International Journal of Information & Network Security (IJINS)
Vol.2, No.3, June 2013, pp. 229~238
ISSN: 2089-3299

Enhanced 4-way Handshake Process in IEEE802.11i with Cookies

Hemraj Saini*, Kapil Dev Sharma, Pankaj DadheechAuthor***, T.C.Panda******
* Departement of Computer Science & Engineering, Jaypee University of Information Technology, INDIA
** & ***Departement of Computer Science & Engineering, SKITMG, INDIA
**** *Orissa Engineering College, INDIA*

Article Info

Article history:

Received Jan 03rd, 2013
Accepted Feb 15th, 2013

Keyword:

4-Way Handshake Process
Enhanced 4-Way Handshake Process
DoS Attacks
Confidentiality
Integrity

ABSTRACT

In today's fast online information processing era, it is mandatory to deal with the security issues in the computer networks. WiFi Protected Access (WPA), IEEE802.11i, Data Encryption Standard (DES), Advanced Encryption Standard (AES) are used to achieve better security. The paper deals to explain and avoid the two types of attacks, Denial of Service (DoS) and Memory Exhaustion (ME), generated during the 4-way handshake process used for connection establishment over IEEE802.11i. Some amendments in 4-way handshake process are made to reduce these types of attacks. An enhanced 4-way Handshake Process over IEEE802.11i with Cookies Implementation is proposed with discussion. Finally, a conclusion and future work is provided with an exhausted result discussion and analysis of the work.

Corresponding Author:

Hemraj Saini,
of Computer Science & Engineering,
Jaypee University of Information Technology,
Wakanaghat, solan-173234, INDIA
Email: hemraj.saini@juit.ac.in; hemraj1977@yahoo.co.in

1. INTRODUCTION

Wireless local area network (WLAN) is a widely popular area in current era of the information transmission. Presently WLAN technology [1, 2, 3] is widely used in university campuses, resident hostels, corporate offices, security agencies and national army. The main reason of the popularity of WLAN technology is the transmission rate which is higher than cellular and Ethernet transmission rate. The security of the data is another main concern in WLAN Technology due to the data transmission in public shared network. As in public shared network there is a maximum chance to attack the data by the unauthorized personals by exploiting the vulnerabilities of the network for propagating various threats [4, 5, 6]. Therefore, the efficient security measures in WLAN Technology against the unauthorized personals are to be implemented to protect the confidential data in network. Security of a network can be ensured by the fulfillment of the entire security principals such as [7, 8]

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

Confidentiality-"Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Confidentiality is one of the important design goals for all cryptosystems. Confidentiality also refers to an ethical principle associated with several professions (e.g., medicine, law, religion and journalism). In ethics or law, some types of communication between a person and one of these professionals are 'privileged' and may not be discussed or divulged to third parties. In those

jurisdictions, in which the law makes provision for such confidentiality, there are usually penalties for its violation. Confidentiality of information, enforced in an adaptation of military's classic 'need-to-know' principle, forms the cornerstone of information security in today's corporate."

Integrity-"To control the level of redundancy, the whole system is divided into various parts. These various parts must be interrelated by some specific relationships, so that they can interact and provide a better way of control and communication. Integrity comprises the personal inner sense of 'wholeness' deriving from honesty and consistent uprightness of character. The etymology of the word relates it to the Latin adjective integer, i.e., whole or complete. Evaluators, of course, usually assess integrity from some point of view, such as that of a given ethical tradition or in the context of an ethical relationship."

Access Control-"It refers to mechanisms and policies that restrict access to computer resources. It creates the hierarchy of all the resources in the form of independent layers so that one layer can have its own access rights and cannot interfere in the functioning of other layer."

