Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1243 – 1246

REVIEW ARTICLE

Security in WLAN- Review of Security and Throughput Tradeoff

Avinash Kaur[1], Harwant Singh[2]

[1]Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
[2]Department of Computer Science and Engineering, Lovely Professional University, Punjab, India

Abstract— ***An IEEE 802.11 WLAN is a group of wireless nodes located within a moderate physical area. It provides intensified productivity, less cost of installation and mobility. The open to air nature of wireless channel that give us great convenience of mobility also make it vulnerable to attack. Various security issues are described in paper. The tradeoff between security and throughput is main focus in WLAN.As if the security increases the throughput gradually decreases. To solve this problem various techniques are used which reduces this problem.***

Keywords— ***Throughput; Encryption; Decryption; X-OR; WLAN***

I. INTRODUCTION

In today's era Wireless local Area Networks (WLANs) becomes the most convenient way to communication without wired environment. WLAN's 802.11-1997 was the first standard of wireless networking, 802.11b was the first which comes into fashion, called Wireless-Fidelity [1]. WLAN 802.11 is a set of standards having computer communication in the 2.4GHz, 3.6GHz and 5 GHz frequency bands. The familiarity of wireless local area networks is because of their suitability, cost, efficiency and ease of consolidation to other networks. It also provides intensified productivity, less cost of installation and mobility. Wireless local area networks uses electromagnetic air waves to exchange information from source to destination without relying on any physical link [2].

II. VULNERABILITIES IN WLAN

The risk factor is considered to be greater in case of wireless rather than wired network because data is transformed by air medium. So attackers are always tried to grab the confidential data. Access Points can be the reason for compromising the security in WLAN [3]. Spoofing is one of the causes which may reduce the security. An unsafe station which may be unknown can create the activity which is harmful for network. Attackers have numbers of ideas to break the security in WLAN network. Some of the major reason to do attack which corrupt the network from normal activities are as follow:

- To get the private information confidentiality attack is done by attacker.
- To misguide the recipient integrity attack is performed by managing the network.

- To get access of legitimate user authentication attack is done by attacker.
- To access the services provided in any network availability attack is done by attacker.

III. SECURITY IN WLAN

Cryptography provides the facility to camouflage our data so that transmitted information can not reveal by eavesdropper. Cryptography means switch information into ostensible unintelligible way that permit a secret method of witching. In this plain text is our well known original message. The switched words or text is converted text called cipher text. No one can understand the format of cipher text [4].This cryptography technique reduces the vulnerabilities issues and protect our data from malicious activities. Cryptography systems manage both an algorithm with a secret quantity with the different cryptographic primitives are as follow:

A. Encryption

It means taking a plain text and transforms it into a special as cipher text. The cipher text is scrambled message produced as output. Message produces by encryption cannot be easily inferred by unauthorized persons.

B. *Decryption*

It is the conversion of encryption technique. A cipher text is reconverting into its original form. So the text in decryption is what the sender writes at first time to the authorized receiver.

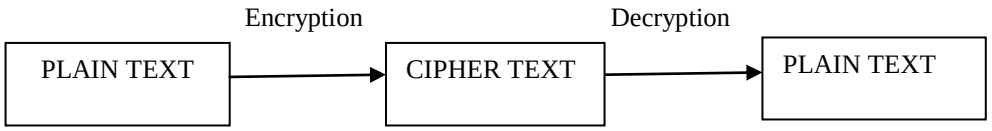

Fig.1 Encryption and Decryption

C. Authentication

It means to verify someone who is authentic. In other words, to examine knowledge of a secret without divulge it. Authentication can be attained by digital signature and certificate authority. There are three kind of cryptographic functions. Authentication gives guarantee of secure environment.

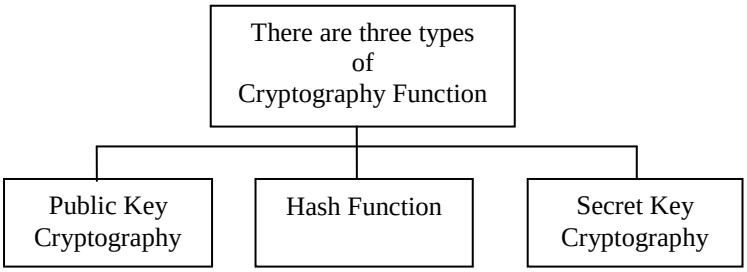

Fig.2 Types of cryptographic Function

IV. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography was invented in 1975.In public key cryptography every individual participant has a pair of keys [public key, private key]. The public key can be revealed to the entire world but the private key is not revealed to anyone. The sender encrypts the plaintext with the public key of the intended recipient and the intended receiver decrypt the cipher text by using his private key .So keys on both side are not same. It requires a very less efforts to communicate as key is public [4].

