International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V70I10P102

Volume 70 Issue 10, 8-12, October 2022

Review Article

Comparative Analysis of Security and Privacy Protocols in Wireless Communication

R. Lakshmi[1], Aanchal Sharma[2], S. Bhuvan[3], B. Chinmay[4], G. M. Megha[5]

[1,2,3,4,5] *Department of Computer Science and Engineering, RNSIT, India*

Received: 28 August 2022 Revised: 03 October 2022 Accepted: 15 October 2022 Published: 26 October 2022

Abstract *- The rapid growth of popularity in wireless technologies has led to the source of inventions for more and more resilient protocols that thwart security and privacy threats. Wi-Fi protocols have gained immense interest in present wireless technology because of their flexibility, convenience, and cost-effectiveness. Apart from these features, the protocols have to emphasize also on privacy and security for securing communications over the wireless medium. This paper highlights the various Wi-Fi protocols, from the very basic WEP to widely implemented WPA2 and the next robust WPA3. The paper also concentrates on the vulnerabilities and strengths of each protocol. Each algorithm's key generation mechanisms are unique and improved in each next technology to eradicate the previous vulnerability. The AES algorithm mitigates the susceptible nature of the RC4 algorithm in WEP and WPA in WPA2. The latest technology is WPA3, which provides a vast second defense line for networks with weak passwords rather than focusing only on encryption strength.*

Keywords *- Wi-Fi, Security, Privacy, WEP, WPA, WPA2, WPA3, Keys, Encryption.*

1. Introduction

Wi-Fi technology is used to connect various devices over the internet. Wireless networks may be vulnerable to hackers. Unauthorized users may steal meaningful information, resulting in a great loss. And this iswhere the concept of privacy and security comes in. Eavesdropping on wireless communication may allow hackers to access wireless networks. The malevolent codeincludes spyware, worms, viruses, trojans, or any other risky programs that may cause damage to the files or maylead to a system crash

Wi-Fi security ensures that the networks and devices connected in a wireless medium are safe from intruders[10]. Without Wi-Fi security, any network device, like a router or wireless access points, could be easily trespassed on by the intruder without any consent of the user. It is risky for organizations and users to use an unsecured Wi-Fi network, as there might be a chance of stealing the user's personal information or sensitive data. Wi-Fi security creates a barrier by encrypting private information, such as network requests or files transferred over the airwaves. Compared to a wired network, the wireless network is now dominating the world by providing a network to every possible areaat a lower cost. Afterward, concerns about privacy and security led the government of Sweden to implement security measures. It explains how aware the country council is about its security implementations. The processof increasing security is never-ending and keeps running in a loop.

2. WEP (Wired Equivalent Privacy)

WEP protocol is derived from the IEEE 802.11 [8] standard. The main issue concerned with wireless networks is data security and privacy [1]. To protect data, a protocol was needed, and hence Wi-Fi Alliance introduced WEP in 1997. Originally called Wired Equivalent Privacy, WEP was designed to provide the same level of safety and confidentiality as wired local area networks. It used an encryption algorithm known as the RC4 algorithm for data security. It initially used a 64-bit key size but was upgraded to 128-bit and 256-bit when a greater level of security was needed [2].

A WEP is a unique key that is used for encrypting all the traffic in the network. Traffic in the network was encrypted using the same key across all the devices. Its key was 40 bits in size, and a 3-byte random numbergenerated by a computer was added with the WEP key, which is called an initialization vector (IV). At the receiving end, the IV will be removed first, followed by the decryption of the cipher text [1].

2.1. How WEP works?

A keystream is produced by processing the initialization vectors (IVs) and WEP keys through the R4 algorithm. The Cyclic Redundancy Code (CRC) is computed and finally added to the plain data. Later, the cipher message is derived through the XOR function between the data obtained from the previous step and the keystream. In this process, the IV will be prepended or appended to the ciphertext before transmission. The reverse procedure is then applied at the receiving end.

In the same way, the key is generated using the shared key and the IV. Then using the RC4 algorithm, the keystreams are generated. The XOR operation is then performed between the message that arrived and the keystream[1].

