A Critical Review on Secure Authentication in Wireless Network

Manoj Diwakar, Prabhishek Singh, Pramod Kumar, Kartikay Tiwari, and Shashi Bhushan

Abstract Wireless network connectivity is capable of addressing various mobility issues and helps users of smartphones to navigate around and remain connected to the network without taking control of their location. The 802.11 architecture is similar to cell architecture. This paper provides a short overview of wireless networks, their benefits over wired networks and urgent exposure to security concerns. The 802.11 architecture and the different facilities it delivers are pursued and then the motivation for doing the study is followed.

Keywords Handshake protocol · Network security · Denial of service · WLAN

1 Introduction

Wireless network communication is able to address various mobility issues and provides freedom to mobile users to roam around and still remaining connected to the network, without worrying about their location [1–6]. The 802.11 architecture is similar to the cellular architecture. The whole system is divided into different cells called basic service set (BSS) where each cell is controlled by its respective stations (access points). Now, in order to support mobility issues, AP of the respective cells are connected by some backbone system, generally a distributed system, which is a wired network [7–12]. This whole system of interconnected cells which includes

M. Diwakar
Graphic Era Deemed to be University, Dehradun, India

P. Singh (✉)
Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India

P. Kumar
Krishna Engineering College, Ghaziabad, Uttar Pradesh, India

K. Tiwari
Thapar University, Patiala, Punjab, India

S. Bhushan
UPES, Dehradun, India

A. Tomar et al. (eds.), *Machine Learning, Advances in Computing, Renewable Energy and Communication*, Lecture Notes in Electrical Engineering 768,
https://doi.org/10.1007/978-981-16-2354-7_55

their respective APs and the distribution system is called extended service set (ESS) [13]. Various components of the architecture are[1]:

- **Stations**

Any entity that can be connected to a wireless network is termed as stations. These stations are generally battery-driven and include laptops, palmtops and notebooks [14–18]. All of them have a network interface card (NIC) which has a unique MAC address and helps in identifying the system over the network. Stations can be classified into two sub-categories [3]: access points and clients. Access points are normal wireless clients with have higher computational power and other resources. They are connected to a distributed system which in turn is connected to other wired networks and thus enables wireless clients to transmit and receive radio frequencies. Wireless clients include mobile and portable devices like palmtops, notebooks having wireless network interface card.

- **Basic Service Set**

It is the atomic unit of IEEE 802.11 WLAN comprising some stations which run the copy of similar MAC protocol and compete with one other for getting access to the wireless medium shared between them. The BSS resembles the cell as present in cellular architecture. Every BSS has its id known as BSSID that serves the wireless clients within that BSS. BSS exists in two modes [19–23]: independent BSS and infrastructure BSS. IBSS is generally like ad hoc networks in which stations communicate with one another in a direct manner and is set up for a very short period or interval; when the communication ends, it gets dissolved while in infrastructure BSSs if two nodes wish to communicate, then they are able to perform this by means of AP, i.e., first they send data to AP which then sends it to other communicating nodes [24–28].

- **Extended Service Set**

BSS makes the communication over a small range, i.e., within the coverage range of AP. Therefore, in order to enhance and lengthen or expand the range of the AP, i.e., the coverage area, BSSs are linked to each other by having some backbone network (distributed system) in the back of the network to form a region known as extended service set (ESS) [29]. All the APs within the ESS have the same service SET identifier (SSID).

- **Distributed System**

The main role of DS is to connect several BSSs to the wired network to result in an ESS. Several BSSs are connected via their respective APs which are connected to a

[1] Please note that the LNEE Editorial assumes that all authors have used the Western naming convention, with given names preceding surnames. This determines the structure of the names in the running heads and the author index.

distributed system which in turn gets connected to different 802.1x wired networks [4]. When a frame is received by the distributed system, it checks the MAC address and relays it to the appropriate AP, which in turn relays the frame to the destination client.

