Chapter

Security in Wireless Local Area Networks (WLANs)

Rajeev Singh and Teek Parval Sharma

Abstract

Major research domains in the WLAN security include: access control & data frame protection, lightweight authentication and secure handoff. Access control standard like IEEE 802.11i provides flexibility in user authentication but on the other hand fell prey to Denial of Service (DoS) attacks. For Protecting the data communication between two communicating devices—three standard protocols i.e., WEP (Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol) and AES-CCMP (Advanced Encryption Standard—Counter mode with CBC-MAC protocol) are used. Out of these, AES-CCMP protocol is secure enough and mostly used in enterprises. In WLAN environment lightweight authentication is an asset, provided it also satisfies other security properties like protecting the authentication stream or token along with securing the transmitted message. CAPWAP (Control and Provisioning of Wireless Access Points), HOKEY (Hand Over Keying) and IEEE 802.11r are major protocols for executing the secure handoff. In WLANs, handoff should not only be performed within time limits as required by the real time applications but should also be used to transfer safely the keying material for further communication. In this chapter, a comparative study of the security mechanisms under the above-mentioned research domains is provided.

Keywords: WLAN security, WEP, WPA, 802.11i, denial of service (DoS), lightweight authentication, secure handoff

1. Introduction

Wireless Local Area Networks (WLANs) provide an extension to the wired network. The wireless stations (STAs) connect to an Access Point (AP) for communication. The messages involved in the communication between STA and AP are visible to other STAs lying in the communication range. This makes WLANs insecure and hence WLANs requires protection.

As with any other computer network, the major security goals in WLANs are: confidentiality, integrity and availability (termed as CIA triad). Prominent techniques that help in attaining these goals include: access control, authentication, encryption, message authentication codes (MAC). Under Access control domain, the entity authentication is performed initially. Depending upon the entity authentication results, access into the WLAN network is controlled. For controlling access into the WLANs IEEE 802.11i (WPA2) is the main standard [1]. This standard though provides flexibility in user authentication but has several issues under the Denial of Service (DoS) attacks [2]. For providing protection to individual WLAN data frames encryption mechanisms like WEP (Wired Equivalent Privacy),

TKIP (Temporal Key Integrity Protocol) and AES-CCMP (Advanced Encryption Standard—Counter mode with CBC-MAC protocol) are used. Lepaja et al. [3] have demonstrated through experiment that WPA with AES provides high TCP throughput. Also, AES-CCMP protocol provides strong security properties, and hence is mostly used in the enterprises [3]. In WLANs, sometimes handoff by the STA is required to maintain communication continuity. There exist several protocols like CAPWAP (Control and Provisioning of Wireless Access Points), HOKEY (Hand Over Keying) and IEEE 802.11r that claim safe and continuous handoff by the STAs [4]. These protocols transfer safely the keying material to STA for further communication. The time limit constraint is imposed on such handoff as the handoff should be performed within short interval required by the real time applications.

This chapter is further divided into four sections. Section2 discusses access control methodologies in WLANs while section3 provides understanding of frame authentication methodologies. Section 4 explains secure handoff methods along with the requirements of secure handoff in WLAN environment. Each of these sections also provides comparative analysis among various methodologies. Section5 provides conclusions and future directions.

2. Access control

Traditionally, the entity authentication and access control is provided by the legacy authentication standard i.e., WEP. It has proved insufficient [2] and is hence, deprecated. Currently, IEEE 802.11i (WPA2) [1] security standard is used as an entity authentication and access control mechanism. This security standard is used to secure data communication over 802.11 wireless LANs. The IEEE 802.11i authentication specifies 802.1X authentication mechanism for large networks. The 4-way handshake follows an 802.1X authentication process to confirm the shared keys on Wireless Station (STA) and AP, evolving alongside the Pairwise Transient Key (PTK). This key is used to secure the data sessions between STA and AP using either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) in counter mode with a Cipher Block Chaining Message Authentication Code (CBC-MAC) Protocol (CCMP). As per the findings of Asante and Akomea-Agyin, use of simple passwords/passphrases makes CCMP susceptible to dictionary attacks [5]. The authentication and 4-way handshake are performed sequentially in 802.11i. Once STAs are authenticated, the standard evolves fresh secret keys to secure data communication over 802.11 wireless LANs. A large numbers of packets are used in these processes [2], which results in an increased process length, communication overhead and network overhead. The authentication and 4-way handshake both are prone to Denial of Service (DoS) attacks. This is due to the lack of proper authentication and insecure message communications between wireless devices [2, 6].

In 802.11i based Networks, 4-way handshake is used for evolving and sharing the keys between the two communicating partners. This 4-way handshake is one of the major concerns in WPA2/802.11i because of Denial of Service (DoS) attacks and therefore researchers target to reduce the 4-way handshake latency. Some suggested to make it 3-way while other suggested to make it 2-way [7]. One such improvement is proposed by Singh and Sharma [7]. In their proposal, the authors try to eliminate the entire 4-way handshake while maintaining the security and key refreshing requirements. For their purpose, they have utilized frame sequence numbers and the striking feature of the proposal is that the key freshness is maintained for each communicating frame. The key refreshed is used for fulfilling the security aspects like frame encryption and integrity management. The overheads in the proposal are bare minimum and it is lightweight as no changes in the existing MAC frame

are done. Also, no extra messages are required. Their improvement is more useful under frequent key refreshing situations where users are joining and leaving the wireless environment frequently like in a short duration conference/workshop or in lounge of railway station/airport. The improved technique provides a secure authentication mechanism and no explicit synchronization is required in case of loss of frames. The timings analysis done in the work shows that this technique is effective while security analysis shows that it enjoys almost equivalent security as compared with 4-way handshake of 802.11i. Removal of handshake ensures that the attacks conducted in the 4-way handshake are also removed.

