Comparative Analysis of Authentication Protocols For Wi-Fi Network

Nehashankardas[1], Praveen Misra[2], Ajay Sehrawat[3]

[1]Mca Mtech , usict, GGSIPUDwarka, [2]Addl. Director & Scientist E, ERNET India, [3]Project Manager, ERNET India

[1]n88jaitly@gmail.com, [2]misrap@gmail.com, [3]ajaysehrawat.1001@gmail.com

Abstract: ***The*** Wireless Local Area Network (WLAN) is becoming quite popular because it is cost-effective and easy to use. Among the networks, Wi- Fi which stands for "Wireless Fidelity" is the most prominent technology. It has now become a vital part of daily life due to the need of important information at all times of the day. But every technology has its shortcomings as well. Wi-Fi though helps in cutting costs yet it is vulnerable to security threats like replay attack or denial to services that is problematic. The paper here provides a comparative analysis of the numerous security protocols so far by elucidating on the encryption details and limitations.

Keywords: ***Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA 2), Robust Security Network (RSN), authentication, integrity***

1. INTRODUCTION

Communications help in transfer of vital information from one source to another. There are two major forms of communication which are: wired and wireless. In today's advancing world, wireless technologies have gained utmost importance due to their ease of usability but they carry a serious security issue of data tapping due to authentication errors since they use air as the main medium of communication and hence any person who has access to equipment can intercept the information. To overcome the security issue, many security protocols have been introduced and each of them is unique in its own way. The amount of efforts in securing WLAN clearly points at the huge underlying security issues. There are three main security challenges in wireless networks. One of them is confidentiality that is only the required person cannot read the encrypted message. The major problem arises due to the mode of transmission of the wireless signals which is through air and hence it seriously affects the authentication. Integrity is another security issue again due to the transmission medium where the message is not received in the format as sent by the party.This paper provides a brief overview and comparison of the security protocols till date to better understand where exactly they lack in their structure. The next section builds on the review of recent work on the security protocols. Section 3 presents a comparative table of the various security protocols till date which is followed by conclusion.

2. LITERATURE REVIEW

The first kind of security protocol is the Wired Equivalent Privacy (WEP) which was the first algorithm to secure Wireless Local Area Networks just like wired LAN. Rivest Cipher4 (RC4) stream cipher is used by WEP to secure wireless network in terms of confidentiality and CRC32 is used for data integrity. The standard specified for WEP provides support for 40-bit key only but non- standard extensions have been provided by various vendors providing support for key length 128 and 256 bits as well [1]. The process of WEP encryption is shown in Fig. 1. The encryption is followed by decryption procedure which is elucidated in fig. 2 below.

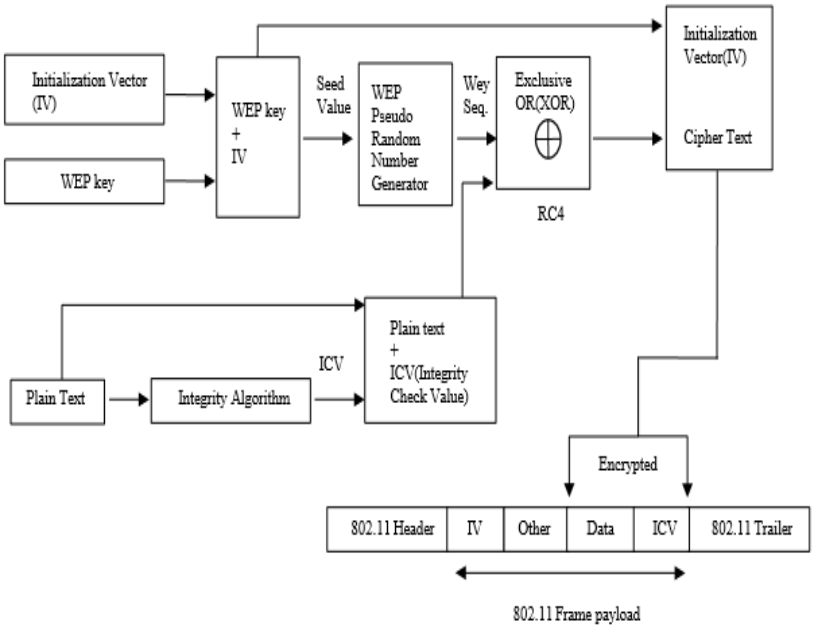

Figure 1- WEP encryption process [2]