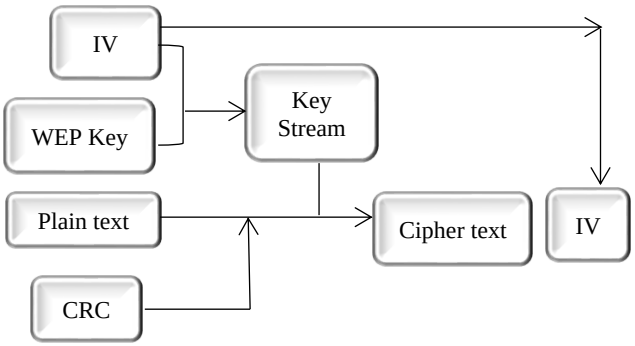

Fig. 1 WEP Working

3. WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access (WPA) was presented by IEEE 802.11 Task Group 1 as a new protocol by improvising the features of WEP. WPA uses a protocol called TKIP for encryption. TKIP is a suite of algorithms that uses RC4 stream cipher for basic encryption. Still, it differs from WEP by using a Message Integrity Check (MIC), Initialization Vector (IV), and key mixing for each packet[1]. The shared key generates several other keys, unlike WEP, which uses the shared key directly for encryption. This protocol relies on the concept of the per-packet key that allows 128-bit keys to be generated dynamically for each packet [4]. It is less vulnerable to attacks than WEP. WPA utilizes Message Integrity Check(MIC) to ensure data integrity, which would prevent attackers from modifying and sharing erroneous data packets. The hash function generated a new key for each packet using the IV sequence and the TKIP key. TKIP is termed a temporal key as it changes as time elapses.

A Generation of the key using TKIP consists of 2 phases: The first phase is the computation of the hash function, which uses the temporary key of the session, the 32-bit IV sequence, and the MAC address of the sender. When the session's temporary key changes, this stage is calculated. The second stage involves calculating the hash function based on the lower 16-bits of IV and the output of phase 1. The output is keystream containing 128-bits.

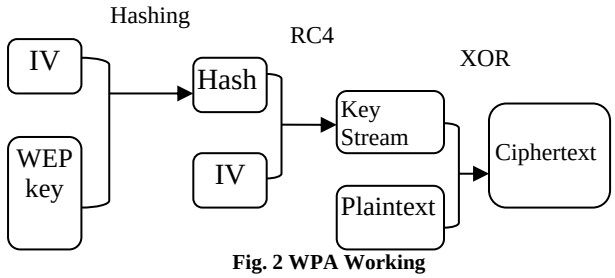

Fig. 2 WPA Working

After the hash function is generated, the base key and IV are combined, and the RC4 algorithm is applied. The result is used to generate sequential keys. Then the plain textis XORed with the sequential key to obtain the encrypted message. IV was increased from 24-bit (in WEP) to 48-bit (in WPA).

WPA authentication generally works in two approaches: the Pre-Shared Key (PSK) and Enterprise mode.WPA Personal, also known as WPA Pre Shared Key (WPA- PSK), is typically used in smaller networks without the intervention of an authentication server. The devices use a bit key size of 256 bits to authenticate themselves to the access points (AP), and the shared key is never transmitted between clients and APs. In this method, WPA and the client use a 4-way-handshake to authenticate the users. During the handshake, the first four encryption messages are exchanged between the client and the Access points

3.1. WPA 4-Way Handshake

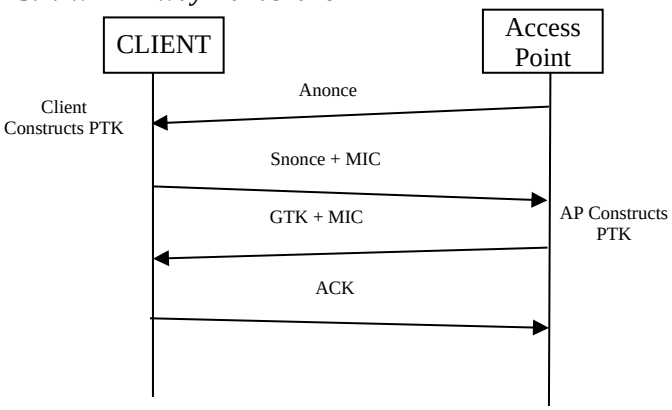

Fig. 3 WPA 4-way Handshake

A first handshake is commenced by the AP's sending Anonce to the client. As soon as the Anonce is received, the client generates the Snonce. As it already knows the MAC address of the AP and other elements to construct the PTK, the client constructs the PTK.

PTK = PMK +Anonce +Snonce +MAC(client) +MAC(AP)

As soon as the PTK is formed, the client sends the already generated Snonce to the AP, which starts the second handshake. After that, the access point constructs PTK with the aid of Snonce and other known elements. Additionally, the client sends a MIC to the access point to verify this message. AP transmits the GTK and the MIC as part of the third handshake. During the fourth handshake, the client acknowledged that all keys had been installed.

