UNIVERSITI PUTRA MALAYSIA

ENCRYPTION SELECTION FOR WIRELESS LAN 802.11g

ZAHROL AZAM AHMAD

FSKTM 2013 20

COPYRIGHT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the partial requirements for the degree of Master of Science

ENCRYPTION SELECTION FOR WIRELESS LAN 802.11g

By

ZAHROL AZAM AHMAD

November 2013

Chairman : Azizol Hj Abdullah, Ph D
Faculty :Computer Science and Information Technology

Wireless local area network (WLAN) has emerged over the past few years and has become a new channel in communication and shared resources. As the utilization of WLAN increased, it is important to study the impact on the performance of WLAN. The performance of this network is always a priority when users want to use this facility. In IEE802.11 WLAN, the users need to ensure the security of their data and the best performance. The performance is always related with the use of encryption protocols. IEEE802.11 contains encryptions protocols that have three major generations, which are wired equivalent privacy (WEP), Wi-Fi protect access (WPA) and counter mode with cipher block chaining Mac protocol (CCMP). However, there are several opinions about the effect of using encryption on the performance of WLAN.

A recent study claimed that encryption gives negligible impact to WLAN performance, while other studies showed that it degrades WLAN performance about 20%. Thus, these different findings have motivated this research. As for the solution, it proposes a mechanism of selecting encryption algorithms, which is able to help users to select the suitable encryption algorithm and encryption protocols for their secured communication in IEEE 802.11g WLAN. The impact on throughput and time success can be examined based on encryption algorithms and encryption protocols by using this proposed mechanism.

In this study, MATLAB was used for the simulation and the parameters for the simulation were different size of text file, type of encryption algorithms and type of encryption protocols. The data size of text file used were 50 bytes to 300 bytes. The encryption algorithms consist of AES, DES and Blowfish while the encryption protocols consist of WEP, TKIP and AES/CCMP. There were two scenarios that have been tested in the simulation. In the first scenario, the data was tested with encryption protocols and for the second scenario, the data was tested with encryption algorithms and also encryption protocols. Meanwhile for encryption algorithms, the data was encrypted using Kryptel, an encryption freeware. This encryption process occurred before transmitting the data through IEEE802.11 WLAN and encryption protocol at the access point.

The results obtained from this simulation were time success and throughput. Through the results, time success was increased in both scenarios, as the data size became larger after it was encrypted. It also showed that DES algorithm produced the best time success along with WEP encryption protocol. As for the throughput, AES algorithm with WEP produced the best throughput in both scenarios, except when the size of data was 300 bytes, the results showed that Blowfish was the best encryption algorithm to be coupled with WEP encryption protocol.

Based on the findings, it showed that this proposed mechanism can act as a guide to select which encryption algorithms and encryption protocols that provided in IEEE802.11 standards and also can ensure the best performance in WLAN.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia

sebagai memenuhi keperluan untuk Ijazah Master Sains

PEMILIHAN PENYULITAN BAGI SISTEM RANGKAIAN TANPA WAYAR BERDASARKAN STANDARD IEEE 802.11g

Oleh

ZAHROL AZAM AHMAD

November 2013

Pengerusi : Azizol Hj Abdullah, Ph.D
Fakulti : Sains Komputer dan Teknologi Maklumat

Sistem rangkaian setempat tanpa wayar telah digunakan secara meluas semenjak kebelakangan ini. Ianya menjadi budaya baru dalam penyaluran maklumat serta perkongsian sumber. Dengan meningkatnya penggunaan sistem rangkaian tanpa wayar ini, adalah amat penting untuk mengkaji kesan prestasi penggunaannya. Ini kerana prestasi sentiasa diambil berat oleh pengguna. Di dalam sistem rangkaian tanpa wayar ini yang berdasarkan standard IEEE802.11, pengguna perlu memastikan keselamatan data mereka serta prestasi sentiasa menjadi keutamaan. Prestasi sentiasa dikaitkan penggunaan protokol penyulitan.