WLAN is secured with some of the security protocols like WEP, WPA, IEEE802.11i, MIC etc. [9, 10, 11, 12]. Wired Equivalent Privacy (WEP) is a wireless security protocol which encrypts the transmitted data in computer network. It is an earlier protocol used in WLAN technology that encrypts the data with RC4 stream cypher algorithm [13, 14] having key-length and initialization vector (IV) 40 bits and 24 bits length respectively with integrity of CRC checksum. Therefore, WEP is difficult to crack but it reduces the performance of the computer network due to computational overhead.

Now days, for better security, WiFi Protected Access (WPA), IEEE802.11i, Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are used. WPA is designed by IEEE802.11i and WiFi alliance. WPA helps to reduce the bugs generated in WEP. WPA is considered as the best security dynamic protocol because it resolves inconsistency. WPA encrypts the data with the help of (MIC). In this paper, two types of attacks, Denial of Service (DoS) and Memory Exhaustion (ME) [15, 16, 17] are included. These attacks are generated in 4-way handshake process. Now, some amendments in 4-way handshake process are made to reduce these types of attacks. This is marked as enhanced 4-way handshake process with cookies. In this process the enhanced authentication mechanism, encryption algorithms and key management systems are to be used with cookies implementation. In the text enhanced 4-way handshake process is discussed with an extensive literature survey, overview of 802.11i framework, various confidentiality and integrity protocols being used in potential threats. Finally, a conclusion and future work is provided with an exhausted result discussion and analysis of the work.

2. SECURITY ANALYSIS

2.1. Overview of IEEE802.11i standard

In IEEE802.11i [18, 19] there are three encryption algorithms CCMP, TKIP and WEP. Counter Mode with CBC-MAC Protocol (CCMP) is long-term encryption mechanism requiring additional hardware compatibilities because it is difficult to make it hardware compatible and acceptable dynamic key distribution. TKIP is a short-term protocol to fix to WEP problems. WEP is a backward compatible algorithm used to handle the privacy of wired equivalent transmission. However, the present paper mainly concern over the protocol authentication only. In WEP IEEE802.11i it gives an architecture which is further modified for WPA as IEEE802.1X/ (Extensible Authentication Protocol) EAP. The framework for IEEE802.1X/EAP has three entities to transmit the data-

a. Supplicant (A client)
b. Authenticator (Ethernet switch or Access point)
c. Authentication Server (RADIUS and EAP Protocol)

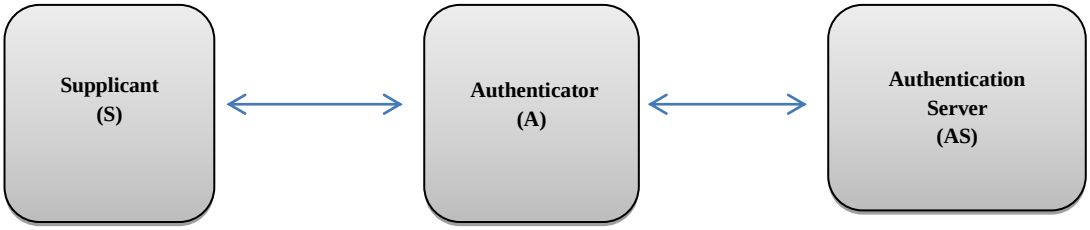

Figure-1: IEEE802.1X/EAP Architecture

In IEEE802.1X/EAP architecture, the supplicant S is a client or end user that asks for access the network. The authenticator A, an access point (AP) or Ethernet switch that offer to access the authenticate service. Authentication server AS provides the authentication for an authorized clients i.e. Remote Authentication Dial in user service (RIDUS). IEEE802.1X/EAP framework secures transmission on Robust Security Network Association (RSNA) concept. RSNA is a key management scheme in IEEE802.11i with Pairwise Master Key Establishment (PMK). RSNA performs secure transmission with the help of following six stages-

a. Network discovery stage

Network discovery is first stage for transmission between two devices S and A. In WLAN the authenticator such as AP continuously broadcast a special frame in a limited area and such frames are called as beacon frames. Beacon frames represent the security of network.