PMK:- Pairwise Master Key [key derived fromPSK or 802.1x authentication]
Anonce:- Random number created by the Accesspoint
Snonce:- Random number created by the client
MAC :- MAC address
PTK:- Pairwise Transient Key [encrypts all unicast traffic]

The second authentication method is Enterprise mode. This mode may be more complex to implement, but it guarantees to be more secure. In this mode, the users' authentication depends on a method called the 802.1x

authentication standard. It provides central control over authentication using a single server called the Radius server. This method uses Extended Extensible Authentication Protocol (EAP) which has five norms.

Data security was improved by using the WPA2 protocol, which was upgraded from WPA.

4. WPA 2 (Wi-Fi Protected Access 2)

An elevation of WPA, which is an amendment to the IEEE 802.11i standards, is WPA2. Due to WEP's security weaknesses and because WPA uses only a subset of the IEEE 802.11i standard policy, it is deemed a better alternative to WEP. WPA2 uses a part of AES(Advanced Encryption Standard) called Counter mode, Cipher Block Chaining, and Message Authentication code (MAC) protocol (CCMP) which helps provide both integrity and data security [13]. It is currently possible to use WPA and WPA2 security protocols with the currently used Wi-Fi routers. WEP and WPA both use the RC4 stream cipher. The AES algorithm proves tobe more secure. Generally, the WPA2 standard is categorized into two divisions: encryption and authentication. The major encryption algorithm is AES, and TKIP is preferred in existing WAP hardware for backward compatibility. Concerning authentication, WPA uses exactly the same method as WPA.

4.1. Counter Mode with Cipher Block Chaining MAC Protocol (CCMP)

CCMP is derived based on the AES. It is a block cipher mode that uses AES for encryption. It employs a key of 128 bits, and the same number of bits is also taken as the sizeof the block. Along with this, a 48-bit long IV is also utilized, termed CCM Nonce. A MAC Protocol Data Unit(MPDU) is an exchange of messages between devices in a communication system. The packet numbers are incremented to get a new number for each MPDU. It also contains the data that must be sent to the destination.

MPDUs are formed by combining many sections.

- It has a MAC header that contains the source and destination MAC addresses.
- Next, it has a CCMP header that contains the packetnumber and a key.
- Additionally, it contains the duty unit which will besent to the destination and MIC, i.e., Message Integrity Check, to ensure the data integrity.
- For detecting and correcting errors, a field called FCS is also present.

The data field and MIC are encrypted using AES encryption and later delivered to the destination. Soon after the receiver obtains the data, it calculates MIC. It is considered successful if it is the same as the MIC received.

[17] Proposes a Revised AES (RAES) algorithm for enhancing the security of the existing Rijndael algorithm. This new algorithm has proven to perform Sac analysis better than the existing one. [4] Suggests the usage of the RAES algorithm in the WPA2 encryption process to achieve better privacy and confidentiality in wireless communication.

5. WPA3 (Wi-Fi Protected Access 3)

Wi-Fi Protected Access 3, abbreviated as WPA3, was launched in 2018 by the Wi-Fi alliance. It belongs to the third iteration of the security certification program. Among all the networks being used currently, WPA3 is comparatively moresecure. At the consumer level, WPA3 uses 128-bit encryption, which is huge in number when compared to other networks. WPA3 also aims at providing a vast second defense line for networks having weak passwords rather than focusing only on encryption strength. Its advantage over other networks is that it allows users to use weak passwords with the same level of security as strong ones, allowing them to remember passwords without issues in security.

Simultaneous Authentication of Equals (SAE) is one principle algorithm in WPA3. Earlier, attackers would decrypt an encrypted message being transmitted by trying several password combinations, this technique is called Brute Forcing. WPA3 eliminates cyber-attacks such as Brute forcing to keep the data safe and secure. The main concept SAE focuses on is that the messages will be allowed to decrypt only once after transmission. It would reduce the possibility of networks with weak passwords prone to attacks and would not allow attackers to try to steal the data multiple times.

We usually prefer to connect to more secure connections to keep our data safe from attacks. Public networks are more vulnerable to such attacks, and we are responsible for always using secure networks. Although WPA3 proves to be more secure than other networks, it is yet to be implemented in devices that do not support WPA3 service, and it would take time to do so.

The following are some of the SAE features which replaced the Pre-Shared Key:

- Individualized data encryption: This refers to theuse of QR codes for easy access to the data.
- Simultaneous authentication of equal protocol: Providing a secure handshake.
- Strong Brute Force attack protection: A single chance is given to decrypt the message.
- Larger session keys: It provides a larger session keywith 198-bit encryption

There is another technique called PFS (Perfect Forward Secrecy), which was earlier used.

