Intensification of 4-way handshaking in IEEE802.11i

Kapil Dev Sharma, Pankaj Dadheech
Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur
Email- skmkapil@gmail.com

Abstract: **Wireless Computer Network is most dominant network for information transmission in modern age. Today due to lack of network security various threats propagate in network. Therefore, security of wireless computer network is big issue,to remove these threats various security algorithms such as Data Encryption Standard (DES), Advanced Data Encryption (AES), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), IEEE802.11i used for achieve enhanced security in wireless network. Wireless network can be protectedif security principles can be bounded with these algorithms. Authentication one of security principlecan be achieved by Three Way Handshake approach, 4-way handshake approach etc. respectively. 4-way handshake approach introduces by many researchers but this approach has some inadequacy eg. Denial of Service (DoS), Memory Exhaustion (ME), Distributed Denial of Service (DDoS), Flooding attacks. These attacks in authentication process make him as unsecure authentication algorithm. Due to exploiting the vulnerabilities in 4-way handshake approach Denial of Services (DoS), Memory Exhaustion (ME) threats propagate in computer network, these attacks can be remedy with the help ofproposed algorithm known as enhanced 4-way handshake approach in IEEE802.11i. Enhanced 4-way handshake process made to reduce these types of attacks Denial of Services (DoS), Memory Exhaustion (ME). Proposed algorithm simulates and gives better result instead of existing 4-way handshake algorithm. The proposed algorithm is secure and efficient algorithm for IEEE802.11i 4-way handshake process.**

Keywords: **4-Way Handshake, DoS attack, ME attack, WPA, AES, Cookies.**

1. INTRODUCTION

Wireless Local Area Network (WLAN) [1-3] succeeded in providing wireless network access at acceptable data transmission rate. Data transmission rate is higher in wireless network so wireless network is much more popular than cellular network and ethernet network. The Institute of Electrical and Electronic Engineering (IEEE) have set a standard IEEE02.11 for data communication in wireless environment. The security is main concern in this technology because in above techniques data transmission is in public shared network. So it is big challenge to secure a data in public shared network. In such types of network there are maximum chances to break the security by unauthorized person. An unauthorized person exploiting the vulnerabilities of the network for propagating various threats [4-6] in secure network. Therefore, to prevent the threats and protect the confidential data by efficient security algorithm for WLAN technology. Such efficient security approach must be fulfillment the entire security principals [7-8] such as integrity, authentication, confidently and access control. In this manuscript handover keying for authentication discuss in details. Authentication defines as:

Authentication- "The identification of individual by the computer system is known as authentication. Authentication can be performs asuser name and password having different forms such as a face reorganization, smart cards,complex word, finger print, or eye prints. Authentication tells about the individual but says nothing about the access rights of the individual."

Some security protocols like WEP, WPA, IEEE02.11i, MIC etc.[9-12] are used for secure WLAN. Wired Equivalent Privacy (WEP) is an earlier wireless security protocol, which is based on "RC4" [13-14] stream cipher encryption technique with key length and initialization vector (IV) 40 bits and 24 bits respectively with integrity of CRC checksum. Therefore, WEP has many drawbacks such as small initialization vector and short RC4 key length as well as XOR operation to encrypt the key with plain text generates the cipher text. So WEP protocol is not an efficient for security principles.

There are so many better security algorithms such as Wi-Fi Protected Access (WPA), IEEE802.11i, Data Encryption Standard (DES), Advanced Encryption Standard (AES) are used. IEEE802.11,Wi-Fi alliance released new security standards for solving the authentication problem and preserve the privacy and integrity of data in air called "Wi-Fi Protected Access" (WPA). IEEE802.1x/EAP (Extensible Authentication Protocol), TKIP (Temporal Key Integrity Protocol) technologies added in WPA to improve the authentication and integrity of information data respectively.