Another improvement in the 802.11i standard is proposed by Singh and Sharma [8] wherein a novel sequence number based scheme is proposed to reduce the MIC field overhead in the WLANs. The existing security frameworks (WPA, 802.11i) provide MIC for maintaining the integrity and authentication for each data frame. MIC is kept in separate field in the frame, and hence adds to the communication overhead. The scheme of Singh and Sharma [8] introduces the notion of authentication token (AT). This AT is calculated based upon the existing sequence number of the WLAN frame. The AT serves both frame integrity and frame authentication purposes. After calculation, it is placed instead of sequence number in the sequence number field of the WLAN frame which means no extra bit or field overhead involvements. As MIC field is removed and AT placement requires no overheads, the scheme is effective as far as WLAN communication overheads and space managements are considered. In addition, the authors have shown that their method is resistant against replay attacks and also provided details on how to attain synchronization in case of frame loss.

In October 2017, a new and major weakness was documented in WPA2 WLAN standard termed as Key Reinstallation AttaCK or KRACK [9]. It was noted that this affected all kinds of WLAN security and hence the reputation of WPA2 got decreased. The WPA2 standard also suffered under DoS attacks. Hence, Wi-Fi Alliance comes up with the improvement. The improvement is termed as WPA3. Its main features involve: (1) ease of use (2) natural password selection (3) an improved and robust handshake and, (4) forward secrecy. The WPA3 is backward compatible with WPA2 which means the upgraded devices can work in WPA2 or WPA3 modes [10]. The market adoption of this standard is now picking and it will take some more time for getting stabilized. Thus, this work on WLAN security considers the present widespread standard i.e., WPA2.

Li et al. proposed an initial entity authentication scheme termed as fast WLAN initial access authentication protocol (FLAP) [11]. FLAP is targeted towards making access authentication faster by reducing the number of initial authentication messages. It is assumed in the protocol that STA and AS share common secret key which simplifies the entire mechanism. Overall, this method involves 6 messages (approx. Two round trip times, **Figure 1**), proves STA authentication at the AS via shared key, has key hierarchy equivalent to 802.11i and protects the messages by MIC. Through practical measurements it is shown that FLAP can improve the efficiency of EAP-TLS by 94.7 percent. It is suggested that this method is compatible with 802.11i and can coexist with existing 802.11i standard. Depending upon circumstances either 802.11i or FLAP can be chosen from suite selector. Like standard 802.11i security protocol, FLAP scheme also depends upon MIC for frame integrity and authentication despite of the fact that MIC verification is computation intensive. This protocol hence may fall an easy prey to Denial of Service (DoS) attacks wherein the attacker may send large number of frames having incorrect MICs. The successive MIC failures on the receiver results in a kind of DoS attack termed as computation DoS attack [12].

Singh and Sharma [13] proposed an access control authentication scheme—SWAS (Secure WLAN Authentication Scheme). The scheme introduces the concept

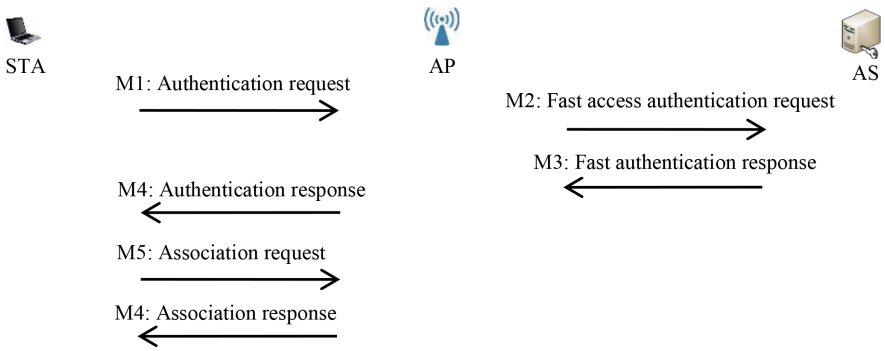

Figure 1.
A simplified overview of initial access authentication protocol (FLAP).

of delegation in WLANs and provides access to clients only upon authentication. SWAS provides authentication of all parties (STA, AP and AS) and evolves a fresh key for securing the data sessions. In addition, it provides security to all messages by utilizing cryptographic primitives, such as encryption and Message Integrity Code (MIC). The proposed scheme reduces the length and complexity compared to IEEE 802.11i authentication and key deriving process. The use of cryptographic techniques does not increase the authentication time of the proposed method. The scheme reduces the communication cost, network overhead and is also resilient against DoS attacks. Therefore, the main contribution of SWAS is to provide a secure and efficient authentication mechanism that evolves fresh communication keys.

The SWAS scheme involves three parties: STA, AP and AS. It has three phases: registration phase, request phase and authentication phase. Initially, STA registration is performed at AS and is required only once in a given network. In registration, AS utilizes delegation concept, and generates shared secret key (σ) for AS and STA [14]. The registration phase is followed by the request phase, where the existing 802.11 probe requests, and the probe response messages are utilized by the STA to request the network connection and access. After the request phase, SWAS authentication is performed for authentication and to derive a new communication key that is used to protect the data packets in subsequent sessions.