Perfect Forward Secrecy is a system that modifies the key information automatically at frequent intervals and is one of the methods used for transmission. It generates a unique key for encryption and decryption, which, when compromised, would not cause harm to the data being transmitted. Hence it proves to be advantageous over all other systems. With PFS, a key would be valid for a

stipulatedtime and less prone to hacker attacks.

The major characteristics of WPA3, which uses SAE over PFS, are:

- The password can be selected without any restrictions (National Password Selection)
- It is easier to use
- Protects data in data traffic even when the key is compromised (Forward Secrecy)

WPA3 is further divided into two types: WPA3 Personal and WPA3 Enterprise.

The WPA3 personal standard provides better password authentication even when using a weak combination. It uses Simultaneous Authentication of Equals to provide strong fortification against password guessing. as mentioned before,it is a secure key establishment protocol.

WPA3 Personal is further divided into two categories:

- WPA3 only.
- WPA3 Transition Mode.

Using 192-bit encryption, WPA3 Enterprise presents a higher level of security to the community transmitting sensitive data. There are very few enhancementsmade from WPA2 to WPA3, and WPA2 continues to be comfy and usable. One of the most important advancements in WPA3 is the RADIUS server.

The Remote validation Dial-In User Service is a centralized authorization and computing management protocol for connecting and using network services. A 'RADIUS' server allows the storage of user profiles in a central database. Thus, if we have this server, you have complete control over who can access your network. Using this server will prevent outsiders from accessing confidential information. It is also possible to assign individual users with unique permissions on the network. It has also been discovered that there are vulnerabilities and flaws in theWPA3 protocol that could allow advisories to rupture Wi-Fi passwords and enter into encrypted traffic exchangedbetween the devices.

There are 2 main imperfections in WPA3 are:

1. Downgrade Attacks
2. Side-Channel leaks.

The following devices are compatible with WPA3:

- iPhone 7 or next-generation device
- PCI adaptors, routers, Deco home mesh Wi-Fi systems, etc.
- iPad 5th generation or next generation device.

The devices mentioned above previously supported these deprecated protocols:

- WEP opens
- TKIP (Temporal key integrity protocol)
- Shared WEP
- Dynamic WEP

Clearly, they are no longer secure from the standpoint ofsecurity, performance, reliability, and compatibility.

6. Comparative Analysis

Table. 1 Comparison of various protocols

PROPERTIES	WEP	WPA	WPA2
Encryption Method	RC4	RC4 with TKIP	AES-CCMP
Encryption Key Size	40 bits / 104 bits	128 bits	128 bits
Data Integrity	Cyclic Redundancy Check(CRC)	MessageIntegrityCode (MIC)	Cipher blockchaining message authentication code (CBC-MAC)
Cipher type	Stream	Stream	Block
Authentication	WEP OpenWEP Shared	WPA-PSK WPA-Enterprise	WPA2-PersonalWPA2-Enterprise
Security level	Low	Medium	High
Passwordlength	5 / 13 characters	8 to 63 characters	8 to 63 characters

7. Conclusion

Paper has presented the various Wi-Fi protocols with their strength and weaknesses. It covered the aspects of key generation and encryption process and how the vulnerabilities can be mitigated through enhancements. The basic WEP protocol is fragile concerning IVs and keystreams and is eradicated in WPA with the procedure of TKIP and MIC. WPA2 is a widely implemented protocol by employing CCMP and the most robust AES algorithm for encryption. The most recent protocol is WPA3 which is intended to provide a second line of defense in communications comprising weak passwords rather than focusing only on the encryption strength.

References

[1] Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaidy, and Anwar Althubyani, "A Survey on Wi-Fi Protocols: WPA and WPA2," *Springer-Verlag Berlin Heidelberg*, 2014.

[2] Saurabh Malgaonkar, Rohan Patil, Aishwarya Rai, Aastha Singh, "Research on Wi-Fi Security Protocols," *International Journal of Computer Applications* (0975 – 8887), vol. 164, no. 3, 2017.

[3] Mayank Verma, Jitendra Yadav, "Comparative Analysis: Wi-Fi Security Protocols," *International Journal of Engineering Research & Technology (IJERT)*, Vol. 2 , no. 12, 2013.