Now IEEE release new security protocol for enhancement of authentication and integrity of information by IEEE802.11i standard. This protocol solves all shortcomings of WEP and WPA. IEEE802.11i adopts "Advanced Encryption Standard"(AES) algorithm for encrypt the data. In this paper two type of attacks, Denial of Services (DoS) and Memory Exhaustion [15-17] are introduced in 4-Way Handshake process. Now some amendments in 4-way handshake process to reduce these threats in during connection establishment between resources.

2. WLAN SECURITY ANALYSIS

2.1 Overview of IEEE802.11i standard

IEEE802.11i [18-19] is an authentication approach in wireless network. In this technology there are three encrypted algorithm CCMP, TKIP and WEP provide security. Temporal Key Integrity Protocol (TKIP) is a short-term protocol to fix WEP drawbacks. However WEP is used for wired equivalent transmission and it is backward compatibility process. WEP is not secure for data transmission with confidently, integrity and authentication. Counter mode with CBC-MAC Protocol (CCMP) is a long-term encryption protocol which required additional hardware compatibilities. So it is difficult to make encryption with key distribution process. However, in this paper our main concern is only on authentication protocol.

RSN IEEE802.11i defines a new logic of Robust Security Network (RSN). According to IEEE802.11i RSN, is description of network that can establish an RSN Association (RSNA) between its entities. RSNA equipment's used pre-RSNA security framework for encryption of information and authentication of message. RSNA security protocol used two encryption protocols CCMP and TKIP as well as for authentication IEEE802.1x and advanced key management mechanism called 4-way handshake for communication with RSNA equipment's. IEEE802.1x/EAP (Extensible Authentication Protocol) is an modify mechanism of WPA. The framework for IEEE802.1x/EAP has three entities to transmit the data such as:

a) Supplicant (a client or end user)
b) Authenticator (Access point or Ethernet Switch)
c) Authentication Server (RADIUS)

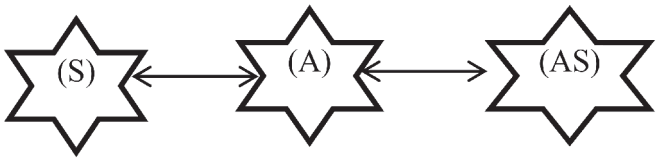

Fig 1: IEEE802.1X/EAP Architecture

In this architecture a client or end user is known as supplicant (S) try to access secure network. The Authenticator (A), an access point (AP) or Ethernet switches offer for access the authenticate services. If client is authorized than authentication server (AS) provides an authentication. Remote Authentication Dial in User Services (RADUS) is an authentication server. In IEEE02.1x/EAP architecture if pairwise master key (PMK) is configure on both supplicant and authenticator side a secure communication established. When PMK configure both side RSNA perform secure communication with the help of following six stages:

a. Network discovery stage

Network discovery is first stage of data transmission in between supplicant (S) and authenticator (A). In this stage AP continuous broadcast a special frames in specify area known as beacon frames for security of WLAN.

b. Authentication and association stage

This is the second stage, when AP continuously broadcast a special beacon frames in a certain area supplicant (S) always try to get the authentication and after that supplicant start associated request frame to authenticator A.

c. EAP / IEEE802.1X / RADIUS Authentication stage

Supplicant (S) gets the authentication connection and starts sending associated request, the RADIUS server (AS) is active and give the authentication

d. 4-way handshake stage

When S and A get a key such as PMK in both ends the 4-way handshake process executes.

e. Group key handshake stage

This is a fifth stage in which, When a fresh Group Temporal Key (GTK) is generated with multicasting applications, this stage is executed. GTK is an optional stage.

f. Secure data communication stage

In this last stage Both S and A exchange cipher suites and security algorithms in this phase data communicate securely if Pairwise Transient Key (PTK) or GTK install at both ends successfully. In this text the focus will be on 4-way handshake process and the reason why this process is open for security vulnerabilities and due to this weakness some DoS attacks and ME attacks are propagated in network.