- **Distribution System Services**

The major role of these services is to interconnect various BSSs with one another with the help of connecting their respective APs to the distributed system so that services of the wired networks can be extended to WLANs by connecting DS to integrated IEEE802.1x LANs. These services [11–15] can be implemented within the respective APs of the BSSs or can be provided by using some special-purpose devices which are attached to the DS.

- **Station Services**

Providing station services is a basic feature of any IEEE 802.11 complying station which also includes access points [16–20]. These services are essential in order to deliver messages to the intended recipients. They provide confidentiality and privacy services in order to protect the messages being communicated between the stations. Also included are the authentication services in order to confirm the identity of the client so that they can avail access to other services.

2 IEEE 802.1X Framework

It provides a port-based access control mechanism to devices connected through various 802 LANs for authorization and authentication services [20]. It also serves the purpose of distributing the secure keys by use of various encryption techniques between different compatible clients, supplicants and access points, thus optimizing the public key authentication.

It has been proved that earlier methods of authentication, namely open system authentication and shared key authentication are not secure, therefore in order to counter the attacks, IEEE802.11i defined RSNA as a mechanism to provide strong mutual authentication and generate fresh temporal keys in order to provide strong confidentiality services. In network discovery, a wireless client always searches the available channels for these Beacon frames and responds with Beacon response frames to the access points depending on the available signal strength. In authentication and association, once the supplicant is authenticated, it sends the association request frame to the AP and indicates its security capabilities. AP replies with the association response frame indicating the association result. After this stage, the client/supplicant is said to be authenticated and associated.

3 A Comparative Study

However, the authentication achieved is not very strong, therefore subsequent phases are followed in order to make it more secure. Here, the RADIUS server and the client execute a mutual authentication protocol, i.e., EAP-TLS between them and AP just acting as a relay to forward messages. At the end of this stage, a shared key called PMK is generated between the two which is used for the derivation of subsequent keys. The authenticator only permits the 802.1X messages to allow it through port (off) before the client is being authenticated. The EAP messages or frames from the client are then relayed to the authentication server by means of an authenticator port access entity (PAE) [20].

3.1 Temporal Key Integrity Protocol

With many inherent weaknesses found in the use of WEP, a new scheme was introduced which can provide far better security. An attacker can easily get the secret key being used in the WEP technique within few minutes and in some situations even can decrypt the packets without having any apprehension about the secret key, thus is prone to very serious attacks. TKIP [18, 22] was used on top of an already used scheme, i.e., WEP in order to make it more secure and hide its weaknesses.

TKIP made many modifications in WEP which can limit many of the earlier attacks on WEP:

- Use of MIC as a means to protect the integrity of the generated message by making use of a new algorithm called Michael.
- Involving the use of a per-packet sequence counter in order to protect the entities from replay attacks.
- Use of per-packet key-mixing technique (function) in order to make it secure against weak-key attacks of the attacker on WEP secret key.
- Use of some countermeasures to handle attacks against MIC since due to some design constraints it is not deemed to be very secure.

3.2 Vulnerabilities of IEEE802.11i Standard

- Prone to denial of service (DoS) and DoS flooding attacks like RF jamming, session hijacking.
- Unprotected management frames lead to pinpoint the location of devices, thus making them vulnerable to DoS attacks and to guess the network topology.
- Control frames are also unprotected and send in plain text over a network.
- Possibility of de-authentication and disassociation attacks is very high.
- Vulnerable to offline guessing attacks.

- No protection for EAPOL frames.

The temporal key (TK) is generated by means of the EAPOL handshake procedure. The very first step of this technique is to get the per-packet key which is done in two phases. The first phase key mixing procedure takes a temporal key (TK), transmitting station address (TA) and 32 MSBs of TKIP sequence counter (TSC) as its input and outputs TTAK which is of 80 bits. The second phase key mixing procedure takes TK, TTAK and 16 LSBs of TSC as its input which results in the generation of WEP seed represented as 128-bit key (104-bit RC4 secret key and 24-bit IV for WEP).