[4] Guru Karthik S, Lakshmi R, Rahul Bhat T.R, "Extending the confidentiality in Wi-Fi protocol - WPA2 using Revised Advanced Encryption Standard (RAES) Algorithm," *International Journal of Engineering Applied and Management Sciences Paradigms (IJEAM)*, vol. 54, no. 1, 2019.

[5] Mylonas, P., Mavridis, I.P., Androulakis, A.-I.E.,Halkias, A.B, "Real-life paradigms of wireless network security attacks," *IEEE Xplore*, 2011.

[6] Sukhija, S., Gupta, S, "Wireless Network Security Protocols a Comparative Study," *Semantic Scholar*, 2012.

[7] Frank H. Katz, "WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?" 2016.

[8] Mathews, M., Hunt, R, "Evolution of Wireless LAN Security Architecture to IEEE 802.11i (WPA2)," *In: Proceedings of the fourth IASTED Asian Conferenceon Communication Systems and Networks*, 2007.

[9] Ciampa, Mark , "CWNA Guide to Wireless LANS," *Networking*, Thomson.

[10] Sukhija, S., Gupta, S, "Wireless Network Security Protocols a Comparative Study," *Semantic Scholar*, 2012.

[11] Lehembre, G, "Wi-Fi security – WEP, *WPA and WPA2*, 2005.

[12] Katz, F.H, "WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?" *In: 2010 4th Annual Computer Security Conference (CSC 2010), Coastal Carolina University*, Myrtle Beach, SC, April 15-16 , 2015.

[13] Frankel, S., Eydt, B., Owens, L., Scarfone, K, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," NIST Special Publication 800- 97, *National Institute of Standards and Technology* , 2007.

[14] Sukhija, S., Gupta, S, "Wireless Network Security Protocols a Comparative Study," *Semantic Scholar*, 2012.

[15] Wolter Lemstra, Vic Hayes, John Groenewegen, "The Innovation Journey of Wi-Fi: The Road to Global Success," *Cambridge University Press)*

[16] Bulk, Frank, "(27/1/2006) Learn the basics of WPA2 Wi-Fi security," *Network Computing*, 2013. http://www.informationweek.com/story/showArticle.jht ml?articleID=1 7710533 (accessed March 18, 2013).

[17] Lakshmi R, Mohan H S, "Implementation and Performance Analysis of Modified AES Algorithm with Key-Dependent Dynamic SBox and Key Multiplication," *International Journal of Mathematics and Computer Applications Research (IJMCAR)*, Vol. 5, no. 3, pp. 1-10, 2015. ISSN(P): 2249- 6955; ISSN(E): 2249-8060,

[18] Ritu Ratra, Preeti Gulia, "Privacy Preserving Data Mining: Techniques and Algorithms," *International Journal of Engineering Trends and Technology*, vol. 68, no. 11, pp. 56-62.

[19] Wang, Y., Jin, Z., Zhao, X, "Practical Defence against WEP and WPA-PSK Attack for WLAN," *IEEE*, 2010.

[20] Scarfone, K., Dicoi, D., Sexton, M., Tibbs, C, "Recommendations of the National Institute of Standards and Technology," *Guide to Securing Legacy IEEE 802.11 Wireless Networks* , 2008.

[21] "Cracking Wireless," Ryan Curtin Ryan at, igglybob.com

[22] Saleem Ahmed, "Security and Privacy in Smart Cities: Challenges and Opportunities," *International Journal of Engineering Trends and Technology*, vol. 68, no. 2, pp. 1-8, 2020.

[23] Bulbul, H.I., Batmaz, I., Ozel, M, "Wireless Network Security: Comparison of WEP (WiredEquivalent Privacy) Mechanism," *WPA (Wi-Fi ProtectedAccess) and RSN (Robust Security Network) Security Protocols*, e-Forensics 2008, Adelaide, Australia, January 21-23, 2008.

[24] Arockiam, L., Vani, B, "A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network," *International Journal on Computer Science and Engineering*, vol. 2, no. 5, pp. 1563–1571, 2010.

[25] Beck, M., Tews, E, "Practical Attacks Against WEP and WPA‖. In: WiSec 2009," *Proceedings of the Second ACM Conference on Wireless Network Security*, New York, 2009.

[26] Lashkari, A.H., Danesh, M.M.S., Samadi, B.: FCSIT, " A Survey on Wireless Security Protocols (WEP, WPA and WPA2/802.11i)," *In: 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT* , 2009.

[27] Park, S.H., Ganz, A., Ganz, Z, "Security protocol for IEEE 802.11 wireless local area network," *Mobile Networks and Applications*, vol. 3 , 1998.