Prevention of DoS and Memory Exhaustion Attacks: Key Distribution with Confidentiality and Authentication

Paridhi Singhal
(Dept. of CSE)
FET, Mody
Institute of Technology and
Science, Lakshmangarh,
Rajasthan, India

Manoj Diwakar
(Dept. of CSE)
FET, Mody
Institute of Technology and
Science, Lakshmangarh,
Rajasthan, India

Mandeep Katre
(Dept. of CS),
Inderprastha Engineering College,
63 Site IV, Surya Nagar Flyover
Road, Sahibabad, Ghaziabad,
U.P. India

ABSTRACT
Now a day's most of the organizations are moving from wire-connected LAN to wireless LAN. The popularity of the 802.11 network standards stems from the fact that they provide for wireless connections with simplicity and convenience. But, there are many security issues which have been identified in the operation of 802.11 networks, and the 802.11i protocol has been announced to protect these types of networks. 802.11i protocol security has with a focus on an active attack and a passive attack. These types of attacks exhaust the client's memory using a vulnerability of the key derivation procedure in 802.11i. It is vulnerable to various active and passive attacks which include de-authentication and disassociation attacks. For active and passive attacks(denial of services and memory exhaustion) which are possible in 4-way handshake, this paper provides a secret key distribution with confidentiality and authentication and can also say that this procedure of secret key distribution is free from these active and passive attacks in comparison to original protocol and is more secure.

General Terms: Security

Keywords: Secret key distribution, 4-Way Handshake, De-authentication, Active Attacks, Passive attack, IEEE 802.11, IEEE 802.11i, public key, private key.

1. INTRODUCTION
The increased demands for mobility and flexibility in daily life are demands that lead the development from wired LANs to wireless LANs (WLANs). Today a wired LAN can offer users high bit rates to meet the requirements of bandwidth consuming services like video conferences, streaming video etc. With this in mind a user of a WLAN will have high demands on the system and will not accept too much degradation in performance to achieve mobility and flexibility. This will in turn put high demands on the design of WLANs of the future. Security is main concern for many networks and for wireless network it is very important because wireless medium is open for public access within certain range. Only authenticated users and computers can access this network to solve any type of WLAN issues related to security and take care of two-way authentication between the communicating entities, method of dynamically allocating the encryption keys, use some kind of centralized Authentication mechanism, enhanced encryption algorithms and efficient key management techniques . Various services being offered by any security mechanism includes:

- Data Secrecy/Privacy
- Data Integrity
- Access Control

Wired Equivalent Privacy (WEP) [1] protocol (WEP) was implemented into the IEEE 802.11 standard for wireless LAN communications in the late 1990s. It only took a few months for the first research papers on WEP's poor implementation of the RC4 encryption key stream to surface in the scientific community. Fluhrer, Mantin and Shamir (FMS) were the first to submit that by collecting enough data packets from a wireless communication protected by WEP, a computer could calculate, with high statistical accuracy, the secret encryption key and thus break the encrypted cipher text. [15]. However, WEP was an early attempt to secure wireless networks, and better security is now available such as DES, VPN, and WPA [2]. WEP is not difficult to crack, and using it reduces performance slightly. . In order to remove these vulnerabilities a technique called WPA(Wi-Fi Protected Access)[3] was developed. It was deprecated in 2004 and is documented in the current standard. It is an interim solution that is used now until 802.11i comes out. It still using RC4, but the Key was changed to TKIP.TKIP basically works by generating a sequence of WEP keys based on a master key, and re-keying periodically before enough volume of information could be captured to allow recovery of the WEP key. The IEEE 802.11i amendment introduces a range of new security features that are designed to overcome the shortcomings of WEP. It introduces the concept of a Robust Security Network (RSN) [4], which is defined as a wireless security network that allows the creation of Robust Security Network Associations (RSNA) only which acts as a key management scheme in IEEE 802.11i framework and validates that Pairwise Master Key (PMK) has been established. It further helps in the synchronization of temporal keys which are installed for the process of authentication and encryption being carried out in 802.11i Framework that overcomes the WEP and WPA flaws.

