed and which resources were used. An effort has been made to improve the accuracy of the data collected, by collecting information from different countries on different days for different time spans, a data set more representative of the general population is produced. All the data has been included and analysed together so not to introduce researcher bias. Strong justified conclusions are reached.

Chenoweth et al. (2010) looks into how prevalent security vulnerabilities are amongst public wifi users. The research conducted a study into the extent of the presence of vulnerabilities in users of a university wireless system. It was found that 9.13% of users of a wireless hotspot did not have even basic firewall protection in place to protect their clients and went on to conclude that "A small proportion of insecure devices can still be a large absolute number and a large threat with very important implications"

Although the study provides an insight into how prevalent security vulnerabilities may be present amongst students, and although the claims that a small number of users compromised can be a large threat to other users of the wireless network, it is difficult to infer that the general population would have as a significant or as limited amount of problems.

Security issues surrounding wireless access points are not only limited to the public users of the access points, often vulnerabilities can be exploited allowing an attacker access to the business behind the wireless access point. These issues are beyond the scope of this research paper but for further reading examples include Leon (2008), Breeding, M, (2005) and Sheldon et al. (2012).

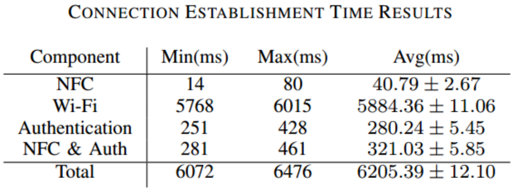
It is evident that there are a large range of security issues which can cause problems for public wireless hotspot users. More work needs to be done to establish the extent that general public users are at risk from simply just connecting their device to the network, or worse, their device automatically connecting to an open network. There are a number of issues surrounding availability of access as users come to rely on the networks which are present today. This problem, if not rectified, can only become more significant in the future as new research is currently in progress to develop the range and interactivity of public wireless hotspots, using them to possibly even order your food at a restaurant in the future (Vanderhulst & Trappeniers 2012).

So far we have looked at a range of research into the vulnerabilities and security issues surrounding wireless hotspots. We now turn our attention towards some of the currently suggested solutions.

3 Solutions

Recent research by Matos et al. (2012) aims to reduce some of the security issues surrounding the use of public wireless hotspots by introducing a Wi-Fi hotspot architecture complemented with the use of NFC technology to verify the identity of a wireless accesspoint. His research introduces some of the major problems around public hotspot security including how simple it is for a rogue access point to mimic the ESSID and login portal for a public network which can trick a user into providing private information, perhaps even credit card information if the user is expecting to pay to use the wireless access. Matos et al.'s (2012) research builds upon previous research into the use of a separate authentication side channel where connection security information was confirmed with a public key hash transferred through a barcode scanned with a camera (McCune et al. 2005), LED binary sequences (Saxena et al. 2006) and colour light sequences (Roth et al 2011). Mato's research goes on to explain that not only can WPA Security information be exchanged through NFC but the client can also go on to confirm the access points trustworthiness by contacting a certificate authority to confirm the identity of the wireless access point. A prototype is developed which shows that such a connection is possible with simple equipment purchasable today and that the connection time using the NFC authentication process is only increased by approximately 5%.

Research by Matos et al. (2012) both outlines clearly the problems faced, the solution they have provided and includes data from their test findings (Table 3). It is worth noting that although it is explained in the research that the NFC authentication takes only an additional 280ms, in a real life setting extra time would be taken by the user to walk up to the NFC receiver.



CONNECTION ESTABLISHMENT TIME RESULTS

Component	Min(ms)	Max(ms)	Avg(ms)
NFC	14	80	40.79 ± 2.67
Wi-Fi	5768	6015	5884.36 ± 11.06
Authentication	251	428	280.24 ± 5.45
NFC & Auth	281	461	321.03 ± 5.85
Total	6072	6476	6205.39 ± 12.10

Table 3 Connection establishment time results

Research conducted by Choi et al (2011) suggests a different method of improving public hotspot user security. the research begins by explaining problems which are still present in the way that public users access hotspots, It is noted that there are solutions to the problem currently out there that require a subscription service, such as when users use AT&T's access points which are secured with 802.11i-Enterprise or by using a VPN when using other wireless access points. The research outlines a hierarchical identity-based cryptography implementation which could utilize a factory installed cryptographic key and for their scheme to be added as a new 802.11 implementation or network standard. The research concludes that the new method suggested is not only practical but also defends against MAC address spoofing, rogue access points and DoS attack.

Both Matos et al. (2012) and Choi et al (2011) present ways in which a user can be protected from rouge access points and captive portals. Matos' method builds upon previous research and has the advantage of being tested more thoroughly, using equipment which is available today. However both methods are not without their own drawbacks – Matos' suggested NFC authentication requires the device that is connecting to have a compatible NFC chip, something which is common on mobile phones but less common on laptop computers. We recall that research by Potter (2006) suggested that users will be using a range of equipment, of various ages and as a result a public access point secured with Matos' system will not be compatible with a large number of devices which are currently available. The model of walking up to the access point which you would like to connect to and touching your device to it is not without its own limitations, often access points are located securely with the best line of sight possible to increase signal strength. Sometimes wireless networks are covered by several independent access points using the same SSID. As small installations are unlikely to have a managed wireless controller it is likely that the access points will be working independently and it wouldn't be possible to walk up to each of them to authenticate and guarantee the best signal, especially whilst roaming the venue.

Choi's research solves the problem of having to physically access a wireless access point in order to securely pair with it and has the advantage of having a more transparent and automatic connection. However Choi's research relies on a cryptographic key being installed physically into the network card of the network device. For the moment there are millions of devices which would simply be incompatible with the new technology, something which is incompatible with companies who want to continue offering their customers simple access to the internet.

Customers are unlikely to want to buy a brand new laptop as a result of standards changing and the companies who offer free public access are unlikely to only provide access to people with the newest technology, restricting their clients. Technology needs to be developed which will allow for backward compatibility with the devices which exist and are used today, perhaps a software based solution can be found that users can install onto their laptops to make them compatible with new levels of security?

4 Conclusions

There are a myriad of security issues that surround the use of public wireless access points. A number of countermeasures to help protect some aspects of a user's connection require specialist hardware investment and or significant technical knowledge which is often in short supply when setting up a public wireless hotspot. Some good research has been conducted into solving the security issues which face users however none of the solutions provided so far have been backwards compatible with existing users hardware and as a result will be difficult to implement successfully.

It would appear that for the present moment the only way to protect users of public access points is to educate them in the use of VPNs and the importance of valid anti-virus and firewall software. Users will have to secure their own connections by tunneling their data through a trusted third parties' network. As most VPN services are subscription based and the cost of good quality antivirus/firewall software rises, the concept of 'free' public wireless access begins to fade. A backward compatible solution to protect users transparently without them relying on a subscription service needs to be developed for only then can public wireless access truly be free.

References

Aime M. D., Calandriello G. and Lioy A. , 2007, 'Dependability in Wireless Networks: Can We Rely on WiFi?' *Security & Privacy*, IEEE, 5(1):23--29.

Bicakci K. and Tavli B., 2008, 'Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks.' *Computer Standards & Interfaces* 31(5):931--941.

Breeding M., 2005, 'The Library Wireless Hotspot.' *Library Technology Reports*, 41(5):31--36.

Cheng N., Wang X., Cheng W., Mohapatra P. and Seneviratne A., 2013, 'Characterizing privacy leakage of public WiFi networks for users on travel.' *INFOCOM, 2013 Proceedings IEEE*, pages 2769--2777.

Choi J., Sang-Yoon C., Diko K. and Yih-Chun H., 2011, 'Secure MAC-Layer Protocol for Captive Portals in Wireless Hotspots.' *Communications (ICC), 2011 IEEE International Conference on*, pages 1--5.

Chenoweth T., Minch R. and Tabor S., 2010, 'Wireless Insecurity: Examining User Security Behavior on Public Networks.' *Communications of the ACM*, 53(2):134-138.

Fahmy S., Nasir A. and Shamsuddin N., 2012, 'Wireless network attack: Raising the awareness of Kampung WiFi residents.' *Computer & Information Science (ICCIS*), *2012 International Conference on*, 2:736-740.

Leon J. F., 2008, 'Protect Your Wireless Network-- And Your Business.' *Journal of Accountancy*, 206(5):88--91.

Matos A., Romao D. and Trezentos P., 2012, 'Secure hotspot authentication through a Near Field Communication side-channel.' *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*, pages 807--814.

McCune J. M., Perrig A. and Reiter M. K., 2005, 'Seeing-is-believing: using camera phones for human-verifiable authentication' *Security and Privacy, IEEE Symposium on*, pages 110--124.

Potter B., 2006, 'wireless hotspot: petri dish of wireless security' *Communications of the ACM*, 49(6):51--56.

Roth V., Polak W., Rieffel E. and Turner T., 2008, 'Simple and effective defense against evil twin access points' *In Proceedings of the first*

ACM conference on Wireless network security, pages 220--235.

Saxena N., Ekberg J. E., Kostiainen K. and Asokan N., 2006, ‘Secure device pairing based on a visual channel’ *Security and Privacy, 2006 IEEE Symposium on*, pages 6 and 313

Vanderhulst G. and Trappeniers L., 2012, ‘Public WiFi hotspots at your service’ *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, pages 411—414

An Evaluation of Information Hiding Techniques Using Image Steganography

Muhammad Hussaini

Abstract

Steganography has become the technique of choice for hiding secret messages in a cover media, presenting and transmitting it as a harmless piece of content, therefore making it hard to detected unlike encryption. This paper provides an adept evaluation of some of the prominent image steganography methods, showing their strengths, weaknesses and applicability, further conclusions were made regarding the effectiveness and otherwise of the techniques evaluated.

1 Introduction

Protecting the privacy of information for organizations, governments and individuals have become increasing challenging in recent times due to the increased use of computers and digital means of communication. Various methods of protecting information and privacy have been researched and developed, the most obvious being encryption and then steganography. Encryption differs from Steganography due to the fact that encryption is generally observable and arouses suspicion, while steganography aims at being un-observable and difficult to detect, this is achieved by hiding the secret message in unremarkable carrier media (Chanu et al 2012).
Image Steganography is achieved using either transform or spatial domain methods, in spatial domain the cover media and the secret message are both modified, this involves encoding at the Least Significant Bits of the image and also by transforming the image pixel blocks into 64 Discrete Cosine Transformation co-efficient and putting the pixels into groups, the image is transformed into a frequency representation from an image representation, the transform domain utilizes this method for embedding the secret data into the cover image that is transformed (Das and Tuithung, 2012), the LSB replacement technique is however vulnerable to statistical analysis (Ghebleh and Kanso, 2013).

Further research have therefore been carried out into developing more secure methods of image steganography such as that by Prabakaran and Bhavani (2012) which uses Discrete Wavelet Transform to achieve a high capacity steganography scheme that enables large size of secret data to be embedded into smaller sized cover images.

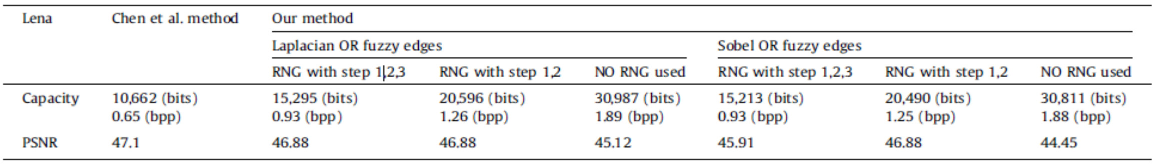
Raftari and Moghadam (2012) also claimed that by combining Integer Wavelet Transform and Discrete Cosine Transform which are both transform models, a more secure image steganography method was achieved based on results that showed good value of Peak signal to noise ratio (PSNR) in the secret image, an acceptable visual quality which leaves the secret data unnoticed, Mean structural similarity index measure (SSIM) and the Histogram error (HE).

The aim of this paper is to critically evaluate and analyze current research focused on developing more secure methods of image steganography, models and techniques used, conclusions and claims reached based on experiments carried out and there results.

2 Evaluation of Current Steganography techniques

Anastasia, et. al (2012) proposed a technique of achieving a robust image steganography using a high payload method and edge detection, where hybrid edge detector is derived by unifying the fuzzy edge detector and the sobel and the Laplacian filters for simplicity, this method does not compute the real edges in an image but distinguishes between the sharp and smooth areas of the image so as to hide more secret data bits into the edge pixels. In this method, as well as the secret message, two property files which contain information regarding extraction of the secret message are also encrypted using 3-DES with the secret key provided by the user during the embedding process.

The experiments carried out to test this algorithm used the same images used by Chen et. al (2010) for their image steganography scheme, this is used in order to enable seamless comparison of both techniques, although they used colored images while Chen et. al (2012) used grayscale images. Factors used for comparing the two schemes included the hiding capacity in bits divided by three, the peak signal to noise ratio (PSNR) is also measured, a higher value of PSNR is considered better. Figure 1 below shows the result of comparing this method and that of Chen et. al(2010).



Lena	Chen et al. method	Our method					
		Laplacian OR fuzzy edges			Sobel OR fuzzy edges		
		RNG with step 1|2,3	RNG with step 1,2	NO RNG used	RNG with step 1,2,3	RNG with step 1,2	NO RNG used
Capacity	10,662 (bits) 0.65 (bpp)	15,295 (bits) 0.93 (bpp)	20,596 (bits) 1.26 (bpp)	30,987 (bits) 1.89 (bpp)	15,213 (bits) 0.93 (bpp)	20,490 (bits) 1.25 (bpp)	30,811 (bits) 1.88 (bpp)
PSNR	47.1	46.88	46.88	45.12	45.91	46.88	44.45

Figure 1. Comparison of test result from the proposed method by Anastasia et., al (2012) and the method proposed by Chen et., al. (2010).

Based on the results presented above, Anastasia, et. al (2012) claimed that there method which uses a hybrid edge detector together with the sobel and laplatian filters to enable embedding additional secret messages in the edge pixels outperforms the hybrid edge detection method proposed by Chen et., al (2010).

The result of evaluating this method showed that colored variants of the image set used by Chen et al (2010) were used in the experiment, these image set are used in many other image steganography experiments, making it a good choice. The experiment is repeatable due to the fact that it is the most widely used for testing image steganography. The use of colored variants of the images in the experiment with the new method might not give an accurate representation of the performance when compared to the method of Chen et., al (2010) which uses grayscale variant of the same images, the use of encryption as part of the algorithm may also cause potential issues with performance and may cause significant change in the size of the stego image as compared to the original cover image, testing the new algorithm with only one other method might also not give an accurate measure of its potential performance as compared to other current algorithms in the market and those proposed in current research papers.

Ghebleh and Kanso (2013) proposed an algorithm of implementing image steganography by hiding the secret message as binary in a pseudo-randomly chosen detail co-efficient of the cover image based on discrete wavelet transform and a 3-dimensional chaotic cat map. The algorithm also uses discrete wavelet transform to achieve robustness against image processing filters and steganalytic attacks, it also utilizes edge adaptability in order to hide more data in the edge pixels where it will be less visible to the human eye, whereas lossless extraction of the secret hidden message is achieved by using lifted discrete wavelet transform. The extraction process uses the same lifted wavelet transform used in the embedding process to find the detail and approximation co-efficient, this enables retrieving the hidden information from the exact pixels they were hidden in.

The experiment carried out by Ghebleh and Kanso (2013) was performed in order to gauge the performance of the proposed image steganography algorithm on the basis of its security, imperceptibility and feasibility. Randomization of the position of the stego-image which carried a secret message of size 2bpp and was embedded in the cover image ensured that a visual inspection of both the stego and cover image does not unveil the difference between the images. The histogram of both the cover and stego image was calculated, as well as the difference which shows that there is no significant difference between the two images as shown in figure 2 below.

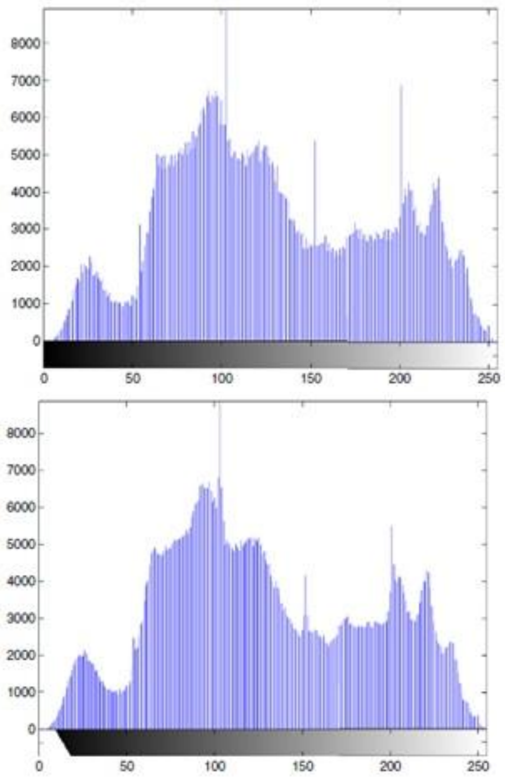


Figure 2. Cover media Image Histogram (Top), Stego Image Histogram (Bottom) (Ghebleh and Kanso, 2013).

The experiments they carried out measured the image histogram, the similarity measures were also calculated and presented based on existing units of similarity measure - the mean square error (MSE), peak signal to noise ratio (PSNR), and the structural similarity index (SSIM). The results of the experiment was also compared with three (3) current transform domain based image steganography schemes by (Raja et., al. 2008), (Souvik and Gautam, 2012) and (Gandharba and Saroj, 2012), this were chosen due to the fact that they all used colored images for their experiments, this enabled direct comparison of these schemes with the proposed scheme. The comparison table is shown in figure 3 below.

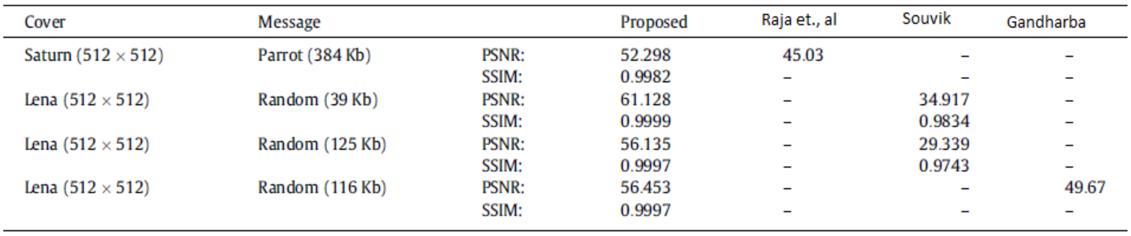
Ghebleh and Kanso (2013) concluded that there proposed algorithm is superior to the algorithms it was compared to, they also presented evidence that showed they achieved a good imperceptibility measure based on the two units of similarity measure, which are PSNR and SSIM index, as well as having a high secret key sensitivity.

The research carried out by Ghebleh and Kanso (2013) was rigorous due to the fact that there proposed method was tested against attack from different steganalysis methods which use LSB replacement, the methods include the Chi-Squared Test (Westfeld Andreas, 2000), Weighted-stego analysis (Fridrich and Goljan, 2004) and Sample Pair analysis (Dumitrescu et al, 2003).

Results have shown that the method is effective against these techniques of steganalysis, although more test will need to be carried out to ascertain its strength against other forms of attack such as statistical steganalysis which are also very popular. The choice of 3D Cat map is applauded due to its sensitivity to even small changes in secret key used. Although, the application of a transform domain technique and the randomness of the choice of bits where data is hidden proves effect, the transform domain is known to cause reduction in the quality of stego-image produced.

3 Comparison of current Steganography techniques

The methods of image steganography described above are similar because they both used the least significant bits (LSBs) of the cover image as well as utilized edge detection in their own different ways, both methods could benefit from the techniques used by the other. The edge detection method used by Anastasia et. al (2012) enabled the hiding of larger secret



Cover	Message		Proposed	Raja et., al	Souvik	Gandharba
Saturn (512 × 512)	Parrot (384 Kb)	PSNR:	52.298	45.03	–	–
		SSIM:	0.9982	–	–	–
Lena (512 × 512)	Random (39 Kb)	PSNR:	61.128	–	34.917	–
		SSIM:	0.9999	–	0.9834	–
Lena (512 × 512)	Random (125 Kb)	PSNR:	56.135	–	29.339	–
		SSIM:	0.9997	–	0.9743	–
Lena (512 × 512)	Random (116 Kb)	PSNR:	56.453	–	–	49.67
		SSIM:	0.9997	–	–	–

Figure 3. Comparison of the results of Proposed algorithm (Ghebleh and Kanso, 2013) with that of Raja et., al (2008), (Souvik and Gautam, 2012) and (Gandharba and Saroj, 2012).

messages, this can be useful in Ghebleh and Kanso's (2013) method which uses a 3D cat map to find random bits for storing secret message without considering the size of the hidden data, thereby enabling it to hide larger sizes of secret messages. Another significant difference between the two methods is in the way they store information about the bits where the secret data is hidden in the cover image, Anastasia et. al (2012) stored this information in two information files which are encrypted using 3-DES with a secret key provided by the user during the steganography process, these files are required during the message extraction process, where as Ghebleh and Kanso (2013) regenerates the 3D cat map used during the embedding process, this gives the exact information needed to recover the secret message from the bits they were hidden in, this method could be beneficial in Anastasia et. al (2012) method by eliminating the need for encryption which may cause performance lags.

Both Anastasia et. al (2012) and Ghebleh and Kanso (2013) used colored images in their experiments. The methods for testing the strengths of steganography methods rely on the SSIM, HE value and PSNR, both methods have carried out calculations to determine its strength based on these values, this also enables seamless comparison with other methods. To compare the methods evaluated above, both used colored JPEG images although Anastasia et. al (2012) compared there results with another experiment which uses the same images but of grayscale variant, this may not give a realistic comparison of performance and effectiveness.

Ghebleh and Kanso (2013) on the other hand compared there results with three different other method which use the same steganography technique and also uses colored images, they also carried out the same tests as those three and compared them to their own results, this shows quite a bias free methodology. Generally, both methods could complement each other.

