Survey on Security and Authentication Techniques of WLAN

Komalpreet Kaur[1], Gurmeet Kaur[2]
[1] PG Student, Department of Electronics and Communication Engineering, Punjabi University, Patiala, India
[2]Professor, Department of Electronics and Communication Engineering, Punjabi University, Patiala, India
Email : [1]shining4ever12@gmail.com [2]farishta02@yahoo.co.in

Abstract: Security is the most important aspect considered while using the wireless local area networks. Various techniques have been used in the past to increase the security of WLAN's while simultaneously making the authentication process faster. The paper presents the review of various such techniques that have been used in the past for the enhancement of the security and achieving fast authentication in wireless networks.

Keywords: Wireless Local Area Network, Wireless Security, Fast Authentication.

1. INTRODUCTION

In recent years, wireless local area network has gained much popularity due to the convenience and flexibility with which it can be used. But the security of the WLAN from various external threats and simultaneously achieving fast authentication also become important at the same time. Various techniques that have been used in the past for this purpose have been discussed in the section II and the conclusion of the review has been given in section III summarizing the whole discussion.

2. LITERATURE SURVEY

There has been a trend of using wireless networks as a medium of communication with the advancement of computer network technology in late twentieth century [1]. Young Yu et al. in their work in 2010 emphasized the need of using wireless local area network to replace the LAN technology due to rapid development in wireless technology and a stable, safe, efficient and convenient environment provided by it to the users to work securely and safely. Authors also analyzed the current major problems in security due to hackers or man-in-middle attacks etc., studied the existing security measures to be taken to make the communication over WLAN's safe and free of threats.

In 1997, IEEE created the first WLAN standard 802.11 with the goal to create a standardized approach for wireless communications in various domains [2]. Joon S. Park and Derrick Dicoi in their work in 2003 discussed various standards developed by IEEE for WLANs in public places and enterprises. Initially the three standards developed were IEEE 802.11b, a and g. However, these standards failed to address the security concerns and so a new standard was developed i.e. IEEE 802.11x. Various security threats were also posed by WLAN like MAC address spoofing and default configuration of access points etc.

WEP (Wired Equivalent Protocol) is a security algorithm for IEEE 802.11 wireless networks which was ratified in 1997 [3]. Peisong Ye and Guangxue discussed WEP in 2010 in the context of wireless security issues. All IEEE standards were compatible with this protocol and it was used for securing the wireless network and was based on RC4 symmetric algorithm. However it was not effective to deal with security issues because of short length and poor management of secret keys. Also since it implements Cyclic Redundancy Check (CRC)-32 algorithm which has non cryptographic value, it's vulnerable to attacks.

Deng Shiyang in 2010 discussed the comparison of existing WEP algorithm with WPA (Wi-Fi Protected Access) which was developed in 2003 and is referred to as draft 802.11i standard [4]. Further WPA2 was developed in

2004 which is shorthand for 802.11i. It was the latest patch of IEEE 802.11 standard which strengthened the authentication and also provided the new key management system thus removing the shortcomings of WEP. Concept of RSN was put forward in 802.11i. It used two kinds of data encryption and integrity protocols i.e. TKIP and CCMP. However it was susceptible to eavesdropping attacker and man-in-middle attacks.

WPA2 was an advancement of WPA and A.S.Rumale et al. in 2011 surveyed IEEE 802.11i based WPA2, also called Wi-Fi protected mode protocol popularly called as Wi-Fi Protected Access [5]. Before 802.11i was finalized, IEEE 802.11 relied on security method known as WEP, which has several well documented security problems. IEEE 802.11i introduced more advanced security features than the WEP with the concept of Robust Security Network (RSN). It uses Extensible Authentication Protocol (EAP) for the authentication phase of establishing RSNA.

Matija Sormon et al. mentioned 802.11X which is a next generation draft of IEEE. It made use of EAP (Extensible Authentication Protocol) in the integration which is a transport protocol and is used to negotiate the WLAN user's secure connection to network [6]. There are various types of EAP for achieving user efficiency and robust security, lightweight computation and forward secrecy. However all EAP methods and authentication protocols designed for WLAN's so far do not satisfy all the above properties and it showed significant delay in initial access authentication.

Different EAP types showed different properties [7]. Some fulfilled security requirements but consumed high computation energy so Chun-I Fan et al. proposed a complete EAP method in 2013 that utilizes stored secrets and passwords to verify users so that it can fully meet the requirements of RFC 4017, provide for lightweight computation and allow for forward secrecy. However it still showed significant delays in initial access authentication.

With the increasing use of WLAN, it is increasingly important to have more efficient initial link setup mechanism along with achieving security of the thus developed connection [8]. Xinhua Li et al. in 2014 proposed an efficient initial access authentication protocol i.e. FLAP which realizes the authentications and key distribution through two roundtrip messages [8]. They proved that their scheme was more secure than the four way handshake protocol and that it improved the efficiency of EAP-TLS by 94.7%. Also they presented that FLAP was compatible with 802.11i through a simple and practical method. However this existing model does not include any pre-shared information for the purpose of authentication, which may add the gap in security against the guessing attacks. Also it is based upon centralized authentication using AS (Authentication Server) connected with AP (Access Point). No security measure has been used between AS and AP for secure information exchange.