Both online and offline authentications are used in the SWAS scheme. Online authentication provides authentication and security to all messages among STA, AP and AS. The online authentication utilizes three random numbers (r1, r2, r3) and a sequence number (s1) to ensure proper encryption, authentication and key freshness. In addition, it maintains a key hierarchy similar in purpose to 802.11i with a Master Session Key (MSK), Pairwise Master Key (PMK) and Pairwise Transient Key (PTK). The PTK evolved on the STA and AP during the authentication process is used to encrypt the data packets between them. A simplified view of the SWAS online authentication message exchanges (M1, M2, M3 and M4) is shown in **Figure 2**. In this figure it is clearly visible that each one among STA, AP and AS authenticates each other through various passcode/digital signature verification. The passcode is nothing but protected information (secured through cryptographic means) for the other party. Offline authentication is required whenever a new session key between the same STA and AP is required. This does not involve AS for authentication rather it uses prior stored information at STA and AP. The offline authentication is done via a re-association request and utilizes loosely synchronized sequence number scheme [15].

The salient features of SWAS include: (1) Resistance to DoS attacks in almost all the phases, (2) Less communication and computation time as compared with

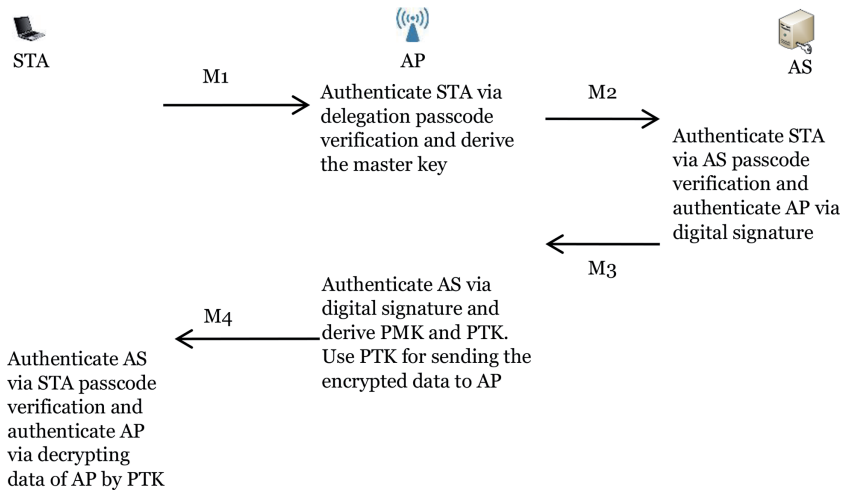

Figure 2.
A simplified overview of online authentication phase of SWAS scheme.

IEEE 802.11i standard, (3) authentication of all the associated parties i.e., STA, AP and AS by each other and, (4) authentication of all the messages used during all the protocol communication phases. The shortcomings include: (1) lack of practical demonstration of the protocol and (2) no extension of the scheme under the handoff situations is provided till date.

Authentication per frame and symmetric key based encryption is an implicit necessity for security in Wireless Local Area Networks (WLANs). Singh and Sharma [16] proposed a novel symmetric key based Access Control and per frame authentication scheme for WLANs termed as Key Hiding Communication (KHC) scheme. KHC scheme has two phases: initial phase and communication phase. Former is utilized for sharing and evolving the master key (MK) between STA and AP whereas latter is utilized for onwards data frame communication using the (refreshed) keys. The major establishment of this scheme is the introduction of novel concepts of refreshing the key, protecting the key and initial vector (IV) using different counters and then mixing the bytes of protected key and IV together for each communicating frame. The mixing is based upon the shared secret key and hence only the two communicating parties i.e., STA and AP can mix and separate the bytes of key and IV. The protected mixed bytes are termed as codeword while the concept of mixing the protected key and IV bytes is termed as key hiding. The codeword is added in the WLAN frame. This addition of codeword to the existing WLAN frame occupies extra space and hence the scheme has extra space overheads. Integrity to the frame is provided via MIC. A new key and new IV for the new frame to be transmitted is evaluated based upon existing secret key and existing IV. Evaluation of new key and new IV is termed as key and IV refreshing. The refreshed new key and new IV are first protected using incremented values of counters and then mixed together to form new codeword. The verification and separation of the key and IV from the transmitted codeword provides frame authentication. Once the frame is authenticated, its integrity is verified through MIC verification involving key. The frame authentication is lightweight in KHC as it involves trivial increment, XOR and modulus operations. Thus, KHC follows the notion of frame authentication first and then checking the frame integrity for protection against computation DoS attacks. The separated key and IV are used to decrypt the frame contents and are also used to confirm the frame integrity via MIC. The simplified overview of KHC communication process is shown stepwise in **Figure 3**.

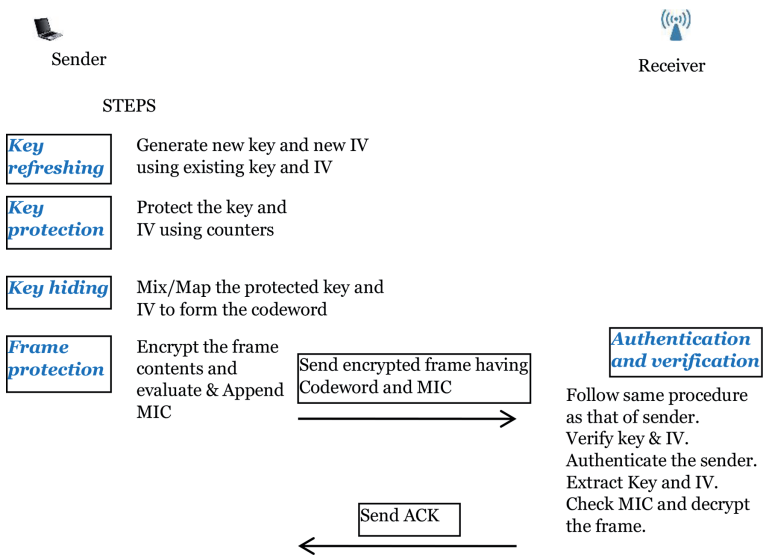

Figure 3.
A simplified overview of communication phase of KHC scheme.