3 Conclusions

Steganography is a technique of hiding secret data in a cover media, mostly images. A lot of research have been carried out towards both producing more effective methods of steganography as well as countering it. The research by Anastasia et al (2012) focused on hiding a larger size of secret message in the stego-image, this was achieved by using a hybrid edge detection algorithm with the SOBEL and Laplacian filters, although the main objective was achieved as shown by experiments, its conclusion based on comparison with the method of Chen et al (2010) may not have shown an accurate representation of the performance due to the fact that they used the same set of images but of colored variant. The use of encrypted information files as part of the steganography process may also cause some significant performance issues depending on the size of secret message and the cover image as well, since encryption is a resource intensive process and rivals the essence of steganography which is to remain unnoticed.

Ghebleh and Kanso (2013) proposed a steganography method which utilizes the irregular output of a 3 Dimensional cat map to embed the secret data in randomly chosen bits of the cover media, the experiment was rigorous and was tested against steganalytic methods which targeted LSB based steganography schemes, although it was not tested against other steganalytic attacks such as statistical attacks which are very popular.

The choice of using 3 dimensional cat map to provide randomness of the bits where the secret message is hidden is applaudable, the 3 dimensional cat map's sensitivity to even slight changes to its secret key makes it unique. The method is based on the transform domain technique of embedding which has been proved to be effective, but tends to produce a reduced quality of final stego-images.

References

Anastasia Ioannidou, Spyros T. Halkidis, George Stephanides., 2012, 'A novel technique for image steganography based on a high payload method and edge detection', *Expert Systems with Applications*, vol. 39, no. 14, pp. 11517 - 11524.

Chanu Y.J, Tuithung T, Manglem Singh K., 2012, 'A short survey on image steganography and steganalysis techniques', Emerging Trends and Applications in Computer Science

(NCETACS), 3rd National Conference on, 52-55.

Chen Wen-Jan, Chang Chin-Chen, Le T., 2010, 'High payload steganography mechanism using hybrid edge detector', *Expert Systems with Applications*, vol. 37, no. 4, pp. 3292--3301.

Das Rig, Tuithung Themrichon., 2012, 'A novel steganography method for image based on Huffman Encoding', Emerging Trends and Applications in Computer Science (NCETACS), 3rd National Conference on, 14-18.

Dumitrescu Sorina, Wu Xiaolin, Wang Zhe., 2003, 'Detection of LSB steganography via sample pair analysis', *Signal Processing, IEEE Transactions on*, vol. 51, no. 7, pp. 1995-2007.

Fridrich Jessica, Goljan Miroslav., 2004, 'On estimation of secret message length in LSB steganography in spatial domain', *Proc. SPIE*, pp. 23-34.

Gandharba Swain, Saroj Kumar Lenka., 2012, 'A novel approach to RGB channel based image steganography technique', *The International Arab Journal of e-Technology*, vol. 2, no. 4, June.

Ghebleh. M, Kanso. A., 2013, 'A robust chaotic algorithm for digital image steganography', *Communications in Nonlinear Science and Numerical Simulation*.

Prabakaran. G, Bhavani. R., 2012, 'A modified secure digital image steganography based on Discrete Wavelet Transform', *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, 1096-1100.

Raftari. N, Moghadam. A.M.E., 2012, 'Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT', *Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on*, 295-300.

Raja K.B, Sindhu S, Mahalakshmi T. D, Akshatha S, Nithin B. K, Sarvajith M, Venugopal K. R, Patnaik L.M., 2008, 'Robust image adaptive steganography using integer wavelets', *Communication Systems Software and Middleware and Workshops, COMSWARE. 3rd International Conference on*, 614-621.

Souvik Bhattacharyya, Gautam Sanyal., 2012, 'A Robust Image Steganography using DWT Difference Modulation (DWTDM)', *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 4, July, pp. 27-40.

Westfeld Andreas, Pfitzmann Andreas., 2000, 'Attacks on Steganographic Systems', *Information Hiding*, pp. 61-76.

An Evaluation of Current Intelligent Parking System Research

Suhail Abdelhafiz Abdelwahid Karar

Abstract

This paper describes new research and analysis that has been conducted to improve intelligent parking systems. The paper covers different methods about intelligent parking systems such as ultrasonic sensor whereby sound effects in the parking slot is detected and analysed to the control computer, camera adoption and visual navigation this is because the evaluation of different methods would provide a clear picture on how car parking systems have been evolved from different stages and era. The researchers have provided different point of views regarding of the methods used for intelligent car parking systems. As far as parking system is concerned, there were certain methods which brought some limitations when they were deployed but then different researchers have come up with some more features to overcome all those limitation in advanced. As the research talking more about the evaluation of intelligent car parking systems, author of this research paper has provided analysis of different methods with experimental test and result, apart from that, some limitations of conventional parking systems have been researched and analyzed. After having seen some limitations, author has produced some solutions which have implemented but then more methods have been evaluated and compared together with experimental analysis and the corresponding results.

1 Introduction

As far as car parking is concerned, it has been provided various studies among different researchers on how to simplify car parking in different places, since now the numbers of cars keep on increasing and resources used to pack cars are limited.

There are a number of research papers discussing about intelligent parking systems. For example Amin, K et al. (2012) who are doing research into improving intelligent parking systems by using ultra sonic sensors. There is also research by Tang et al. (2006) that was looking into using camera adoption which is to capture the available slot in the parking lot. According to Tang et al. (2006) conclude that there are a number of limitation of using some methods such as camera adoption for car parking. Also there is research by Zhong, Y et al. (2010) who were looking into improve intelligent parking system by using visual navigation method to give driver in parking lot to find the available parking slot.

According to Yan, G et al. (2008) conclude that Manhattan Central Business District (MCB) has got more than 109222 off-street public parking, and also when this figure is compared upon number of employees in MCB it can clearly be that each one spot is for every 16 employee of MCB and yet more number of parking spot are wasted in day-today. Currently, automating car parking systems have been developed and provide magnificent advantages to the users, though some more reliable resources have to be used in order to improve cost effectiveness of car parking systems. According to Yan, G et al. (2008) have further explained that “in large parking lots, a driver may exit the lot without knowing about new spots that have just become vacant”; which most certainly driver might feel frustration to find the vacant slot but sometimes before reaching to the vacant slot, the slot might already be taken by another driver as explained by J.P, B et al. (2006). This will result to tremendous time wastage to driver and wasting some other resources like fuel just to find another vacant slot inside the parking lot.

The main point of this research is to research and analyze the current intelligent parking systems. For this paper, the author will look at different research source such as conference papers, journals and analyze the findings.

2 Limitations of Current Research on Intelligent Parking Systems

Car parking systems have been researched in advanced in few decades ago, different weaknesses of parking systems have been found. However, preliminary investigation on car parking systems from different researchers were aimed to focus in other perception but since limitation of those systems provide obstacle to conclude as the reliable method to be used. Among the method used in car parking system is camera adoption which is using video to capture the existing slot in the parking lot, though this method previously was highly adopted by different parking lot; but Tang et al. (2006) provided a numerous limitation using camera adoption method for car parking. In the research done by Tang et al. (2006) they found that video is energetically expensive, since more power is needed to run video footage to capture cars in the parking slot. As it can be estimated that in one public car parking lot may contain at least hundreds parking slot, hence when each slot using the camera adoption more power energy would be required and for hundreds parking slot would be costly. According to Tang et al .(2006) have further stated that "video can generate a very amount of data"; by this statement, it shows that video is not reliable method to be used since more data would be required to be stored and more capacity would be required which is then to be expensive.

Interestingly, other method which was researched by J.P, B et al. (2006) was to use monitoring mechanism by using a routing protocols and MAC address. This method preliminary was not required other resources to be build, is just normal parking slots would have existing components and protocols to design sensor for car park. But, J.P, B et al. (2006) has stated that "The quality could not be achieved due to high unreliable message delivery due to communication methods and protocol". This is typically due to what is observed by the sensor network nodes were deployed on the ground at the center of parking spot, when car has to drive above the sensor it has low profile. Then J.P, B et al. (2006) have provided another solution of replacing antenna few centimeters above ground which was also limited communication range since when a car is parked can obstruct communication dramatically. Similarly, using Ground Position System (GPS) can limit the accuracy of parking since GPS accuracy is just five to twenty meters (Zhong, Y et al. 2010).

Overcoming limitations, further researches have been done and evaluated so as to provide reliable services in car parking systems. According to Tang et al. (2006) have provided as solution of wireless sensors networks (WSNs) in the parking systems so as to eliminate camera adoption which was used before. As Tang et al. (2006) stated that "A wireless sensor network consists of a large number of low-cost sensor nodes which can be self-organized to establish an ad hoc network via the wireless communication module equipped on the nodes". This means that wireless sensor is low cost which is highly self-organized by establishing ad hoc networks by using all equipped communication modules.

3 Methods used in Intelligent Parking System

As explained before, car parking systems is highly required to date, eventually intelligent car parking systems is the most vital aspects which is came to crucial recently. Making car parking system to be in intelligence manner, different methods are used so far, and they have been researched and implemented in different aspect.

3.1 Visual Navigation

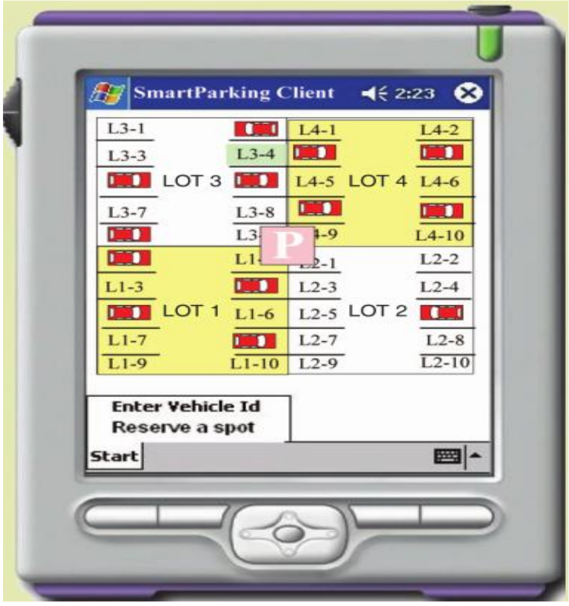
Among the method which is commonly used in car parking system is visual navigation method which has been researched by Zhong, Y et al. (2010). This method is all about giving driver in parking lot to find the available parking slot by using visual navigation to the slot. Similarly, visual navigation using real-time localization system (RTLS) which is definitely using Ultra Wideband (UWB) [2-3] technology as stated by Zhong, Y et al. (2010), "the system consists of four parts: navigator, server, wireless network and position sensor network". Each vehicle inside parking lot gets the visual navigation to the parking slot whereby this navigator containing UWB tag in order to get clear positioning and wireless network card which is performing communication to a server.

Furthermore, the position sensor which is at individual parking slot containing tag which transmitting UWB pulse to navigator for determining the location, and also sensor which receive and evaluate signaling from the tag, and also there is locate engine which is performing aggregation to the positional data, and hence this data generated communicate with the server software. Hence this method is basically using server architecture to read the position of carport in real-time and navigation is done to help driver to find where exactly the carport is located.

3.2 Infrared Device (IFD)

There is another method in parking system which is recently bombarded; and this method is of using Infrared Device (IFD), this method provide secure and smart parking system as researched by Yan, G et al. (2011). IFD provide very tactic method of implementing secured parking. There is research show that by using this method, each vehicle is given a short range transceiver and a processor, though transmission range is about 1 m (Yan, G et al. 2011). The carport contain sensor which receiving signal from vehicle but before that, driver has to book at the parking booth to get the exactly carport and then parking booth there is control computer which can see all parking details whether the carport is occupied or vacant as show in fig 1 bellow is also another means of mobile booking whereby driver can book remotely.

Fig 1: User Interface for Smart Car Park



By (Yan, G et al 2011)

3.3 Ultrasonic Sensors

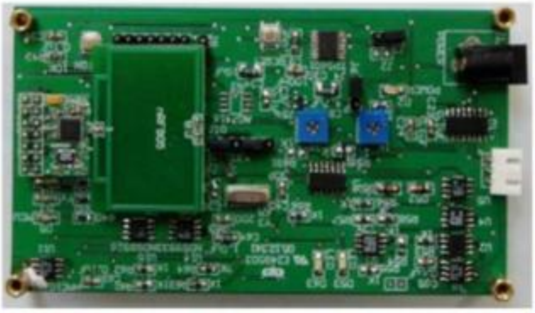
Another method which is also used in intelligent car parking systems is by ultra-sonic sensor. Ultra-sonic sensor is other wireless sensor but this sensor using sound frequency to determine the location of source of sound. As explained by Mahapatra, et al. (2008), they provided much detail about ultra-sonic on how it can be used, though in their research they went in deep on how ultra-sonic can be used to prevent accident, yet this method can also be used parking systems using the same phenomenon. Furthermore, Wang, Y et al. (2006) has provided further usage of ultra-sonic waves to monitor available parking slot in parking lots. In each and every carport, there is device which periodically provides very short ultra-sonic waves. When the carport has been occupied, the reflection of the ultra-sonic wave will determine whether the slot is occupied and update control computer and ask driver to select another parking slot, similarly the available parking will have green light to show its available and red light to show the carport is occupied. Hence, this is simulated by control computer in which when driver coming to book parking can see all available parking slot without going inside and look for available parking slot. Computer can determine whether a slot is occupied or vacant and inform driver to locate the carport which is available at the moment.

4 Experimental Test Analysis and Results

After having seen different methods which are used for intelligent car parking systems, in this session it is going to describe how the test has been undertaken of visual navigation method, IFD method, and ultra-sonic**.** All these methods have been done experimental test to justify how they are going to provide car parking services. When starting with visual navigation method, as stated by Zhong, Y et al. (2010) "We use the series 7000 of Ubisense precise real-time location system to construct the experiment". All of the 7000 series Ubisense sensors determine both azimuth and elevation angle of arrival (AOA) independently of the UWB signal, which providing baring to each tag. Also measuring time differences of arrival (TDOA) is done by pair of sensors which are connected by timing cable. According to Zhong, Y et al. (2010) stated that "this unique combination of AOA and TDOA measurement techniques delivers a flexible, powerful and robust location system that can achieve accuracy better than 15cm in 3D". Four sensors have been configured in lab of 60 square meters together with PDA which is bound with navigator. Also wireless network which is communicating between PDA and a server was wireless area network which was using D-Link as the access point (AP). A large-sized simulation toy car was used as the experimental car and boxes were drawn to represent the carport. The results has been found that, using 7000 series of ubisense product, the goal of parking can be achieved but when GPS is used the goal were not be able to be achieved, and hence this method it can be done and implemented for real car parking system after results have been found in the lab (Zhong, Y et al. 2010).

For secured smart parking system, was simulated using MATLAB 7.0 and tested, using custom simulators. The results were collected and processed using various simulators for different parking systems. Simulations have been designed using Visual studio.Net and eclipse. Similarly, after different comparison between conventional parking and smart parking in the test have been done so as to justify upon smart parking as the feasible parking system. However, wireless detectors nodes in parking system have been tested by Wang, Y et al. (2006) and they have taken hardware of fabricated wireless sensor node which as shown in figure 2 bellow.

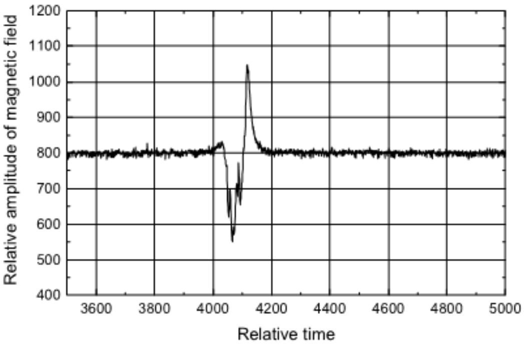
Fig 2: Hardware of Wireless Sensor Node



By (Wang, Y et al. 2006)

In the experiment, two wireless nodes have been tested to detect magnetic field changes in the surrounding environment. This shows that, when car is moving in the parking lot there is a change of magnetic field, similarly when the car is placed on the carport, the change of magnetic field remained zero (0) since magnetic field would have the same value from entire time when car still at the carport. These measurements were sent to the gateway in allocated time slot. Hence, according to Wang, Y et al. 2006 "The gateway can transmit data to the PC computer by means of RS232 interface." As result shown in the figure bellow (Fig.3) upon magnetic field changes, it shows that whenever car is passing to the sensor node, the magnetic field is increasing significantly.

Fig. 3 Magnetic Signal Detected by Sensor No



By (Wang, Y et al. 2006)

In the graph shown in Fig. 3 above, shows that when car passing at sensor node, the graph rise to 1050 of relative amplitude of magnetic field. Furthermore, the magnetic intensity seem to be at higher value when the car stop at that particular node, threshold can be determined and when the magnetic intensity is bigger than the threshold, it has been found that node has car and hence that particular carport is occupied.

5 Conclusions

After having these results, it shows that there are numerous ways of implementing intelligent car parking systems. However, many methods which were researched were about to bring more changes from the previous limitation of car parking systems. All those changes were due to simplicity of the work to be done by driver to find parking slot, and also reducing much involvement of human during parking, eventually during the time of looking available carport to park the car.

Moreover, there are other methods which are used to date like light sensor parking system which used as the sound sensor of ultra-sonic waves. But when different testing has been done by Mahapatra, et al. (2008) using ultra-sonic sensor to detect available carport, it has been found that different size of car provide different results. As example provided, for small car was producing low value of ultra-sonic waves changes in graph but when family car is placed the changes of ultra-sonic were higher as compared with small car. Hence, using ultra-sonic sensor, there must but more consideration to be taken. By far most important is that ultra-sonic is more cost effective as compared with other sensors, as stated by Kumar, R et al. (2007); it is easy to manage rather than light sensors; also light sensors sometimes can produce side effects due to electromagnetic waves produced by sensors. Hence ultra-sonic can be used to provide efficient way in the car parking systems; only it has to be considered that, the carports have to be differentiated from small to lorries or family cars so as to get reliable solution of car parking system. This separation can help of producing different threshold in the carport, when the threshold is smaller than ultra-sonic wave changes produced by sensors, it will be definitely realized that the car is occupying the carport. Also these thresholds should be different from different carports which are significantly differentiated upon the size of cars to be packed.

References

Amin Kianpisheh, N. M. P. L. a. P. K., 2012, ‘Smart Parking System (SPS) Architecture Using Ultrasonic Detector’, *International Journal of Software Engineering and Its Applications*, Volume Vol. 6, pp. 51-54.

Benson, J.P., J O'Donovan, T., O'Sullivan, P., Roedig, U., Sreenan, C., Barton, J., Murphy, A., O'Flynn, B., 2006, ‘Car-Park Management using Wireless Sensor Networks.’, *Local Computer Networks Proceedings* 31st IEEE Conference , pp. 588-595.

I. M., Liang , S., . K. H. & N. Y., 2003, ‘Ripple-suppressed multirate control and its application to a system with an ultra sonic sensor’, *Decision and Control Proceedings. 42nd IEEE Conference* , Volume 6, pp. 5979-5984.

Kumar, R. Soh, B. Chilamkurti, N.K., 2007, ‘A Comparative Study of Different Sensors forSmart car park Management’, *International Conference on Intelligent Pervasive Computing*, p.499-502.

M., . M., K. & K., 2008, ‘Ultra Sonic Sensor Based Blind Spot Accident Prevention System’ *Advanced Computer Theory and Engineering, 2008. ICACTE '08. International Conference* , pp. 992- 995 .

Tang. Zheng, Y. & Cao , J., 2006, 'An Intelligent Car Park Management System based on Wireless Sensor Networks', *Pervasive Computing and Applications, 1st International Symposium* , pp. 65-70.

Wang, Y. Guangrong, Z. Tong, L., 2006, ‘Design of a Wireless Sensor Network for Detecting Occupancy of Vehicle Berth in Car Park’, *Proceedings of the Seventh International Conference on Parallel and Distributed Computing,Applications and Technologies (PDCAT'06)*, p.1-4.

Yan , G., . A., M.C., W. & S, O., 2008, ‘SmartParking: A Secure and Intelligent Parking System Using NOTICE’, *Intelligent Transportation Systems, ITSC 2008. 11th International IEEE Conference on,* pp. 569-574.

Yan , G., Yang , W., D.B., R. & S, O., 2011, ‘SmartParking: A Secure and Intelligent Parking System. Intelligent Transportation Systems Magazine’ IEEE , 3(1), pp. 18-30.

Zhong , Y., ming Zeng , L. & gang Guo, W., 2010, ‘Visual navigational method of parking management based on indoor precise real-time location’, *Computer and Communication Technologies in Agriculture Engineering (CCTAE), International Conference* , Volume 1, pp. 227-229 .

An Evaluation of Current Research for Solving Mobile Touch Screens Accessibility Problems for the Blind and Visually Impaired

Tumo Modimoeng

Abstract

Touch screen interface has evolved into the most popular and prevalent display unit in mobile phones over the years. Many assistive technologies have been developed to make such mobile phones accessible to blind and visually impaired users. This paper evaluates some of the most current research to make touchscreens accessible to the blind and visually impaired users with some recommendations for further work.

1 Introduction

With the boom of the touch screen interface, touch screen mobile phones have become more popular(Altinsoy & Merchel 2012). Over the years mobile phones have evolved into an everyday necessity, now being capable of performing more complex tasks other than the basic calling and texting as it were before. This can be seen from smartphones such as android e.g. Samsung Galaxy™ and iPhone™ which host a wide variety of applications.

Although the integration of touch screen interface with mobile phones enables easy accessibility for ordinary users, it imposes a barrier to the blind and visually impaired (Nishino et al. 2011). There still is a need for assistive technology that the blind and visually impaired can use to easily operate mobile phones and also enjoy the innovations in mobile technology.

Research by Nishino et. al. (2011) suggests a method that uses haptic technology in touch screen and Atkinson et. al. (2010) recommended a system that uses electro tactile feedback to simulate roughness in touchscreens for mobile phones

Many other technologies have been developed such as intelligent personal assistants like Apple Inc. Siri and Google Voice. These are however error-prone, and inefficient and are still at a development stage (Guerreiro et al. 2008). Their expensiveness also hinders most blind and visually impaired users to have access to them(Bigham et al. 2008). These Intelligent personal assistants such as Apple Inc. Siri which use voice recognition to carryout user commands on mobile phones were thought to be a breakthrough to such problem and make it much easier for the blind and visually impaired users. This however proved to be less efficient due to misinterpretation of user commands, limited languages and most of all require internet connection to function well (Kane et al. 2008).