Though various protocols and standards have been developed to ensure a secured transmission of data over wireless local area networks, there is still immense scope of research in this field since with the advancement in technology, new attacking methods are being developed to breach the security. Still more efforts are required to meet the security requirements while simultaneously making the authentication process faster and efficient.

Table 1. Comparison of different Security and Authentication protocols.

Sr no	Title	Journal/ Conference	Author & Year	Findings	Weakness
1	WLAN Security: Current and Future	IEEE Computer Society.	Joon S. Park and Derrick Dicoi in 2003 .	Standards compatible with available WEP .	Eavesdropping, MAC address spoofing and default configuration of access points.

2	Security Research on WEP of WLAN	Proceedings of the Second International Symposium on Networking and Network Security.	Peisong Ye and Guangxue Yue in 2010 .	Easier and compatible with 802.11a,b,g standards.	short length and poor management of secret keys .
3	Compare of New Security Strategy with Several Other in WLAN	International Conference on Computer Engineering and Technology.	Deng Shiyang in 2010 .	Provided the new key management system.	Eavesdropping and man-in-middle attacks.
4	Implementing Improved WLAN Security	International Symposium Zadar, Croatia.	Matija Sorman, Tomislav Kovac, Damir Maurovic in 2004.	User efficiency and robust security	High computation energy.
5	Complete EAP method: User Efficient and Forward secure Authentication Protocol for IEEE 802.11 Wireless LAN's	IEEE Transactions On Parallel And Distributed Systems.	Chuan-I Fan, Yi- Hui Lin and Ruei-Hau Hsu in 2013.	Lightweight computation and provides forward secrecy.	Initial access authentication delay is very high.
6	FLAP : An Efficient WLAN Initial Access Authentication Protocol	IEEE Transactions on Parallel and Distributed Systems.	Xinghua Li, Fenye Bao, Shuxin Li, Jianfeng Ma in 2014.	Improves the efficiency of initial access by 94.7%.	1)Here the connection between Authentication Server and Access Point is assumed to be secure. 2)No security mechanism has been discussed.

3. CONCLUSION

Different techniques have been discussed by the authors to increase the security by making use of various security protocols like WEP, WPA, EAP etc. and different IEEE standards. They also presented the method to make initial access authentication efficient and faster while simultaneously increasing the security. Systems were so developed so as to make them compatible with previously developed protocols and standards.

REFERENCES

[1] Young Yu, Qun Wang and Yan Jiang, " Research on Security of the WLAN Campus Network," International Conference on E-Health Networking, Digital Ecosystems and Technologies, pp. 175-178, 2010.
[2] Joon S. Park and Derrick Dicoi, "WLAN Security: Current and Future," Published by the IEEE Computer Society, pp. 60-65, 2003.
[3] Peisong Ye and Guangxue Yue, "Security Research on WEP of WLAN," Proceedings of the Second International Symposium on Networking and Network Security, pp. 39-42, 2010.
[4] Deng Shiyang, "Compare of New Security Strategy With Several Others in WLAN," 2nd International Conference on Computer Engineering and Technology, vol. 4, pp. 24-28, 2010.
[5] A.S. Rumale and Dr. D.N. Chaudhari, " IEEE 802.11x, and WEP, EAP, WPA/WPA2," International Journal of Computer Technology and Applications, vol. 2, no. 6, pp. 1945-1950, 2011.
[6] Matija Sorman, Tomislav Kovac, Damir Maurovic, "Implementing Improved WLAN Security," 46th International Symposium Zadar, Croatia, pp. 229-234, 2004.
[7] Chun-I Fan, Yi- Hui Lin and Ruei-Hau Hsu, "Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LAN's," IEEE Transactions On Parallel And Distributed Systems, vol. 24, no. 4, pp. 672-680, 2013.
[8] Xinghua Li, Fenye Bao, Shuxin Li and Jianfeng Ma, " FLAP: An Efficient Initial Access Authentication Protocol," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 488-497, 2014.
[9] Liu, Yong-lei, and Zhi-gang Jin, "SAEW: A Security Assessment and Enhancement System of Wireless Local Area Networks (WLANs)." Wireless Personal Communications, vol. 82, no. 1, pp. 1-19, 2015.
[10] Latha, P. H., and R. Vasantha, "Novel Key-Management to Resist Illegitimate Intrusion from Rogue Access Points in WLAN." In Emerging Research in Computing, Information, Communication and Applications, Springer India, pp. 231-237, 2015.
[11] Tseng, Yuh-Min, "USIM-based EAP-TLS authentication protocol for wireless local area networks." Computer Standards & Interfaces, vol. 31, no. 1, pp. 128-136, 2009.