In this paper , mainly concentrate on 2 types of attacks they are: active attacks and passive attacks (i.e. denial of services and memory exhaustion)which are present in 4-way handshake mechanism which makes IEEE802.11i amendment vulnerable to attacks and thus making the encryption and authentication process more secure This paper is organized as follows: Section 2 overview of IEEE 802.11i framework, various confidentiality and integrity protocols being used and the potential threats arising from them. Section 3 modified, enhanced and proposes authentication mechanism for key management. Section 4 conclusion and future work.

2. IEEE802.11I SECURITY ANALYSIS

To analyze the various types of active and passive vulnerabilities, it is mandatory to GIVE BRIEF overview of IEEE802.11i amendment which is then followed by 4-Way Handshake and possible DENIAL of services and memory exhaustion.

2.1 Overview of IEEE802.11i Standard

IEEE 802.11i [5] there are many data encryption algorithms defined by IEEE 802.11i [5]:

1-CCMP is the long-term solution requiring additional hardware capabilities
2-TKIP is the short-term solution to fix WEP problems
3-WEP is included for backward compatibility.

This paper is mainly focused on the protocols authentication and do not investigate these data confidentiality protocols in any detail. The basic elements of 802.1X authentication framework are as follows:

- Supplicant/Client
- Access Point which serves as Authenticator
- Authentication Server(RADIUS)[10]

RSNA [6, 7] establishment use mainly 802.1x authentication protocols followed by protocols for key management. Like any other authentication procedure, firstly a shared key is generated between the client and the authenticator, then this key subsequent temporal keys are generated which is then followed by distribution of usable keys by the key managements protocols for the particular communication session. Figure1 shows the different stages involved in generation of a secure RSNA. The stages involved in generation of RSNA [8] are as follows:-

- Network Discovery Stage
- Authentication and Association Stage
- EAP/802.1X/RADIUS Authentication Stage
- 4-Way Handshake Phase
- Group-Key Handshake
- Secure Data Communication

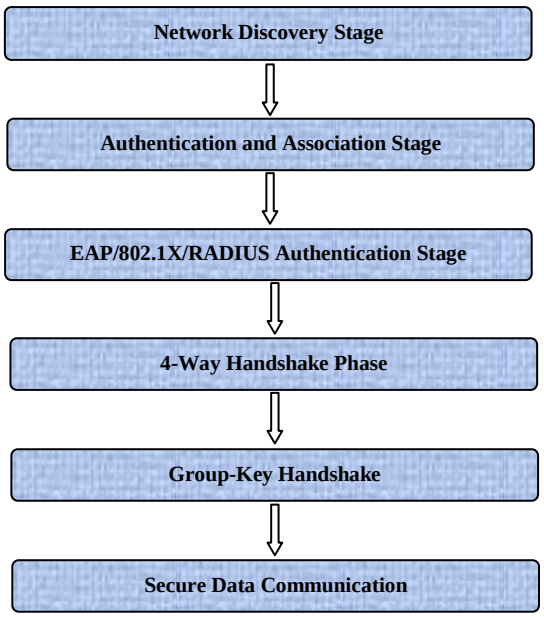

Figure 1: IEEE802.11i Authentication Procedure

Mainly focus here on 4-Way Handshake [9] procedure and various types of Dos Attacks against it.

2.2 Four-Way Handshake

In figure2 there are 4 types of messages that are exchanged between the communicating entities i.e. Supplicant and the AP [11, 12]. First step is the procedure begin by sending of Message1 from AP to Supplicant. Here AP generates ANonce which is a random number, starts a Sequence Number and encapsulates these inside Message1. The Supplicant after receiving message1 generates other random value SNonce, MAC address of the supplicant that is SPA and derives a fresh temporal key Public Transient Key (PTK) which is a function of both SNonce and ANonce and stores both ANonce and SNonce in the memory. Than supplicant generates other message, Message2 which consist of SNonce, Sequence Number, SPA and MIC value which is a function of all other fields and is generated using calculated PTK as the key [7,13]. Now MIC is calculated in order to preserve the integrity of the send message as other fields are sent as plain text. On receiving Message2, AP generates PTK using the same method and verifies received MIC with the calculated one in order to guarantee its integrity [13]. Now it will constructs Message3 as shown in Figure2 which is like an acknowledgement of message2 which is verified at supplicant side in order to confirm that correct PTK has been generated at other end, Message4 is again the acknowledgement for message 3 by the supplicant.