The screen readers and magnifiers are also amongst the most popular current methods available to make touchscreen accessible to the blind and visually impaired although their functions are limited to basically reading screen context and cannot be used to navigate touchscreens (Dorigo et al. n.d.).

This paper serves to evaluate and discuss various methods that have been proposed by other researchers to assist the blind and visually impaired users easily use mobile touch screens, determining their effectiveness and if their methodologies are sound and have addressed the problem.

2 Slide Rule Method

Slide Rule is an interface that uses standard multi-touch screen and audio developed by Kane et. al. (2008) for the blind and visually impaired**.** This application uses a set of multi-touch interaction techniques on touch screen interfaces and converts the touch-screen interface into non-visual "talking" surface. The interface enables users to access phone contacts, messages such as email, and multi-media applications such as music using four basic motions: (1) one-finger scan to browse lists, (2) a second-finger tap to select items, (3) a multi-directional flick gesture for additional actions, and (4) an L-select gesture to browse hierarchical information.

An experiment was carried out to evaluate the effectiveness of the slide rule against the Pocket PC reader of which it aimed to improve against. To measure if it's faster, less/more error prone and the time spent reading out each item. The test featured two mobile devices; iPhone and Asus Pocket PC and 10 blind users with at least 10 year screen reader experience. The iPhone contained the Slide Rule while the Pocket Pc contained an application similar to the Slide Rule. On the Pocket PC, users used the buttons to navigate coupled with simple tapping gestures on the screen, while on the iPhone they used the touch screen for slide rule.

Each user was given clear instructions and practice of the tasks before the experiment begun. 3 tasks were performed on both devices starting out with Slide Rule then the Pocket PC for each user; (1) carrying out a call, (2) reading email and (3) playing music of which each user had a maximum of 5 trials. Participants carried out each task to completion rapidly and with accuracy as they were instructed.

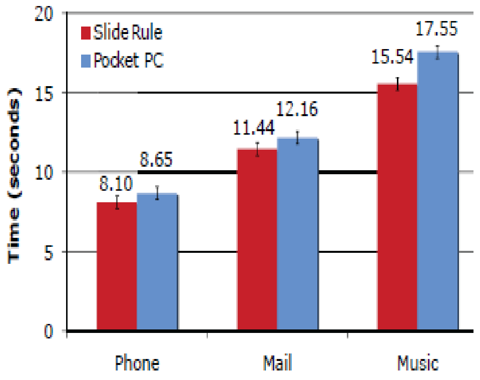


Figure1. Task completion time for 3 tasks for each device (Kane et al. 2008)

In this results, Slide Rule completed tasks much faster with an average of 11.69 seconds and 12.79 seconds for the Pocket PC.

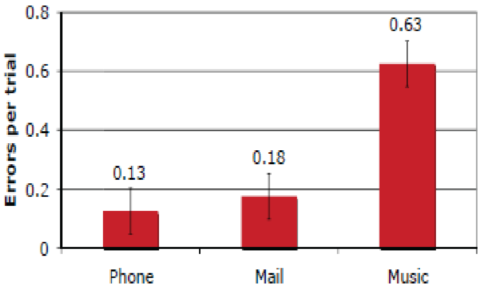
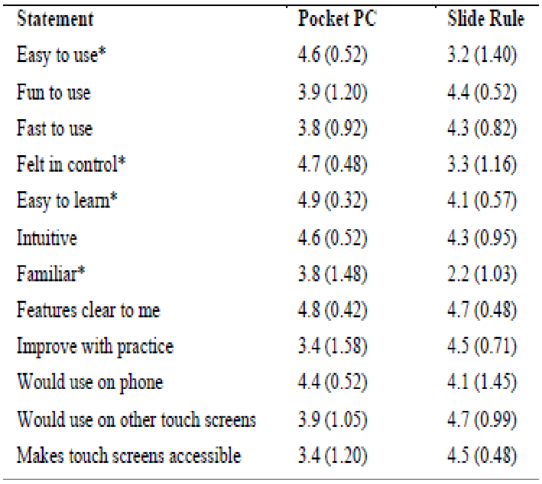


Figure2. Slide Rule average errors per application (Kane et al. 2008)

It was observed that despite Slide Rule being fast, it was more error-prone whereas no errors were experienced using the Pocket PC**.** Slide Rule had 0.20 average errors per trial while the Pocket Pc had none.

Users were also able to scan faster through items with Slide Rule which had a lower time spent listening to each item of 0.95 seconds compared to 1.42 seconds of the Pocket PC.

The researchers went on to make a follow up on the participants to give out their preferences between the two devices using a questionnaire containing some closed questions for numerical analysis and open questions for opinions and recommendations.



Statement	Pocket PC	Slide Rule
Easy to use*	4.6 (0.52)	3.2 (1.40)
Fun to use	3.9 (1.20)	4.4 (0.52)
Fast to use	3.8 (0.92)	4.3 (0.82)
Felt in control*	4.7 (0.48)	3.3 (1.16)
Easy to learn*	4.9 (0.32)	4.1 (0.57)
Intuitive	4.6 (0.52)	4.3 (0.95)
Familiar*	3.8 (1.48)	2.2 (1.03)
Features clear to me	4.8 (0.42)	4.7 (0.48)
Improve with practice	3.4 (1.58)	4.5 (0.71)
Would use on phone	4.4 (0.52)	4.1 (1.45)
Would use on other touch screens	3.9 (1.05)	4.7 (0.99)
Makes touch screens accessible	3.4 (1.20)	4.5 (0.48)

Figure3. Questionnaire results (Kane et al. 2008)

The researchers conducted a good testing strategy for the hypothesis. Testing out the usability and performance of the Slide Rule against current innovations provided a clear point to measure out if their innovation is an improvement and necessary. All the participants were familiar with screen readers and had dexterity to use mobile devices; these skilled participants ensured that the usability testing of Slide Rule is more credible. An expert or familiar user will always provide more insight into what needs to be improved as they have more experience and knowledge of what is expected of a touch screen assistive device. It was also ensured that the gestures of the Slide Rule are working properly before the primary test by conducting a pilot study, which featured 3 blind and two sighted participants to identify any improvement possibilities. The pilot study was necessary to ensure that the devices are working properly hence ensuring more accurate test results. However using skilled participants may not clearly reflect the usability of the Slide Rule, the researchers did not test how long an unfamiliar user may take to learn Slide Rule. Therefore the claims that Slide Rule is easy to learn cannot be verified and need further evaluation.

However with Slide Rule, touchscreens for mobile devices can be made accessible for blind and visually impaired users without the use of additional buttons. The researchers went follow up with qualitative feedback from participants, this provided a more insight into that the Slide Rule is a success. 7 out of 10 users preferred the Slide Rule over the pocket Pc mainly due to its speed and ability to randomly access lists which is a high turnout. The researchers went on to conclude that Slide Rule is a success and that with more use and familiarity, the users speed would improve and the task error rate decrease.

Therefore a conclusion can be reached that Slide Rule allows full accessibility of touch screen mobile devices but an evaluation containing inexperienced users would have provided more convincing results.

3 NavTap and NavTouch

Guerreiro et. al. (2008) in their research suggested two touch screen gesture based text-input methods, NavTap and NavTouch.

NavTap is intended for touch-screen mobile phones with a keypad, of which the touch screen is mainly used for navigational purposes. This method uses the standard keypad to input text and introduces a new navigation system to rid blind and visually impaired users the load of having to memorise key-letter associations. The alphabet is rearranged so that four letters (2,4,6 and 8) are used to navigate through the letters instead. Each selected letter is readout with audio feedback.

NavTouch is similar to NavTap but uses touch-screen in which people perform directional gestures on the screen to navigate the alphabet. It also uses audio feedback with additional functions such as Ok and erase.

There was only one experiment to evaluate the interfaces. This experiment evaluated the ease to learn and the usability of the two methods; NavTap, NavTouch against traditional MultiTap using three groups of blind users with different educational backgrounds. Of that test group, 40% completed elementary, 40% secondary, 20% high schools and one have university degree with no experience using mobile devices for text-entry .Each group was tasked with writing senses using each of the input methods; the error rate for each method was recorded together with the difference between the proposed and transcribed sentences using MSD (Minimum String Distance).

For each session, a 30 minute training session of training was held to familiarise the uses with the method used in that session. Users learned and familiarised themselves faster with the NavTap and NavTouch much faster than the traditional MultiTap. With this the researchers had reached their hypothesis of developing a gesture based method that is easier to learn than the current available methods e.g the traditional MultiTap.

This test uses a good approach of evaluation due to the even distribution of participants, of which had different educations levels therefore avoideing bias in the experiment.. Therefore NavTap/NavTouch is so user-friendly that it can be easily learnt by all people regardless of age or experience with screen readers. The methods also yielded great results and it was also good of the researchers to test out a method in different approaches which lead to a much better and efficient implementation of the method. The error rate for the traditional MultiTap increased from 47% to as high as 71% and decreased with

NavTap to 4% and ended with 14% for NavTouch.

Minimum String Distance (MSD) was used to measure the difference between the proposed & transcribed sentence. MultiTap had an average MSD error rate of 15.6%, NavTap 10% and NavTouch with the least of 4%.

The researchers also recorded the keystrokes for per character for each method to determine which is faster. MultiTap had the least in the frist session followed by NavTap and NavTouch respectively. However with more familiarity of the methods by users, bystrokes per character decreased. MultiTap had a decrease to 5.68, NavTap 5.47 and NavTouch 4.68.

The researchers extensively evaluated their proposed method as a good comparison with a current popular method; MultiTap was conducted. The researchers concluded the research a success as NavTouch proved to be the most efficient method from the experiment. NavTouch had the lowest MSD error rate of 4%, users input text faster and were also learnt it faster than the other methods.

Therefore we can conclude that text input using navigational gestures is more effective than traditional methods.

4 Braille Input Method

A research by Rantala et. al. (2009) focused on the presentation of braille on touch screen mobile devices. They propose to improve the available braille displays for mobile devices of which are externally attached to mobile devices by introducing a portable method that does not require to be linked externally to the mobile device. They developed a braille display method that uses piezoelectric actuator embedded under the touch screen of the mobile device.

The braille is read using a rhythmic pattern or is explored one at a time in which the braille characters are read one at a time. These are implemented using three interactive methods; scan, sweep and rhythm.

4.1 Braille Scan Method

The braille characters in the braille scan are presented using a six-dot braille layout placed in a 2x3 matrix. Tactile feedback is produced for the dots and the dots are then read with a downward movement of the stylus.

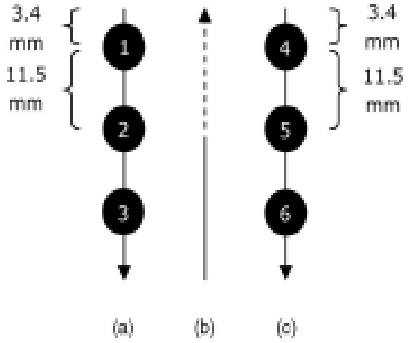


Figure4. Column (a) is read first then the stylus is moved one step upward to (c) to read last column (Rantala et al. 2009).

The stylus is placed on the screen and moved downwards to read the first column. The second column is read by moving the stylus one step upward for the second column to appear which will be read in the same downward movement of the stylus.

4.2 Braille Sweep Method

The braille characters are placed horizontally across the screen and are read with a sweeping movement of the stylus from either the left-right or right to left.

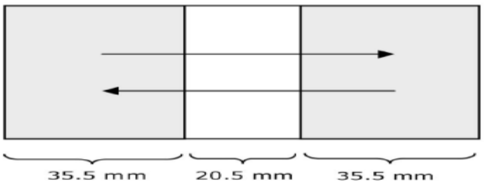


Figure5. The braille is read by either sweeping stylus from left-right or right to left (Rantala et al. 2009).

4.3 Braille Rhythm Method

The braille characters are read by placing the stylus on the screen and then presented with tactile pulses in a numerical order.

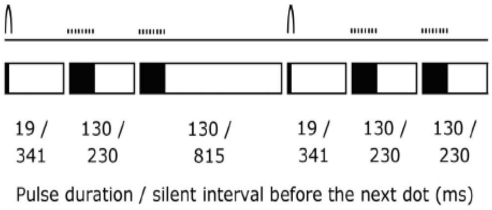


Figure6. Dots 1 and 4 present the feedback pattern for letter “c” in Braille. The first and the fourth dots are raised (higher pulse shapes) and the other four lowered (lower pulse shapes) (Rantala et al. 2009).

Two experiments were conducted for this research. The first experiment was to evaluate if the users can recognize the braille dots using each of the three methods. The test comprised of 3 sessions to monitor the improvements and stability of presentation methods. The experiment was done by 6 blind users, each with an average of 24 years reading Braille. However the 6th participant was excluded from the test due to not understanding the instructions and therefore results are based from 5 participants. A Nokia 770 Internet Tablet together with a stylus were used in the experiment. The participants used hearing protector headphones to listen to a pink noise to block out the piezoelectric actuator noise while the instructions and verbal feedback were given out by the instructor using the microphone. An application written in C was used to control the character presentation; this was implemented on the Linux operating system of the device.

Stylus down to stylus up events was used to measure the reading times of characters.

After the three sessions the scan method had 97%, sweep 91% and rhythm with 92% mean recognition accuracies. Over 9 out of 10 characters were recognised using 2 motions.

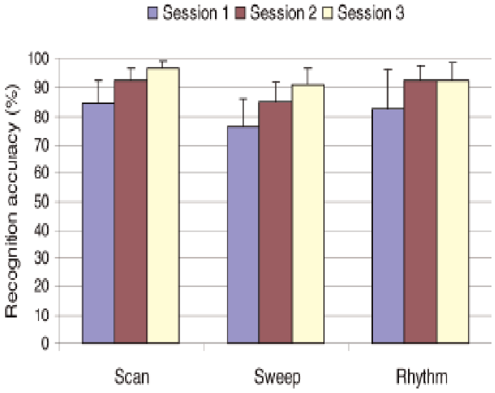


Figure7. Mean recognition accuracies for each method and session (Rantala et al. 2009).

As for the reading times, they were as follows after the 3 sessions for each method; scan 5.7 seconds, sweep 5.1 seconds and rhythm with 3.7 seconds. However the statistical analysis did not contain the rhythm method as the dots were presented to the screen with fixed interval and therefore constant reading time.

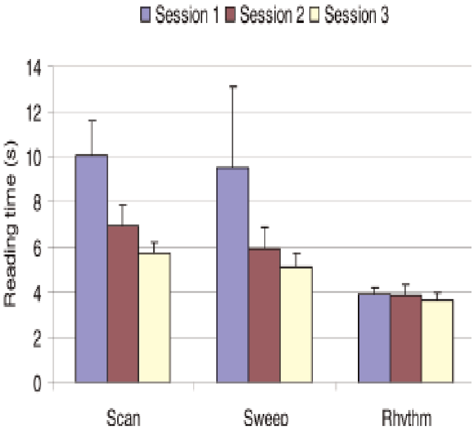


Figure8. Mean reading times for each method with each session (Rantala et al. 2009).

The rhythm method was concluded as the most efficient method amongst the three methods by the researchers. It was the fastest and can be used without the stylus and also the dots are read by placing the stylus in one point on the screen. The rhythm method had a high recommendation rate by participants; four out of five opted for it.

The second experiment focused on testing the rhythm method further evaluating the performance of participants with the character duration shorter than in the first experiment. The other difference is that the participants did not use the stylus but their fingers.

The test experiments performed have evaluated if the characters can be read using the three methods; scan, sweep and rhythm. The results were great and all methods scored high results although the rhythm method was selected as the best. The researchers also conducted a pilot study to ensure that each method is working as required in order for the test results to reflect true without any method being disadvantaged. The second test evaluated the effectiveness of using different apparatus to read the rhythm. This is good as it allows for the discovery of most effective way to read the rhythm and changes be applied to make the reading of the rhythm more effective. Although the test carried out were good, there were some months separating the two experiments. This may affect the test negatively as it was observed that the mean recognition time for test two was lower than test one, some users may have forgotten some aspects of using the rhythm method. Therefore further evaluation is needed for the recognition time of experiment two with no significant separation between the tests. The experiments were also conducted using highly experienced braille users who may provide a good insight into the usability of the methods. The tests were complex and therefore needed experienced braille readers to effectively identify the difference between the methods as it was observed that the test results between them were slight. Although this a good approach, we cannot ignore that the number of participants was quite small and the second test was also performed with the same five users. This may bring a doubt into the credibility of the results and therefore the tests need to be performed with a much larger population of participants.

Therefore it can be concluded that a piezoelectric actuator can be used to produce a method for braille presentation on mobile devices without the use of an external device.

5 Conclusions

In this paper, three touchscreen methods were evaluated. These methods are essential to allow blind and visually impaired users to fully access the touchscreen in mobile devices without the use of external devices for display. It can be concluded that tactile feedback is the most effective method as it eliminates the problem of using screen readers in noisy environments where they tend to be useless.

An interface that uses tactile feedback combined voice recognition would be ideal. Users would be able to easily switch between using voice or braille for screen reading and navigational text input for fast and accurate text input. Such a user interface is recommended.

References

Altinsoy, M.E. & Merchel, S., 2012. 'Electrotactile Feedback for Handheld Devices with Touch Screen and Simulation of Roughness'. *IEEE Transactions on Haptics*, 5(1), pp.6–13.

Bigham, J.P., Prince, C.M. & Ladner, R.E., 2008, 'Addressing Performance and Security in a Screen Reading Web Application That Enables Accessibility Anywhere'. *Eighth International Conference on Web Engineering, pp.273–284.*

Dorigo, M., Stengel, I. & Dowland, P.S., Survey : Assistive technologies for blind and visually impaired people 1 Introduction. , pp.1–8.

Guerreiro, T., Lagoa, P., Nicolau, H., & Jorge, J. A., 2008, 'From Tapping to Touching: Making Touch Screens Accessible to Blind Users' 48-50.

Kane, S.K., Bigham, J.P. & Wobbrock, J.O., 2008, Slide Rule : Making Mobile Touch Screens Accessible to Blind People Using Multi-Touch Interaction Techniques. , pp.73–80.

Nishino, H., Goto, R., Kagawa, T., Yoshida, K., Utsumiya, K., Hirooka, J., Osada, T., Nagatomo, N., Aoki,E., 2011, 'A Touch Screen Interface Design with Tactile Feedback'. *International Conference on Complex,* *Intelligent, and Software Intensive Systems*, pp.53–60.

Rantala, J., Raisamo, R., Lylykangas, J., Surakka, V., Raisamo, J., Salminen, K., Pakkanen, T., Hippula, A., 2009, 'Methods for Presenting Braille Characters on a Mobile Device with a Touchscreen and Tactile Feedback'. *IEEE Transactions on Haptics*, 2(1), pp.28–39.

An Evaluation Of Sector/Sphere When Mining Large Distributed Datasets

Gorata Pearl Modutlwa

Abstract

This paper evaluates high performance storage and processing facilities necessary to close the gap between the amount of data that is being produced and the capability of current systems to store and analyze this data. Cloud computing platform known as Sector/Sphere is looked at through evaluation of published research focusing on applications, experimental studies and their results and problems it has. This paper compares two versions of Sector/Sphere the first and second with the second version focusing on version one shortcomings. It then recommends the platform looking at experiments carried out in both versions which proved Sector/Sphere performance better than its competition.

1 Introduction

Performance while data mining is an issue in today's time as data capacity is growing bigger and bigger every day. Due to this increase, users experience difficulties figuring out which server hosts a particular file, which replica is the latest version as they are randomly done and it's difficult to keep them consistent as they span across multiple data servers. Users also experience low throughput when downloading files from remote locations using Internet (WordPress.com 2010).In order to address these problems current research has moved away from being processor focused to focus on data locality, speed and data handling, this move is achieved by cloud computing platforms (Gu and Grossman 2009) .

Sector/Sphere is a cloud computing platform which mines data across data centers without need to move the data, with processing of the data being done only when needed while also providing back up for data by replicating it (Gu and Grossman 2009) and (Ali and Khandar 2013).This thou does not mean Sector/Sphere is out of fault, challenges of load balancing, data locality and fault tolerance were realized after version one (Gu and Grossman 2010).

In this paper academic journal's experimental work and Sector/Sphere applications will be critically evaluated focusing on high performance, wide area networks and data mining. This paper focuses on the research currently published concerning Sector/Sphere and how it improves data mining using high performance networks. To make this possible this platform assumes high performance, wide area networks are in place and specialized protocols are used together with user defined functions to manipulate data (Mishra, Sharma and Pandev 2013). Since this platform employs a layered architecture parallelizing is easily achieved which is needed for efficient management and manipulation of data.

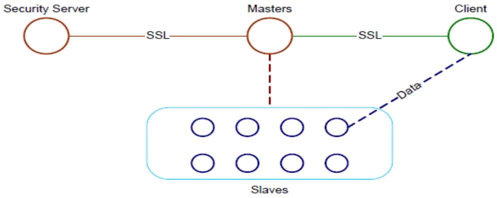


Figure 2 Sector/Sphere architecture (Gu and Grossman 2009)

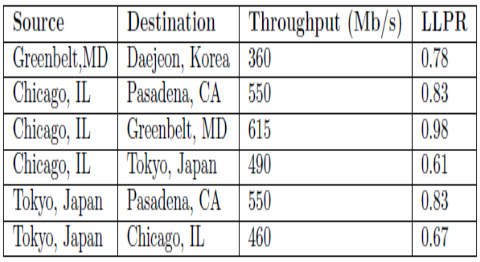
2 Presentation and Evaluation

In order to carry out this evaluation an extensive literature review was done. Firstly version one of Sector/Sphere is looked at then version two is looked as it counters for some challenges experienced in the first version all of which will show how performance of data mining can be improved. The paper is divided into two parts focusing on these versions.

2.1 Sector/Sphere Version 1.0

Grossman et al (2009) focuses on a cloud based architecture which is optimized for wide area high performance. They carried out three experiments, one of which focused on Sector while two others were about Sphere. These experiments which are in the form of applications will be looked at closely experiment by experiment so as to see how they were done and if proper steps were followed. Firstly a high performance wide area test bed connected using 10Gbps networks and 4core Opteron servers each with 2.4 GHz CPU and 4GB memory was made which the applications ran on.