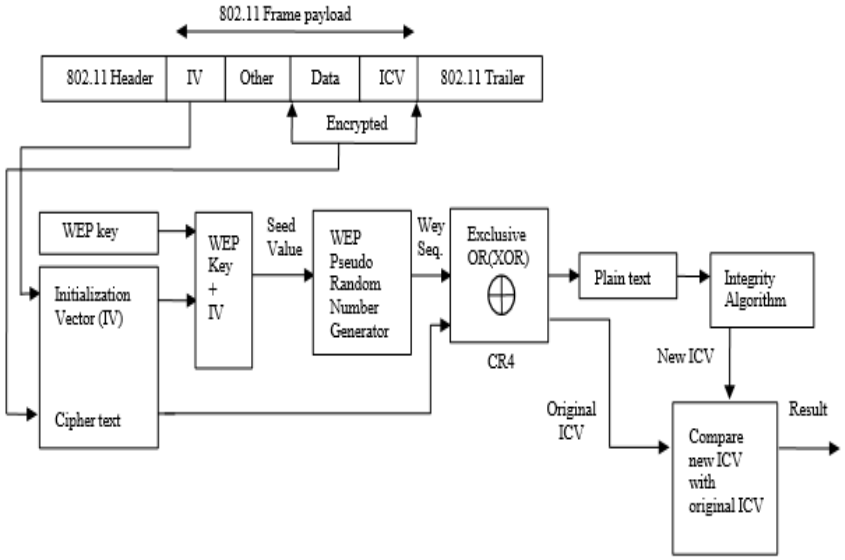

Figure 2-WEP decrypting

Wi-Fi Protected Access (WPA) is another encryption algorithm which was introduced in 2003 to overcome the faults in WEP. It was observed over quite some time that WEP was prone to lot of security attacks and hence it was recommended to go with WPA. It uses Temporal Key Integrity Protocol (TKIP) based on WEP for encryption and does not require a lot of updates. TKIP encryption works in a way where keys are changed for each packet and Michael algorithm is used to provide a message integrity check and a re-keying mechanism, hence fixing the flaws of WEP. The TKIP encryption is shown in Fig. 3. WPA has two authentication methods which are WPA-Personal (WPA-PSK) that is used at a small scale like houses. Another mechanism is the WPA-Enterprise that is used for big companies and corporations. WPA-enterprise set up 802.1x authentication by means of a Remote Authentication Dial In User Service (RADIUS) and Extensible Authentication Protocol (EAP) to provide stronger authentication ways. The Enterprise mode gives dynamic encryption keys distributed securely after a user logins with their username and password or provides a valid digital certificate. Users never see the actual encryption keys and they aren't stored on the device. WPA-Enterprises provide excellent security to the wireless network traffic.

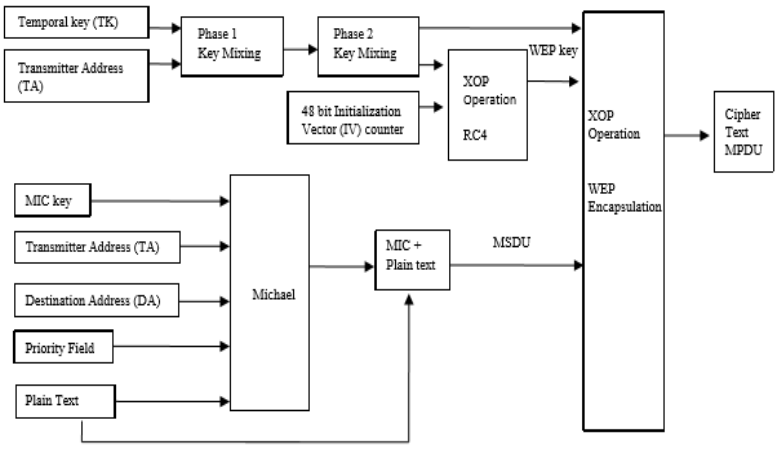

Figure 3-TKIP encryption

The WPA2 is an improvement over the protocols till yet which was available in 2006 where data encryption algorithm is changed majorly. The Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) uses a block cipher which is the Advance Encryption Standard (AES) for data encryption. Figure 4 describes the CCMP encryption process for WPA2.