PTK = PTK = PRF (PMK, SNonce, ANonce, AA, SPA)

Here:

- AA: Access Point's MAC address
- SPA: supplicant's MAC address
- ANonce: random number generated by AP
- SNonce: random value generated by Supplicant
- SN: Sequence Number
- MsgX: type of message
- PTK: pairwise transient key
- MIC: message integrity code

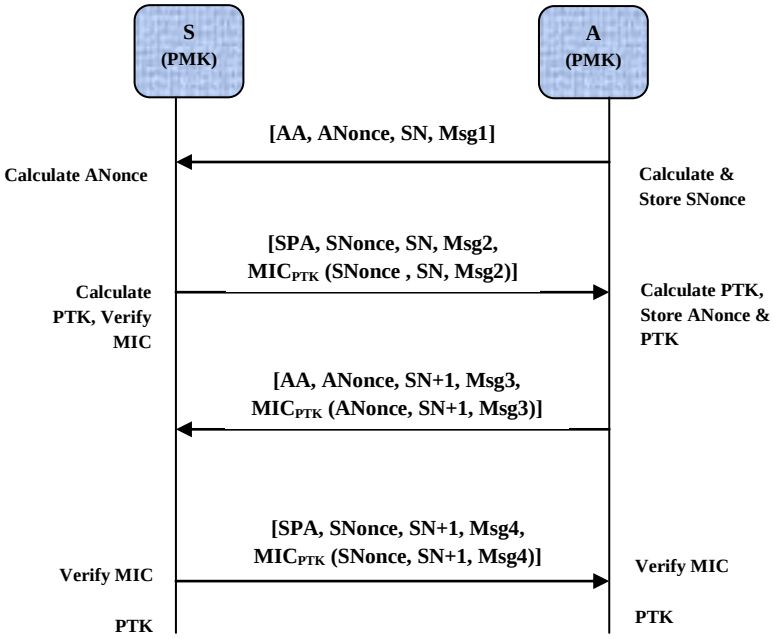

Figure2: 4-Way Handshake Process

2.3 DoS and Memory Exhaustion Attacks on 4-Way Handshake

The mechanism defined by IEEE 802.11i is vulnerable to memory exhaustion attacks [11], [13], [14] and DoS flooding. To handle these types of attacks, need to develop some security mechanisms. The main weakness of 4-way handshake of 802.11i standard is the first message because of not using any MIC field in order to guarantee the message integrity. That's why it can be easily eavesdrop by any hacker since it is broadcasted and all fields of it can easily be known to the hacker. As, supplicant side will have both of the random values SNonce and ANonce as stored and new key PTK is derived from function of these random values.

Then Message 2 is generated and MIC field is calculated using this PTK as secret shared key to preserve the integrity of the message and is attached with the message. On the other side PTK is again calculated with the help of same procedure and MIC is calculated and verified [7]. After sending of Message2 attacker can plays its role and constructs a fake message Message1' which differs in ANonce field value only as it is random value generated by AP and sends it to the supplicant .Suppose the fake nonce value be ANonce'. Supplicant thinking it as genuine stores ANonce', calculates PTK which let be denoted as PTK' and updates the original PTK value to PTK'.

PTK' = PRF (PMF, ANonce', SNonce, AA, SPA)

If the attacker is able to send Message1' between Message 3 *(from AP to Supplicant)* and Message 2 *(from Supplicant to AP)*, then this will lead to storage of ANonce' and PTK' at the supplicant side and sending of Message2' with appended MIC as a function of PTK'. Then the authenticator will send Message3 where attached MIC will be a function of ANonce value. This will lead to failure in integrity check since MIC_{PTK} is not equal to $MIC_{PTK'}$ and hence the Message3 will be discarded without any notification to authenticator.