TKIP also introduces a mechanism for checking the integrity of the message called MIC which is generated by means of the Michael algorithm which takes three inputs. Then the computed MPDU plus generated MIC is fragmented based on network packet size if required which is then send for WEP encapsulation as plain text.

3.3 Flaws in WPA

- Use of pre-shared keys as an alternate mechanism for providing authentication is a serious drawback.
- Dictionary or brute-force attacks are still possible.
- Vulnerable to DoS and DoS flooding attacks.

3.4 Wi-Fi Protected Access (WPA)

In 2002, Wi-Fi Alliance (WFA) presented a new mechanism called WPA [10] as a temporary or provisional solution to counter the attacks which were prevalent in WEP. Some of its benefits over WEP are:

- Usage of temporal key integrity protocol (TKIP) for providing confidential services.
- More secure user authentication mechanism.
- Proper use of the RC4 algorithm makes networks more secure.
- Use of more complex and secure hash functions.
- Avoids re-use of the initialization vector.

There exist two modes of WPA, namely enterprise WPA; personal/WPA-PSK (pre-shared key). In enterprise mode, there is a centralized network entity called RADIUS server which provides services related to authentication, authorization and access control, while in personal mode there is no such concept of the RADIUS server and the client needs to know the WPA shared key generated by the AP and SSID of the network to be connected.

3.5 Working of WEP

WEP was the very first technique to provide security in WLAN by use of the RC4 encryption algorithm [1, 2]. Its working at sender and receiver side can be explained as follows:

3.5.1 At Sender Side

As shown in Fig. 1 at the start, both the sender and receiver share a secret key K_s. Assume S to be the supplicant/client which sends M (message) to the receiver at the other side [1, 18]. S then also calculates checksum known as cyclic redundancy check, which is then appended or concatenated with message M. Let this be represented as X = (M, CRC). Then supplicant encrypts this X using the RC4 encryption algorithm that takes two inputs to generate a keystream KS. The two inputs are:

(1) Shared key K_s of length 40 bits.
(2) An initial seed, which is called initialization vector IV.

Now this keystream KS is XORed with X which in turn produces the desired ciphertext C. The major drawback is that IV is sent without using any encryption algorithm, i.e., clear text is communicated over the network. To re-produce the original keystream, the generated ciphertext is XORed with the same keystream KS, i.e.

$KS \oplus X = ((X \oplus KS) \oplus KS) = X \oplus (KS \oplus KS) = X.$

But in order for the receiver to reconstruct KS, IV should be known. Therefore, IV is appended to ciphertext before being sent over the network. The major drawback is

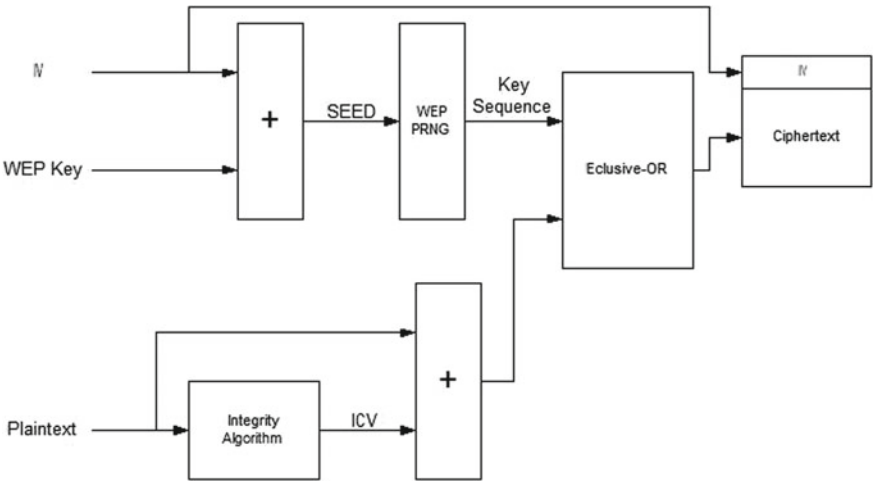

Fig. 1 WEP encryption algorithm (sender side)

that IV is sent without using any encryption algorithm, i.e., clear text is communicated over the network.