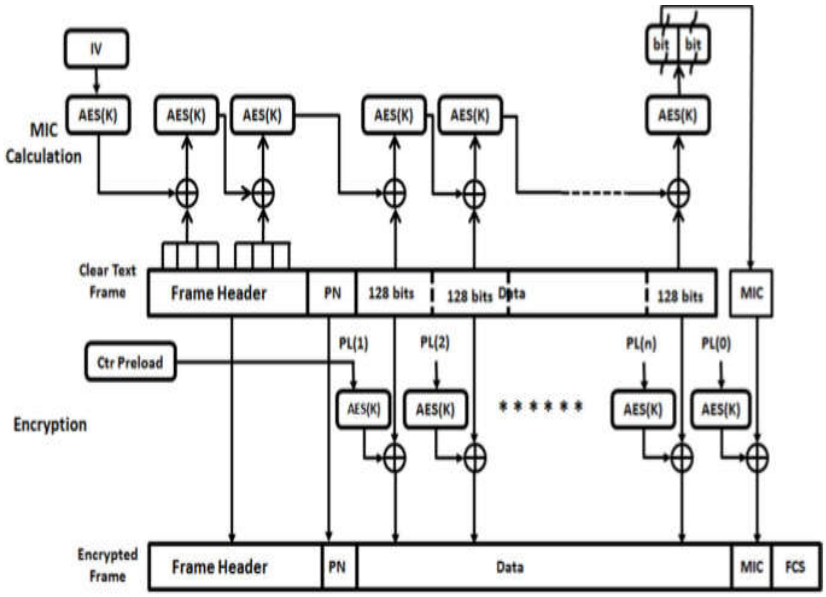

Figure 4-CCMP encryption

In [4], WEP structure has been described on sender as well as receiver side. It also lists generation of wireless security protocols. It is followed by second generation of wireless security as WPA along with major improvements taken place like message integrity code or MIC, new sequencing and re-keying mechanism. Finally, they discusses about third generation of wireless security protocol as WPA2/802.11. In [7], Erik et.al had focused over the one of the three main security protocols of wireless network namely WEP in which process and working of encryption process has been described. It also gives information about attacks that can occur in WEP. The attack process with the help of software named "Aircrack-ng" has been shown. In [8], Author has described the authentication process of WPA standard and a way of cracking WPA. After studying about the authentication protocols, they got the knowledge related to the breaking and cracking of the WPA. They hacked the WPA by using software named "Aircrack" in backtrack operating system.

3. COMPARITIVE TABLE

Mechanism features	WEP	WPA	RSN	WPA2
Encryption Key Size	40 bits	128 bits	128 bits	128 bits
Encryption Cipher Mechanism	Cipher Mechanism RC4 (Vulnerable - IV Usage)	RC4 / TKIP	AES / CCMP / TKIP	AES/CCMP
Encryption Key Per Packet	Concatenated	Mixed	No need	Mixed
Encryption Key Change	None	For all packets	No need	For all packets
IV Size	24 bits	48 bits	48 bits	48 bits
Authentication	Weak	802.1x – EAP	802.1x - EAP	WPA2-personal and WPA2-enterprise
Data Integrity	CRC 32 - ICV	MIC (Michael)	CCM	Cipher block chaining message authentication code (CBC-MAC)
LIMITATIONS	Authentication issues Absence of key management Low protection in case of replay Short IV (Initialization vector) which is reused that can cause data decryption without right key. Forgery of packets by third party members and huge flooding of huge packets.	Very vulnerable to dictionary attacks if there is weak passphrase Vulnerable to Denial of service (DOS) attack, WPA-PSK Attack Huge data packet size causing huge transmissions	Not easy to add hardware and requires proper configuring Delay in response may be there due to major authentication issues.	Huge risks of DOS attacks, brute force attack Poorly encrypted systems pose security risk Legacy hardware not supported. Very expensive

4. CONCLUSION

The various security protocols in the field of wireless networks have certain boons and banes. The security protocol has to be chosen depending on the needs of the household or corporation. Even though most of them have authentication and integrity issues due to the transmission of signals through air but every other has been an improvement over the preceding protocol. Wireless local area networks have become a part of our daily life because they are cost-effective but the protocol must be suited by looking at pros and cons to overcome security concerns as described in the paper.

References

[1] Baek, K. H., Smith, S. W., &Kotz, D. (2004). A Survey of WPA and 802.11 i RSN Authentication Protocols. Technical Report TR2004-524, Dartmouth College Computer Science.

[2] Wong, S. (2003). The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. URL: http://www. sans. org/rr/whitepapers/wireless/1109. php Retrieved, 28(7), 05.

[3] Moon, J., & Jung, I. Y. (2017). Authentication for Wireless Personal Area Network. Advanced Science Letters, 23(10), 9713-9717.

[4] Lashkari, A. H., Danesh, M. M. S., &Samadi, B. (2009, August). A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i).In Computer Science and Information Technology, 2009.ICCSIT 2009. 2nd IEEE International Conference on (pp. 48-52). IEEE.

[5] Pandikumar, T., &Yesuf, M. A. (2017). Wi-Fi Security and Test Bed Implementation for WEP and WPA Cracking. International Journal of Engineering Science, 13571.

[6] Martellini, M., Abaimov, S., Gaycken, S., & Wilson, C. (2017). Vulnerabilities and Security Issues.In Information Security of Highly Critical Wireless Networks (pp. 11-15).Springer International Publishing.

[7] Tews, E. (2007). Attacks on the WEP protocol. IACR Cryptology ePrint Archive, 2007, 471.

[8] Ambavkar, P. S., Patil, P. U., Meshram, B. B., &Swamy, P. K. (2012). WPA exploitation in the world of wireless network. Int J Adv Res ComputEngTechnol, 1(4), 609-618.