Now after the timer expire at Authenticator and it has still not received Message4, it will again send Message3 predicting it of being lost during communication but it will again be discarded by Supplicant S because of MIC mismatch. After nth attempt by authenticator and still not getting Message4 it will de-authenticate the supplicant and S will be disassociated and hacker is successful in launching DoS attack. And also attacker is able to launch memory exhaustion attack since sending of each of the fake Message1' result in storing of ANonce' and PTK' value at supplicant side leading to memory exhaustion if continuous flooding of Message1' is done.

According to 802.11i standard, in order to stop the attacker from updating the PTK value to PTK', a mechanism called Temporal Pairwise transient key (TPTK) was developed in which TPTK represents PTK value until Message3 is received and verified. Whenever the supplicant receives Message1 it will generate a TPTK where TPTK = PTK and on all subsequent receiving of Message1' it will update only TPTK value and store them until new Message3 is received and verified. It will not update the value of PTK. But this solution is acceptable only when supplicant has successfully installed PTK and receives Message1' after Message3 has been verified but here they are send before Message3, therefore it is not helpful in preventing the attacks.

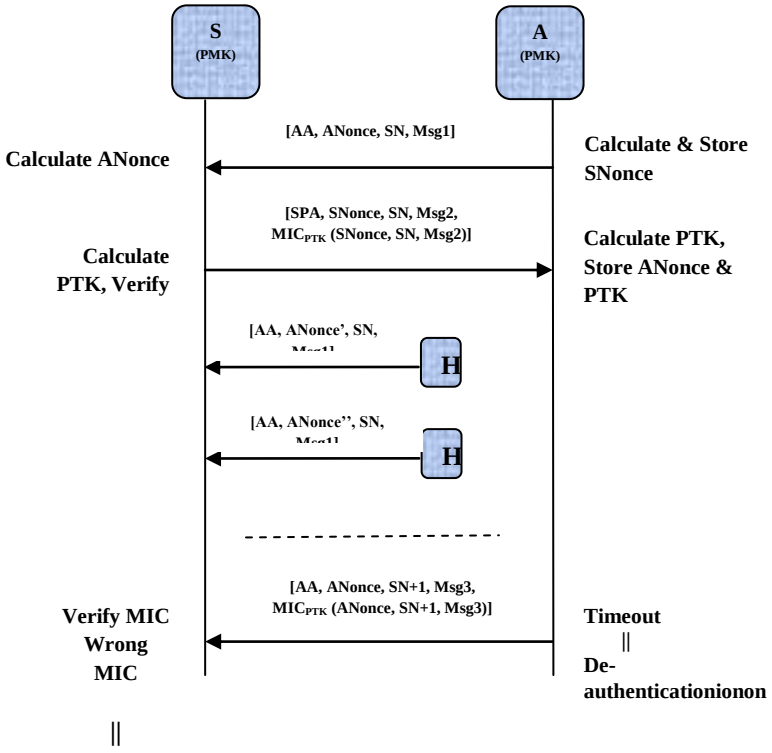

Figure3: DoS Flooding Attack in 4-Way Handshake

2.4 Related Work

According to Mitchell [11], if, add MIC in Message1 then we can easily prevent possible DoS attack because the 4-Way Handshake phase begins both Authenticator and Supplicant shares a common secret key PMK. As we know that PMK is used for adding the MIC value and it is the basic and mandatory element in deriving the series of other keys, so using of it directly in communicating any of the messages

over the network is risky and should be avoided as it becomes vulnerable to attacks.

Second method given by him, were of reusing the SNonce value, that is, as supplicant receives Message1 it will generate and store the value of SNonce, it will not store ANonce and the calculated PTK. Now in case S receives Message1' , in that case S should not update its SNonce value till it will receives message 3 which is verified and then PTK is installed. That's why S will store single SNonce value and re-calculate PTK whenever it receives Message3, this method will solves the problem of memory exhaustion but in case Message3 is flooded than, have to re-calculate the value of PTK again and again but this will again lead to CPU exhaustion attack.