2.2 4-way handshake process

In 4-way handshake process messages transmitted in between transmission entities such as supplicant S and authenticator A the 4-way handshake mechanism is implemented in which PMK successfully shared on both ends. After sharing of PMK on both sides Msg-1 is transmitted from authenticator A to supplicant S

$$\begin{Bmatrix} \text{Msg}-1: \text{A to S} \\ \text{AA}, \text{ANonce}, \ \text{SN}, \text{Msg}-1 \end{Bmatrix} \quad (1)$$

In Msg-1, ANonce is a random number which starts a sequence number for packet forwarding. AA is MAC address of authenticator A and SN is a sequence number of message. The supplicant S receive a Msg-1 and after that Fresh Temporal Key (FTK) generates a PTK. PTK is used to store ANonce and SNonce, another randomly generated value by supplicant S. In Ms-2 SPA is an MAC address of supplicant and Msg-2 authenticate the message bySPA. Msg-2 is passing from supplicant S to Authenticator A.

$$\begin{Bmatrix} \text{Msg}-2: \text{S to A} \\ [\text{SPA}, \text{SNonce}, \ \text{SN}, \text{Msg}-2, \\ \text{MIC}_{\text{PTK}}\,(\text{SNonce}, \text{SN}, \text{Msg}-2)] \end{Bmatrix} \quad (2)$$

Message integrity code (MIC) is generating when Msg-2 is being sent from S to A. MIC consists the integrity of the message. MIC is to be sent as the plain text message from S to A. Authenticator (A) is receivedMsg-2, authenticator A generates a PTK in the same method as generated by supplicantafter receiving the Msg-2. MIC verifies the consistency and integrity of the message by PTK key. Msg-3 is an acknowledgement of Msg-2 passing from authenticator to supplicant.

$$\begin{Bmatrix} \text{Msg} - 3\text{: A to S} \\ [\text{AA}, \text{ANonce}, \ \text{SN} + 1, \text{Msg} - 3, \\ \text{MIC}_{\text{PTK}}\,(\text{ANonce}, \text{SN} + 1, \text{Msg} - 3)] \end{Bmatrix}$$

After receiving the acknowledgement by supplicant S, S again sends a final message as acknowledgement to A as the Msg-4.

$$\begin{Bmatrix} \text{Msg} - 4\text{: S to A} \\ [\text{SPA}, \ \text{SNonce}, \ \text{SN} + 1, \text{Msg} - 4, \\ \text{MIC}_{\text{PTK}}\,(\text{SNonce}, \text{SN} + 1, \text{Msg} - 4)] \end{Bmatrix}$$

IEEE802.11i has transmitted the data by 4-way handshake process but in this process has some drawbacks (discussed in next section) which are the reason for security vulnerabilities over which DoS attacks and ME attacks can be occurred.

2.3 Dos Attacks and ME Attacks on 4-way handshake process

WLAN associates with an authentication by 4-way handshake process but 4-way handshake process have some weaknesses to provide the ways to compromise the security of the confidential data during the process. Msg-1 in 4-way handshake process is the weak point. In Msg-1 ANonce and SN parameters are sends from authenticator A to supplicant S. Authenticator A calculate PTK after that PTK calculate ANonce. Due to the absence of MIC in Msg-1, it is not a secure communication between A to S.

Unauthorized personals can easily hijack or attack in Msg-1 due to some vulnerability. Which is the biggest eavesdrop of this technique and unauthorized personals steal the information such as MAC address, ANonce, SN and message type therefore, DoS attacks are easy to mount in the network. After receiving the Msg-1 by supplicant S PTK is calculated and ANonce, SNonce both value store on supplicant's side. In response of Msg-1 the supplicant sends the Msg-2 to the authenticator. As the MAC address, ANonce, SN and message type are prone to DoS attacker the DoS attack can easily be carried out by generating the fake message Msg-1' from the authenticator's (attacker) side after receiving the Msg-2. Msg-1 and Msg-1' both are different from each other. Msg-1 sends ANonce to Supplicant S and S calculates PTK and ANonce' is generated by hacker due to the lack of MIC in Msg-1. S sends Msg-2 to A after Msg-2 receives at authenticator side the hacker generates Msg-1' and sends to S which is actually a different from Msg-1 before the actual Msg-3 is to be sent by A. After it a novel PTK i.e. PTK' has been generated by the hacker and can be used for the DoS attack.