3.5.2 At the Recipient Side

As shown in Fig. 2, the WEP key and initialization vector is passed through the pseudorandom generator in order to obtain the keystream which is then XORed with the ciphertext to get the IV and the plaintext combination [2]. Now the plaintext is separated from the initialization vector and plaintext is passed through the integrity algorithm to get the new initialization vector IV_1, which is then compared with the received IV.

3.6 Flaws in WEP

WEP is considered very weak and it has been verified and justified that the WEP secret key can be broken within few minutes by the attacker. The major flaws [2–10] in WEP which make it insecure and vulnerable to various attacks are:

- Use of 24-bit initialization vector which exposes it to diverse attacks since it is of very short length and is appended with ciphertext as it is without using any encryption technique.
- No mechanism to prevent replay attacks.
- No support for key management and mutual authentication.
- Improper use of RC4 algorithm for providing privacy and authentication services since at every stage of RC4 encryption the same keystream is being used for encryption.
- Use of a 40-bit WEP key for encryption has been proven to be insecure as the key can be broken within few minutes. Therefore, a larger key of 128 bits is suggested.

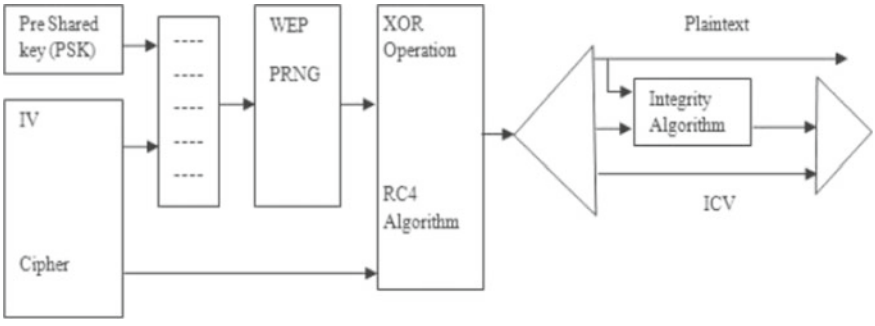

Fig. 2 WEP decryption algorithm (recipient side)

- Data source authentication: There is no mechanism for the source of data being authenticated. The use of CRCs permits attackers to frame their fake messages which have the same CRC as of original message and impersonate them as they are being originated and arrived from an authentic or known entity. Using MAC can be a very good measure in order to prevent this type of attack as they are used for data source authentication. Other measures can be to make CRC inaccessible to attackers by encrypting it or applying some kind of technique, but WEP failed to achieve this.
- Use of only one mechanism to implement all security services which are presently based on data privacy service in case of WEP which is also a major drawback of any security service.

3.7 Enhancements Over WEP

In order to counter the inherent flaws in WEP, a new algorithm was developed which was more secure and is interoperable with wired equivalent privacy (WEP), i.e., no extra hardware required for its implementation.

3.7.1 Enhanced WEP (eWEP)

eWEP [14] is one of the leading accomplishments in securing the wireless network. Its applications are analogous to that of WEP except it tries to probe the mechanisms to protect the initialization vector which is dispatched and relayed in plaintext over the network, thus providing one of the solutions for securing the network from attacks.

3.7.2 Working

To start or begin the process of encryption, sender S and receiver R mutually agree on some initial IV (IV_1) [14]. Then a new random IV, i.e., IV_2 is generated by S. Now sender S with the help of key K_s and IV_1 generates a keystream KS by using RC4 as encryption algorithm. Then CRC is calculated and succeeded or attached to M_1 which in turn is equivalent to $X_1 = (M1, CRC)$, IV_2 is appended to X_1. Then this whole message is XORed with previously generated keystream KS_1. The process continues this way for all the fragments M_1, M_2 … M_n as shown in Fig. 3. This whole message is then sent over the network to receiver R.