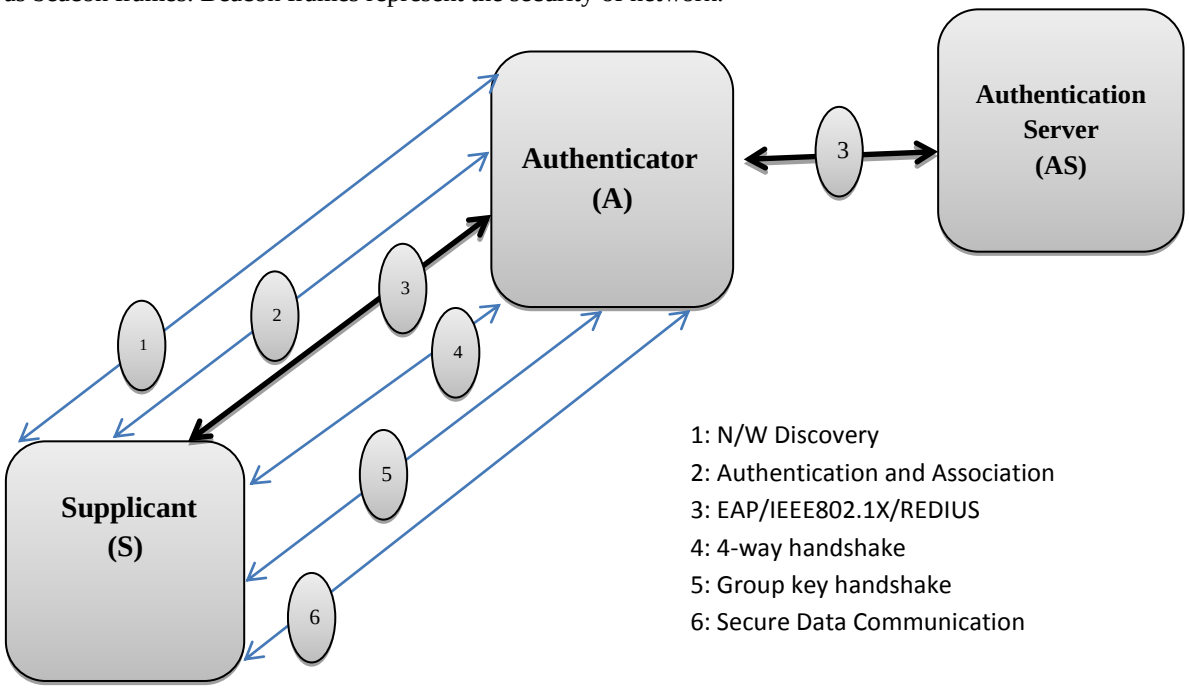

Figure-2: RSNA is used to perform secure transmission in IEEE802.11i

b. Authentication and association stage

AP continuously broadcast the beacon frames at the limited coverage criteria, the supplicant S tries to get the authentication and get connection. After that supplicant starts associated request frame to authenticator A.

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

Supplicant gets the authentication connection and starts sending associated request, the RADIUS server is active and give the authentication.

d. 4-way handshake stage

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

e. Group key handshake stage

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

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

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 sides. After sharing of PMK on both sides Msg-1 is transmitted from authenticator A to supplicant S.

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

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 receives a Msg-1 then Fresh Temporal Key (FTK) generates a PTK which is used to store ANonce and SNonce, another randomly generated value by supplicant S. SPA, is a MAC address of Supplicant for the authentication of Msg-2. Msg-2 is passing from supplicant S to Authenticator A.

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

When Msg-2 is being sent from S to A the message integrity code (MIC) is generating which consists the integrity of the message. This MIC is to be sent as the plain text message from S to A. Msg-2 is received by the authenticator A, after receiving the Msg-2, authenticator A generates a PTK in the same method as generated by supplicant. The PTK verifies MIC consistency of the integrity of the message. Msg-3 is an acknowledgement of Msg-2 passing from authenticator to supplicant.