Xiaodong Zha and Maode Ma [7] presented an enhanced 2-Way handshake protocol, according to which AP will generate 2 random numbers ANonce and BNonce, and encrypt these numbers and supplicant MAC address with PMK. AP then encapsulate this inside Message1 and sends it to the supplicant. Supplicant after receiving Message1 decrypts it with PMK and calculates PTK as stated in standard protocol. After this it encrypts the BNonce and generated SNonce with same PMK and encapsulates this inside Message2 and sends it to AP. After receiving Message2, AP again decrypts it with PMK and verifies BNonce value and once verified calculates PTK with the help of same method. It prevents DoS attacks since ANonce value is encrypted but it increases computation power and it is vulnerable to chosen plaintext attacks since PMK is used directly for providing confidentiality services.

3. PROPOSED SOLUTION

Here, public key encryption schemes instead of secret key PMK. As discussed above that the 4-Way Handshake phase begins both Authenticator and Supplicant shares a common secret key PMK and it is used for adding the MIC value which is basic and mandatory element in deriving the series of other keys, so using of it directly in communicating any of the messages over the network is risky and should be avoided as it becomes vulnerable to attacks.

Public key encryption schemes are secure only if the authenticity of the public key is assured. A simple public key algorithm is Diffie-Hellman key exchange. This protocol enables two users to establish a secret key using a public key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established. One of the major roles of public key encryption has been address the problem of key distribution. There are actually two distinct aspects to the use of public key cryptography in this regard:

- The distribution of public keys
  - Public Announcement
  - Publicly Available Directory
  - Public Key Authentication
  - Public Key Certificates
- The use of public key encryption to distribute secret keys
  - Simple Secret Key Distribution
  - Secret Key Distribution with Confidentiality and Authentication
  - A Hybrid Scheme

Now, go for *Secret key distribution with confidentiality and authentication* is based on an approach suggested in [16], provides protection against both active and passive attacks. Let, begin at a point when it is assumed that A and B have exchanged public key. Then the following steps occur:-

- A uses B's public key to encrypt a message to B containing an identifier of A (IDa) and a nonce (N1), which is used to identify this transaction uniquely.
- B sends a message to A encrypted with PUa and containing A's nonce(N1) as well as a new nonce generated by B (N2). Because only B could have decrypted message (1), the presence of N1 in message (2) assure A that the correspondent is B.
- A returns N2, encrypted using B's public key, to assure B that its correspondent is A.
- A selects a secret key Ks, and sends M=E(Pub,E(PRa,Ks)) to B. encryption of this message with B's public key ensures that only B can read it; encryption with A's private key ensures that a could send it.
- B compute D(PUa,D(PRb,M)) to recovery the secret key.

Here:

- PU_a: Public Key of A
- PU_b: Public Key of B
- PR_a: Private Key of A
- PR_b: Private Key of B
- N1: Random Number Generated by A
- N2: Random Number Generated by B
- K_S: Secret Key
- ID_A: Identifier of A
- E: Encryption
- D: Decryption