In nutshell, KHC introduces the concept of key hiding which involves protecting the key using counters followed by mixing of refreshed key & IV i.e., mapping of refreshed key & IV. Through this process of formation of the codeword, the secret symmetric key remains concealed from the attacker. The recipient extracts the key from the codeword, compares it with its own evaluated key, thereby authenticating the sender. Key along with IV, is then used to decrypt the data frame of the sender. Thus, KHC is a useful WLAN communication scheme that is not only secure but is also efficient. The major contributions made by KHC are: (1) lightweight WLAN communication methodology, (2) utilization of symmetric key based encryption/decryption, (3) Per frame Key refreshment, (4) protection against computation DoS attacks and, (5) comparable security as that of 802.11i.

2.1. Comparisons of various WLAN access control mechanisms

A property wise comparison between prominent WLAN access control security mechanism is presented in **Table 1**. WEP is though deprecated but mentioned here for the sake of completeness. It can be noted that WEP provides weak authentication, integrity and encryption support. Further, WEP does not consider key and IV refreshing. IEEE 802.11i is a strong protocol as it maintains strong authentication, integrity and encryption. It involves large number of messages and hence consumes times during initial authentication. For key refreshing, it involves 4-way handshake having 4 message exchanges between STA and AP. This 4-way handshake is the major concern in 802.11i. It is prone to DoS attacks and KRACK attacks. FLAP and SWAS both enjoys features similar to that of 802.11i with a difference that the messages exchanged for symmetric key evaluation are less in FLAP and SWAS. In FLAP, very few i.e., approx. 6 messages are exchanged for the key evaluation (including those between STA and AP). In SWAS, only four (4) initial messages are required during online authentication (including those between STA and AP) for sharing the PTK. During offline authentication for refreshing the shared symmetric key only two messages are required. The KHC scheme adopts an interesting methodology which is different from the other access control protocol.

WLAN access control—Security mechanisms					
Property	**WEP**	**802.11i [1]**	**FLAP [11]**	**SWAS [13]**	**KHC [16]**
Authentication	Yes, weak	Yes, strong, initial entity authentication followed by MIC based per frame auth.	Yes, strong, initial entity authentication followed by MIC based per frame auth.	Yes, strong, initial authentication followed by MIC based per frame auth.	Yes, strong, initial entity authentication followed by continuous, lightweight per frame auth.
Integrity support	Yes, weak, CRC based	Yes, strong, MIC based	Yes, strong, MIC based	Yes, strong, MIC based	Yes, strong, MIC based
Encryption support for confidentiality, strength of encryption	Yes, low, RC4 algorithm	Yes, high, TKIP and AES based	Yes, high, TKIP and AES based	Yes, high (Once shared key is evolved, rest process is same as that of 802.11i)	Yes, high, any one of RC4/ TKIP/ AES can be used
Synchronization Algorithm	No	No	No	No	Yes
Initial message Exchange for symmetric key exchange	No, done manually	Yes, large	Yes, few – 06 messages (two round trip times)	Yes, few -only four (4) initial messages during online authentication	Yes, few
Key freshness	No	Yes	Yes	Yes	Yes
IV freshness	No	N.A.*	N.A.*	N.A.*	Yes
Messages exchange for key renewal	N.A.*	Yes, four, explicitly	Yes, four (between STA and AP), explicitly	Yes, two using offline authentication	No, done implicitly

**Not Applicable in this mechanism.*

Table 1.
Property wise comparison of WLAN access control security mechanisms [16].

It does not use any third party like AS in the authentication process and hence involves less number of messages. It provides an implicit key hiding per frame authentication procedure that is capable of communicating the key to the other entity and is able to refresh not only the shared key but also the IV for encrypting each frame. Thus, least messages are required for key refreshing among all the access control WLAN security mechanisms. Also, the adopted methodology of key refreshing, protection and mapping makes the cracking of key difficult for the attacker. In contrast to WEP, IV is hidden and not visible to the attacker. Other access protocols do not have the notion of IV.

As shown in **Table 2**, memory requirements of WEP is least. 802.11i has more memory requirements than WEP but less than others. Among others, SWAS has highest while FLAP has lowest memory requirements. Communication overhead analysis shows that (1) KHC and WEP involves per frame overheads whereas in others it is done implicitly and, (2) KHC is efficient in key refreshing as compared to others. For key refreshing each of 802.11i and FLAP requires 4 frames,

WLAN access control—Security mechanisms					
Overheads	**WEP**	**802.11i [1]**	**FLAP [11]**	**SWAS[13]**	**KHC[16]**
*Memory requirements***	Storing key and IV	Storing Master Key, Refreshed key	Storing Master Key, Refreshed key and counter	Storing delegation key, public key pairs, Symmetric keys: MK, PMK, MSK, PTK, two counters, one sequence number. (Also pool of random numbers at AP)	Storing Master Key, Refreshed key, IV and two counters
Communication overheads					
For per frame authentication	IV (128 bits) per frame	Implicitly by MIC	Implicitly by MIC	Implicitly by MIC/ authentication information	256 bits per frame
For key refreshing	N.A.*	4 data frames	4 data frames	2 data frames	implicit

*Not Applicable in the scheme.
**Considered per participating node.

Table 2.
Performance comparison of WLAN access control security mechanisms [16].