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

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

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

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.

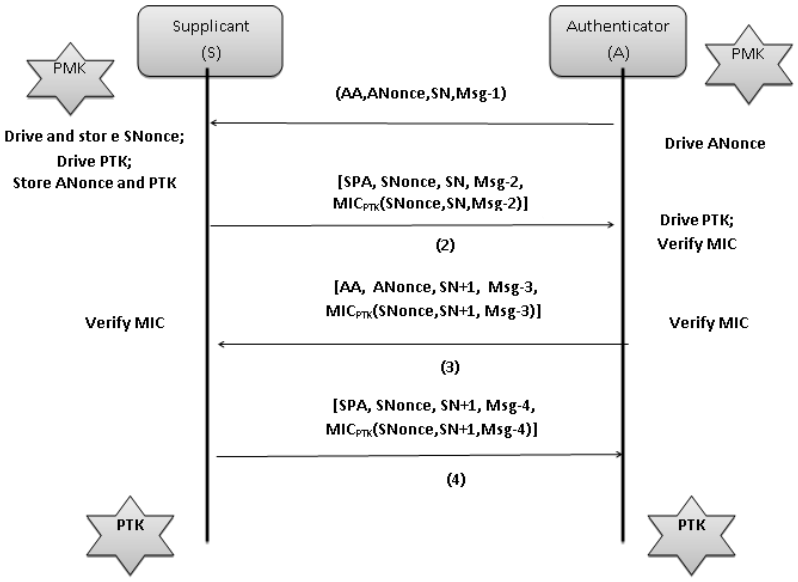

Figure-3: 4-way handshake process

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 is the weak point of 4-way handshake process. In Msg-1 authenticator A sends ANonce and SN to supplicant S. Authenticator A calculate PTK. PTK calculate ANonce. Due to the lack of MIC in Msg-1, it is not a secure communication between A to S.

Unauthorized personals can easily hijack Msg-1 which is the biggest eavesdrop and Unauthorized personals hijack MAC address, ANonce, SN and message type therefore, DoS attacks are easy to mount. 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 A. 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 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 ANonc' is generated by hacker due to the lack of MIC in Msg-1. S sends Msg-2 to A after the A receives Msg-2 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 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. Msg-3 has to be sent again and again for the authentication. After nth attempt as the time stamp expiration session occur, A will be unauthenticated and the message will be considered as disintegrated message. Thus, the attacker successfully achieves its task to generate a DoS attack and flooding. DoS flooding attack, all the value of ANonce and PTK store in Supplicant's local station, hence, the reason for DoS Flooding attacks.