Di dalam standard IEEE802.11, ianya mengandungi tiga protokol iaitu *Wired Equivalent Privacy* (WEP), *Wi-Fi Protect Access* (WPA) dan juga CCMP. Namun begitu, wujud pandangan yang berbeza mengenai kesan penggunaan penyulitan ini terhadap prestasi rangkaian tanpa wayar.

Berdasarkan kajian yang dibuat sebelum ini, ianya memberi kesan yang kecil namun ada kajian yang menyatakan ia mengurangkan prestasi rangkaian ini sehingga 20%. Ini telah mendorong kepada tujuan kajian ini dibuat. Ianya melibatkan

cadangan penggunaan mekanisme pemilihan algoritma dan pemilihan penggunaan protokol algoritma. Kesan penggunaan protocol penyulitan dan protocol algoritma terhadap masa ketibaan dan kadar purata mesej yang dihantar dapat dilihat dengan menggunakan mekanisme yang dicadangkan.

Bagi melaksanakan kajian ini, kaedah simulasi dipilih dan menggunakan pengaturcaraan MATLAB. Input yang digunakan adalah fail teks data (.txt), jenis algoritma protokol seperti WEP, TKIP dan AES/CCMP dan enkripsi algoritma seperti AES, DES dan Blowfish. Bagi saiz data, ianya melibatkan saiz 50 bait sehingga 300 bait. Senario simulasi ini terbahagi kepada dua iaitu dengan menggunakan protokol penyulitan sahaja manakala senario kedua adalah menggunakan algoritma penyulitan dan juga protokol penyulitan. Bagi proses algoritma penyulitan, data telah disulitkan dengan menggunakan perisian Kryptel. Ianya berlaku sebelum data dihantar kepada penerima manakala bagi proses protokol penyulitan, ianya berlaku semasa di punca capaian data.

Output yang terhasil adalah masa ketibaan data tersebut dan juga kadar purata mesej yang dihantar. Bagi masa ketibaan untuk kedua-dua senario, masa ketibaan menjadi semakin lama setelah melalui proses penyulitan, di mana keputusan menunjukkan algoritma penyulitan DES dan protokol penyulitan WEP menghasilkan masa ketibaan yang paling cepat.

Manakala untuk kadar purata mesej yang dihantar pula, protokol penyulitan WEP dan algoritma penyulitan AES menghasilkan prestasi kadar purata mesej yang dihantar yang memuaskan bagi kedua-dua senario. Perubahan berlaku hanya untuk algoritma penyulitan apabila saiz data adalah 300 bait, di mana algoritma penyulitan yang sesuai adalah Blowfish dengan protokol penyulitan WEP.

Secara keseluruhannya, mekanisme yang dicadangkan dalam kajian ini boleh dijadikan panduan untuk memilih penyulitan algoritma enkripsi dan penyulitan protokol yang disediakan dalam standard IEEE802.11g. Di samping itu, ia boleh menjamin prestasi yang baik dalam sistem rangkaian setempat tanpa wayar bagi standard IEEE802.11g.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Allah s.w.t for giving me the strength to finish this thesis. I would also like convey my greatest gratitude to my dearest supervisor, Dr. Azizol Hj. Abdullah for his invaluable help, guidance, supervision and support throughout my research. His great ideas, suggestions and expertise are sincerely and highly appreciated. I would also like to express my gratitude to my co-supervisor, Associate Professor Dr. Zuriati Ahmad Zukarnain for guiding me in my study.

I would like to thank Universiti Teknologi Mara for giving me study leave and to the Ministry of Education for providing the financial support during my study. Their help are highly appreciated.

Special thank to my family, especially my mother Mrs. Zaharah Hamzah, my beloved wife Mrs. Roslili Mat for the encouragement, sacrifice and motivation throughout my study, and not forgetting my dearest daughters, Nur Batisya Balqis and Nur Fatin Zahirah.