SWAS requires 2 frames whereas it is handled implicitly in KHC. In [11], the average authentication delays of the EAP-TLS and FLAP are evaluated as 260.253 and 13.884 ms, respectively. In [13], the total time for SWAS authentication is found to be of the order of 26.46 ms (including time for DoS protection). In [16] Key refreshing timings of 802.11i and KHC are shown as 13.5 ms and 7.5 ms, respectively.

The security comparison shown in **Table 3** clearly indicates that SWAS and KHC scheme provides almost equivalent and better security. 802.11i is prone to DoS attacks whereas FLAP is prone to replay and man-in-middle attacks. Obviously, security of FLAP is least and hence it is not much used presently.

In most of the WLAN access control mechanisms (except KHC), authenticity to the data frame is usually provided by MIC. The MIC based per frame authentication may lead to computation DoS. Hence, lightweight per frame authentication solution is required. It is discussed next.

Attacks	**WEP**	**802.11i [1]**	**FLAP [11]**	**SWAS[13]**	**KHC [16]**
Possibility of frame contents overwritten by attacker	Yes	No	No	No	No
Possibility of modification of authentication bits	N.A. as authentication is implicit	No	No	N.A.*	No
Man-in-middle attack	Yes	No	Yes	No	No
Replay attack	Yes	No	Yes	No	No
Reduce DoS attacks	No	No	No	Yes	Yes

*Not applicable in this mechanism.

Table 3.
Comparison of WLAN access control security mechanisms under attacks [16].

3. Frame authentication

In WLANs, a two layer redundant security exists. One at the Medium Access Control (MAC) layer while other at the higher layer dealing with End to End security. In former, 802.11i provides security while in latter, higher layer protocols like IPSec, SSL-TLS etc. provides security. Hence, it is suggestive that lightweight authentication and symmetric key based cryptographic measures per frame should be used.

For providing individual frame level protection, two kinds of per frame authentication exist in WLANs: MIC based authentication and lightweight authentication. MIC based frame authentication for data frames is utilized by standard WLAN protocols like IEEE 802.11i, FLAP etc. In these protocols, each frame is accompanied by a unique MIC calculated using sender's shared secret key. The receiver verifies it by recalculating and matching using its share secret key. The MIC calculations and verification consume computation time of the order of 1.5 ms and as shown in Section 2 for FLAP protocol, computation DoS attacks are a possibility [12, 17, 18]. Main reason for computation DoS attack is attributed to the fact that MIC is serving two purposes: authentication and message integrity. Instead, first lightweight authentication should be used. If it succeeds, frame integrity (MIC) should be checked only for those frames whose authentication has succeeded. This will reduce the DoS attacker chances. Thus, lightweight authentication techniques which uses less computation time may prove useful.

The lightweight authentication schemes [19–25] generate the random authentication bits at sender and receiver using random bit generator with commonly shared secret seed as input. These authentication bits are inserted into the WLAN frames. Upon verification of the authentication bits, the frame is accepted at the receiver. Though such schemes provides authentication but they usually lack other security measures like key freshness, secrecy and integrity. A brief tabulation of these schemes is presentation in **Table 4**, showing advantage and disadvantage of each.

3.1 Comparisons of various lightweight authentication mechanisms

All the schemes considered in **Table 4** provide per frame continuous authentication. Schemes of Pepyne et al. [25] and Singh and Sharma [26] supports integrity. Former supports CRC based weak integrity while latter supports MIC based strong integrity. Schemes of Pepyne et al. [25] and Singh and Sharma [26] supports encryption. Former supports RC4 based weak encryption while latter supports TKIP/AES based strong encryption. All the schemes considered use their own synchronization algorithm, in fact scheme by Wang et al. [22] uses three different synchronization algorithms. Schemes by Ren et al. [23], Lee et al. [24], Pepyne et al. [25] and Singh and Sharma [26] involves initial message exchanges. Key freshness is incorporated by Pepyne et al. [25] and Singh and Sharma [26]. None of these involves extra messages for evolving new symmetric key (key renewal).

Considering the memory requirements of these schemes Singh and Sharma [26] has the greatest (912 bits) while Lee et al. [24] has the lowest (24 bits). Others except Pepyne et al. [25] have 256 bits memory requirements. Pepyne et al. [25] has 384 bits memory requirements. As far as communication overheads are concern, Johnson et al. [19, 20] and Ren et al. [23] have requirements of 3 bits per frame and 7 bits per ACK frame for counter. Wang et al. [21, 22] has no extra bit requirements as these keep the authentication bits in the unused type and subtype fields of 802.11 frame. Lee et al. [24] requires four extra frames, each having 3 authentication bits. Pepyne et al. [25] has requirements of keeping 128 bits per frame for keeping counter. ASN based scheme by Singh and Sharma [26] has no explicit requirements but requires 48 bits per ACK for synchronization.