PTK'=PRF(PMF, ANonce', SNonce, AA, SPA)S sends Msg-2' to A with the value of ANonce' and PTK' therefore, A silently discarded the message. After that A send Msg-3 to S with A's ANonce value but the ANonce value is changed by ANonce'. After receiving the Msg-3 it gives a failure in integrity of message because MICPTK is not equal to MICPTK'. This is known as man in the middle attack i.e. MITM attack.

Authenticator A will be active and waits for Msg-4 for authentication and association within a time interval. This time interval session is known as time stamp expiration. If the A does not receive the Msg-4 with in a time stamp expiration then A will send Msg-3 again to S but S will discard Msg-3 again because Msg-3' (novel message) has already produced different MIC value. Authenticator A try to sent Msg-3 again and again for the authentication. Finally after the n^{th} attempt as the time stamp expiration session occur, A will be unauthenticated and the message will be considered as disintegrated message. Thus, due to this unauthenticated process the attacker achieves it's task to generate a DoS attack and flooding. Supplicant's local station store the value of ANonce and PTK in his memory, hence the reason for DoS Flooding attacks.

IEEE802.11i protocol provides the solution of updating the value of PTK at the supplicant's side to use a mechanism of temporal PTK (TPTK). TPTK is sent back to the authenticator's side where it is considered as PTK. This process provides a facility to protect the Msg-1 until the Msg-3 is not verified and integrated by the supplicant S. But this is a temporary solution not permanent solution for the problem as the attacker may identifies the association in between TPTK and PTK.

3. INTENSIFICATION OF 4-WAY HANDSHAKING PROCESS IN IEEE802.11i

Proposed enhanced 4-way handshaking process can be improved the security by using following two steps-

1. Encryption of ANonce value- To encrypt the ANonce value use strong encryption algorithm
2. Strengthen the Encryption and securing PTK by using cookies

Above two steps of enhanced authentication process discuss in details under the following four steps-

Initially Message-1 generated by Authenticator (A). A encrypt Msg-1 by strong encryption algorithm. After Msg-1 receives by Supplicant (S) following operations performs:

Step: (i) Receiving of Msg-1 by Supplicant:

Decrypts the ANonce value

Generates SNonce, calculates PTK

Both values, calculated PTK and SNonce sent back as cookie packet

Create and send Msg-2

Step: (ii) Receiving of Msg-2 by A:

Calculation of PTK by same mechanism

Verify MIC

Replay the cookie packet information received from S

Create and send Msg-3

Step: (iii) Receiving of Msg-3 by supplicant:

Decrypt PTK

Verify MIC

Create Msg-4

Step: (iv) Finally when Msg-4 receiving by S, firstly authenticator verifies MIC and then this validates the successful installation of PTK at the authenticator.

4. SIMULATION AND COMPARISON

Initially the existing 4-way handshake process was implemented by the help of Network Simulator (NS2) which is an open source framework for simulating the network behaviour under customized policies. The simulation was carried out under two different situations- (i) There is no flooding or DoS attack, and (b) There is a controlled flooding or DoS attack.

The values for the average delay and success ratio in the receipt of the packets in fixed time durations were collected for both the situations. These values are shown in table-1. Table-1 represents the values for average delay in packet receiving and success ratio for different fixed time durations such as 125, 100, 75, 50 and 25 for both attack and non-attack cases.

In this case, the values for average time delay in packet receiving under attack case are significantly higher than the non-attack case for all the chosen fixed time durations. It represents the effect of flooding attack. Then after the proposed enhances 4-way handshake process was simulated under same two situations i.e. with no flooding or DoS attack and with a controlled flooding or DoS attack. Similarly, the values of success ratio in existing 4-way handshake process show the effect of flooding attack and enhanced 4-way handshake process reduce the effect of flooding attacks.