My greatest thanks are to my colleagues in Universiti Putra Malaysia and my family who have helped me and I wish to extend my sincere appreciation and best wishes to them.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Sciences. The members of the Supervisory Committee were as follows:

Azizol Hj Abdullah, PhD

Senior Lecturer

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

Zuriati Ahmad Zukarnain, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Member)

BUJANG BIN KIM HUAT, PhD

Professor and Dean

School of Graduate Studies

Universiti Putra Malaysia

Date :

DECLARATION

Decralation of graduate student

I hereby confirm that:

- The thesis is my original work
- Quotations, illustrations and citations have been duly referenced
- This thesis has not been submitted previously or concurrently for any other degree at any other institutions
- Intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia
- Written permission must be obtained from supervisor and Deputy Vice Chancellor (Research and Innovation) before thesis is published in book form
- There is no plagiarism or data falsification/fabrication in the thesis and scholarly was upheld as according to Rule 59 in Rules 2003 (Revision 2012-2013) . The thesis has undergone plagiarism detection software

Signature : ..... Date : .....

Name and Matric No : .....

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature:	_____	Signature:	_____
Name of Chairman of Supervisory Committee:	_____	Name of Member of Supervisory Committee:	_____
Signature:	_____	Signature:	_____
Name of Member of Supervisory Committee:	_____	Name of Member of Supervisory Committee :	_____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

AP	Accesss Point
AES	Advanced Encryption Standard
CCMP	Counter Mode with Cipher Block Chaining Mac Protocol
CTS	Clear to Send
CWN	Cognitive Wireless Network
DES	Data Encryption Standard
DCF	Data Coordination Function
DIFS	Distributed Inter Frame Sequence
DSPM	Dynamic Security Policy Management
FTP	File Transfer Protocol
GMAP	Global Mobile Authentication Protocol
IEEE	Institute of Electrical and Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
MANET	Mobile Ad Hoc Network
MATLAB	Matrix Laboratory
MIC	Message Integrity Check
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
QoS	Quality of Services
RTS	Right to Send
SIFS	Short Inter Frame Sequence
SSID	Service Set Identifier
SS/AG	Security Simulator with Attack Simulator
TARA	Throughput Aware Rate Adaptation
TCP	Transmission Control Protocol

TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wifi Protect Access

CHAPTER 1

INTRODUCTION

Nowadays, rapid changes in technology have given the opportunity for users to have various choices of communication channels. As we know, the latest trends in this millennium and the nature of today's life has compelled users to accept and use current technology. Besides, they want all the information to be at their fingertips. They want to access all these information quickly, as faster information retrieval means success and efficiency. Based on that, a variety of handheld devices such as smart phones and tablets have been invented. This paradigm is named mobile computing (Yuan Zhang, 1999).

These devices are supported by wireless technology and enable users to get connected anytime and anywhere. These wireless facilities are available in public places such as cafes, libraries, airports, hotels and also lobbies of office buildings.

Wide usage of mobile computing has urged users to move from desktop to mobile computing. Mobile computing is usually associated with mobility hardware, data and software and its applications. Nowadays, mobile computing has becomes a necessity to those who are always busy working and moving around. This mobile computing can be used in WLAN.

This WLAN system has several standards, such as IEEE 802.11 that can be divided into several types, for example, a, b, g or n. It uses 802.11 MAC protocol as a standard layer 2 protocol. The study by (N.Borisov et.al, 2001) claimed that WLANs are more vulnerable to attacks, including data sniffing and unauthorized access. As a result, appropriate security measures, especially the signal encryption mechanism, needs to be implemented to protect WLAN system (Siwaruk et.al, 2008). There are several encryption protocols available such as WEP, TKIP and CCMP.