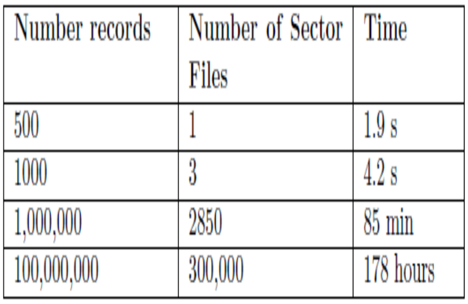
Experiment one of Grossman et al(2009) looks at a content distribution network for large e-science datasets of which its performance was measured by a long distance to local performance ratio (LLPR). The higher the LLPR the better the performance and it has a maximum of 1.0 performance to say that the long distance data transfer cannot be faster than local transfer within the same hardware setup. The following table shows the success of Sector storage cloud from the experiment carried by Grossman et al (2009) meaning the access to the data set is as much as those at the actual data set.



Source	Destination	Throughput (Mb/s)	LLPR
Greenbelt,MD	Daejeon, Korea	360	0.78
Chicago, IL	Pasadena, CA	550	0.83
Chicago, IL	Greenbelt, MD	615	0.98
Chicago, IL	Tokyo, Japan	490	0.61
Tokyo, Japan	Pasadena, CA	550	0.83
Tokyo, Japan	Chicago, IL	460	0.67

Table 1 Sector storage cloud providing performance matching that of scientist at the data (Grossman et al. 2009)

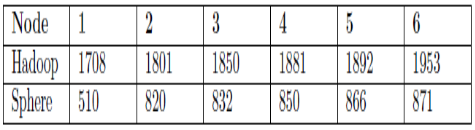
Experiment two was a Sphere application called Angle that looked at identifying problems within a TCP data packet built up across multiple distributed geographical locations. It contains sensor nodes that are attached to the Internet to collect IP data. These nodes are connected to Sector nodes on a high performance network so they could be managed while Sphere identifies the suspicious behavior. This experiment was evaluated using K-means algorithm since the results of Angle are clustered into a feature space (Grossman et al.2009).



Number records	Number of Sector Files	Time
500	1	1.9 s
1000	3	4.2 s
1,000,000	2850	85 min
100,000,000	300,000	178 hours

Table 2 performance of Sector/Sphere when computing cluster model (Grossman et al.2009)

The third and final experiment done by Grossman et al (2009) compared Sphere to Hadoop which is also a cloud computing platform used to enhance performance of data centers. These two were compared on a six node Linux cluster at one place. This experiment focused on the speed in seconds at which these platforms could create a 10GB file on each node and perform a distributed sort on each file.



Node	1	2	3	4	5	6
Hadoop	1708	1801	1850	1881	1892	1953
Sphere	510	820	832	850	866	871

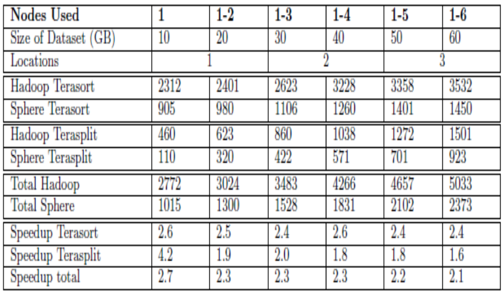
Table 3 performance of sort phase with Hadoop using four core nodes while Sphere uses only two (Grossman et al. 2009)

Looking at this paper it is evident that good experimental skills were put in place since all the experiments were carried out in one controlled environment. This alone increased the chances of unbiasedness in the output of the experiments. Each of the experiments was carried out multiple times so as to eliminate the element of randomness in the output thus confirming the reliability of increased performance when using Sector/Sphere platform.

Performance measures were put in place each targeting the relevant experiment in order for the results to be scrutinized easily while also maintaining the scale of performance to seconds. The research went on to evaluate performance against platforms using high performance networks. However since no original data was provided before carrying out the experiments it's impossible to see if desired performance was reached even though the results show good speed.

Gu and Grossman (2009) adds on to their previous research by writing an updated research focusing on describing Sector/Sphere, its application and experimental studies done comparing Sector/Sphere to Hadoop using two different benchmark being the Terasort benchmark and the Terasplit benchmark which employs a split for regression tress. In this paper they presented control information and separated testbeds into wide area experiments and local area experiments. The wide area experiments used six servers across three different locations being Chicago, Greenbelt and Pasadena, the servers used 4core 2.4Ghz Opteron processors, 4GB RAM, 10GE MyriNet Nic and 2TB of disk whereas local area experiments used newer eight servers with 4core 2.4Ghz Xeon processors with 16GB RAM, 10GE MyriNet Nic and 5.5TB.

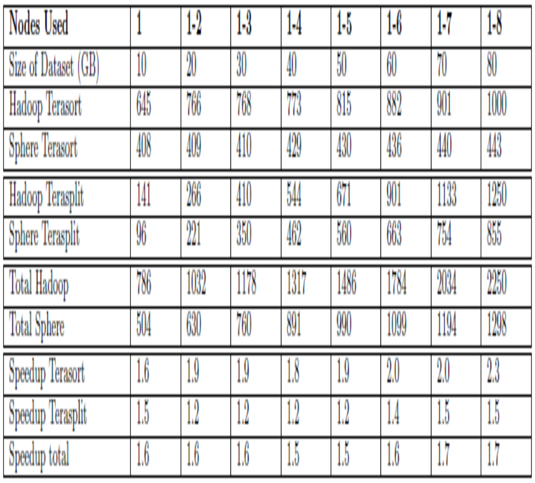
In their first experiment Gu and Grossman(2009) compared Hadoop to Sphere at a wide area testbed while using both benchmarks. At this testbed performance approximating 2.4 to 2.6 for Sector/Sphere as compared to Hadoop were realised for sorting 10GB data at each node with 100 byte record and 10 byte key.



Nodes Used	1	1-2	1-3	1-4	1-5	1-6
Size of Dataset (GB)	10	20	30	40	50	60
Locations	1		2		3	
Hadoop Terasort	2312	2401	2623	3228	3358	3532
Sphere Terasort	905	980	1106	1260	1401	1450
Hadoop Terasplit	460	623	860	1038	1272	1501
Sphere Terasplit	110	320	422	571	701	923
Total Hadoop	2772	3024	3483	4266	4657	5033
Total Sphere	1015	1300	1528	1831	2102	2373
Speedup Terasort	2.6	2.5	2.4	2.6	2.4	2.4
Speedup Terasplit	4.2	1.9	2.0	1.8	1.8	1.6
Speedup total	2.7	2.3	2.3	2.3	2.2	2.1

Table 4 performance of Sphere and Hadoop sorting a 10GB file with 100byte records (Gu and Grossman 2009)

Gu and Grossman (2009) continued their comparison between Sector/Sphere and Hadoop by carrying out the same experiment as above but focusing on a single location still using both benchmarks. Here perfromance levels between 1.6 and 2.3 at Terasort benchamrk were realised while at the Terasplit performance approximating 1.2 to 1.5 were reached making Sector/Sphere faster than Hadoop. Nonetheless “Hadoop performed better on clusters employing 1GB than 10GB” (Gu and Grossman 2009).



Nodes Used	1	1-2	1-3	1-4	1-5	1-6	1-7	1-8
Size of Dataset (GB)	10	20	30	40	50	60	70	80
Hadoop Terasort	645	766	768	773	815	882	901	1000
Sphere Terasort	408	409	410	429	430	436	440	443
Hadoop Terasplit	141	266	410	544	671	901	1133	1250
Sphere Terasplit	96	221	350	462	560	663	754	855
Total Hadoop	786	1032	1178	1317	1486	1784	2034	2250
Total Sphere	504	630	760	891	990	1099	1194	1298
Speedup Terasort	1.6	1.9	1.9	1.8	1.9	2.0	2.0	2.3
Speedup Terasplit	1.5	1.2	1.2	1.2	1.2	1.4	1.5	1.5
Speedup total	1.6	1.6	1.6	1.5	1.5	1.6	1.7	1.7

Table 5 Performance of Sphere over Hadoop at a single location (Gu and Grossman 2009)

Gu and Grossman (2009) also describes one of their application known as Angle unlike in their previous paper they state that it identifies emergent behaviour in multiple ways. Firstly Sphere combines feature files into temporal windows each known as length ‘d’ then clusters are computed for them using different centres. Due to their temporal evolution these clusters are called emergent clusters and they can be used to identify feature vectors with emergent behaviour.

$$\rho(x) = \max_k \rho_k(x)$$

$$\rho_k(x) = \theta_k \exp\left(\frac{-\lambda_k^2 \|x - a_k\|^2}{2\sigma_k^2}\right),$$

Figure 3 function to score feature vectors (Gu and Grossman 2009)

Taking into consideration how Gu and Grossman (2009) handled their experiments and presented their work, I concluded that it was a good research since all experiments were done under a controlled environment. Unlike in their previous paper Gu and Grossman(2009) started by presenting constant variables which acted as controls for the experiments they carried out. This data helped in evaluating results since both versions of the data are available thus eliminating uncertainty when reviewing experiments results. These experiments were also carried out at local and wide area network using both test beds at each network thus allowing for the capabilities of the two platforms to be fully exhausted proving Sector/Sphere performance better at high performance networks of 10Gbps while Hadoop does at low performance networks of 1Gbps.

2.2 Sector/Sphere version 2

This version of Sector/Sphere focuses on providing support for fine tuning data placement to improve data locality, multiple input/output, multiple user defined functions as well new features like fault tolerance and load balancing. Gu and Grossman (2010) starts off introducing Sector/Sphere, its application aware capabilities, data processing framework and some new eperimental studies undertaken to cater for the abov mentioned problems.

Data Locality and Reliability

Since Sector/Sphere does not split files into blocks but places them as they are on single nodes it means users have to manually split the data this creates additional work. On their paper Gu and Grossman (2010) handles this challenge using file families which applies specific rules concerning data locality, it places all related files together in one segment thus reducing data moved when querying multiple columns. These families are also coupled with index files so as to reduce search time.

Since Sector/Sphere runs on wide area networks to improve on its previous replication strategy, it allows the user to select the time for creating replicas that is periodically or after data is written this enables it to be independent from its system replicas (Gu and Grossman 2010).

Load Balancing

Since Sphere applies the same User Defined Function independently to enable parallel processing of data load balancing and fault tolerance of data segments /set are handled and these are normally distributed over multiple Sector nodes. As these datasets are many they are sent to a bucket list which experienced bottleneck problems (Gu and Grossman 2010).

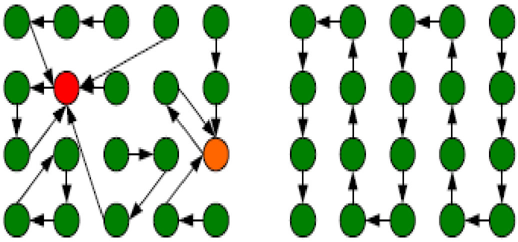


Figure 4 Congestion problems (Gu and Grossman 2010)

A decentralized approach is used to counter for this problem by eliminating hot spots that is to say before a node could send results to a bucket list, a request for recent data transfer is sent to the destination node and if the results are greater than s threshold a different bucket is considered (Gu and Grossman 2010).

Fault Tolerance

Sector/Sphere uses data replication to handle this issue, this thou is complicated by UDF sending data to multiple bucket lists since its transferred between source and destination nodes which means if the source node fails the data will be incomplete at the destination node and if it happens at the destination then data from multiple sources will be lost. To counter for this previously, buckets list were duplicated which lead to overheads and higher chances of failures.

Gu and Grossman (2010) in their paper introduces splitting of UDF that generate bucket list into those focusing on generating local files while another gathers and places them in their final bucket list. They continue to introduce the Sphere voting system which identifies and eliminates poor performance nodes. This system measures low performance if a node gets more than fifty percent of its votes in a given time period then its eliminated. Thse votes are cleared after their time collapse so as to avoid eliminating all nodes as their vote increase.
Data processing

As Sphere processes multiple input/outputs iterative processing using K-means clustering algorithm are done. With the in memory objects and indexes time spent reconstructing data structures and locating output bucket lists is reduced. These two when used with the join operation related bucket lists can be co-located enabling them to be read at the same location (Gu and Grossman 2010).

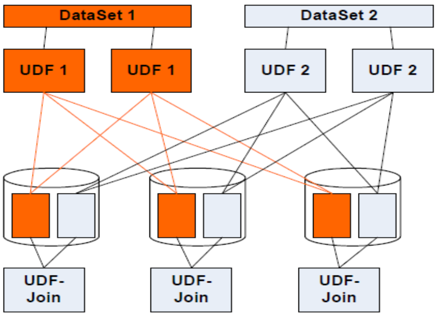
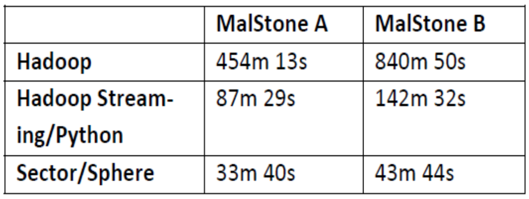


Figure 5 Joining datasets (Gu and Grossman 2010)

Three experiments were carried out one focused on optimizing batch processing done at the MalStone benchmark, the second compared resource usage of sector/sphere to Hadoop done at the Terasort test beds while the third looks at how Sphere parallelizes data processing (Gu and Grossman 2010).

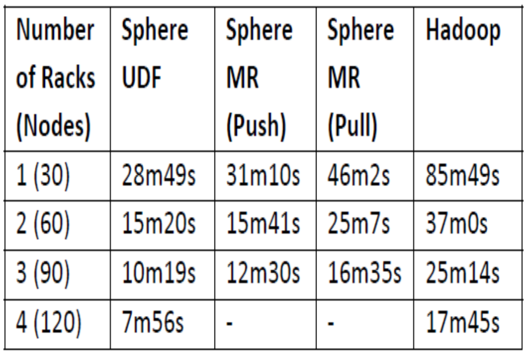
The first experiment was done in two benchmarks of MalStone, both of which run on synthetic data generated by a utility called MalGen. Each consists of 10billion records. The first benchmark computes a ration for each site w, by collecting entities that visited the site at any time and calculate their percentages for which the entity will cross checked in future. The second benchmark works the same with an exception at the computation as it happens for a particular week per site for the past visits marking them as computed.



	MalStone A	MalStone B
Hadoop	454m 13s	840m 50s
Hadoop Streaming/Python	87m 29s	142m 32s
Sector/Sphere	33m 40s	43m 44s

Table 6 Hadoop against Sector/Sphere MalStone Benchmark (Gu and Grossman 2010)

The second experiment is the same as the one in Sector/Sphere version with an exception of examined resources usage. As it is the same results were obtained as before but aggregate network input/output on hundred and twenty nodes running Sector is greater than 60 GB/s unlike Hadoop has 15 GB/s. This indicates resources are used efficiently due to higher input/output although Hadoop used much processing. This experiment included comparisons against Sphere and MapReduce (Gu and Grossman 2010).



Number of Racks (Nodes)	Sphere UDF	Sphere MR (Push)	Sphere MR (Pull)	Hadoop
1 (30)	28m49s	31m10s	46m2s	85m49s
2 (60)	15m20s	15m41s	25m7s	37m0s
3 (90)	10m19s	12m30s	16m35s	25m14s
4 (120)	7m56s	-	-	17m45s

Table 7 Sphere against Hadoop Terasort benchmark (Gu and Grossman 2010)

It is clear from this work that the Gu and Grossman (2010) paper address problems which affected Sector/Sphere and could have possible affected data mining of large datasets. The problems were first mentioned together with their causes, previous solutions and new solutions. This enabled a distinction between these to be clear. Good experimental skills were applied during their research since they had being previously done so they were able to test new solution and also compare the results easily thus removing unbiasedness.

3 Conclusions

Large dataset are inevitable as data is growing so effective management and manipulation of them is needed. From the above evaluation it’s evident that Sector/Sphere is an optimal solution for anyone experiencing problems concerning mining of large datasets. I recommend this cloud computing platform since it has proved to be reliable, efficient and good for handling large data sets. This platform is able to consolidate data from multiple data centers and prepare it user manipulation this in turn helps users as all their needs are handled concerning large datasets. As seen most of research was done by the same authors but they were able to define and handle different aspects concerning this platform which makes them credible as well as the works they presented. From the detailed experiments they carried out and good experimental skills there were able to support their hypothesis that Sector/Sphere is the best solution. With this I conclude this research into Sector/Sphere.

References

Ali, U. and Khandar, P., 2013, 'Data Mining For Data Cloud and Compute Cloud', *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 1, No. 5, July, pp. 1-5.

Grossman, R.L., Gu, Y., Sabala, M. and Zhang, W., 2009, 'Compute and Storage Clouds Using Wide Area High Performance Networks', *FGCS - Future Generation Computer Systems*, Vol. 25, No. 2, February, pp. 179-183.

Gu, Y. and Grossman, R.L., 2009, 'Data Mining Using High Performance Data Clouds:Experimental Studies Using Sector and Sphere', *IEEE Xplore*, Vol. 1, No. 1, August, pp. 1-10.

Gu, Y. and Grossman, R., 2009, 'Exploring Data Parallelism and Locality in Wide Area Networks', *Many-Task Computing on Grids and Supercomputers*, Austin,Texas, 1-10.

Gu, Y. and Grossman, R.L., 2009, 'Sector / Sphere: High Performance Distributed File System and Parallel Data Processing Engine', *Philosophical Transactions of The Royal Society A: Mathematical, Physical and Engineering Sciences ,* Vol. 367, No. 1897, January, pp. 2429-2445.

Gu, Y. and Grossman, R.L., 2009, 'Sector and Sphere: The Design and Implementation of a High Performance Data Cloud', *Philosophical Transactions of the Royal Society,* Vol. 0053, No. 1, October, pp. 2429-2445.

Gu, Y. and Grossman, R., 2010, 'Towards Efficient and Simplified Distributed Data Intensive Computing', *IEEE Transactions on Parralel and Disdributed Systems*, *Manuscrip*t ID, Vol. 2, No. 6, August, June, pp. 1-12.

Mishra, N., Sharma, S. and Pandev, A., 2013, 'High performance Cloud data mining algorithm and Data mining in Clouds', *IOSRJCE*, Vol. 8, No. 4, Jan-Feb, p. 54.

WordPress.com, 2010, 'A Private “DropBox” for Your Enterprise', *VeryCloud Accelerate Your Data,* 12 December, pp. 1-2.

A Detailed Analysis on Data Mining Techniques Used For Detecting Credit Card Fraud

Thato Carol Mosimanemotho

Abstract

Credit card fraud has proven to be many financial institutions' big problem. Banks are losing a lot of money due to credit card fraud. This paper evaluates three models for detecting credit card fraud using different data mining techniques. Data mining is a way of generating patterns from the data and divides this data according to how it relates. Data mining techniques includes clustering, decision trees, association rules, classification and neural networks. This paper will focus only on three techniques of data mining being clustering, decision trees and neural networks.

1 Introduction

Credit card fraud has turned out to be a major problem for the banks using this technology. It is an e-commerce technology of paying for goods and services without using cash in hand. With the current systems of detecting credit card fraud, there is a problem of accessing bank databases because most bank databases are huge and they are many (Ogwueleka 2011). Most of these systems fail to work with these kinds of databases; this hinders the solving of the problem. Some banks also fails to frequently obtain updated fraud patterns, these banks might continuously suffer fraud attacks (Chaudhary et al. 2012). This situation also fails the systems because most of the credit card fraud detection system uses the fraud patterns to discover if a transaction is fraudulent or it's legitimate. If the database does not update the fraud patterns frequently then the system will not be able to work to its level best because these patterns changes, so they need to be updated frequently. There is also a chance that transactions made by the fraudsters in the past fit in the pattern of normal behaviour that is being counted as a legitimate transactions. Also the profiles of a fraudulent behaviour changes constantly so the system has to take into account this problem (Sahin et al. 2013).

2 Data Mining Techniques Used for Credit Card Fraud Detection

2.1 Clustering

(Dheepa & Dhanapal (2009); Modi et al. (2013); Delamaire et al (2009)) agree that clustering breaks down data in a way that generates patterns. Clustering allows for identification of an account which has their trend of transactions changing, that is displaying a behaviour it has never displayed before. Unlike other techniques clustering does not require the model to know the past fraudulent and non -fraudulent transactions (Ganji 2012). Clustering is an unsupervised learning model. Ganji (2012) proposes a model which uses the outlier and reverse k Nearest Neighbour which are both clustering techniques. With outlier technique an observation is made that diverges so much from other observations that raise suspicion. It does not learn from past transactions from the database, instead it detects changes in behaviour or transactions which are not usual (Ganji 2012; Dobbie et al. 2010). The graphs below show how outlier classifies transactions.