Table1: Simulated values for existing and proposed end to end delay and success ratio of 4-way handshake process under flooding / DoS attack and without flooding /DoSattack for different fixed time durations i.e125,100,75,50 and 25

Comparison	Time duration	Average delay in packet receiving (msec)	Success Ratio (msec)
Connection establishment through old 4-way handshake algorithm (prone to DoS attacks)	125	1.946565	84.33668
	100	1.632322	89.40327
	75	1.212343	91.65329
	50	0.945555	93.66607
	25	0.753553	94.74312
Connection establishment through proposed 4-way handshake algorithm	125	1.546565	92.33668
	100	1.232322	93.40327
	75	0.912343	95.65329
	50	0.495555	96.66607
	25	0.453553	97.74312

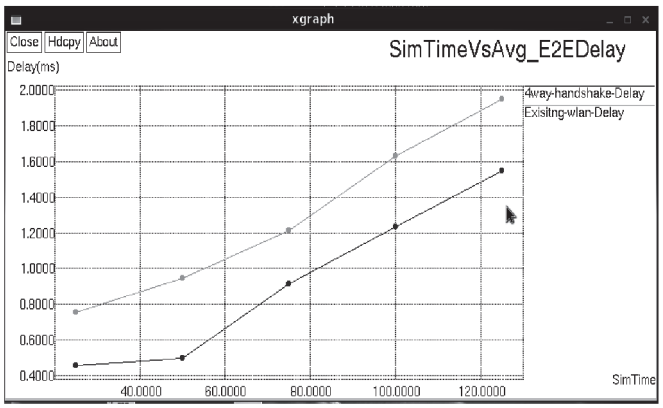

Fig 2: Proposed Avg. Delay and Existing Avg. Delay xgraph

In this case, the values for average time delay in packet receiving under attack case are almost same as in the non-attack case for all the chosen fixed time durations. It represents that there is no effect of flooding attack in the packet transfer. Figure-3 depicts the comparison of proposed and existing 4-way handshake process with flooding/DoS attack and without flooding / DoS attack. In above figure proposed enhanced 4-way handshake process reduces packet delay time and figure 4 shown high delivery ratio. These simulated results enhance handover keying process in IEEE802.11 network

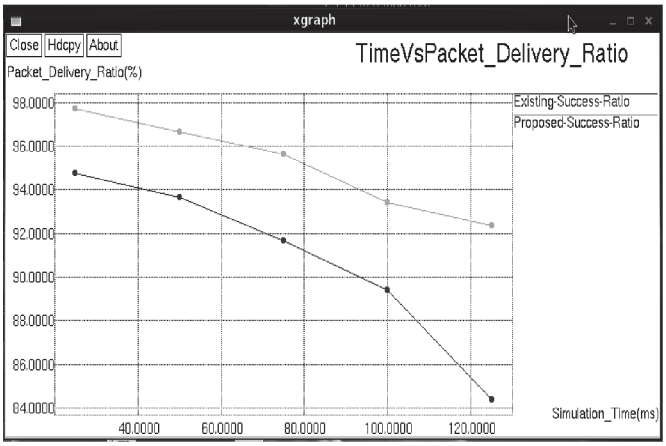

Fig 3: Proposed success ratio and existing success ratio xgraph

5. CONCLUSION

The manuscript explains the 4-way handshake process in IEEE02.11 WLAN network and also explains vulnerabilities towards flooding / DoS attacks. These gaps in 4-way handshaking process breach the security of the information transfer therefore, an intensification of 4-way Handshaking Process over IEEE802.11i.in details. The manuscript simulate on NS-2 platform with getting enhance results instead of existing 4-way handshake process. The comparison of simulated values for both the versions was clearly depicted in the manuscript. The comparison representsthat enhanced 4-way handshake process reduced end to end delay and increase success ratio. These comparison results represent that there is no effect of the flooding/ DoS attacks in the proposed scenario for enhanced 4-way handshake process. This approach simulates over IEEE802.11i with cookies implementation and performance of the network is also improved instead of existing 4-way handshake process.