1.2 Background

The advancement and rapid change in technology has created new landscapes in communications. Today, wireless technology is commonly used to access internet or intranet. It can be used to transfer information either in short or long distances. The remarkable innovation of mobile computing has led to the same security issues. It is because of the variety of mobile devices and their applications and services, which are widely available in the market today. The authors (Jun-Zhao et.al, 2001) have listed a few scenarios which could lead to the security in wireless environment, such as:

i) Physical weakness and limitations of mobile and wireless communications such as high error rate, unpredictable error due to interference and mobility;

ii) Exposed environment of wireless that is open to malicious attacks;

iii) Application and services that become important features and high demand by users; and

iv) Content of provided services becomes valuable not only for users, but also to composers and providers.

Mobile wireless networks are generally more prone to physical security threats than fixed cable. The increasing possibility of attacks should be considered. The criteria of security need to be matched with the basic criteria in security, which are availability, integrity, confidentiality, authentication, non-repudiation and authorization.

It should comply with the security protocol that exists in the WLAN. In WLAN, privacy is achieved by data contents protection with encryption. Without the encryption, any other standard wireless devices can read all traffic in the network. There have been three major generations of security approaches, which are known as WEP, WPA and WPA2/802.11i.

The impact of security on the WLAN performance was studied by (Barka & Boulmalf, 2006), which focused on WEP and the results showed that the throughput decreased when WEP was enabled.

1.3 Problem statement

The popular standard in WLAN nowadays is IEEE802.11. It show that the utilization of WLAN increased, it is important to evaluate the performance of this network. Beside that the users also need to ensure that their sent data are secured and received by their partner in appropriate time. In most WLAN encryption used, to overcome the security problem.

In most scenarios, it shows that the data need to be encrypted before it is transmitted to the sender. The use of encryption protocols, it might affect the performance of the WLAN networks. There are inaccurate perceptions about the effect of encryption performance of WLANs.

Most of the study were focus on the effect of using encryption protocols in WLAN. A recent study claimed that encryption gives negligible impact to WLAN performance, while other studies show that it degrades WLAN performance about 20%. Since there is no study about the effect of using encryption algorithm and encryption protocols in WLAN, it is important to study the impact of these algorithms on WLAN.

As for that, the main focus of this research is to propose the mechanism for selection of encryption algorithm used in WLAN that is based on IEEE802.11g standard against the throughput. The standards IEE802.11g was choose because most of the access point used this standard and it was already established. This is to ensure the confidentiality of the data is not compromised and the throughput of the network can be maintained or improved.

It also can give users an option to choose the encryption algorithm that is provided in the IEEE802.11g environment. As the different encryption algorithms will produce different results. This will ensure the performance of data between two peers, which are based on the time success and throughput.

1.4 Research objective

The objectives of this research are:

i) To propose a mechanism for selecting a suitable encryption protocols and algorithms on WLAN IEEE802.11g and;

ii) To analyse the impact of encryption protocols and algorithms on WLAN IEEE802.11g based on throughput and time success.

1.5 Scope

This research only focuses on IEEE 802.11g wireless network, which is the most common standard in the WLAN environment. This standard was chosen because it has been used by Siwaruk et.al, 2008. Another reason that IEEE802.11g has been chosen because all the formula used are based on the IEEE802.11g standard. Meanwhile, the transmission rate depends on the standard WLAN IEEE 802.11g, which is 54 Mbps.

It is important to refer to their study because this research is an enhancement from their findings, as their study used only encryption protocols of WEP, WPA, and AES/CCMP, but this research used the encryption algorithm such as DES, AES and Blowfish.

Communication factors such as channel error, routing algorithm and other factors will not be considered in this research to simplify the study. Performance analysis of the proposed techniques was evaluated based on throughput that depends on the success time of data received and the size of the text file used in the experiment.

1.6 Contributions

The main contribution in this research work is to propose a mechanism for users to select or to help users in selecting the best encryption algorithm for data privacy with the encryption protocol provided in IEEE WLAN 802.11g environment. This research can be used as a guide for users to determine which encryption algorithm should be used in IEEE802.11 that could maintain their application performance. It will be able to maintain the application performance while having a secured environment and communication.