V. HASH FUNCTION

A cryptographic hash function is a mathematical translation or shift that handles a message of any length, alters it into a string of bit and then computes from it a fixed-length short number. The hash algorithms are also known as message digest or one way transformations. It is basically used for generating symmetric key[2]. It is considered a function because it takes an input message and produces an output. It is considered one way because it is not practical to figure out what input corresponds to a given output. For a message digest function to be considered cryptography secure, it must be computationally infeasible to find a message that has a given prespecified message digest and it similarly impossible to find two messages that have the same digest. Also, it should be impossible to find a different message with the same message digest. It overcome the problem of

collision of same key [5].The other problem of storing the items are solved by hash tables.The various hash algorithms are as follow:

- Secure Hash Algorithm (SHA-1).
- Message digest 2
- Message digest 4
- Message digest 5
- Hashed Message Authentication Code (HMAC).

VI. SECRET KEY CRYPTOGRAPHY

It involves the use of single key. For a given message (plaintext) and the key, encryption produces unintelligible data (cipher text), which is of same length as the plaintext. The decryption which is reverse of encryption uses the same key as encryption. As secret key cryptography uses the same key for encryption and decryption so it's also refer as symmetric key cryptography [5]. So in secret key cryptography the secret key should be shared between the two parties before the communication start.

VIII. LITERATURE SURVEY

Poonam Jindal works on "study and Performance evaluation of security-throughput tradeoff with link adaptive encryption scheme. Security is optimized in terms of brute force attack. Security of cipher is measured by calculating the cipher strength or the optimal block length. Results were analyzed for the link adaptive encryption scheme and a fixed block length encryption scheme operating in two different modes of cipher. Throughput is calculated for both variable and fixed block length encryption scheme. It is observed that throughput is increased with variable block length encryption scheme operating in ECB mode of cipher. Same calculations are done in CBC mode of cipher. The better results are appeared in case of CBC [6]. To reduce the compromise a technique is come into account which is called as link adaptive technique. It Intensified security level and no any kind of compromise take place with this technique.

Jian Liu, jian Sun and Shoutao Lv proposed a paper A novel throghput optimization approch in wireless system.It works on a mathematical framework to maximize the throughput in WLAN using various parameters such as symbol rate packet length and the constellation size as optimization variable[7].In this paper, author presented optimization equation on each of above mentioned parameter also present some implementation constrints and their effects on performance of system.

Mohamed Haleem and other three members work on optimization the security throughput tradeoff in the wireless networks and Adversaries [8]. It studies probabilistic framework for adversary strength to break a cipher. There is an optimal block length allocation algorithms for the attacker strength with linear adversary model and exponential adversary model. With this throughput is gained with multi rate modulation schemes (BPSK and MQAM).

Katinka wolter works on the paper for performance and security tradeoff. By understanding these terms it is concluded that both terms are contradicting each other. If one factor goes on high state other factor has to pay for that.If security is high with performance the parameter such as cost also increases. So there are algorithms which are used to solve this trade off [9].

Zhang Longjun, Han Wei, Zheng Dong, Chen Kefeiks works on paper for Security Solution of WLAN in which security defense mechanism should be designed for WLAN to protect confidentiality, integrality, to carry out authentication and access control to WLAN[10].encryption is a basic technique to protect information security in various fields such as mathematics , computers , electronics and communications. Other important function of encryption is digital signature and identity certification. As WLAN focus on user requirements of accurate data, authentication and access management. It provides the balance between security cost and system performance. To overcome security problems in WLAN public key cryptosystem and elliptic curve cryptosystem are introduced.