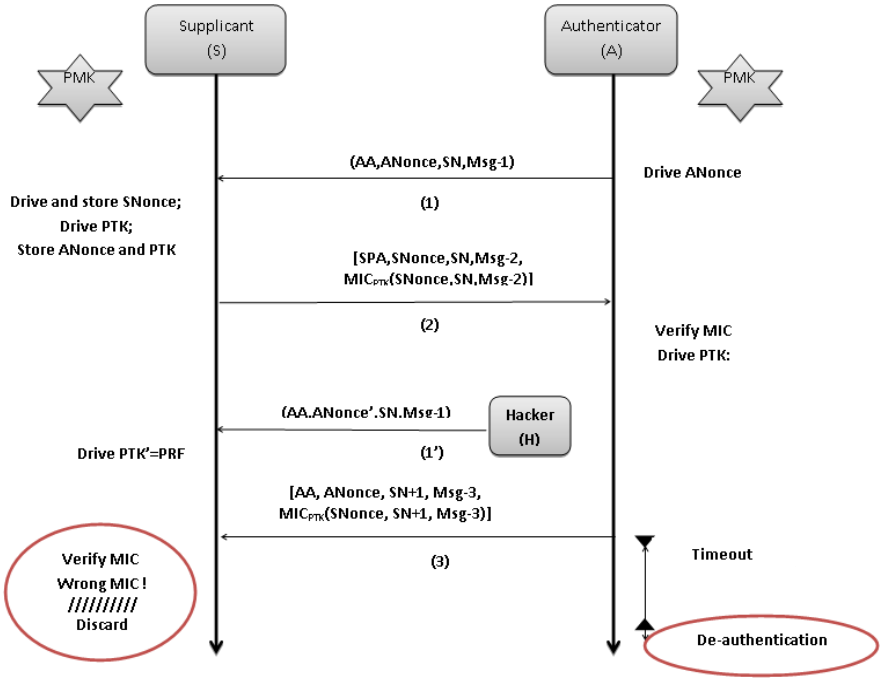

Figure-4: DoS Attack in 4-way handshake Process

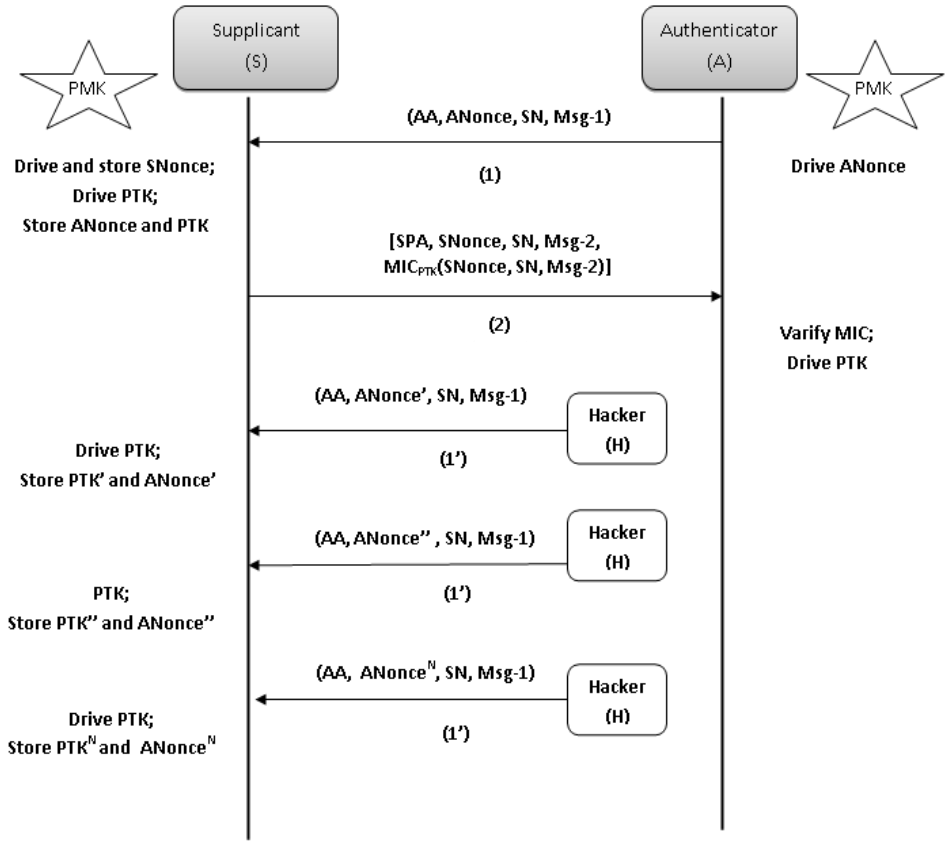

Figure-5: DoS Flooding Attack in 4-way handshake Process

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 provides a facility to protect the Msg-1 until the Msg-3 is not verified and integrated by the supplicant S. But it is not the permanent solution for the problem as the attacker may identifies the association in between TPTK and PTK.