1.7 Methodology

The methodology for this research is through simulation using MATLAB. It will involved experiments in two scenarios: the first scenario deals with data and encryption protocols provided in IEEE802.11 but without the encryption algorithm, while the second scenario used using both encryptions. The comparison between these scenarios will be done to observe their performance of the three selected encryption algorithms, which are DES, AES and Blowfish.

Based on that, the simulation will involve different size of data that starts with 50 bytes up to 300 bytes, encryption algorithms and encryption protocols in the IEEE 802.11.

Meanwhile for encryption, the data firstly was encrypted by using Kryptel, a type of encryption software. The size of the data before and after encryption will be an input to this simulation.

Then, the calculation will be made by simulation. The output produces time success of the data received and the throughput of the networks. These findings will be an indicator of the performance in WLAN based on IEEE802.11 standard. The detail of this methodology is described in Chapter 3.

1.8 Thesis organizations

The thesis is organized as follows. Chapter 2 provides a detailed discussion on the related work pertaining to the performance of wireless local area network and their relation with security in wireless local area network. The throughput of networks and the way the findings are produced will be compared.

Chapter 3 discusses the material and method used for the performance analysis. The elaboration includes detail on methodology and the experimental setup will be explained. In the next chapter which is Chapter 4, details about the proposed mechanism will be explained.

Meanwhile for the findings, the analysis of the results will be presented in Chapter 5. Lastly, Chapter 6 will cover the summary of the thesis with conclusion and also recommendations for future work.

REFERENCES

Akio Takubo (1998), Security Simulator in Mobile Computing Environment, Proceedings of 12th International Conference on Information Networking (ICOIN-12), 1998, Tokyo, 21-23 Jan 1998. pp89-pp94.

Andrew Gin, Ray Hunt (2008), Performance Analysis of Evolving Wireless IEEE802.11 security Architectures, Proceeding Mobility '08 Proceedings of the International Conference on Mobile Technology, Applications, and Systems

Arash Habibi Lashkari, Mir Mohammad Seyed Danesh (2009), A Survey On Wireless Security Protocols (WEP, WPA and WPA2.802.11i) . *2009 2nd IEEE International Conference on Computer Science and Information Technology,Beijing,China. 8 August – 11 August 2009.*

Avesh K Agarwal, Wenye Wang (2005), Measuring Performance Impact of Security Protocols in Wireless Local Area Networks**.** 2nd International conferences Broadband Networks, 2005.Boston, USA, 3 October – 7 October 2005, pp625-634.

Avesh K Agarwal, Wenye Wang (2006), DSPM ; Dynamic security Policy management for optimizing Performance in Wireless Networks. Military Communication Conferences 2006, Washington DC, USA, 23 October – 25 October 2006, pp1-7.

Barka, Boulmalf, Amal Alteniji, Hanadi Al Suwiadi, Huda Khazaimy, Meera al Mansouri (2006), Impact of security on the performance of Wireless Local Area Network**.**IEEE WCNC 2007 Conference ,March 2007 *;32(2):490-9*

Barka, Boulmalf,(2007), Impact of encryption on the Throughput of Infrastructure WLAN IEEE 802.11g. IEEE WCNC 2007 Conference ,March 2007 *;32(2):490-9*

Barka, Emad Eldin Mohamed, Kadhim Hayawi (2006) , End to End Security for WLAN; A Performance Analysis for the Underlying Encryption Algorithms in the Lightweight Devices. IWCMC 2006. Proceedings of the 2006 , International Conference on Wireless Communications and Mobile Computing, pp1295 – 1300.

Borisov, Ian Goldberg, David A.Wagner (2001), Intercepting Mobile Communications: The Insecurity of 802.11. ACM SIGMOBILE 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, 16 July – 21 July 2001.