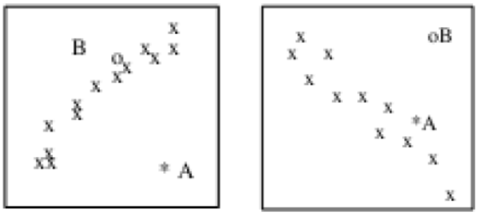
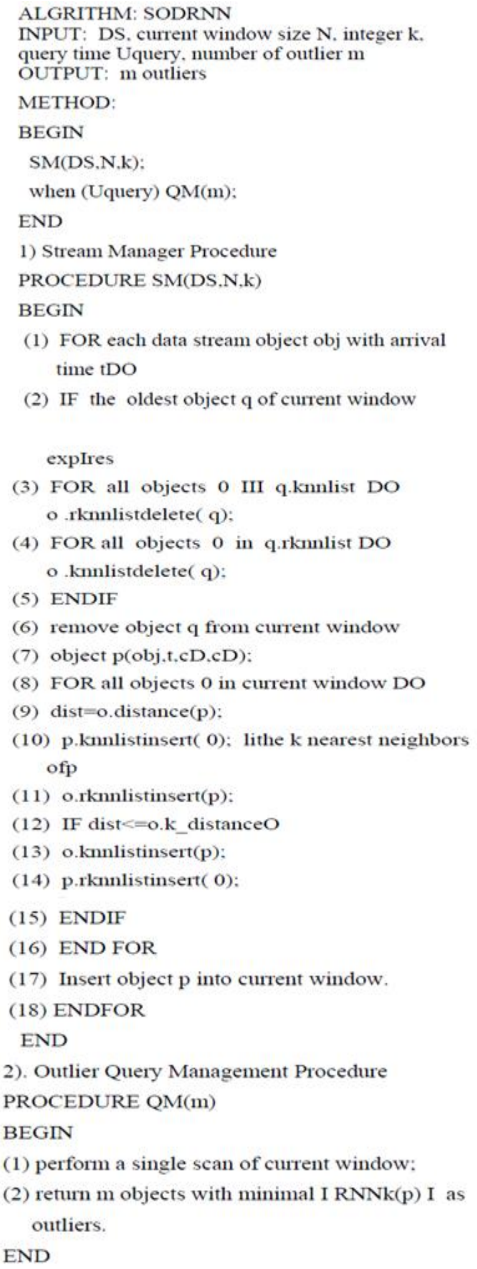


Figure 1.graphs showing how outliers work (Ganji 2012)



```
ALGRITHM: SODRNN
INPUT: DS. current window size N. integer k.
query time Uquery. number of outlier m
OUTPUT: m outliers
METHOD:
BEGIN
  SM(DS.N.k);
  when (Uquery) QM(m);
END
1) Stream Manager Procedure
PROCEDURE SM(DS.N.k)
BEGIN
  FOR each data stream object obj with arrival
    time tDO
  IF the oldest object q of current window

    explres
  FOR all objects 0 III q.knnlist DO
    o .rknnlistdelete( q);
  FOR all objects 0 in q.rknnlist DO
    o .knnlistdelete( q);
  ENDIF
  remove object q from current window
  object p(obj.t.cD.cD);
  FOR all objects 0 in current window DO
  dist=o.distance(p);
  p.knnlistinsert( 0); lithe k nearest neighbors
    ofp
  o.rknnlistinsert(p);
  IF dist<=o.k_distanceO
  o.knnlistinsert(p);
  p.rknnlistinsert( 0);
  ENDIF
  END FOR
  Insert object p into current window.
  ENDFOR
 END
2). Outlier Query Management Procedure
PROCEDURE QM(m)
BEGIN
perform a single scan of current window;
return m objects with minimal I RNNk(p) I as
  outliers.
END
```

Figure 2 SODRNN algorithm pseudo code (Ganji 2012)

The outlier detection was combined with reverse K-nearest neighbour to develop Stream Outlier Detection on Reverse K- Nearest Neighbours algorithm (SODRNN). This algorithm has two processes being stream managing process and the query managing process. There is also a window which should be allocated in memory. The incoming data stream objects are received by the former procedure and it efficiently brings up to date the current window. Upon the coming of the new stream objects, to keep the current window, it keeps the k-nearest neighbour list and the reverse k- nearest neighbour list of the influenced objects in the current window instead of that of the whole data stream objects in the current window. During the insertion of the new oncoming objects, it will scan through to the current window to look for the objects that their K-nearest neighbour is influenced. When the k-nearest neighbour list of the objects in the current window is updated, they also update reverse k- nearest neighbour list. When the top *m* query of the outliers is demanded by the user, the latter process will scan the current window and return *m* objects whose reverse k- nearest neighbour (p) is small as of this query.

Real datasets were used to perform the experiments. To evaluate the detection performance, information about the outliers were assumed in all the experiments. SODRNN was implemented and conducted on a PC with the following features:

- Pentium D 3.1GHz
- 1 GB Memory
- Windows XP

To carry out the experiment, a dataset with a certain magnitude was chosen, the random number generator created in the highest dimensional space equally spread data, which includes the 10, 000 multi-dimensional space point data. The equally spread data ware tested the X * X tree index structure and actual take up memory. This is shown on Figure 3, when the dimension increases, X * X tree index structure and the actual memory space which is occupied by an equivalent increase, because all the nodes in the array of dataset with the MBR with the increase of dimension up more memory space, and the X directory tree wants all the nodes in all the dataset additional storage node split in the history record. The following figure shows the results.

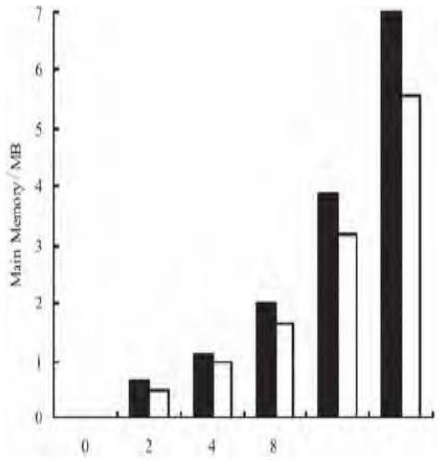


Figure 3 Main memory requisitions of the two indexes structure for different dimension (Ganji 2012)

This model is good since there is no need to train data. Because to implement methods which train data is usually expensive. It is also able to detect previous undiscovered types of fraud unlike supervised methods. This model has reduced the number of scans to one as compared to other models. With the experiment that was carried out, the model has proven to be efficient and effective. Also this model makes it easier to determine fraudulent transactions and legitimate transactions looking at the spending nature of the card holder. Although clustering can be a very good technique, there are situations where this technique is likely to fail. Situations like when the fraudulent transactions fall in the same pattern as the legitimate transactions. This will be difficult to notice and difficult to solve. Frausters can learn the pattern of the legitimate transactions and make sure that their transactions follows the same patterns, to make it hard for the system to notice.

2.2 Neural Networks

Neural networks work like a brain of a human being. The technique learns from past experience for it to predict and classify the data (Akhilomen (2013); Ogwueleka (2011); Günther & Fritsch (2010); Chaudhary et al. (2012); Sherly (2012)). In this way neural nets in credit card fraud does the same thing, they learn the legitimate and fraudulent transactions. Then after learning they will be in a position to predict and classify transactions. Other methods used for credit card fraud apart from neural networks have limitations such as; they do not have the ability to learn from past experience; they do not have the ability to predict the future looking at the present situation. Neural networks work in such a way that the linear combination of the nodes are compared and if the input weight connections exceeds the threshold the activation key fires.

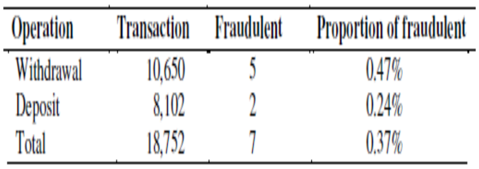
Ogwueleka (2011) proposed a system application that used neural networks method called Self-Organizing Maps (SOM) to predict transactions which are fraudulent and the ones that are legitimate. The system used four categories being low, high, risky and high risky. Only legitimate transactions are processed the ones which falls in other groups are labelled suspicious or fraudulent and they will not be processed. Ogwueleka (2011) carried out the experiment which was done following the steps below:

- Choose a suitable algorithm.
- Use the algorithm with dataset that is known
- Evaluating and refining the algorithm which is being tested with other datasets.
- Discuss the results.

According to Ogwueleka (2011) when a transaction is made, this application will run secretly in the background and check if the transaction is legitimate. The system has two subsystems being the database, where the transactions are read into the system and the credit card fraud detection engine which checks if the transactions are legitimate when they are performed.

The detection system has two components which are the withdrawal and the deposit. Each component has subcomponents which are: the database, the neural network classification and visualization. The database was tested to make sure that all the needed dataset is brought into the model and the model uses it. SOM algorithm was used in neural network classification. This is where the dataset loaded from the database will be divided into a training dataset and a test dataset. The training dataset was divided further into sub units used for elimination of the model and a subset will be used to evaluate the system performance.

The data being tested was prepared and used on the system with the program that is being tested. Results from the test were analysed with physically arranged results for the effectiveness of the new model to be determined. To measure effectiveness of the application, this was done in terms of classification errors. Classification errors consisted of system detection rate and false alarm rate. The dataset was designed from transactions made per day in a month in a Nigerian bank. The table below shows the performance results.



Operation	Transaction	Fraudulent	Proportion of fraudulent
Withdrawal	10,650	5	0.47%
Deposit	8,102	2	0.24%
Total	18,752	7	0.37%

Figure 4 performance results (Ogwueleka 2011)

MATLAB software package was used to analyse the performance of the detection algorithms and the results were compared with the collected data which are shown below.

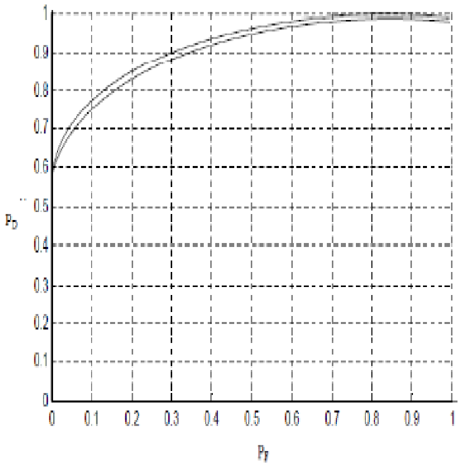


Figure 5 Receiver Operating Curve (ROC) for withdrawal fraud detection (Ogwueleka 2011)

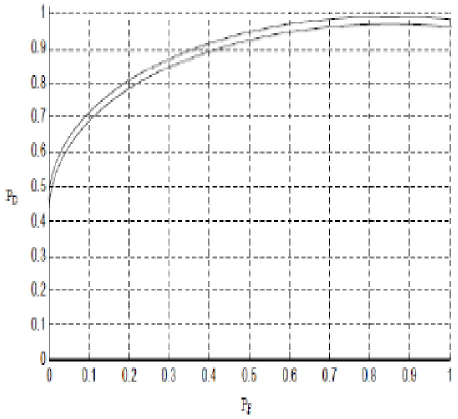


Figure 6 Receiver Operating Curve for deposit fraud detection (Ogwueleka 2011)

P_D =probability of false negative
P_F =probability of false positive

When compared to other models used for detecting fraud using the ROC curve, credit card fraud detection watch has proven to be the best in performance. The results also proved the reliability and accuracy of the credit card fraud detection using neural network. When testing for the feasibility neural network tools for credit card fraud detection watch, two commercial products being quadratic discriminates analysis (QDA) and logistic regression (LOGIT) were used. Figure 6 shows results of the comparison of performance analysis of the credit card fraud detection watch model with QDA and LOGIT.

In figure 7, credit card fraud detection watch ROC curve shows the detection of over 95% of fraud cases without causing false alarms. It is followed by logistic regression ROC curve which shows the detection of 75% of fraud cases with no false alarm. With quadratic discriminant analysis, it detected only 60%. This proves that credit card fraud detection watch performs better.

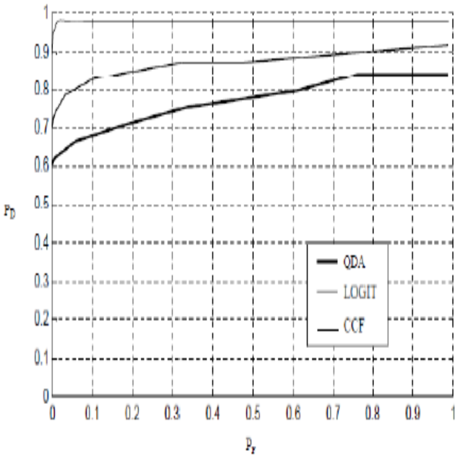


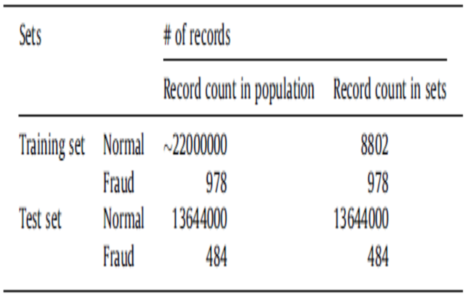
Figure 7 comparisons of credit card detection watch with the fraud detection system ROC for deposit fraud detection (Ogwueleka 2011)

The experiment results prove that indeed this model is efficient and reliable. Its performance of detecting 95% of fraud cases shows that it is suitable for solving credit card fraud. The model uses four clusters unlike other models which uses 2 clusters which are normally used and has bad performance. For the performance of the model to be increased, the author should consider the use of back propagation technique of neural networks which when fraud is detected the system will send back the transaction for the patterns to be updated. This will help in fast and reliable pattern updates and to help the model deal with different feature types and detect the errors in large amount of transaction of credit card system.

2.3 Decision Trees

A decision tree is a technique where nodes are given names of the attributes and branches given attributes values that fulfil certain condition and 'leaves' that contain an intensity factor which is defined as the ratio of the number of transactions that satisfy these condition(s) over the total number of legitimate transaction in the behaviour (Delamaire et al, 2009). When the decision tree starts there has to be a question which has more than two answers. Every answer points to more questions to help with the classification and identifying the data so it can be grouped and a prediction can be made.

Sahin et al. (2013) proposed a fraud detection model called cost-sensitive decision tree. The main aim of this model is to minimize misclassification cost, thus making the model highly accurate. This will recover large amount of financial loses and increase customer loyalty. To test the approach the credit card data from the bank's credit card data warehouse was used. This data was used to form training dataset used in the modelling of the technique and the test dataset which is involved in the testing of trained models. 978 of fraud transactions and 22 million of legitimate transactions made the sample dataset, which was then sampled using stratified sampling to reduce the number of legitimate transactions until the number reached 11344000 left with 484 of the transactions being fraud transactions (Sahin et al. 2013). The table below shows distribution of the training and test dataset.



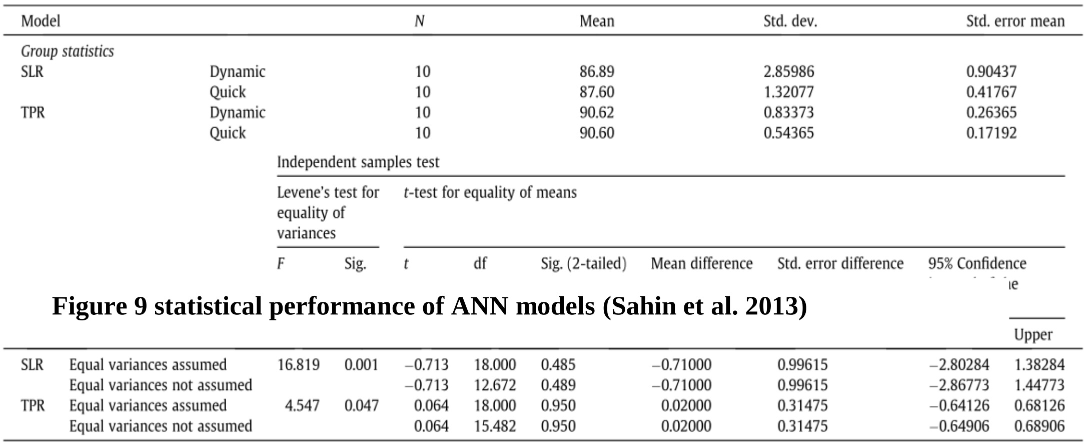
Sets		# of records	
		Record count in population	Record count in sets
Training set	Normal	~22000000	8802
	Fraud	978	978
Test set	Normal	13644000	13644000
	Fraud	484	484

Figure 8 Distribution of the training and test data (Sahin et al. 2013)

In other decision tree algorithms, the splitting criteria can be insensitive to cost and class distributions or the cost is fixed to a constant ratio in a way that classifying fraudulent transactions as legitimate (that is false negative) is "n" multiplied by the cost of legitimate classification transactions as fraudulent (that is false positive). These misclassification algorithms are considered when pruning takes place, not the induction process. In this new approach fraud will be classified looking at how much it will cost, that is the fraudulent transaction with the highest cost will be detected first then the ones with the small cost will follow. The performance of this model together with the other models is compared over test data which is done over saved loss rate (SLR). Saved loss rate depicts the saved percentage of the possible financial loss.
The models that prove to be the best in this experiment among ones developed using the same method but using different parameters is compared with other method developed with the

cost sensitive decision tree algorithm proposed. Six models that were developed using traditional decision tree algorithm were chosen and applied in SPSS PASW modeller. The chosen models were developed using C5.0, CART, CHAID and CHAID with a fixed cost ratio of 5-1, Exhaustive CHAID and Exhaustive CHAID with a cost of ratio 5-1.

The table below shows the performance of all the chosen models.

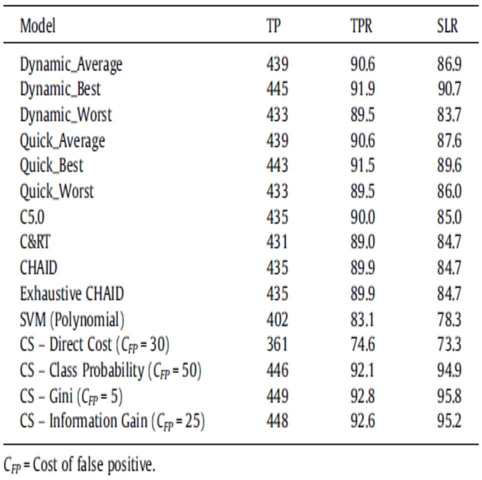


Model		*N*	Mean	Std. dev.	Std. error mean
Group statistics					
SLR	Dynamic	10	86.89	2.85986	0.90437
	Quick	10	87.60	1.32077	0.41767
TPR	Dynamic	10	90.62	0.83373	0.26365
	Quick	10	90.60	0.54365	0.17192

Independent samples test

		Levene's test for equality of variances		*t*-test for equality of means						
		F	Sig.	*t*	df	Sig. (2-tailed)	Mean difference	Std. error difference	95% Confidence	
										Upper
SLR	Equal variances assumed	16.819	0.001	−0.713	18.000	0.485	−0.71000	0.99615	−2.80284	1.38284
	Equal variances not assumed			−0.713	12.672	0.489	−0.71000	0.99615	−2.86773	1.44773
TPR	Equal variances assumed	4.547	0.047	0.064	18.000	0.950	0.02000	0.31475	−0.64126	0.68126
	Equal variances not assumed			0.064	15.482	0.950	0.02000	0.31475	−0.64906	0.68906

Figure 9 statistical performance of ANN models (Sahin et al. 2013)



Model	TP	TPR	SLR
Dynamic_Average	439	90.6	86.9
Dynamic_Best	445	91.9	90.7
Dynamic_Worst	433	89.5	83.7
Quick_Average	439	90.6	87.6
Quick_Best	443	91.5	89.6
Quick_Worst	433	89.5	86.0
C5.0	435	90.0	85.0
C&RT	431	89.0	84.7
CHAID	435	89.9	84.7
Exhaustive CHAID	435	89.9	84.7
SVM (Polynomial)	402	83.1	78.3
CS – Direct Cost (C_{FP} = 30)	361	74.6	73.3
CS – Class Probability (C_{FP} = 50)	446	92.1	94.9
CS – Gini (C_{FP} = 5)	449	92.8	95.8
CS – Information Gain (C_{FP} = 25)	448	92.6	95.2

C_{FP} = Cost of false positive.

Figure 10 performance table (Sahin et al. 2013)

Figure 11 and 12 shows the performance of cost sensitive tree models and other models. The figures prove that the cost sensitive decision tree models excluding CS-Direct Cost have saved more resources than others. Mostly banks are more concerned with the overall financial loss or how to recover than the fraudulent transactions detected. This new proposed method will help the financial institutions in recovering the money lost due to fraud. Also the cost sensitive models work well than traditional classifiers in terms of the number of detected false transactions. The decision trees are a good initiative because they keep pruning themselves to remove the data that reflects noisy data. They remove this kind of data from the tree to prevent a situation where the tree becomes large and complex with features that are not important. Also the decision trees automatically create knowledge from data and can discover new knowledge. Most systems do not implement decision trees because they cannot deal with contradictory examples. Also because tree can become large and difficult to understand, this makes it difficult for the developers to use this technique that is why the technique is not widely used.

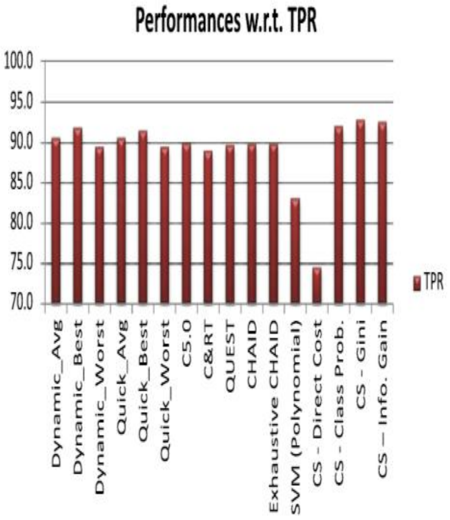


Figure 11 Performance of models w.r.t. True Positive Rate (TPR) (Sahin et al. 2013)

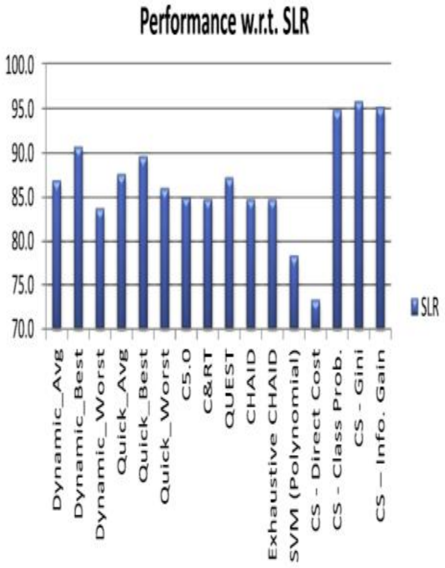


Figure 12 Performances of models w.r.t. Saved Loss Rate (SLR) (Sahin et al. 2013)

3 Lessons Learnt

Data mining techniques has been proved to be efficient and effective in the field of credit card fraud detection. With the techniques explored in this paper, the results of the experiments carried out have proven beyond unreasonable doubt that indeed data mining techniques can be applied in this field. And also it can help solve this problem of credit card fraud. The models that have been developed using data mining techniques have capability of updating its patterns whenever a change occurs in the transactions database. Also the models developed using data mining techniques detect fraud in real time. Real time models detect fraud at the time of the transaction that is that time when the transaction takes place. Unlike models which detect fraudulent transactions after they happen. These models are able to stop the transaction process when they think it is fraudulent and 95% of the time, the models are correct.