3. ENHANCED 4-WAY HANDSHAKE PROCESS IN 802.11I WITH COOKIES IMPLEMENTATION

4-way process can be improved by using following two steps-

1. Encryption of ANonce value
2. Strengthen the Encryption and securing PTK by using cookies

The whole enhanced process can be summarized as under-

(i) Receiving of Msg-1 by Supplicant:

- Decrypts the ANonce value
- Generates SNonce, calculates PTK
- Sent back the calculated PTK and SNonce as cookie packet
- Create and send Msg-2

(ii) Receiving of Msg-2 by AP:

- Calculation of PTK by same mechanism
- Verify MIC
- Sent back the information received from the cookie packet
- Create and send Msg-3

(iii) Receiving of Msg-3 by supplicant:

- Decrypt PTK
- Verify MIC
- Create Msg-4

(iii) After receiving Msg-4, firstly Authenticator verifies MIC and then this validates the successful installation of PTK at the authenticator.

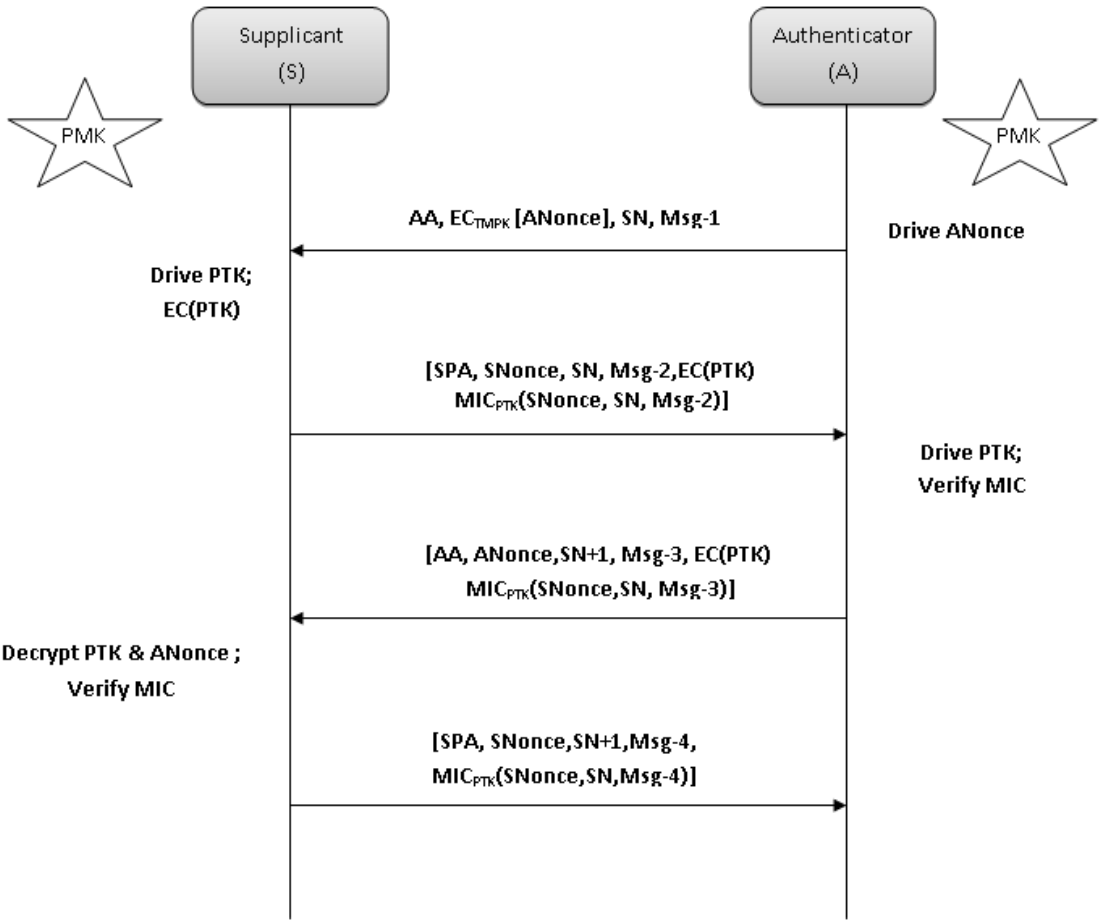

Figure-6: Enhanced 4-way Handshake Process in 802.11i with Cookies Implementation