Boukerche, Yonglin Ren, Lynda Mokdad (2011), Performance Analysis of Selective Encryption Algorithm for Wireless Ad Hoc Networks**.** IEEE WCNC 2011,Quintanna Roo, Mexico, 28 March- 31March 2011, pp1038-1043.

Bruno , Emilio Ancilotti, Marco Conti (2009), Design and performance evaluation of throughput-aware rate adaptation protocols for IEEE802.11 wireless networks**.** Performance Evaluation Journal, vol 66, pp811-825.

Capra, S.Blair, Mascolo Cecilia (2002),Exploiting Reflection in Mobile Computing Middleware**.** *Mobile Communications and Review ;6(4);34-44.*

Chendeb, Bachae El Hassan, Hossam Afifi (2004), Performance evaluation of the security in wireless local area network (WiFi) ,2004, International Conference on Communications Technologies,19 April- 23 April 2004 ,pp215-216.

Defeng and Bagrodia (2011), Impact of Complex Wireless Environments on rate Adaptation Algorithms. *IEEE WCNC 2011,Mac,pp 168-170*

G Ramesh, Prof Dr R Umarani (2010), UMARAM : A Novel Fast Encryption Algorithm For Data Security In Local Area Network. IEEE International Conference on Communication Control and Computing Technologies, 7 October 2010 – 9 October 2010 (ICCCCT), pp758-768.

Gurkas, A.H Zaim, M.A. Aydin (2006), Security Mechanism And Their Performance Impacts on Wireless Local Area Networks**,** International Symposium on Computer Networks, June 2006.

Hatem M.Abdual-Kader, Diaa Salama Abdul Minaam, Mohiniy Mohamed Hadhoud (2010), Wireless Network Security Has No Clothes. Informatics and System , 7th International Conferences ,Cairo, 28 Mac – 30 Mac 2010, pp 1- 8.

Higaki (2009), Reactive TDMA Slot Assignment Protocol in wireless Ad Hoc Nettworks. *2009 First International Conferences on Advances in Future Internet.18 june-23 June, Athens, Greece. pg6-11.*

IEEE 802.11 Standard.(2012). Retrieved Feb 17, 2013, from : http://standards.ieee.org

Jun-Zhao Sun, Douglas Howie, Anntti Koivisto,Jaakko Sauvola, (2001)**,** A Hierarchical Framework Model of Mobile Security**.** Personal, Indoor and Mobile Radio Communication , 12th IEEE Symposium, San Diego, USA,30 Sept 2001 – 3 Oct 2001,pp56-60.

Kadlec, Radek Kuchta, Radimir Vrba (2009), Performance Tests of the Dynamic of the Wireless Networks. *2009 Eighth International Conferences on Networks, 1 March – 6 March 2009 , Cancun, Mexico, Pg112-115.*

Kai Shi, Yantai Shu, Chunfeng Liu, Oliver Yang (2009). A Principal Agent Method to Prevent Selfish MAC Layer Behaviour in Wireless Networks.

Kitahara H, Okada H, Mase K.(2010), Experimental Evaluation of a Novel Transmission Rate Assignment Scheme in Wireless Mesh Networks. *Consumer Communication and Networks Conference , 7th IEEE , 1-5.*

Kuo, Yi-Hung Huang, Kuan-Cheng Lin(2012), Performance enhancement of IEEE802.11 DCF using novel back off algorithm, Eurasip Journal on Wireless Communications and Networking 2012;274 doi:10.1186/1687-1499-2012-274.

Liqiang Zhang, Yu-Jen Cheng, Xiaobo Zhou (2009), Rate avalanche : Effects on the performance of multi rate 802.11 wireless networks. *Simulation Modelling Practice and Theory (17); 487-503*

Marek Natkaniec, Andrzej R.Pach (2000), An analysis of the Back off Mechanism used in IEEE802.11 Networks, 2000 , 5th IEEE Symposium on Computer and Communication, pp444-449.