Light weight authentication schemes	Features	Advantage(s)	Disadvantage(s)
Johnson et al. [19] Wu et al. [20]	Only one bit from the authentication stream generator is placed in the link layer data frame	• scheme provides originator sender identity authentication • has low communication overhead • as one bit can easily be damaged, synchronization algorithm is also proposed	• attack leading to non-synchronization can easily be launched via successive frame authentication failures • The number of bits used for authentication purpose is too less due to which attacker has 50% chances • the data packets are not encrypted in SOLA nor MIC per frame is provided, hence payload may be changed (overwrite attack)
Wang et al. [21]	• the sender and the receiver generates an authentication stream using same seed value • The bit from the authentication stream is put in the frames by the sender and are verified by the receiver using its authentication stream	lightweight protocol with synchronization algorithm and low communication overhead	• The authentication bits are not bound to the frame contents • synchronization process is affected by flooding DoS attack where the attacker confuses the sender via unauthenticated ACK frames • long authentication bits of continuous 0's or 1's by attackers in the frames can cause confusion
Wang, et al. [22]	• single bit lightweight authentication solution • Concept of discrimination among legitimate STAs and attacker nodes is used	efficient in terms of computation cost, communication cost and synchronization efficiency	Possibility of authentication bit manipulation by attacker exists
Ren et al. [23]	3 bit authentication solution	Has synchronization algorithm that uses 7 bit counter value put in the ACK frame by the receiver for attaining synchronization	still utilizes less number of bits and therefore high probability of attacks
Lee et al. [24]	Scheme selects 3 bits for authentication of management frames	Protection from DoS attack performed by unauthenticated management frames	• scheme protects only the management frame whereas the data frame are not protected • DoS attack is still possible by using frames other than the management frames
Pepyne et al. [25]	• based upon improvising the WEP protocol • uses random stream generator for generating the authenticator variables and fresh encryption keys	Frame counter 'k' is used for synchronization purpose	attacker can easily modify 'k' and launch the attack leading to non-synchronization and Denial of Service

Light weight authentication schemes	Features	Advantage(s)	Disadvantage(s)
Singh and Sharma [26]	• utilizes sequence number of the frame along with the authentication stream generators for authentication • provides authentication by modifying sequence number of the frame by trivial math operations by sender such that the modification is verified at the receiver	• it requires no extra bits or messages for authentication purpose and also no change in the existing frame format is required • lightweight authentication • helps in protecting against computation DoS attacks • prohibits replays and maintains the synchronization	AP maintains sequence numbers per STA

Table 4.
Comparison of per frame WLAN authentication solutions.

On comparing the computational performance of the lightweight authentication schemes mentioned in **Table 4**, it is found that Pepyne et al. [25] and Singh and Sharma [26] take more computational time as compared with others. Singh and Sharma [26] takes more computational time due to the fact that it involves MIC evaluation and encryption of frame for enhancing the security. It is shown in [26] that considering only the authentication the time taken for computational cost for is 0.5 micro seconds which implies that it is same as that of other lightweight solutions.

Except, Pepyne et al. [25], the chances of Brute Force attacks on authentication bits embedded in the frames are quite high in these schemes. Except Pepyne et al. [25] and Singh and Sharma [26] the possibilities of frame contents modification, man-in-the middle attack, replay attacks and DoS attacks are quite high. Pepyne et al. [25] and Singh and Sharma [26] do not allow frame contents modifications and DoS attacks. Pepyne et al. [25] suffers under man-in-the middle attack and replay attacks.

Though KHC is considered in this chapter initially under the Access control mechanisms, it involves lightweight per frame authentication also and needs a special mention in this sub-section. In comparison with the schemes mentioned in **Table 4**, KHC has longer initial entity authentication process. KHC also has raised memory requirements but meets important security features like forward secrecy, key refreshing, lightweight per frame authentication, per frame encryption etc. required by any WLAN security protocol.

Apart from the two main authentication types i.e., MIC based authentication and lightweight authentication, the others are password key exchange mechanisms and layered authentication. The password key exchange mechanisms [27, 28] provide mutual authentication between client and authentication server (AS), identity privacy, half forward secrecy and low computation cost for a client. These mechanisms lack some of the mandatory and recommended requirements for the key exchange methods [29]. Also, these schemes provide authentication at the AS level only while ignoring the authentication at the AP level. The layered authentication achieved by EAP which acts as basis for higher layer authentication protocols, contains certain vulnerabilities e.g. no identity protection, no protected cipher suite negotiation, and no fast reconnection capability [29].

4. Secure handoff

WLANs handoffs are essential for providing continuous mobility to a wireless Station in an Enterprise LAN. Two important requirements of the handoff are: (1) establishment of a secure connection of the roaming STA with new access point (AP) and (2) completion of handoff within time limits such that the undergoing communication remains unaffected. The time limit on handoff for multimedia and real time WLAN applications is approximately 50 ms [30]. During this period no data packets transfer occurs. As per the 802.11i WLAN security standard, the complete secure STA authentication (default Full EAP/TLS) via AS evolving shared secret key between STA and AP takes time of the order of 300 ms to 4 s [12] and hence is unfit for the handoffs. For reducing this time, notion of pre-authentication is introduced wherein full 802.1X authentication involving AS is done utilizing old AP and candidate AP (new AP). Hence, at the time of handoff only 4-way handshake is required between STA and candidate AP. In this pre-authentication process, an inaccurate candidate AP prediction has associated resource wastage issues as full 802.1X will again be required [31]. Researchers have considered predictive authentication and proactive key distribution for reducing the handoff times. Former involves predicting the candidate AP whereas latter involves locating a group of candidate APs. Thus, in former the problem of inaccurate candidate AP prediction exists whereas in latter the problem of extra communication overhead for authentication with group of APs exists.

Researchers have also worked towards reactive solutions wherein the candidate AP is selected by STA and then the security context is transferred to this AP. In such solutions, STA requests to AS via old AP, then AS transfer security context and material to the candidate AP. Singh and Sharma [32] proposed one such novel secure handoff scheme that maintains security properties while evolving and transferring the security context (key and initial vector) to the candidate AP. The scheme is lightweight and uses reactive method for handoff. Two kinds of APs are defined in the scheme: normal AP and Domain Controller AP (DCAP). STA request DCAP through AP by putting ID of the candidate AP. DCAP in turn distributes the STA context (key and initial vector) to the candidate AP. Thus, when STA roams into the area of candidate AP, less time is involved in the STA authentication at the candidate AP.