4. SIMULATION AND COMPARISON

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

The values for the average delay in the receipt of the packets in fixed time durations were collected for both the situations. These values are depicted by table-1. In the first row of table-1 represents the values for average delay in packet receiving for different fixed time durations such as 1000, 900, 800, 700 and 600 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 affect 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.

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 affect of flooding attack in the packet transfer. Figure-7 and figure-8 respectively depicts the comparison of proposed and existing 4-way handshake process with flooding/DoS attack and without flooding/DoS attack.

Table1: Simulated values for existing and proposed 4-way handshake process under flooding/DoS attack and without flooding/DoS attack for different fixed time durations i.e 1000, 900, 800, 700 and 600.

	Flooding/DoS Attack			**No Flooding/DoS Attack**		
	Time duration for test	Average time delay in packet receiving (msec)	Packet Flooded	Time duration for test	Average time delay in packet receiving (msec)	Packet Flooded
Connection establishment through Old 4-way Handshake Algorithm (Prone to DoS attack)	1000	73	32	1000	65	31
	900	68	29	900	58	27
	800	63	26	800	55	23
	700	56	22	700	56	19
	600	52	19	600	47	18
Connection establishment through Proposed 4-way Handshake Algorithm (Not prone to DoS attack)	1000	66	35	1000	65	33
	900	59	31	900	60	30
	800	57	28	800	56	29
	700	55	23	700	54	24
	600	48	21	600	49	20