4 Conclusions

The use of data mining techniques for detecting credit card fraud brings in models of better performance. The models that were discussed in this paper are good enough to be used to stop credit card fraud because many banks around the world are losing a lot of money due to this fraud. And its every bank’s wish to have an effective and efficient credit card fraud detection system (Raj & Portia 2011). The proposed models uses the real data from the banks’ databases to test their models which proves that if they can be given a chance they can reduce fraud because they have proven to be working in with the same everyday transaction data of card holders. Most of these models runs in the background of the bank system therefore it does not introduce anything new to the customer, nor does it interfere with their purchasing and paying of the goods and services. In short the customers will hardly know it even exist because it will be hidden from users. Some techniques like neural networks are able to find fraudulent transactions then update the database by so doing it updates the patterns of the network.

References

Akhilomen, J.,, 2013, ‘Data Mining Application for Cyber Credit-card Fraud Detection System.’ In *Proceedings of the World Congress on Engineering 2013*. London, UK 3-5 July 2013.

Chaudhary, K., Mallick, B. & Noida, G., 2012, ‘Credit Card Fraud : The study of its impact and detection techniques.’ *International Journal of Computer Science and Network*, 1(4), pp.2–6.

Delamaire L., Abdou H., Pointon J., 2009, ‘Credit card fraud and detection techniques : a review.’ *Banks and Banks Syatems* , 4(2), pp. 57-68.

Dheepa, V. & Dhanapal, R., 2009, ‘Analysis of Credit Card Fraud Detection Methods.’ *International Journal of Recent Trends in Engineering* , 2(3), pp.126–128.

Dobbie, G., Riddle, P. & Naeem, M.A., 2010, ‘A Swarm Intelligence Based Clustering Approach for Outlier Detection.’ *IEEE*,.

Ganji, V.R., 2012, ‘Credit card fraud detection using anti-k nearest neighbor algorithm.’ *International Journal on Computer Science and Engineering*, 4(06), pp.1035–1039.

Günther, F. & Fritsch, S., 2010, ‘Neuralnet : Training of Neural Networks.’ *Contributed Research Articles*, 2(1), pp.30–38.

Modi, H., Lakhani S ., Patel N., Patel V., 2013, ‘Fraud Detection in Credit Card System Using Web Mining.’ *International Journal of Innovative Research in Computer and Communication Engineering*, 1(2), pp.175–179.

Ogwueleka, F.N., 2011, ‘Data Mining Application In Credit Card Fraud Detection System.’ *Journal of Engineering Science and Technology*, 6(3), pp.311–322.

Raj, S.B.E. & Portia, A.A., 2011, ‘Analysis on Credit Card Fraud Detection Methods.’ In *International Conference on Computer, Communication and Electrical Technology March 2011*. pp.152–156.

Sahin, Y., Bulkan, S. & Duman, E., 2013, ‘A cost-sensitive decision tree approach for fraud detection.’ *Expert systems with Applications*, 40(15), pp.5916–5923.

Sherly, K.K., 2012, ‘A Comparative Assessment of Supervised Data Mining Techniques for Fraud Prevention.’ *International Journal of Science and Technology Research*,1, pp.1–6.

An Analysis Of Current Research On Load Balancing In Mobile Ad-Hoc Networks

Luther Mosung

Abstract

Load balancing is a very huge problem in mobile Ad Hoc networks due to traffic congestion and routing in its wireless infrastructure. This paper provides critical review of current research on mobile Ad Hoc networks (MANETs) and looks at the various means employed in order to better its Quality of Service. Experiments and results carried out by the authors are considered, and it has shown that the factors that lead to load balancing issues are mostly due to the wireless orientation of the infrastructure which in turn causes load congestion. Routing has emerged as the key component of these problems and all other factors follow suite. This paper draws a conclusion by looking at the strength and weaknesses of the proposed methodologies employed and at the end of it all draws a conclusion as to what method would work best in mobile Ad Hoc networks.

Keywords-Adhoc;loadbalancing;QoS;MANET

1 Introduction

The past couple of years have seen a significant influx in the use of mobile devices from phones to PDA's to tablets. All these devices can and use the Mobile Ad Hoc Networks (MANET) for data sharing, pervasive internet access and distribution (Huang et al., 2010). Hence it has been a hot topic of contention in the computing and technological fraternity. Meghanathan and Milton (2009) define a mobile Ad Hoc network (MANET) as, "A dynamic distributed system of wireless nodes that move independently and arbitrarily". Therefore MANET's nodes move randomly and not only act as nodes of end devices but also has the functionality of a router incorporated as it directs some data to its intended destination. These nodes have limited functionality necessary for communication such as battery power, bandwidth and buffer space to mention but a few. It is such limitations in MANETs that makes it necessary for traffic to be distributed in the right manner between the hosts. Otherwise if the hosts are to be heavily loaded there may be bottlenecks which will lead to delays, delays; which may lead to over usage of power, which will eventually lead to session failure. Hence the emergence of load balancing

has been a very imperative tool necessary for the betterment of MANETs and their services. Load balancing is critical as it will minimize network over flooding, hence realize reduced packet delays, maximized node lifespan and sensible energy consumption.

Research indicates that there has been some previous works fixated on load balancing in mobile Ad Hoc networks. Goel, Sangwan and Jangra (2012), Tran and Kim (2013) and Yamamoto, Miyoshi and Tanaka (2012) propose methods by which mobile Ad Hoc networks can be improved. The methods proposed here are mostly protocols as they are the key for insuring efficient communication from one node to the other. Routing protocols can be either single or multi path protocols. Research claims that the routing protocols used in MANETs are mostly single path (M et al., 2012).However the methods proposed by the three fore mentioned research, proposes multipath routing protocol in order to improve consistency and robustness. As compared to the latter, single path routing can easily break the intended routes due to the constant movement of nodes and inconsistent link states. This is likely to cause network transmission errors. Single path routing takes a prolonged period of time to recuperate and re-trace the lost routes. Therefore in order to surpass these shortcomings, methods that learn multipath routes between the source and the destination have been sort.

2 Evaluation and Analysis

Load balancing which in one way or the other intertwined with routing seems to be the core element necessary for efficient MANETs. Researchers Yong and Ko (2010) have suggested a routing metric which is aware of load and based on traffic loads computed from the MAC layer and in joint forces with airtime link cost metric. This research claims that incorporation of a load balancing capability link cost calculation matric and the traffic conscious routing could be a stepping stone in delivering consistent, effective and robust communication in MANETs. As a way of capitalizing and maximizing the network capability the research also incorporated the metric into a multi-hop routing protocol (Yong and Ko, 2010). This just goes to show the great significance that multipath routing can bring to a network.

Another researcher, Akyol (2008) has studied the seatbacks of incorporating both the traffic control and scheduling in MANETs such that the link queues remain attached together and the flow rates received from there fulfils a related network utility boosting problem.

It shows how wireless networks really are bandwidth constricted hence the constant need to try to maximize the situation, while at the same time insuring the full performance of individual nodes and the network as a whole. This is so as an unbalanced use of bandwidth by the nodes may lead to bottlenecks and eventual over-flooding of the network which will bring about redundant packet retransmissions. An imbalance in node bandwidth can also bring about nodal inequality difficulties leading to discouraged routing efforts. This is why Zhi and Jun (2010) argues that the most ideal protocol to use in mobile infrastructureless networks is shortest path routing as they are energy efficient and use resources sparingly hence poses the general routing competence.

On the other hand researchers Yin and Lin (2005), propose a Prediction based Adaptive Load Balancing (PALB) mechanism. They claim that this mechanism is dependent upon forecasting network congestion and like most of the fore mentioned tools or methods, its dependent on multipath routing. The mandate of the PALB once deployed into the network is that of finding the root node and then dispensing its packets along numerous separate routes on the basis of traffic forecast, all in a quest to lower network congestion and load disparity. The root node sporadically forecast the cross-traffic of each node in the multi-hop routes and alter congestion distribution across the multiple separate routes. A traffic pattern is required, in order to predict traffic accurately. Fortunately for these researchers they had an Ad Hoc network test bed, hence collected traffic data and they evaluated it and found out that it is self-similar. Therefore with their findings they proposed a wavelet analysis based traffic forecaster for the forecasting of mobile ad hoc network traffic. Yin goes on to define wavelet analysis as, “A powerful tool for the treatment of non-stationary stochastic time series signals”.

At the end of it one would realize that this research is mostly just dependent on the wavelet and it is the one that brings originality of the PALB mechanism as it is the one that predicts traffic at the end of the day, and it is the key and only mechanism that makes PALB be what it is. Its mandate as already stipulated is to determine the route path having analyzed the network traffic and it is incorporated in a multipath protocol. So this mechanism is not limited to, but can also be incorporated into other multipath routing protocols and architectures like that suggested by Huang, Lee and Tseng (2010) as this would bridge its gap on load balancing and its overall mobile Ad Hoc QoS which seems to be mainly successful and concentrated to internet access capability but neglect the traffic that comes with it. The use of only this mechanism by Yin to Huang’s proposed model would however be adequate.

This researcher Huang (2010) is focused on two-tier architecture and the fundamental bone of contention in this setup is the maximization of efficient bandwidth consumption provided by the high-tier gateway. First and fore most these upper tier links which are delivered by the cellular networks have much limited bandwidth as matched to the lower ones. Second, the upper tier is one way or the other duty bound to serve the lower tier hosts, and it is such traffic overflow that can easily congest the higher tier. This is a clear indication that it is imperative for load balance routing to be employed so as that the host could share the gateways. Factors such as the mobility of hosts which may constantly change the hosts of a gateway as well as the heterogeneity of the gateways have to be took into consideration hence suggestion would be to outsource a suitable model from the existing as earlier stated, or in-house development like Yamamoto, Miyoshi and Tanaka (2012) who were not so happy with the load balancing in the 'conventional' methods hence proposed his traffic aware method based on transmission control and neighbor terminals monitored.

The figure below shows sample two-tier architecture.

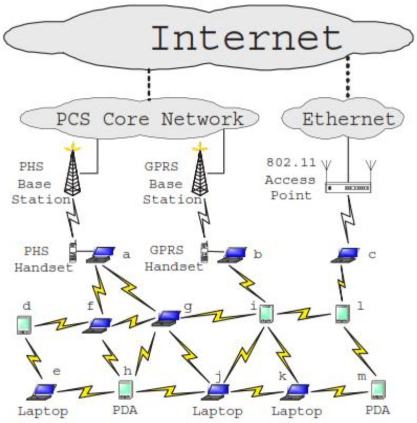


Figure 6: An example of the two-tier heterogeneous mobile ad hoc network architecture. (Huang, Lee and Tseng, 2010)

The suggested architecture is described in Figure 1 above. The higher tier interfaces are said to be heterogeneous as they can be a combination of various handsets e.g. GPRS and PHS or IEEE's 802.11, all these have various latency and bandwidth capabilities. Very few researchers consider the amount of energy that these backup multipath routes use. The researchers mostly seem to be concerned about the instant evident benefits. Vassileva and Barcelo-Arroyo (2012) is one of the very few who stipulate that it is such activities that catalases the spread of residual energy in the network. Vassileva provides a strong claim that none of the proposed load balancing routing protocols provides an energy saving matrices incorporated in it, and goes on to suggest that such a metrics would however work optimally in single path routing.

Huang (2010) analyzed the validity of his proposed load balancing method. The aim of the proposed two-tier architecture is to reduce route congestion and better route determination they propose two load balancing schemes with which they can try employ in order to archive a lower LBI. These schemes include the shortest path (SP) and Minimum Load Index (MLI). And the overall simulation results carried out under the same state shown in the figure below indicate that MLI has better load balancing capability than SP.

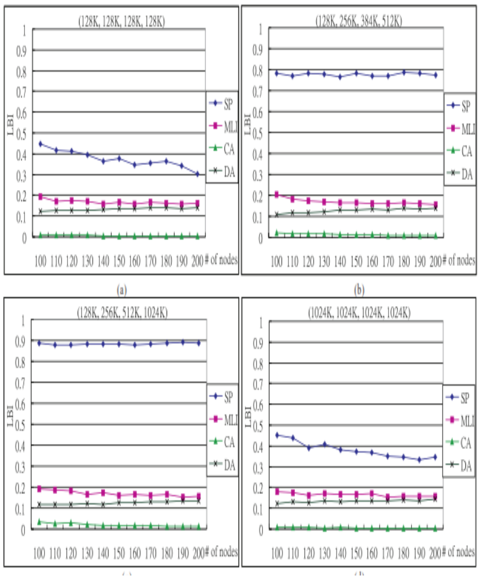


Figure 7: LBI vs number of hosts under a regular deployment of gateways, where gateway's capabilities are (a) (128k, 128k, 128k), (b) (128k, 256k, 384k, 512k), (c) (128k, 256k, 512k, 1024k), and (d) (1024k, 1024k, 1024k, 1024k) (Tran and Kim, 2013)

Most if not all literature derived from research has went to indicate that mobile Ad Hoc networks (MANETs) are independent unconnected networks. However it is in their paper that Huang (2010) and company brought a different broader perspective to MANETs, by extending these networks and combining them to higher tiers that connect them to sophisticated networks which increases the communication distance as compared to the standard IEEE 802.11. This therefore positively impacted in ad hoc network Internet access ability. However the means employed are not convincing enough therefore still stand to believe that there is a much better routing protocol which can be employed to perform even much better than the Minimum Load Index which proved robust than Shortest Path protocol. This believe due to the many and strictly sensitive rules that the MLI is ran under.

On the other hand, the literature that never fails reveled that there has been a newly formed routing protocol called Multipath-Based Reliable Routing Protocol (MRFR). It is a real time data transmission protocol for MANETs which Tran and Kim (2013) seems to be very confident with and guarantees it to be very reliable. Giving it the attention it required revealed that despite its reliable dependability it has a flaw when it comes to load balancing, which ends up leading to bottlenecks. The research argues that these load balance incapability of the MRFR protocol are brought about by the fact that it cannot compute the load balancing ratio. Tran and Kim hence decided to upgrade this real time routing protocol to incorporate the load balancing capability and termed it Real Time Load Balancing (RTLB) protocol.

Below are figures 3-6 showing the evaluation of the proposed RTLB against the fairly good AODV and MRFR routing protocols. They have all been sourced from Tran and Kim (2013) and were carried out using the Qualnet simulator.

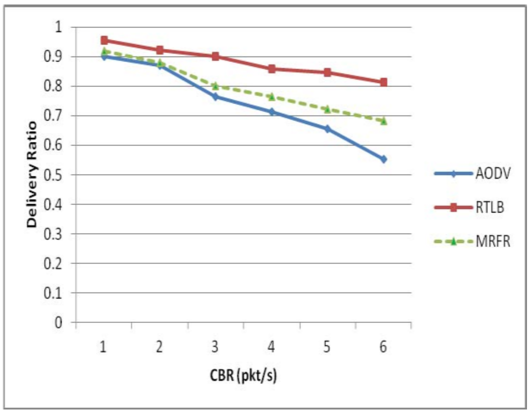


Figure 8: Packet Delivery Ratio

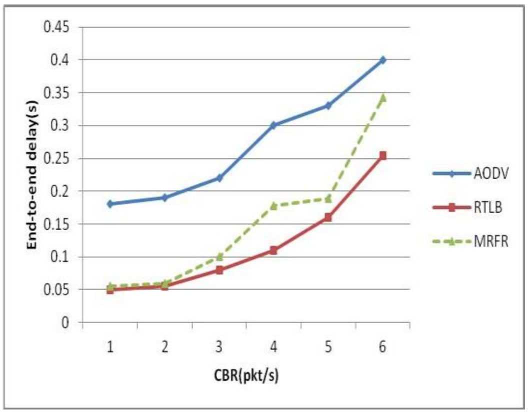


Figure 9: Average End to End delay

The first figure shows the packet delivery ratio and the second one shows the average end to end delay at various data packet rates. The RTLB protocol proves to be having an upper hand as it gets a high delivery ratio of about 90% of packets per second followed by the MRFR and AODV respectively. Even as the data rate increases the RTLB still remains prominent. In figure 4 even as the data rate increases RTLB still manages to make end-to-end delivery in the lowest time than its other two counterparts which is very commendable considering the fact that it is being paired against major methods which are trusted and employed with believe to be good (Parichehreh, Javadi and Hahgighat, 2010).

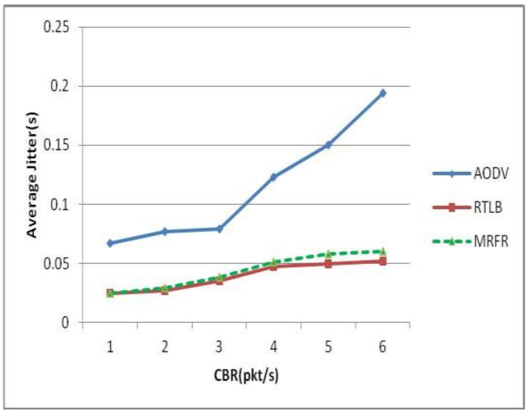


Figure 5: Jitter Load Balancing

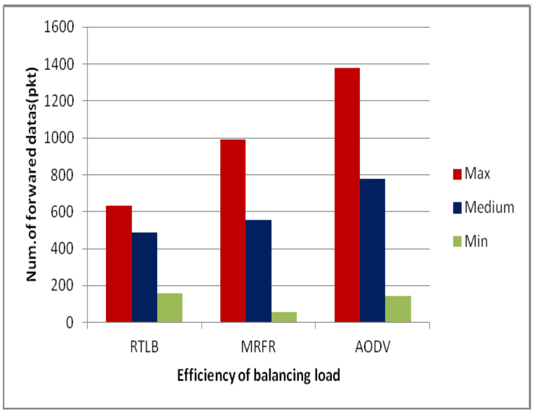


Figure 6: Average Efficiency

Figure 5 shows the average rate at which the protocols jitters. RTLB continues to show its robustness and dominace over the counterpart protocols as it shows a very little difference in jitters average despite reaching the peak data rate. Figure 6 evaluates the load balancing capabilities of the three stipulated protocols being tested here; RTLB, MRFR and AODV against number of data forwarded being the energy consumed, so they used the assumption that the more the data forwarded the more the energy consumption. Even though RTLB still ‘obviously’ forwards data, but the fact that they considered the energy consumption point which was earlier raised by Vassileva (2012) of lack of conventional methods to address energy issues, Parichehreh and RTLB sure did prove otherwise here, because the more the effort to transmit and forward less data the more the device energy is saved and the less the residual energy dispersed within the network. The last constraint is that the protocols are tested against various categories of data packets forwarded being; maximum, medium and minimum. However RTLB seems to have delivered in the least amounts of energy overall, and this is brought about by the fact the load in the network is now balanced. Having analyzed the results presented by Tran’s research one can comply that the proposed RTLB protocol has better load balancing and communication capability than MRLR from which it was developed through upgrading and AODV which is common to MANETs.

Analysis of these research methodologies show that some methodologies can complement each other, for instance the routing matric proposed by Yong and Ko (2010) can be well incorporated into a multi-hop method. Despite that most research call for multi route protocols as the ultimate route to the elimination of load congestion problems, it is interesting to get advocates for shortest path routing such as Zhi and Jun (2010) who give a different perspective even though their case is really not nullified by research such as that of Huang (2010) who proves beyond doubt that for the sake of range and accessibility shortest path is not the solution. Even though a larger part of his case is valid Huang too has his own shortcoming in utilizing modern technological advancements to catapult the ability of his model. Yin and Lin (2005) too provided a mechanism expected to could have brought about change by means of forecasting the traffic, commendable as it is, substantial testing and evidence of this tool was not advanced as compared to arguments by Tran and Kim (2013) who really put their proposal to scrutiny, that they identified its shortcoming addressed it, experimented and provided simulation of their model performance in a real environment setup against already well-established prominent methods. Therefore this particular methodology provided by Yin and Kim can be thee ideal solution thus far, with addition of few traffic smart mechanism like the cache and traffic matrices (Parichehreh, Javadi and Hahgighat, 2010) (Yong and Ko, 2010).

3 Conclusions

The wide spectrum of problems in mobile ad hoc networks that lead to load balancing issues have been identified above. A critical review and comparison of literature has revealed the various methodologies employed that try mitigate these issues. It has shown that the factors that lead to load balancing issues are mostly due to the wireless orientation of the infrastructure which in turn causes traffic congestion. Of all the balancing problems routing has emerged as the key component, and everything else follow suite on after it which is why a lot of research is focused more on it because after all there is no communication that can happen without it. Multipath routing has also proved prominent even though they all propose different platform and overall internal orientation. Recommendation therefore can be to use such type of multi hop routing and incorporate all the other essential features such as cache consistency, route monitoring and energy awareness within it to improve MANET robustness and efficiency at a go. This can be achieved by anyone with the passion for the realization of high performing load balanced mobile Ad Hoc networks.

References

Akyol, U., Hobby, J., Andrews, M., Saniee, I., Gupta, P. and Stolyar, A., 2008, 'Joint Scheduling and Congestion Control in Mobile Ad-Hoc Networks', *In procedings of IEEE 27th Conference on Computer Communications*, vol. ii, pp. 13 -18.

Goel, N., Sangwan, S. and Jangra, A., 2012, 'Efficient Weighted innovative Routing Protocol (EWIRP) to Balance Load in Mobile Ad Hoc Networks (MANETs)', *IEEE-International Conference On Advances In Engineering Science And Management (ICAESM-2012)*, vol. v, no. 27, March, p. 278.

Huang, Y., Cao, J., Jin, B., Tao, X., Lu, J. and Feng, Y., 2010, 'Flexible Cache Consistency Maintenance over Wireless Ad Hoc Networks', 1150 *IEEE Transactions on Parallel and Distributed Systems*, Vol. xxi, no. 8, August.

Huang, C., Lee, H. and Tseng, Y.-C., 2010, 'A Two-Tier Heterogeneous mobile Ad Hoc Network Architecture and Its Load-Balance Routing Problem', *IEEE*, pp. 2-5.

Meghanathan, N. and Milton, L.C., 2009, 'A Simulation Based Performance Comparison Study Of Stability-Based Routing, Power-Aware Routing and Load-Balancing On-Demand Routing Protocols for Mobile Ad hoc Networks', *IEEE*, vol. i, pp. 2-4.

M, A., G, S., A, S. and A, V., 2012, 'Congestion Adaptive Multipath Routing For Load Balancing In Adhoc Networks', 2012 *International Conference in Information Technology (IIT)*, vol. v, no. 22, pp. 305-400.