Minho Shin, Justin Ma, Arunesh Mishra, and William A. Arbaugh proposed a paper on wireless network security and interworking. As security in interworking is a not easy because of the large different security architectures used within each and every network. There are different security challenges in first generation, second generation and third generation. In focus in this paper is on use's access control and mobile stations, data confidentiality, data integrity, and user identity privacy[11].Authentication and key agreement protocol also include in security solution in CDMA 2000.But this protocol does not provide full mutual authentication. There is security issues in WPA. Spoofing is major issue in WPA.

Dushuqin, Qin Yi works on WLAN Security System based on the 802.1 and AES. He proposed that RADIUS in WLAN is one of the most important protocol of dial-up access, because of its readily management, good scalability and security .With the combination of RADIUS and IEEEB02[12]. 1x authentication can be maintained. A successful login can be done, in can case of failure it cannot connect with internet.

Hossam M. Faheem works on Multiagent based security for the WLAN. He describes the relation of WLAN attacks policies and security layers. He proposed three security layers[13].First layer secure the WLAN from client to client attack where base station configuration policy, authentication policy, base field coverage policy and intrusion detection policy is described the middle layer that is second layer prevent traffic capturing from interception attack and sniffing attack where traffic encryption policy and implementation policy is mentioned. The last third layer secures the WLAN from unauthorized wireless devices from insertion attack where base station discovery policy and MAC address filtering policy is described. The deployment of a Multiagent Based system to WLAN provides super security without a firewall and with firewall.

IX. CONCLUSION

It can be seen that the provisions for enhancing the security level of data transmitted over the wireless channel which outcome as loss of throughput. Therefore, there is always fundamental tradeoff in security and throughput of the network. The simulation results will reveal that the Link Adaptive Encryption scheme is an excellent candidate for optimizing the security-throughput tradeoff and especially when security is of essence. It will enhance the Security level of data transmitted over wireless channel without compromising channel performance.

REFERENCES

[1] Md. Alimul Haque, Pritam Kumar, Amrendra Kumar,*5th Generation WiFi Networking*, IEEE, Vol.2, No4, April 2012. Pp.235-241.

[2] J W. Stalling, *Cryptography and Network Security – Principle and practice*, Third Edition,Peaterson Education, 2003.

[3] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong,Tai-hoon Kim,*Wireless Network Security vulnerabilities, threats and counter measures*, IJMUE, 2008, vol.3, no.3,pp.77-86.

[4] Zirra Peter Buba, Gregory Maksha Wajiga, *Cryptographic Algorithms for Secure Data Communication*, IJCSS, 2011, vol.5, no.2, pp.227-243.

[5] Ayushi,*A Symmetric Key Cryptographic Algorithm*,IJCA,2010,vol.1 ,no.15,pp.1-4.

[6] Poonam Jindal and Brahmjit Singh, *Study and Performance evaluation of Security throughput tradeoff with link Adaptive encryption scheme*, IJSPTM, 2012,vol.1, no.5,pp.13-26.

[7] Jian Liu, Jian Sun, Shoutao Lv,*A novel throughput optimization approach in wireless systems*,Proc.of 12th IEEE International Conference ,ICCT,2010,pp.1373-1377.

[8] Mohamed A. Haleem, Chetan Nanjunda Mathur, R. Chandramouli, and K. P. Subbalakshmi, *Optimizing the security-throughput Trade-off in wireless networks with adversaries*, Proc. of 4th International Conference, ACNS, 2006, pp.448-458.

[9] Katinka Wolter, Philipp Reinecke, *Performance and Security Tradeoff*, Springer- Formal Methods for Quantitative Aspects of Programming Languages ,2010, vol. 6154, pp. 135-167.

[10] Zhang Longjun, Han Wei, Zheng Dong, Chen Kefei, *a security solution of WLAN based on public key cryptosystem*,Proc. of 11th international conference on parallel and distributed systems,ICPADS,2005,pp.422-427.

[11] Minho Shin, Justin Ma, Arunesh Mishra, and William A. Arbaughe, *wireless network security and interworking*, IEEE, vol. 94,no. 2, 2006, pp.455-466.

[12] Dushuqin, Qin Yi, *WLAN Security System based on the 802.1 and AES*, ICCASM, pp102-105.

[13] Faheem Hossam M. ,*Multiagent based security for the WLAN* , IEEE ,vol24,no.2, April 2005, pp.19-22.