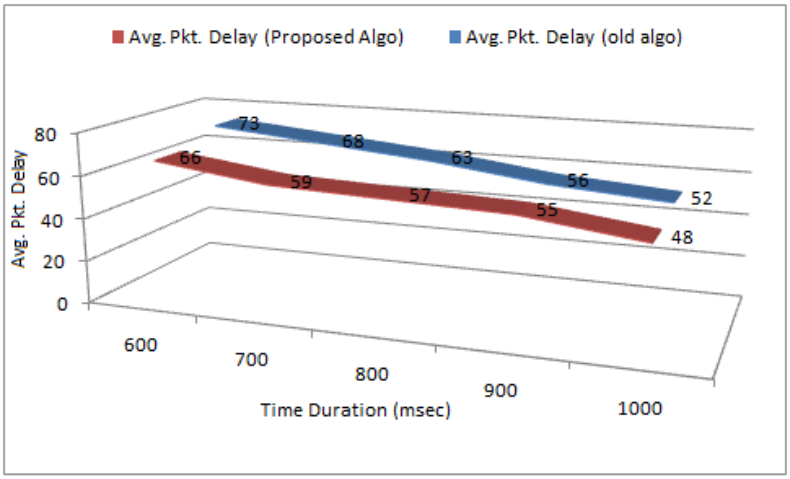

Figure-7: Comparison of Proposed and old 4-Way Handshake process with DoS Attack

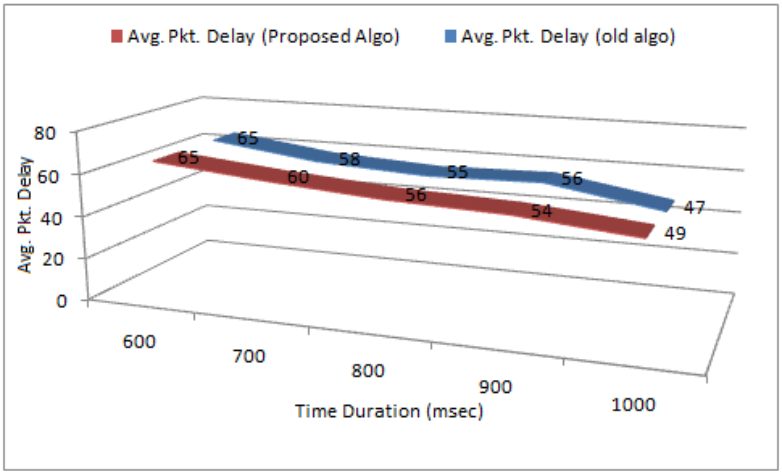

Figure-8: Comparison of Proposed and old 4-Way Handshake process with no DoS Attack

5. CONCLUSION

The manuscript explains the 4-way handshake process in detail and its vulnerabilities towards flooding/DoS attacks. These lacunas in the process may lead to breach the security of the information transfer therefore, an enhanced 4-way Handshake Process over IEEE802.11i with Cookies Implementation is proposed with discussion. The comparison of the simulated values for both the versions was clearly depicted in the manuscript. The comparison represents that there is no affect of the flooding/ DoS attacks in the proposed scenario for enhanced 4-way handshake process over IEEE802.11i with Cookies Implementation and performance of the network is also remain almost same as in 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, Article 9 (January 2010), 42 pages.

[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 pages.

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

BIOGRAPHY OF AUTHORS

Hemraj Saini received his PhD in Computer Science from Utkal University, VaniVihar, Bhubaneswar (ODISHA), M.Tech. degree in Information Technology from the Punjabi University, Patiala, Punjab and B.Tech. in Computer Science & Engineering from National Institute of Technology, Hamirpur (H.P.). Since 1999, he has been actively engaged in Research, Teaching and academic Development activities. Currently he is attached with the Department of Computer Science & Engineering / Information & Communication Technology of Jaypee University of Information Technology, Wakanaghat (Solan) INDIA. His main professional interests are in Cyber Defense, Software Testing, Enterprise Application Integration, Image processing and Intelligent Techniques. He has played an important role for organizing various National and International Conferences successfully funded by Department of Science & Technology, Govt. of India, New Delhi, CSIR, Govt. of India, New Delhi and AICTE, Govt. of India, New Delhi. In addition to it he has published more than 40 research articles in various National/International Journal/Conferences of repute.

Kapil Dev Sharma is M.Tech scholar in Computer Science & Engg. from Rajasthan Technical University (Kota) at Swami Keshvanand Institute of Technology, Management & Gramothan Jaipur (Rajasthan). He has completed his B.Tech degree in Computer Science from Rajasthan University (Jaipur), Institute of Engineering & Technology Alwar (Rajasthan). He actively attended various conferences of National/International repute and continuously publishing papers in conferences and journals. His main professional interests are in Cyber Defense & Image Processing.

Pankaj Dadheech received his M.Tech. in Computer Science & Engineering from Rajasthan Technical University, Kota & B.E. in Computer Science & Engineering from University of Rajasthan, Jaipur, India. He is currently working as a Reader in the Department of Computer Science & Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur. To his credit, he has more than 17 publishing in the proceedings of the reputed National & International Conferences and journals. He is also guiding students for M.Tech affiliate to Rajathan Technical University, Kota. His research interest includes Data Mining Techniques, Grid & Cluster Computing.

T. C. Panda is a Retd. Professor of Mathematics (Berhampur University, India), Founder Professor of Mathematics & Computer Sc. (Mizoram Central University, India) and currently associated as Principal with Orissa Engineering College, Bhubaneswar, Orissa, India-752050. He received his Masters from Banaras Hindu University in 1968 and Ph. D. from Berhampur University in 1975. His main interests are Fluid Dynamics, Air Pollution Modeling, Monsoon Dynamics, Numerical Weather Prediction, Meso-Scale Modeling, Remote Sensing Techniques, Numerical Solution of Partial Differential Equations and Cyber Defense.