Parichehreh, A., Javadi, B. and Hahgighat, A.T., 2010, 'Traffic Reduction in Hybrid Service Discovery Protocol in Mobile Ad-Hoc Grid', I*EEE 2010 Second International Conference on Future Networks*, vol. iv, no. 12, pp. 433-437.

Tran, A.T. and Kim, M.K., 2013, 'A real-time communication protocol considering load balancing in Ad hoc Network', *IEEE*, vol. iii, no. 12, pp. 6-7.

Vassileva, N. and Barcelo-Arroyo, F., 2012, 'A Survey of Routing Protocols for Energy Constrained Ad Hoc Wireless Networks', *IEEE*, vol. ii, no. 13, October, pp. 2-6.

An Evaluation of Current Software Piracy Prevention Techniques

Ogbeide-ihama Osagie

Abstract

Software piracy is a major issue in the software development community. This research paper is aimed at analyzing and critically evaluating current research that has being conducted on techniques used for preventing software piracy, at the end of the evaluation a conclusion will be drawn with reasoned arguments of findings and evidence as to why the conclusion was reached and a more effective technique is proposed to prevent software piracy.

1 Introduction

Software development industries have contributed immensely to the worlds growing technology and economy with the vast number of software applications that is being produced to solve diverse problems in the real world. Unfortunately these industries are faced with a huge challenge which is the increase in software theft that goes beyond control. This issue has become a major concern and as such much research has been carried out on techniques to mitigate software piracy present in the software development community.

Ajay et. al. (2012) shows that SMS gateway is one of the techniques that can be used to mitigate software piracy where the authenticity of a software are been checked at fixed time intervals.
However Mohab and Mohamed (2011) acknowledged the fact that there is need for a more accurate technique for software protection against software theft and as such proposed a piracy prevention technique based on the combination of two software protection techniques which are protection based on smart token and internet activation server which uses the PKCS standards. Also a method based on fingerprint technology was proposed to prevent software piracy (Dinghua He, 2012; Cheng et. al. 2009).

Although Yasir et al. (2009) looks at the birthmark software piracy prevention technique and focused its attention on the angle of a static software method that is being used to identify software theft. The research goes further to give some features of the technique which is the ability of the software not being easy to modify and its simplicity in terms of validation.

Vineet et al. (2010) examined the loopholes in existing techniques and technical drawbacks linked with some of the techniques used to prevent software piracy, the paper further presents a new scheme for prevention of software piracy and the proposed scheme combines smart cards and serial keys which are then used as a mechanism to prevent software piracy. The run once technique was introduced by Yuvaraj et. al. (2011) this technique uses the curbing thumb drive to distribute software to legitimate owners.

This paper would review some current research on piracy prevention techniques available and critically evaluate them, at the end will come up with a conclusion as to which method is more effective to use.

2 Watermarking Based on Staganography

Cheol and Yookun (2012) carried out a research on software watermarking and then proposed a watermarking scheme; this scheme is a combination of steganography and error –correction. In their scheme a watermark is embedded into a program with methods of steganography. An experiment was conducted to demonstrate the reliability of the proposed scheme where they created a Watermark and called it W using a theorem known as the Chinese reminder, W was converted to a collection of values that will be embedded into the program (Cheol and Yookun 2012).

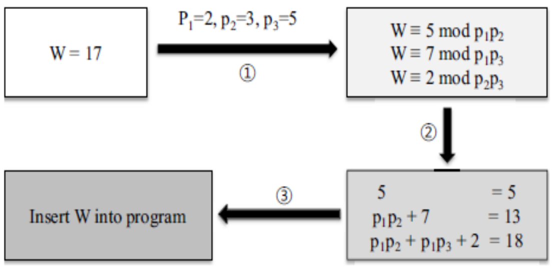

W = 17
P_1=2, p_2=3, p_3=5
①
$W \equiv 5 \bmod p_1p_2$
$W \equiv 7 \bmod p_1p_3$
$W \equiv 2 \bmod p_2p_3$
②
5 = 5
$p_1p_2 + 7$ = 13
$p_1p_2 + p_1p_3 + 2$ = 18
③
Insert W into program

Figure 1. This diagram displays the process involved in creating the watermark (Cheol and Yookun 2012).

The experiment by Cheol and Yookun (2012) was conducted on Ubuntu 11.04 operating system. A watermark was embedded into Bzip2 1.0.6, Gzip 1.2.4 and Lzop 1.03, these compression utilities are the most highly used in the Linux, Unix platform. The time of execution was measured for the three program with the watermark inserted in it and the program without the watermark in it.

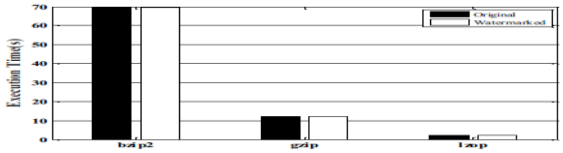


Figure 2. Shows the difference in execution time of the original program and the program after inserting the watermark (Cheol and Yookun 2012).

Also experiment was done to compare the size of the original program and the program with the watermark, they discovered that the program with the watermark inserted is almost the same size as the original program (Cheol and Yookun 2012).

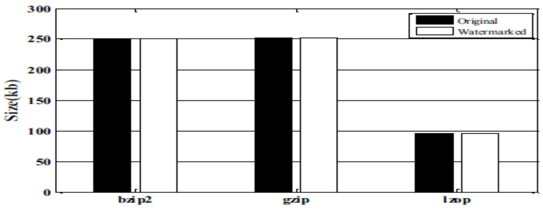


Figure 3. shows the watermark size (Cheol and Yookun 2012).

The last experiment carried out by Cheol and Yookun (2012) tested the error-correction making use of the Chinese remainder theorem, it was tested against code-optimization methods to check how effective the watermark resilience is.

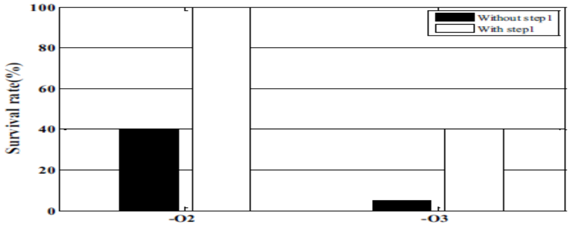


Figure 4. This diagram shows the survival rates of the watermark (Cheol and Yookun 2012).

Based on the experimental results presented above, Cheol and Yookun (2012) reached a conclusion that their watermark scheme is easier to implement as it does not involve complex code, they also claimed that their watermark scheme does not have an effect on the size of the program and its performance, they also acknowledged the fact that more development is needed to improve the watermark scheme, it also claims that the watermark scheme proposed increases resilience and that it is only limited to specific types system architecture.

The experiment conducted in this research is well detailed and focused on the aim of their research which is to achieve watermark scheme that defeats semantic-preserving for code transformation, the experiment proved that the scheme is resilient, however the watermark embedment process was controlled as it was tested on a specific version of Ubuntu operating system, The experiment conducted is repeatable as the data and files used were presented in detailed format and well laid down steps, the authors demonstrated a sense of comparison as they compared the time of execution and size of the program with the watermark inserted in it and the one without the watermark. After critically evaluating the research it confirms that the watermark scheme is resilient to code optimization attacks because the watermark is separated from the code and the steganography used hides the watermark.

3 Zero-Watermarking Obfuscation Method

Guangxing and Guangli (2012) proposed a Zero-watermark algorithm to prevent software piracy, their method is a combination of code obfuscation and software watermarking and they pointed that this method would not alter the information of the software as the watermark will be embedded into the program using code obfuscation without adding any other extra code to the program.

Experiments were conducted to test the ability of the watermarking algorithm against attacks, in their experiments the watermarking algorithm proposed was compared with stem algorithm, adding expression, adding pseudo-switch

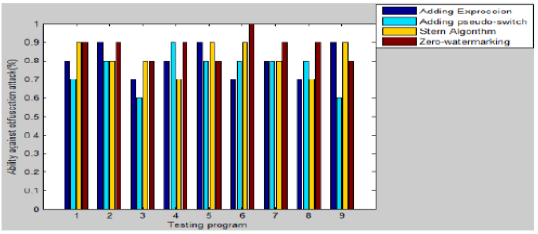
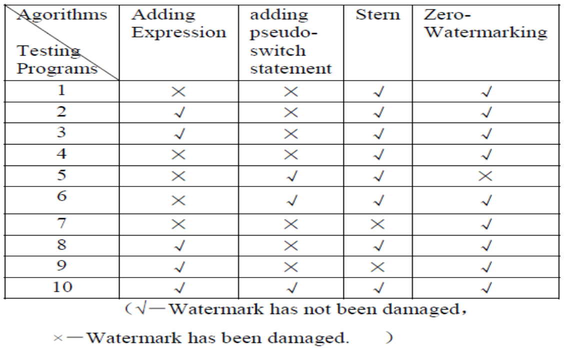


Figure 5. Shows the result of the result of obfuscation attack (Guangxing and Guangli 2012).

The results of the obfuscation attack shows that zero watermarking has more advantage over the other algorithms and it is similar to Stem. They conducted a two step hack to be sure of the results, both steps of the test involved ten programs with watermark embedded in them, the programs were used to carry out the test against code obfuscation attack, also the programs were checked after the attack to know if the watermark was damaged. A second test was conducted with the same number of programs which was used in the previous test but this time the instructions embedded into the testing program where randomly selected.



Agorithms / Testing Programs	Adding Expression	adding pseudo-switch statement	Stern	Zero-Watermarking
1	×	×	√	√
2	√	×	√	√
3	√	×	√	√
4	×	×	√	√
5	×	√	√	×
6	×	√	√	√
7	×	×	×	√
8	√	×	√	√
9	√	×	×	√
10	√	√	√	√

（√—Watermark has not been damaged，

×—Watermark has been damaged.　）

Table 1. Displays the result of the code attack (Guangxing and Guangli 2012).

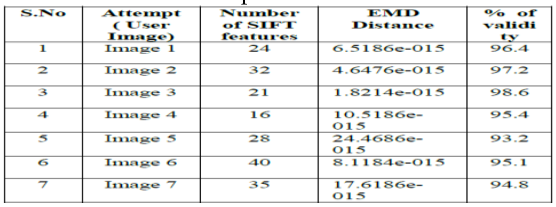
From the result presented above it shows zero-watermarking based on obfuscation can resist code attacks because in the obfuscation based watermark presented, the information of the watermark is hidden in the obfuscation process, doing so makes it difficult for reverse engineering to take place and the security of the watermark is increased.

Guangxing and Guangli (2012) stress that it is possible for a software watermark to loss its function, if it is destroyed by the software pirate, their claims were that the Zero-watermark approach that was proposed will be able to improve the performance of the security of the software to an extent, however they pointed that combining watermarks and obfuscation is a more secure method for protecting the information of the watermark, making it impossible for reverse engineering to place.

To justify their claims experiments were conducted and the proposed method was compared in a hack test with three other algorithms, namely; Adding Expression, Adding Pseudo-switch Statements and Stem which the authors pointed that their method was similar to. However after evaluating the experiments conducted and the results presented, the findings obtained was that the zero-watermark algorithm survived the code obfuscation attack while the other algorithms where not able to withstand the attack as the watermark embedded in them was destroyed by the attack, the experiments exhibited a feature of repeatability as the experiment was repeated with the same number of programs and the same algorithms, a sense of randomness was also demonstrated as the instructions embedded in the second set of programs that was tested was randomly selected, this showed that the experiment was free from bias.

4 SIFT and Earth Movers Distance Algorithm

Srinivas et. al (2012**)** proposed a software piracy prevention technique that is based on image matching and feature extraction, using the SIFT(Scale Invariant Feature Transform) and the earth movers distance(EMD) algorithm, in their method an image of the software buyer is collected, features will be extracted from the image collected with SIFT and it will then be stored in the database, the software is integrated with an activation tool that will be used to validate and activate the software at the user end, during the activation process of the software the user will be asked to submit a copy of his or her image which he or she had submitted earlier when buying the software to the activation server, properties of the users system will also be collected by the activation tool, the image will then be compared with the users image that was stored in the database, this is done using the Earth Mover Distance algorithm, if the two images are validated and verified to be a matching pairs, the servers generates a unique key of size 2Mb based on the feature extracted from the image and the properties of the users system and a key that tracks the usage and activation of the software. Experiments were conducted to justify their claims that the new proposed method would mitigate software piracy, an activation process was performed with 15 software copies and 25 user submitted images which was tested on 6 separate systems, an input of 25 wrong images and 25 right images was given to the system to activate the software copies, a result of 98% activation success was achieved. The table below shows the result of the activation process:



S.No	Attempt (User Image)	Number of SIFT features	EMD Distance	% of validity
1	Image 1	24	6.5186e-015	96.4
2	Image 2	32	4.6476e-015	97.2
3	Image 3	21	1.8214e-015	98.6
4	Image 4	16	10.5186e-015	95.4
5	Image 5	28	24.4686e-015	93.2
6	Image 6	40	8.1184e-015	95.1
7	Image 7	35	17.6186e-015	94.8

Table 2. Shows the Result of the activation and comparison test conducted (Srinivas et. al. 2012**).**

However the SIFT features that was extracted from the users image are used to generate the activation key, so doing give the user a unique identifier for the users activation.

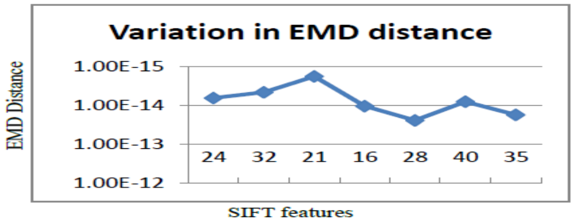


Figure 6. Shows the features points considered for generating key in the EMD (Srinivas et. al. 2012**).**

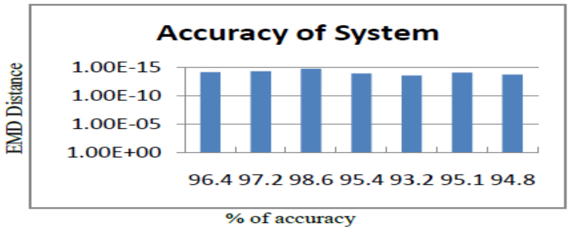
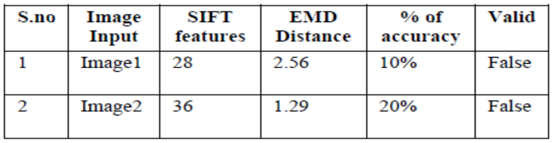


Figure 7. Shows the accuracy of the system after the test (Srinivas et. al. 2012**).**

The accuracy of the proposed system was record after the first experimental test conducted. Fig. 9 shows the result and level of accuracy attained.

To verify the system's ability to identify a fake user trying to impersonate using a morphed image of a legitimate user to attempt activation of the software product, an experiment was conducted to test if their method would activate the software based on the false image, results show that the activation process failed as the morphed image did not match the one in the database with the registered system parameters (Srinivas et. al. 2012).



S.no	Image Input	SIFT features	EMD Distance	% of accuracy	Valid
1	Image1	28	2.56	10%	False
2	Image2	36	1.29	20%	False

Table 3. Comparison between impersonated and original image (Srinivas et. al. 2012**).**

Also an experiment was carried out to check if an image that exist with a particular user and system details can be used to activate a copy of the software on a different computer, results also show that the key generation process will fail, as the image has a key that has already being generated for that image.

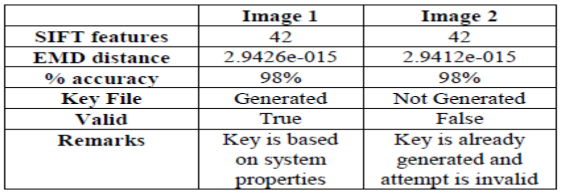


	Image 1	Image 2
SIFT features	42	42
EMD distance	2.9426e-015	2.9412e-015
% accuracy	98%	98%
Key File	Generated	Not Generated
Valid	True	False
Remarks	Key is based on system properties	Key is already generated and attempt is invalid

Table 4. Shows the result obtained after trying to use the same image to activate a different computer (Srinivas et. al. 2012**).**

The claims made by Srinivas et. al (2012) that their proposed method will prevent software piracy was justified by the series of experiments conducted and positive results obtained, the results show that the methods will mitigate software piracy, reasons for supporting their claims is that the EMD and SIFT algorithm does not allow a user to activate a particular software product on a different computer with the same image features collected at the time of the first activation as it already existed in the database and also a unique key has being generated for that user's software using the features extracted from the image and the properties collected from the user's computer that identifies the user and as such the activation server will not generate another key or activate that software copy on any other machine even if the image was stolen, falsified or the legitimate user tries to play smart by attempting a dual installation. However with the reasons presented above, their method will mitigate piracy, although further research is required to improve their method as the authors did not consider a situation where a multi system license can be purchased alongside with the software and registered with the same process as in the case of large organizations that require installation on many computers.

5 Conclusions

Different method for preventing software piracy that has being proposed by current researchers was critically evaluated in this paper. However it may be difficult, if not impossible to completely eradicate the problems posed by software pirates as many of these software pirate are well trained and informed in cracking, most of which are even very good in software programming and as such they are able to identify vulnerability in software programs and crack it with the sole aim of illegal distribution. The aim of these studies is to identify method or combination of methods that will reduce software piracy. Some intriguing and interesting piece of research on techniques for preventing software piracy was reviewed.

The research by Cheol and Yookun (2012) took a well structured approach, they also compared the size of the program before embedding their watermark and the time it took the program to execute, doing this justified their claims that the scheme was easier to implement and as the embedment had no effect on the size of the program. However Cheol and Yookun (2012) did not test the proposed scheme on other platforms before reaching the conclusion that the scheme will make reverse engineering impossible, it was only tested on a specified platform which is the Ubuntu, although they acknowledge the fact that further research needs to be done to improve the scheme, it must be stressed that the watermarking scheme should be tested on other platforms like Mac and windows and the results compared as to ascertain the efficiency of the scheme before reaching a final conclusion.

The experiments carried out by Guangxing and Guangli (2012) also exhibited a sense of comparison similar to the once expressed by Cheol and Yookun (2012), the experiment involved a hack test that compared the efficiency of their algorithm with other algorithms to ascertain if their proposed algorithm could withstand the code obfuscation attack. Unlike the experiments conducted by Guangxing and Guangli (2012) where the sizes of the zip program used in the test was known in advance, the authors exhibited randomness in the selection of the instruction that was embedded into the program in the second phase of the test, doing so eliminated bias in the choice of instructions inserted into the program. However it was clear that the experiment employed features of repeatability as they were able to repeat the test with the same number of programs and the same algorithm.

However the final method that was evaluated was the SIFT AND image matching method proposed by Srinivas et. al (2012), it was acknowledged that the structure and presentation of their method was superb, the authors gave a detailed description of the problem that was needed to be solved and went further to propose a solution, their method which is an image matching method went through series of experimental processes, they did not just theorize about the proposed method they presented valid results from well conducted experiments, for instance the test conducted to see if the proposed system will allow activation of a software with a morphed image of a legitimate user, doing so the authors showed that they considered a real life situation of a pirate attempt to outsmart their method, the results presented justifies the claims they made that the proposed image matching method will mitigate software piracy, although further research is require to solidify and improve the method because the authors did not consider a situation where a software license for multiple system is to be issued to a single user or issuing license for a large organization as the proposed method does not permit duplicate activation of a software on another computer with the same image and system properties that already exist in the database.

In final conclusion of this paper a combination of the image matching method and the zero – watermarking is presented as a superb solution that will gradually prevent software piracy. The reason for combining these two methods is that, the image matching method does not permit duplicate activation of a software product on two separate computers and as such will be difficult to successfully pirate if not totally impossible, also the zero – watermarking will withstand code obfuscation attack. However the solution proposed in this research paper will reduce software piracy.

References

Ajay Nehra, Rajkiran Meena, Deepak Sohu, and Om Prakash Rishi, 2012, ‘A Robust Approach to Prevent Software Piracy’, *Journal of Engineering and Systems,* Page 1-3.

Cheol Jeon, Yookun Cho., 2012, 'A Robust Steganography-based Software Watermarking', *Proceedings of the 2012 ACM Research in Applied Computation Symposium*, Pages 333--337.

Cheng Yang ; Lihe Zhang ; Jiayin Tian, 2009, ‘Secure Scheme of Digital Fingerprint Based Piracy Tracking’, *Computational Intelligence and Software*

Engineering, 2009. CiSE 2009. International Conference on, Pages 1- 5.

Dinghua He, 2012, ‘Remote authentication of software based on machine's fingerprint’, *Software Engineering and Service Science (ICSESS) IEEE 3rd International Conference on,* Pages 543- 546.

Guangxing and Guangli, 2012,’A Method of Soft-Ware Watermarking’, *2012 International Conference on Systems and Informatics,* pages 1791 -1795.

Mohab Usama and Mohamed Sobh, 2011, ‘Software Copy Protection and Licensing based on XrML and PKCS#11’, *Communications, Computers and Signal Processing (PacRim)*, Vol. 1, Pages 856 – 861.

Srinivas B., Dr. Koduganti Venkata, Dr. P. Suresh Varma, 2012, ‘Piracy Detection and Prevention using SIFT based on Earth Mover’s Distance (EMD)’, *International Journal of Computer Applications,* vol. 38, issue 7, Pages. 35-41.

V.K., Sharma, Rizvi, S.A.M., Hussain, S.Z. ,Chauhan, A.S., 2010, ‘Dynamic Software License Key Management Using smart cards’, *2010 International Conference on Advances in Computer Engineering’*, Pages 244 – 246.

Yasir Mahmood, Zeeshan Pervez, Sohail Sarwar and Hafiz Farooq Ahmed, 2009, ‘Method based static software birthmarks: A new approach to derogate software piracy’, *Computer, Control and Communication, 2009. IC4 2009. 2nd International Conference on,* pages 1-6.

Yuvaraj, N. ; Venkatraj, D. ; Yogesh, P., 2011, ‘piracy Curbing Drives’, ‘*Research and Innovation in Information Systems (ICRIIS), 2011 International Conference’ ,* Pages 1 – 3.