For providing fast and secure handoff for the mobile STA in WLANs, standard bodies IEEE and IETF have defined protocols like Control and Provisioning of Wireless Access Points (CAPWAP), HandOver Keying (HOKEY) and IEEE 802.11r (Task group r) [5]. CAPWAP supports centralized management of APs. HOKEY extends the Authentication, Authorization and Accounting (AAA) architecture to support key deriving and distribution with involving full EAP authentication. 802.11r depends upon passing credentials directly between APs for handover. Though CAPWAP takes very less time, it is more or less re-authentication with centralized Access Controller (AC), followed by key transfer to new Wireless Termination Points (WTP). HOKEY is successful in multidomains but it takes more communication time. Among these three (CAPWAP, HOKEY and 802.11r), 802.11r is more efficient in terms of communication overheads. It still has issues concerning the safe transfer of key between APs.

4.1 Comparisons of various handoff mechanisms

CAPWAP and HOKEY does not change the existing 802.11 frame structure. 802.11r is a separate protocol and hence has different frame structure. All except CAPWAP scheme generates fresh session keys. Fresh traffic keys are generated by all the schemes. Communication overhead of KHC based handoff scheme is less as

compared to any other scheme. This handoff scheme shortens the handoff latency by initiating a key transfer process prior to moving to the new AP and performing handoff. It strengthens the security by (1) protecting STAs from re-associating to Malicious APs, (2) evolving fresh keys even during handshake, (3) authenticating all the frames during the handoff and, (4) safeguarding against DoS attacks and, (5) providing continuous authentication during communication.

5. Conclusions

This chapter discusses about the present WLAN security environment. It is clear that the WLAN security environment till date is dominated by WPA2 (IEEE 802.11i) standard. Researchers have pointed out regarding length and complexity of the WPA2. The major point of concern in WPA2 is key refreshing mechanism i.e., 4-way handshake due to which the WLAN security is considered vulnerable. Researchers, hence target to reduce the length of this handshake while maintaining the security properties intact.

The chapter also studies other WLAN security mechanisms proposed by researchers and categories them into: (i) access control, (ii) per frame authentication and (iii) secure handoff mechanisms. It provides category wise comparative analysis of these mechanisms. Three mechanisms are considered in the access control category. Among them Key Hiding Communication (KHC) is the most attractive but it requires changes in the existing WLAN frame structure. Per frame category is further sub-categorized into: (a) per frame authentication mechanisms utilizing MIC and (b) lightweight per frame authentication mechanisms. For enhancing the security, most of the per frame authentication solutions rely on MIC for both authentication and integrity of frame. It is shown that this MIC verification involves computation time and large number of such verifications may result in computation DoS attack on the receiver. The researchers hence advocate separating the authentication and integrity parts in per frame authentication. The lightweight per frame authentication mechanism are though lightweight in nature but lacks security properties like key refreshing, secrecy and integrity. In this chapter, several handoff mechanisms for WLAN environment are also discussed and it is accomplished that none guarantees to maintain required level of security during the specified handoff time limits.

WLAN security is having a transformation from WPA2 to WPA3. WLAN security is strengthened in the upcoming standard i.e., WPA3. It is very early to comment on the effectiveness of WPA3 and it is evident that the existing WLAN devices will continue to use WPA2. The new upcoming WLAN devices will obviously follow the backward compatibility towards WPA2. Thus, researchers can still target to test the implementation of 802.11i with the novel ideas like MIC reduction, 4-way handshake reduction and blockchain application in WLANs [33]. In wireless medium, per frame lightweight authentication mechanisms will prove an edge and in future, researchers may consider developing such solutions. For maintaining uninterrupting communication quick, secure, accurate and secure handoff is the need of the hour. Hence, researchers in future may consider implementation of efficient and secure handoff mechanisms using WPA3.

Acknowledgements

The authors acknowledge and express the gratitude towards their parent Institutes for the support.

Conflict of interest

The authors declare no conflict of interest.

Author details

Rajeev Singh[1*] and Teek Parval Sharma[2]

1 G.B. Pant University of Agriculture and Technology, Pantnagar, Uttarakhand, India

2 National Institute of Technology, Hamirpur, Himachal Pradesh, India

*Address all correspondence to: rajeevpec@gmail.com

References

[1] IEEE 802.11i. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements. 2004; IEEE Standard

[2] Singh R, Sharma TP. On the IEEE 802.11i security: A denial of service perspective. Wiley Journal of Security and Communication Networks. 2015;**8**(7):1378-1407

[3] Lepaja S, Maraj A, Efendiu I and Berzati S. The impact of the security mechanisms in the throughput of the WLAN networks. In: Proceedings of the 7th Mediterranean Conference on Embedded Computing; June 2018; Budva, Montenegra

[4] Clancy TC. Secure handover in Enterprise WLANs: CAPWAP, HOKEY, and IEEE 802.11r. IEEE Wireless Communications. 2008;**15**(5):80-85

[5] Asante M, Akomea-Agyin K. Analysis of security vulnerabilities in Wifi-protected access pre-shared key (WPA-PSK/ WPA2-PSK). International Research Journal of Engineering and Technology (IRJET). 2019;**06**(01):537-545

[6] Singh R, Sharma TPA. Location based method for restricting the flooding DoS effect in WLANs. Journal of Location Based Services. 2016;**9**(4):273-295. Taylor and Francis