The process is almost similar in comparison to that of WEP. The major difference or change is that here we will encrypt X = (M, CRC) and IV (initialization vector) with RC4 encryption algorithm in turn to hide IV from an attacker. In this sender S encrypts X_i appended to IV_{i+1} with the help of an IV_i from the previous step. Therefore, the receiver needs to know only the initial IV, i.e., IV_1 is required to decrypt the first frame, which in turn reveals IV_2 used for the decryption of the

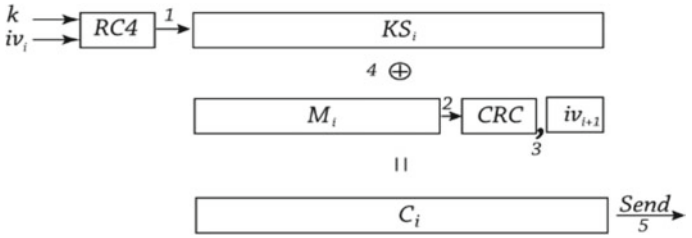

Fig. 3 Encryption process in eWEP

second frame and the process continues in the same manner. At the receiver end, R first decrypts the message by knowing IV_1 and then stores the appended IV_2 with it, which in turn is then used to decrypt the next frame being received from S and this process continues, which ultimately leads to the decryption of all successive frames being received by receiver R.

4 Conclusions

The major contribution of this paper is to analyze the major issues on security in WLAN. IEEE802.11i is the latest standard being used to provide security in WLANs. It specifies two frameworks for being used in 802.11 WLANs, one being the robust security network (RSN) and the other being the pre-RSN. A network entity is assumed to being RSN-capable if it is able to create the RSN associations between the communicating entities, otherwise, it is assumed as pre-RSN entity. Any network is termed as an RSN security framework if it allows robust security network associations with RSN-capable network equipments. Similarly, any network that is able to allow only pre-RSN association between the network entities is termed as pre-RSN framework for network security. The main point of difference between these two frameworks is that of four-way handshake procedure, depending on whether it is included in the authentication and association process.

References

1. Khan MA, Hasan A (2008) Pseudo random number based authentication to counter denial of service attacks on 802.11. In: 5th IFIP international conference on wireless and optical communications networks, WOCN '08, pp 1–5
2. Yao Y, Chong J, Xingwei W (2010) Enhancing RC4 algorithm for WLAN WEP protocol. In: The control and decision conference (CCDC), pp 3623–3627
3. Chen J-C, Wang Y-P (2005) Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. IEEE Commun Mag 43:supl.26–supl.32
4. Gast M (2005) 802.11 wireless networks: the definitive guide. O'Reilly Publication