A Critical Evaluation of Server-side CSRF Attack Protection Methods

Baran Salman

Abstract

Cross Site Request Forgery (CSRF) is regarded as a widely exploited web site vulnerability that can leads to compromised accounts, stolen bank funds or sensitive information leaks. In this paper, major server-side CSRF methods were analysed and critically evaluated in terms of their protection effectiveness performance overhead results and recommendations for the problem as well as future research are made.

1. Introduction

Cross-Site Request Forgery (CSRF) also known Session Riding and Sea Surf (XSRF) is listed in the top 10 vulnerabilities of real world web applications (OWAPS,2013). Although XSS based attacks have higher occurrence rates compared to CSRF based attacks, CSRF has been gaining attention in today's internet world. One of the main factors of a XSS attack is that the attacker need to steal the victim's session cookie to exploit user's session and take control of victim's account. To deal with problems of stealing cookies, the methods have been developed and a detailed research work has produced promising results against XSS attacks (Shar,2012). To cope with those developed protection methods, hackers have had to devise techniques which does not include stealing web browser's cookie, which would be called as CSRF later. These attacks take place imitating user's identity therefore transmitted HTTP request's legitimacy can not be determined by the web servers (Barth et. al. 2008). Siddiqui and Verma (2009) stated that although it is a common vulnerability case of the current web environment, CSRF attacks are still less known to most application developers and confused with XSS attacks. Moreover, the protection methods that are in use against XSS will not protect web applications against CSRF attacks. Research carried out by Lin et. al. (2009) presented review of more than 200 form of CSRF attacks documented in National Vulnerability Database (NVD) and proposed a CSRF threat modelling for web applications to improve defencive perspective.

2. Background

The CSRF attacks utilises vulnerabilities in SOP (Same origin Policy), which is a fundamental security mechanism within web browsers. With the advent of Java script, Ajax and Web services, attackers have found ways to bypass the SOP and exploit web browsers (Saiedian and Broyle 2011). Awareness of SOP weakness has resulted in the development of NoForge method (Jovanovic et. al. 2006) that uses tokens to verify same-origin requests as a server side proxy approach instead of performing modifications on application's source code but Chen et. al. (2011) has revealed how attackers subvert an extending version of NoForge like method based tool in Java EE environments. Czekis et. al.(2013) also argues that the use of simple integrated tokenisation approach is not an efficient method to cope with CSFR attacks emphasising drawbacks of the method for incompatibly issues with GET requests, potential token extraction risk, manual implementation caused errors, poor web development platform support and language dependency.

An intensive literature view has been performed for the listed problems above and many methods have been found but only three method were chosen to be evaluated among them due to their approach to solve the problem.

3. Labelling User Created Contents

Sung et. al.(2013) has proposed a labelling mechanism method to deal with CSRF attacks aiming to decrease performance overhead and provide effective protection without restricting legitimate scripts at client side. They stated that current methods using Java script and AJAX filtering approach decrease the functionality of original script as well as reduce use of User Created Content (UCC) which is one of the key features of social network websites in Web 2.0 environment. It is also stated that a forged UCC can not be distinguished by client browsers and may results in potential CSRF attacks.

The proposed method can be analysed under two sections called labelling function and UCC quarantine policy. The idea of labelling function is to separate UCCs dividing into content owner parts, while UCC quarantine policy deploys determined rules for each labelled content. In this way, an unauthorised UCC can be averted when it attempts to access a service that might be a critical component of the system or includes sensitive information. Labelling function separates web page contents into two different types, “trusted content” is one of the labelled content types that are identified when the contents produced by a legitimate user or web server administrator. The other type of labelled content is “untrusted content” which is not created by a rightful user and the content that contains scripts might create vulnerability issues for CSRF attacks as shown in Figure 1.

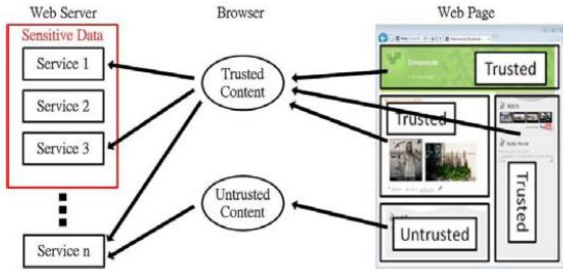


Figure 1: overview of the method
(Sung et. al. 2013)

The labelling function refers to a cookie in order to distinguish trusted UCC and untrusted UCC and also labels every HTTP request created on client side. Once a user logs into the system, a cookie provided by the web server is assigned to the client browser. The method blocks unauthorised access attempts redirecting those requests to a non-UCC web page that is POST and GET method restricted, whenever a non-labelled HTTP requests that might be a possible forged cross site requests is detected. For the untrusted content, in the server side a list of services that include private information and sensitive data is defined by server administrator as “critical services” so that blocking mechanism will be able to identify potential attacks when an untrusted HTTP request involving a critical service access is sent from the client side.

3.1 Evaluation

Sung et. al. (2013) conducted experiments to demonstrate the effectiveness of the proposed method and evaluated the produced results, dividing them into three categories: time overhead, memory use and efficiency of protection. The test was performed with a machine (2.13 GHz CPU, 1 GB RAM) and Apache 2.2 web server with PHP 5.2.12 at the server side. And client side on a machine (CPU 2.2GHz, 2GB RAM) with Firefox 3.6.3 web browser. They also integrated an uncompressed php file 8.8 KB to each tested file and used an untrusted labelled iframe including an uncompressed JavaScript file 4.4 KB files to test. To evaluate time overhead Sung et. al. (2013) used two popular social network websites, Facebook and MySpace as samples and also created modified forms of those sample pages including their proposed methods. The pages contained by a web-service at server side were browsed over one thousand times. Modified Facebook page generation overhead ranged from 1.3% to 2.0% but averagely 1.6%. The modified MySpace reached 1.8% average as shown in Figure 2.

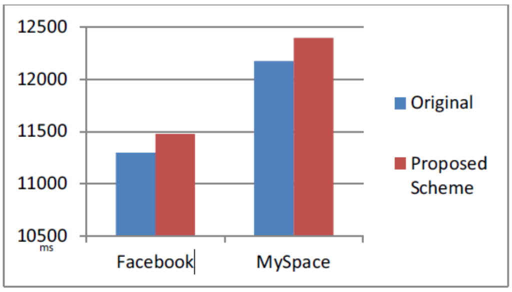
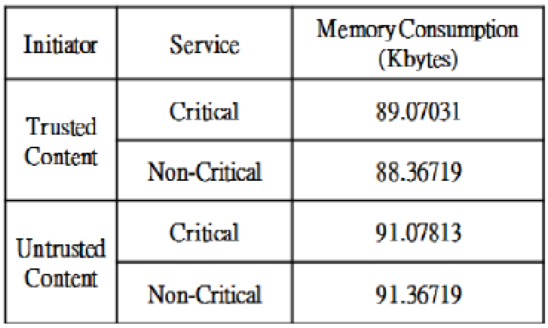


Figure 2: Page generation overhead
(Sung et. al. 2013)

Evaluation of memory consumption test has been carried out with the help of PHP memory_get_usage function and allocated memory use values for each service is shown in Figure 3.



Initiator	Service	Memory Consumption (Kbytes)
Trusted Content	Critical	89.07031
	Non-Critical	88.36719
Untrusted Content	Critical	91.07813
	Non-Critical	91.36719

Figure 3: Memory allocation (Sung et. al. 2013)

According to Sung et. al. (2013) proposed a method to secure web applications against CSRF attacks using labelling mechanism clearly demonstrated impressive results on time overhead and memory consumption issues in the test and provided effective defence for possible forged cross-site requests.

Although the proposed method offers an effective and flexible solution to deal with CSRF attacks without sanitising JavaScript, the experiments they carried out only focused on performance issues and a vulnerability test of sample web pages is limited in theory. For this reason, the conclusion they have drawn might be questionable.

4. White-box Analysis Approach

The method presented by Zhous et. al., (2011) is a White-box followed approach that transforms web application source code and then deploys validating CSRF tokens selectively when a critical HTTP requests are received which aims to improve token-based protection defences. According to Zhous et. al., (2011) the method consisting of online and offline stages protects web application's sensitive services and data against CSRF requests, while enabling access requests including public URIs for non-sensitive resources, without overprotecting the application as show in Figure 4.

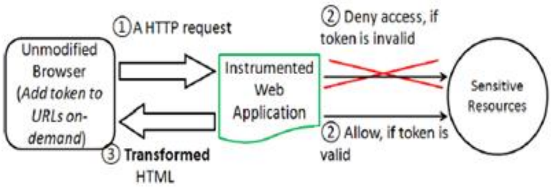

①A HTTP request
Unmodified Browser (Add token to URLs on-demand)
Instrumented Web Application
② Deny access, if token is invalid
Sensitive Resources
② Allow, if token is valid
③ Transformed HTML

Figure 4: overview of the online stage (Zhous et. al. 2011)

The method inserts token check code blocks to application's source code for each sensitive HTTP request in the offline stage so that the token of the request will be validated by application to verify that the request performed by an authorised user. One of the key features of methods is that it adds tokens only to URLs that needs secret token and limits its exposure at the client side avoiding exploit of the token unlike the classical tokinasation approach.

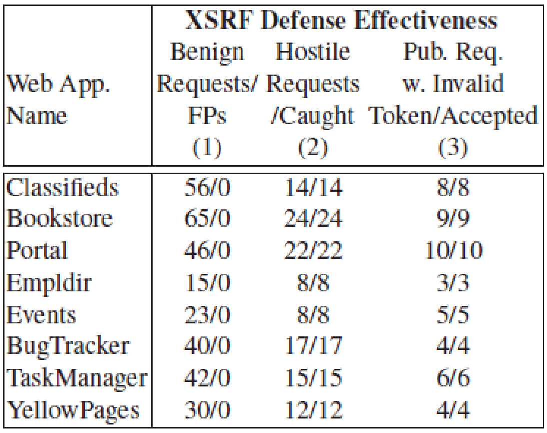
Method identifies defined HTML tags and their event functions that are executed when URLs are in use to assign token to the these request in runtime and then transforms trusted domain URLs with help of JavaScript. Zhous et. al.(2011) also claim that HTML and content containing a token can lead to security leaks, for this reason, proposed method provides the token as a cookie that is read by JavaScript when the related request is in operation. Each trusted domain request that is made to the application includes the token and its defined parameters as a cookie therefore the token validation can only be verified and then related request is granted with access right to sensitive sources when these two parameters match.

4.1 Test and Evaluation

Two test experiments were conducted to evaluate efficiency of proposed method on six medium size commercial web application varied 8K to 27K building a prototype tool of the method. These test were performed on two machines (2GB RAM, 2GHz dual core CPU) with LAMP configuration at the server side and with a computer at client side (1GB RAM, 2GHz dual core CPU).

For the each selected application, a set of test cases that explores "all control paths in these applications by sending public/private HTTP requests with/without valid secret tokens in pre and post-authentication sessions” are produced (Zhous et. al. 2011). Original and method included applications tested using Linux wget command with help of perl script to send HTTP requests automatically and then findings are showed in the table in Figure 5 summarising results of CSRF defence effectiveness test process.

Results from the first test showed total number of public and private request that requires access to critical resources in column one and number of CSRF attacks representing same-origin and cross-origin requests on the original application defended by method in column two. Number of public request including invalid secret tokens is also presented in column three.



Web App. Name	XSRF Defense Effectiveness		
	Benign Requests/ FPs (1)	Hostile Requests /Caught (2)	Pub. Req. w. Invalid Token/Accepted (3)
Classifieds	56/0	14/14	8/8
Bookstore	65/0	24/24	9/9
Portal	46/0	22/22	10/10
Empldir	15/0	8/8	3/3
Events	23/0	8/8	5/5
BugTracker	40/0	17/17	4/4
TaskManager	42/0	15/15	6/6
YellowPages	30/0	12/12	4/4

Figure 5: CSRF defence effectiveness results (Zhous et. al. 2011)

Second test was performed to demonstrate the average browser end response time differences between original and transformed applications using Apache Jmeter measurement tool. Testing each applications 100 times, average results of the performance overheads ranged from 7% - 22% is derived from the experiment without incurring notably network delays as it shown in Figure 6. Zhous et. al. (2011) stated that although results provides moderate performance cost for the transforming phase of application source code, performance overhead may be remarkably lower for the real world web environment with the higher network delays.

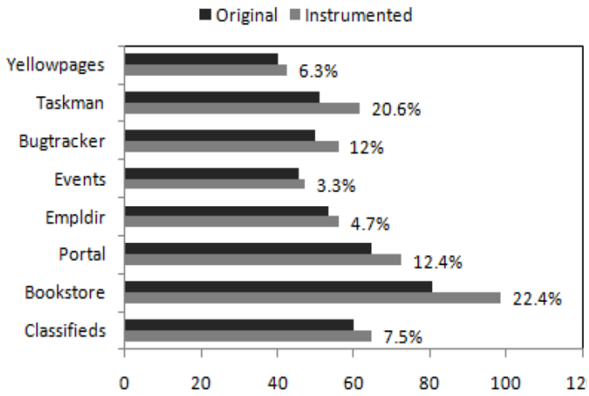


Figure 6: Client end response time (Zhous et. al. 2011)

Zhous et. al.(2011) claimed that according to their experiments conducted and results shown, proposed method by performing a White-box analysis and transforming application source code strengths CSRF defence of existing applications addressing the previous method’s limitations.

Going through this methodology, detailed explanations of conducted experiments and created a set of test cases to measure validity of experiments confirm the reliability of controlled experiment results. When we consider the way test of performed experiments and their outcomes, It seems that they have achieved promising results to justify their claims.

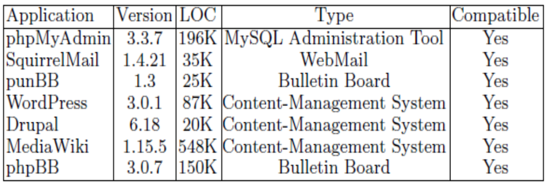
5. Server-side proxy approach

Pelizzi and Sekar (2011) presented a solution that operates as a server-side proxy between client and web application without requiring any application source modification and offered improved defence against multi-stage CSRF attacks addressing the drawbacks of previous token-based approaches. According to Pelizzi and Sekar (2011) the NoForge (Jovanovic et. al. 2006) approach that rewrites the URLs with authentication tokens is not applicable when cross-site requests are dynamically created therefore their approach uses injected JavaScript that performs authorisation checks instead of rewriting the links. The method injects JavaScript code into a page when it is served by a web application. On the browser side, this injected script obtains the authentication token that is issued to pages by web application and supplies it together with every request that is sent by current page. In the final step, the script uses authentication token to confirm legitimacy of performed request. If the request originated from an authorised page, “the request is forwarded to the web server. Otherwise, the request is forwarded to the server after stripping all the cookies” (Pelizzi and Sekar 2011). In this way, stripping of all application cookies at client side will result in authentication failure within web server except for requests requiring no authorisation control or not containing sensitive data access.

Similar to the Labelling Mechanism proposed by Sung et. al. (2013) this method takes advantage of JavaScript event functions to make sure that each request including form submission contains an authentication token therefore the script defines a submit handler for every POST-based form in the web page. Pelizzi and Sekar (2011) also state that their approach is POST and GET compatible, however under some specific circumstances including img and frame elements of HTML that cause the web browser to execute GET request before the injected script attempts to insert an authentication token, their methods currently does not provide full protection against GET-based attacks.

5.1 Test and Evaluation

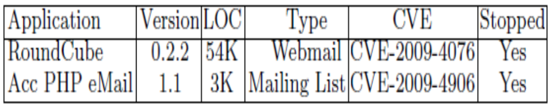
Pelizzi and Sekar (2011) carried out three experiments to prove the efficiency of their approach. In the first experiment, they deployed seven popular complex web applications consisting of over thousand of lines and then accessed them trough the proxy including the method. According to results obtained, the proposed method was capable of defending all the applications without reducing their functionality for each occurred same-origin request as it shown in Figure 7.



Application	Version	LOC	Type	Compatible
phpMyAdmin	3.3.7	196K	MySQL Administration Tool	Yes
SquirrelMail	1.4.21	35K	WebMail	Yes
punBB	1.3	25K	Bulletin Board	Yes
WordPress	3.0.1	87K	Content-Management System	Yes
Drupal	6.18	20K	Content-Management System	Yes
MediaWiki	1.15.5	548K	Content-Management System	Yes
phpBB	3.0.7	150K	Bulletin Board	Yes

Figure 7: Compatibility Testing
(Pelizzi and Sekar 2011)

The second experiment was performed to test protection offered by method attempting to exploit only 2 selected known CVE vulnerabilities due to their claims that effectiveness of the method does not need to be tested with more sample and reproducing the vulnerabilities takes up a great amount of time to obtain a specific version of an application that is vulnerable. Results are shown in Figure 8. Final experiment was done to calculate estimated performance overhead. For this test, a simple web application was built and tested locally with and without including the protection method which has resulted in 2ms maximum overhead on each POST requests that are sent to web server.



Application	Version	LOC	Type	CVE	Stopped
RoundCube	0.2.2	54K	Webmail	CVE-2009-4076	Yes
Acc PHP eMail	1.1	3K	Mailing List	CVE-2009-4906	Yes

Figure 8: Protection Evaluation
(Pelizzi and Sekar 2011)

Pelizzi and Sekar (2011) concluded that their proxy method provides CSRF protection effectively including multi staged attacks for web applications without requiring any source code modifications.

The method seems to provide a reduction of the programmer effort at the sever side but it has not been confirmed that server-side proxy approach achieved the exact conclusion reached by Pelizzi and Sekar (2011) because there were no experiment conducted or presented on the forged cross-origin requests besides the experiments that took place were not detailed and convincing in terms of its repeatability. For this reasons, there are still some remaining questions as to whether the method was tested properly to cover all CSRF attack types.

6. Conclusions

In this paper current server-side CSRF protection methods have been carefully evaluated. All of the analysed solutions represented their test to justify their effectiveness, but due to various reasons, some features of the proposed methods were not fully tested by the authors.

The research carried out by Sung et. al. (2013) including labelling mechanism approach which could be considered an effective solution in terms of supporting JavaScript and AJAX without reducing their functionality and requiring no page modification at server side, if the performed experiments contained defence effectiveness test. Moreover, for the protection evaluation, what they presented was only how the method would deal with two previously known CSRF vulnerabilities on the paper unlike the research by Zhous et. al. (2011) where they performed detailed and rigorous experiments that confirms reliability of performed tests for their White-box Analysis and Source Code Transformation approach.

Research by Zhous et. al. (2011) produced efficient results for both defence and performance evaluation, the experiments were also repeatable and controlled which eliminates the possibility of having biased results. When we analysed the approach deeply, a possible drawback that requires some manual tasks at application side and might also pose some critical problems for the large scaled web applications while upgrading and implementing the method because the proposed method relies on correct specification of files that require to specify landing pages manually which might cause incorrect specification affecting the effectiveness of the method adversely and costing extra effort on modifying the application source code by web developers.

The Server-Side Proxy approach that was proposed by Pelizzi and Sekar (2011) demonstrated significant results on performance overhead test in the experiments compared to the other evaluated methods. The proposed method that provides protection, operating transparently between client and server side does not require any source code modification and configuration at application source code unlike the similar solutions which require modification for outgoing HTML responses but the experiments was performed are not detailed and enough to back up the claim they made. Moreover, due to the way of executing GET method in WEB 2.0 environment, the solution is not fully enabled to protect GET requests therefore the proposed solution is not GET method compatible.

It is clear that more research is required to improve all the methods evaluated and more experiments are needed to be performed on some of the methods being proposed to back up claims made. Based on the methods, conducted experiments and obtained results showed that Zhous et. al.(2011) White-box Approach Transformation method provides more effective protection with the moderate results among the evaluated methods however it would be recommended that current method should be applied for medium-size web applications since it requires manual configuration at application source code. Moreover, for the optimal solution, Labelling strategy proposed by Sung et. al.(2013) could be improved and tested further.

References

Barth A., Jackson C., and Mitchel J. C., 2008, ‘Robust defence s for cross-site request forgery’, *Proceedings of the ACM Conference on Computer and Communications Security(CCS)*, Pages 75–88.

Chen B., Zavarsky P., Ruhl R. and Lindskog D., 2011, ‘A Study of the Effectiveness of CSRF Guard’, *IEEE 3th International Conference on Privacy, security, risk and trust (passat),* Pages 1269-1272

Czeskis A., Moshchuk A., Kohno T. and Wang H.J., 2013, ‘Lightweight server support for browser-based CSRF protection’, *22nd international conference on World Wide Web,* Pages 273-284

Jovanovic N., Kirda E. and Kruegel C., 2006, ‘Preventing Cross Site Request Forgery Attacks’, *IEEE 2nd International Conference on Security and Privacy in Communication Networks(Securecomm),* Pages 1-10

Lin X., Zavarsky P., Ruhl R. and Lindskog D., 2009, ‘Threat Modeling for CSRF Attacks’, *IEEE International Conference on Computational Science and Engineering,* Vol. 3, Pages 486-491

‘Open Web Application Security Project’, 2013, ‘Top 10 2013’. [ONLINE] Available at: *HTTPs://www.owasp.org/index.php/Top_10_2013-Top_10*, [Accessed 15 January 14]

Riccardo P. and Sekar R., 2011, 'A server- and browser-transparent CSRF defence for web 2.0 applications', *ACM 27th Annual Computer Security Applications Conference*, Pages 257-266

Saiedian H. and Broyle D., 2011, 'Security Vulnerabilities in the Same-Origin Policy: Implications and Alternatives', *IEEE computer,* Vol. 44 Issue 9, Pages 29-36

Shar L.K. and Tan H.B.K., 2012, 'Auditing the XSS defence features implemented in web application programs', *IET software,* Vol. 6 Issue 4, Pages 377-390

Siddiqui M.S. and Verma D., 2011, 'Cross site request forgery: A common web application weakness', *IEEE 3rd International Conference on Communication Software and Network(ICCSN),* Pages 538-543

Sung Y., Cho M., Wang C., Hsu C. and Shieh W., 2013, 'Light-Weight CSRF Protection by Labelling User- Created Contents', *IEEE 7th International Conference on Software Security and Reliability (SERE),* Pages 60-69

Zhou M., Bisht P., and Venkatakrishnan V., 2011 'Strengthening XSRF Defence s for Legacy Web Applications Using White-box Analysis and Transformation', *6th international conference on information (ICISS),* Pages 96-110