[7] Singh R, Sharma TP. A key refreshing technique to reduce 4-way handshake latency in 802.11i based networks. In: Proceedings of the Fourth IEEE International Conference on Computer and Communication Technologies, ICCCT'13; September 2013; Allahabad. pp. 157-163

[8] Singh R, Sharma TP. A sequence number based WLAN authentication scheme for reducing the MIC field overhead. In: Proceedings of the Tenth IEEE International Conference on Computer and Communication Technologies, WOCN'13; July 2013; Bhopal. pp. 1-4

[9] Newman LH. The Secure Wi-Fi Standard Has a Hugh Dangerous Flaw [Internet]. 2017. Available from: https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability/

[10] Wi-Fi Alliance. Discover Wi-Fi Security [Internet]. Available from: https://www.wi-fi.org/discover-wi-fi/security

[11] Li X, Bao F, Li S, Ma J. FLAP: An efficient WLAN initial access authentication protocol. IEEE Transactions on Parallel and Distributed Systems. 2013;**25**(2):488-497

[12] Martinovic I, Zdarsky FA, Bachorek A, Schmitt JB. Measurement and analysis of handover latencies in IEEE 802.11i secured networks. In: Proceedings of the European Wireless Conference (EW2007); April 2007; Paris. pp. 1-7

[13] Singh R, Sharma TPA. Secure WLAN authentication scheme. IEEK (Institute of Electronics Engineers of Korea) Transactions on Smart Processing and Computing. 2013;**2**(3):176-187

[14] Tang C, Wu DO. An efficient mobile authentication for wireless networks. IEEE Transactions on Wireless Communications. 2008;**7**(4):1408-1416

[15] Park CS. Two-way handshake protocol for improved security in IEEE 802.11 wireless LANs. Computer Communications. 2010;**33**(9):1133-1140

[16] Singh R, Sharma TP. A key hiding communication scheme for enhancing the wireless LAN security. Springer Wireless Personal Communications. 2014;**77**(2):1145-1165

[17] Singh R, Sharma TP. Simulated analysis of a cryptographic solution for WLANs against Denial of Service (DoS) attacks. Journal of Engineering Science and Technology. 2014;**9**(Special Issue):57-67

[18] Singh R, Sharma TP. Modeling and performance evaluation of computational DoS attack on an access point in wireless LANs. In: Ram M, Davim JP, editors. Advanced Mathematical Techniques in Science and Engineering. Denmark and The Netherlands: River Publishers; 2018. pp. 101-120

[19] Johnson H, Nilsson A, Fu J, Wu SF, Chen A, Huang H. SOLA: A one-bit identity authentication protocol for access control in IEEE 802.11. In: Proceedings of the IEEE Global Telecommunications Conference. Taipei, Taiwan; Vol. 1; 17-21 November 2002. pp. 768-772

[20] Wu F, Johnson H, Nilson A. SOLA: Lightweight security for access control in IEEE 802.11. In: Wireless Security. IEEE IT Professional; 2004;**6**(3):10-16

[21] Wang H, Velayutham A, Guan Y. A lightweight authentication protocol for access control in IEEE 802.11. In: Proceedings of the IEEE Global Telecommunications Conference, GLOBECOM'03. San Francisco, CA, USA; 2003. pp. 1384-1388

[22] Wang H, Cardo J, Guan Y. Shepherd: A lightweight statistical authentication protocol for access control in wireless LANs. Computer Communications. 2005;**28**(14):1618-1630

[23] Ren K, Lee H, Han K, Park J, Kim K. An enhanced lightweight authentication protocol for access control in wireless LANs. In: Proceedings of the 12th IEEE International Conference on Networks. Singapore; Vol. 2; 2004. pp. 444-450

[24] Lee Y-S, Chien H-T, Tsai W-N. Using random bit authentication to defend IEEE 802.11 DoS attacks. Journal of Information Science and Engineering. 2009;**25**(5):1485-1500

[25] Pepyne DL, Ho Y-C, Zheng Q. SPRiNG: Synchronized random numbers for wireless security. In: Proceedings of the IEEE Wireless Communications and Networking, WCNC'03. New Orleans, LA, USA; 2003. pp. 2027-2032

[26] Singh R, Sharma TP. A novel sequence number based secure authentication scheme for wireless LANs. Journal of Electronics Science & Technology (JEST). 2015;**13**(2):144-152

[27] Juang W-S, Wu J-L. Two efficient two-factor authenticated key exchange protocols in public wireless LANs. Computers and Electrical Engineering. 2009;**35**(1):33-40

[28] Lee Y, Kim S, Won D. Enhancement of two-factor authenticated key exchange protocols in public LANs. Computers and Electrical Engineering. 2010;**36**(1):213-223

[29] Lei J, Fu X, Hogrefe D, Tan J. Comparative studies on authentication and key exchange methods for wireless LAN. Computers & Security. 2007;**26**:401-409

[30] Lee I, Hunt R. A novel design and implementation of DoS-resistant authentication and seamless handoff scheme for enterprise WLANs. In: Proceedings of the 8th Australian Information Security Management Conference; Perth, Australia; 2010. pp. 49-61

[31] Kassab M, Belghith A, Bonnin J-M, Sassi S. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. In: Proceedings of the Wireless Multimedia

Networking and Performance Modeling, WMuNeP'05. Montreal, Quebec, Canada; 13 October 2005. pp. 46-53

[32] Singh R, Sharma TP. Secure WLAN handoff scheme with continuous authentication. MIS Review. 2016;**21**(1):35-50

[33] Jiang X, Liu M, Yang C, Liu Y, Wang R. A blockchain-based authentication protocol for WLAN mesh security access. CMC. 2019;**58**(1):45-59