Marsh, Fred Douglis, Ramon Caceres (1993), System Issues in Mobile Computing**.** Technical Report MITL-TR-50-95.

Narayan, Samad S.Kolaihi.Yonathan Sunarto, Du D.T.Nguyen, Paul Mani(2008)**,** The Influence of Wireless IEEE802.11g Encryption Methods on Throughput and Round Trip Time for Various Operating Systems, Communication Networks and Services Research Conference, pg171-175

Papadopoulos (2010), On the scaling IEEE802.11 to facilitate wireless scalable networks. Journal of Computer Networks, Vol 54,*pp1778-1791.*

Pacheco de Carvalho, Nuno Marques, Claudia F.F.P, H.Veiga, (2011). Comparative Performance Studies of Laboratory Wi-Fi IEEE 802.11 b,g WEP Point to Point Links, Proceedings World of Congress Engineering 2011, Vol 11, WCE 2011, July 6-8 2011,London, UK.

R. Masadeh, Shadi Aljawarneh, Nedal Turab, (2010), A Comparison of Data Encryption Algorithms with the Proposed Algorithm : Wireless Security. Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference, 16 August – 18 August 2010, Seoul. Pp 341 – 345.

Rocha, Daniel N.O Costa, Rande A.Moreira, Cristiano G.Rezende, Antonio A.F Loureiro, Azzedine Boukerche (2010), Adaptive security protocol selection for mobile computing**.** *Journal of Network and Computer Applications, Vol (33),pp569-587*

Sung-Hyun Eum, Sung-Jae Cho, Hyoung-Kee Choi, Hyungseung Choo (2008), A Robust Session Key in IEEE802.11i, International Conference on Computational Sciences and Its Applications ICCSA 2008

Scheiner,(1993). Blowfish Algorithm, http://www.schneier.com/blowfish.html

Siwaruk Siwamongsatham, Kridakorn Hiranpruek, Chanin Luangingkasut, Songrit Srilasak (2008). Revisiting the Impact of Encryption on Performance of IEEE 802.11 WLAN. Proceedings of ECTI-CON 2008.

Stallings (2007)**.** Network Security Essentials, Applications and standard, Pearson Education, New Jersey.

TalebiFard, Terrence, Wong, Victor C.M.Leung 2010)**.** Access and services convergence over the mobile internet – a survey. *Computer and Networks;54(4);547-57.*

Train, KE(2003)**.** Discrete choice of method with Simulation. Cambridge University Press.

Uchida, Kazuo Takahata, Yoshitaka Shibata (2010), Proposal of Transmission Control Methods with Multihopped Environments in Cognitive Wireless Networks. 2010 IEEE 24th International Conference on Advanced Information Networking and Application Workshops .Perth, Austaralia, 20 April-23 April 2010,pp127-132.

Verma, Ritu Agarwal, Dhiraj Dafouti, Shohba Tyagi (2011), Performance Analysis of Data encryption Algorithms, www.cs.wustl.edu/~jain/cse567-06/ftp/**encryption**_perf.pdf

Vucinic, Bernard Torancheau, Andrzej Duda(2012), Simulation of a Backward Compatible IEEE802.11g Network **:** Access Delay and Throughput Performance Degradation.

Wong, Hao Yang, Songwu Lu, Vaduvur Bharghavan (2006). Robust Rate adaptation for 802.11 wireless networks. Proceedings of ACM MobileCom Conference ,Los Angeles,California, pp146-*157.*

Yi Li, Lili Qiu, Yin Zhang, Ratul Mahajan, Eric Rozner (2008), Predictable Performance Optimization for Wireless Networks**.** *Special Interest Group in Data Communication Conference,2008. 17 August – 22 August 2008,Seattle, USA,pp413-425.*

Yuan Zhang (1999), Programmable and Active Networks, Master Thesis,McGill University,Montreal.