REFERENCES

[1] Vulic, N., de Groot, S. H., & Niemegeers, I., "A Framework for Integration of different WLAN Technologies at UMTS Radio Access Level", Fourth Annual IEEE International Conference on Communication, Networking & Broadcasting, pp.-441-446, 2006.

[2] Kryvinska, N., Strauss, C., Collini-Nocker, B., & Zinterhof, P., "A scenario of voice services delivery over enterprise W/LAN networked platform". In Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia (MoMM '08), ACM, New York, NY, USA, pp.-332-337, 2008.

[3] Koch, R., Stelte, B., & Golling, M., "Attack trends in present computer networks", IEEE 2012 4th International Conference on Cyber Conflict (CYCON), pp.-1 – 12, 2012.

[4] Mishra, B. K., & Saini, H., "Cyber Attack Classification by Game Theoretic Weighted Metrics Approach", World Appl. Science Journal, 7 (Special Issue of Computer & IT), pp. 206-215, 2009.

[5] Saini, H., & Saini, D., "VAIN: A Stochastic Model for Dynamics of Malicious Objects", ICFAI journal of Systems Management, Vol. 6, No. 1, February 2008, pp. 14-28.

[6] Saini, H., & Panda, T.C., "Extended Cyber Defense Architecture for a University- A Case study", The IUP Journal of Science & Technology, Vol. 6, No. 2, pp. 33-47, June 2010.

[7] Saini, H., Panda, T. C., & Panda, M., "Prediction of Malicious Objects in Computer Network and Defense", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, pp.-161-171, 2011.

[8] Lashkari, A. H., Danesh, M. M. S., Samadi, B., "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)", 2nd IEEE International Conference on Computing & Processing (Hardware/Software), pp.-48 – 52, 2009.

[9] Wong, F. L., & Stajano, F., "Multichannel Security Protocol", Pervasive Computing, IEEE, Computing & Processing (Hardware/Software), Volume: 6, Issue: 4, pp.-31 – 39, 2007.

[10] Comon-Lundh H., Cortier V., & Zălinescu E., "Deciding security properties for cryptographic protocols Application to key cycles". ACM Trans. Comput. Logic, 11, 2, pp 1-39, Article 9 (January 2010).

[11] Boyle, D., & Newe, T., "Security Protocols for Use with Wireless Sensor Networks: A Survey of Security Architectures, Wireless and Mobile Communications", 2007. Third International Conference on Communication, Networking & Broadcasting (ICWMC'07), pp.-54, March 2007.

[12] Yu, Q., & Zhang, C. N., "RC4 state and its applications, Privacy, Security and Trust (PST)", 2011 Ninth Annual International Conference, pp. 264-269, July 2011.

[13] Mantin, I., "A practical attack on the fixed RC4 in the WEP mode". In Proceedings of the 11th international conference on Theory and Application of Cryptology and Information Security (ASIACRYPT'05), Bimal Roy (Ed.). Springer-Verlag, Berlin, Heidelberg, 395-411, 2005.

[14] Lei, C., & Dejian, Y., "DoS and DDoS Attack's Possibility Verification on Streaming Media Application", International Symposium on Information Science and Engineering, 2008. ISISE '08. Volume: 2, pp.-63 – 67.

[15] Lee, B., Bae, S., & Han, D., "Design of Network Management Platform and Security Framework for WSN", IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008. SITIS '08. pp.-640 – 645.

[16] Mathew, R., & Katkar, V., "Survey of low rate DoS attack detection mechanisms". In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (ICWET '11). ACM, New York, NY, USA, 955-958, 2011.

[17] Liu, J., Ye X., Zhang J., & Li J., "Security Verification of 802.11i 4-way Handshake Protocol", ICC 2008 proceedings, IEEE Conference, pp.-1642-1647, May 2008.

[18] Wang, L., & Srinivasan, B., "Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard", Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp.-109-113, 2010.

[19] Xiawen X., Ding J. & Zhou N., "An improved mechanism for four-way handshake procedure in IEEE802.11i", Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference, ISSN-9781424455379, pp-419-422,2010.

◆ ◆ ◆