5. Mohapatra H, Rath S, Panda S, Kumar R (2020) Handling of man-in-the-middle attack in wsn through intrusion detection system. Int J 8(5):1503–1510
6. Mohapatra H, Rath AK, Landge PB, Bhise D, Panda S, Gayen SA (2020) A comparative analysis of clustering protocols of wireless sensor network. Int J Mech Prod Eng Res Dev (IJMPERD) ISSN (P) (2020):2249-6890
7. Abbas K, Afaq M, Khan TA, Rafiq A, Song W-C (2020) Slicing the core network and radio access network domains through intent-based networking for 5G networks. Electronics 9(10):1710
8. Saqib M, Mehmood A, Rafiq A, Muhammad A, Song W-C (2020) Distributed SDN based network state aware architecture for flying ad-hoc network. In: 2020 21st Asia-Pacific network operations and management symposium (APNOMS). IEEE, pp 25–30
9. Abbas K, Afaq M, Khan TA, Mehmood A, Song W-C (2020) IBNSlicing: intent-based network slicing framework for 5G networks using deep learning. In: 2020 21st Asia-Pacific network operations and management symposium (APNOMS). IEEE, pp 19–24
10. Dowling B, Fischlin M, Günther F, Stebila D (2015) A cryptographic analysis of the TLS 1.3 handshake protocol candidates. In: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, pp 1197–1210
11. Diáz G, Cuartero F, Valero V, Pelayo F (2004) Automatic verification of the TLS handshake protocol. In: Proceedings of the 2004 ACM symposium on applied computing, pp 789–794
12. Ma Y, Yan L, Huang X, Ma M, Li D (2020) DTLShps: SDN-based DTLS handshake protocol simplification for IoT. IEEE Internet Things J 7(4):3349–3362
13. Cai J, Huang X, Zhang J, Zhao J, Lei Y, Liu D, Ma X (2018) A handshake protocol with unbalanced cost for wireless updating. IEEE Access 6:18570–18581
14. Wagner D, Schneier B (1996) Analysis of the SSL 3.0 protocol. In: The second USENIX workshop on electronic commerce proceedings, vol 1, no 1, pp 29–40
15. Han S-W, Kwon H, Hahn C, Koo D, Hur J (2016) A survey on MITM and its countermeasures in the TLS handshake protocol. In: 2016 eighth international conference on ubiquitous and future networks (ICUFN). IEEE, pp 724–729
16. Van Berkel K, Bink A (1996) Single-track handshake signaling with application to micropipelines and handshake circuits. In: Proceedings second international symposium on advanced research in asynchronous circuits and systems. IEEE, pp 122–133
17. Yin Z, Leung VCM (2005) Third-party handshake protocol for efficient peer discovery in IEEE 802.15. 3 WPANs. In: 2nd international conference on broadband networks. IEEE, pp 840–849
18. Mzid R, Boujelben M, Youssef H, Abid M (2010) Adapting TLS handshake protocol for heterogenous IP-based WSN using identity based cryptography. In: 2010 international conference on wireless and ubiquitous systems. IEEE, pp 1–8
19. Dowling B, Fischlin M, Günther F, Stebila D (2016) A cryptographic analysis of the TLS 1.3 draft-10 full and pre-shared key handshake protocol. IACR Cryptol. ePrint Arch. p 81
20. Liu Yi, Wang H, Li T, Li P, Ling J (2018) Attribute-based handshake protocol for mobile healthcare social networks. Futur Gener Comput Syst 86:873–880
21. Petridou S, Basagiannis S (2012) Towards energy consumption evaluation of the SSL handshake protocol in mobile communications. In: 2012 9th annual conference on wireless on-demand network systems and services (WONS). IEEE, pp 135–138
22. Du X, Li K, Liu X, Su Y (2016) RLT code based handshake-free reliable MAC protocol for underwater sensor networks. J Sens
23. Mao J, Zhu H, Liu YL, Liu YJ, Qian W, Zhang J, Huang X (2018) RSA-based handshake protocol in internet of things. In: 2018 9th international conference on information technology in medicine and education (ITME). IEEE, pp 989–993
24. Zhang J, Yang L, Gao X, Tang G, Zhang J, Wang Q (2021) Formal analysis of QUIC handshake protocol using symbolic model checking. IEEE Access
25. Park J, Kang N (2014) Lightweight secure communication for CoAP-enabled internet of things using delegated DTLS handshake. In: 2014 international conference on information and communication technology convergence (ICTC). IEEE, pp 28–33

26. Qing L, Yaping L (2009) Analysis and comparison of several algorithms in SSL/TLS handshake protocol. In: 2009 international conference on information technology and computer science, vol 2. IEEE, pp 613–617
27. Sharma P, Lal N, Diwakar M (2013) Text security using 2d cellular automata rules. In: Proceedings of the conference on advances in communication and control systems-2013. Atlantis Press, pp 363–368
28. Diwakar M, Patel PK, Gupta K, Chauhan C (2013) Object tracking using joint enhanced color-texture histogram. In: 2013 IEEE second international conference on image information processing (ICIIP-2013). IEEE, pp 160–165
29. Kumar P, Sehgal V, Chauhan DS, Diwakar M (2011) Clouds: concept to optimize the quality of service (QOS) for clusters. In: 2011 world congress on information and communication technologies. IEEE, pp 816–821