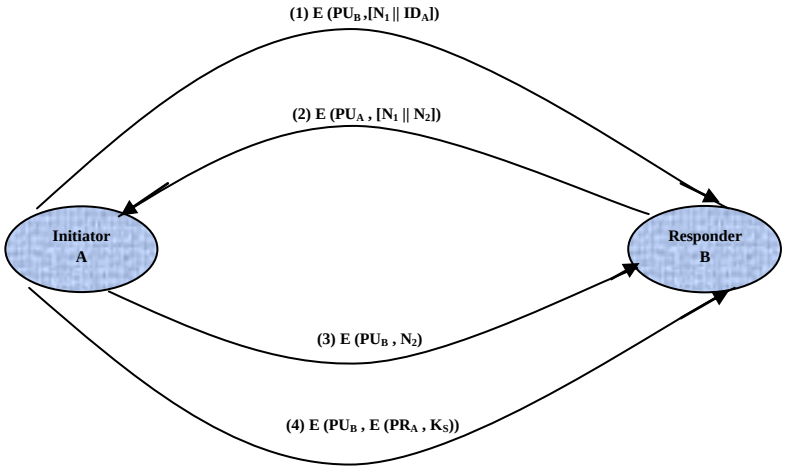

Figure 4: Secret key distribution with confidentiality and authentication

4. CONCLUSION

IEEE 802.11i standard was defined in order to overcome the vulnerabilities in WEP and WPA but still it is not secure against active and passive attacks (DoS attacks and memory exhaustion attacks) in 4-Way Handshake phase. So here Proposed Secret Key Distribution with Confidentiality and Authentication algorithm which provides us secure key distribution over the wireless network. It will work against the active and passive attacks like Denial of Services and Memory Exhaustion. The most vulnerable part of 4-Way handshake phase is message1 which is the first step in this procedure, because this message is send unencrypted over the network. Secret Key distribution procedure will resolves this problem by encrypting ANonce values and by introducing pair of keys that is public key and private key. If Data is encrypted by public key then data should be decrypted by private key. However this solution becomes little complex due to calculation of one more key and using encryption, but it succeeds in providing security against DoS and DoS flooding attacks. This algorithm is also safe for memory exhaustion attacks because ANonce is never stored at the supplicant side since it can be decrypted only by the supplicant. And after ever session these pair's of keys is change to provide security. That's why is procedure is safe from any type of attacks.

5. REFERENCES

[1] IEEE Standard 802.11-1999. Information technology – Telecommunications and information exchange between Systems – Local and metropolitan area networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications. 1999.

[2] IEEE Standard 802.11b-1999. Higher-Speed Physical Layer Extension in the 2.4 GHz Band, Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. September, 1999.

[3] Guide to Internet Security.

[4] What's New in Security: WPA (Wi-Fi Protected Access)?

[5] Seung-Jo HanHeang-Soo Oh JonganPark Dept. of Electron. Eng., Chosun Univ." The improved data encryption standard (DES) algorithm., Spread Spectrum Techniques and Applications Proceedings, 1996.

[6] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1X standard," Tech. Rep. CS-TR-4328, University of Maryland, College Park, Md, USA, February 2002

[7] Xiaodong Zha ; Maode Ma ," Security improvements of IEEE 802.11i 4-way handshake scheme",IEEE International Conference on Communication Systems(ICCS) 2010.

[8] Xinyu Xing; Shakshuki, E.; Benoit, D.; Sheltami, T.; "Security Analysis and Authentication Improvementfor I EE802.11i Specification",Global Telecommunications Conference, 2008.

[9] Jing Liu, Xinming Ye, Jun Zhang, Jun Li, "Security Verification of 802.11i 4-way Handshake Protocol", 2008 IEEE

[10] Sung-Hyun Eum, Yae-Hoe Kim, and Hyoung-Kee Choi,"A Secure 4-Way Handshake in 802.11i Using Cookies", July 2008, Vol.2, No.1

[11] C. He and J. C. Mitchell, "Analysis of the 802.11i 4-Way Handshake," in Proceedings of the 3rd ACM workshop on Wireless security, Philadelphia, PA, USA, 2004, pp. 43 - 50.

[12] V.Moen, H. Raddum, and K. J. Hole, "Weaknesses in the temporal key hash of WPA," ACMSIGMOBILEMobile Computing and Communications Review, vol. 8, no. 2, pp. 76–83, 2004

[13] F. D. Rango, D. C. Lentini, and S. Marano, "Static and dynamic 4-way handshake solutions to avoid denial of service attack in Wi-Fi protected

[14] D. B. Faria and D. R. Cheriton, "DoS and authentication in wireless public access networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe '02), pp. 47–56, Atlanta, Ga, USA, September 2002.

[15] Fluhrer, Mantin, Shamir. "Weaknesses in the Key Scheduling Algorithm of RC4" http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf. 2001.

[16] Needham;R., and Schroeder, M. "Using Encryption for Authentication in Large Networks of Computers". Communications of the ACM, December 1978.