ISSN:0975-9646

Comparison of TPatLetEn with TPF in Detecting and Preventing DoS Attack

Durairaj M [#1], Persia A [*2]
[#] *Assistant Professor, * Research Scholar*
[#*] *School of Computer Science, Engineering and Applications,*
Bharthidasan University
Tiruchirappalli, Tamilnadu, India

***Abstract*—Denial of Service (DoS) attack is the foremost dispute in the Wireless infrastructure network. DoS make the network possessions inaccessible to its authentic users. The appropriate client's identity is hoaxed and deprived of from retrieving the network because of this DoS attack. Dearth of fortification in the Management Frame is the imperative origin which hints to DoS attack. Though 802.11w was developed to protect the management frame, the network is vulnerable to different DoS attacks and unsuccessful to prevent all types of DoS attacks. The network vulnerability on DoS attack motivated us to propose a mechanism to detect and prevent DoS attacks in substantial numbers. We proposed two DoS attacks prevention mechanisms called as TPatLetEn (Traffic Pattern Filtering with Letter Envelop Protocol) a hybrid mechanism and TPF (Traffic Pattern Filtering). This paper compares the effectiveness of TPatLetEn with TPF to perceive and avert DoS attack.**

Keyword-DoS Attack, MAC spoof, 802.11w, TPatLetEn, Infrastructure Network

I. INTRODUCTION

Numbers of security encryption algorithms were deployed over the years to address the security lapses resulted due to DoS attacks but still the weaknesses are there in the management frame. Management frameswere not encrypted until 802.11w standard protocol came into the work [1, 2]. The 802.11w management frames are encrypted using AES-CCMP (Advanced Encryption Standard - Counter mode CBCMAC Protocol) algorithm. The AES-CCMP encryption algorithm could not prevent DoS attacks entirely. This algorithm prevents disassociation and de-authentication attacks which happenonly after key establishment [3]. It is not possible for AES-CCMP algorithm to guard the frames which are sent proceeding of key establishment. The AES-CCMP is not widely accepted mechanism even though it prevents DoS attacks in some extent. AES-CCMP is not popular across wireless community and not applied for security at present. The DoS attacks are the results of vulnerability in management frame and a popular mechanism to detect and prevent DoS attack is the sequence number based detection system but it has limitations [4]. The literatures say that there are no effective IEEE approved ways to address the security lapses in wireless infrastructure network.

Existing Traffic Pattern Filtering (TPF) and Letter Envelop Protocol (LEP) have number of retreatblemishes. These algorithmsare individually effective in some of the enormousness only. TPF is effective in spirited DoS attacks whereas LEP is effective in sluggish rate DoS attack [5]. When there are heavy attacks, LEP mechanism is excruciating; as a result, the whole networkswill be collapsed. The infrastructure network gets damaged when there are slow rate DoS attacks in TPF, which disengagethe genuine client. If both LEP and TPF mechanisms are bludgeoned together, the resulted algorithm becomes remarkably effective in detecting and preventing DoS attack.

In this paper, section II presents the background and related works to understand the paper. Section III explains the architecture of the proposed technique and presents the TPatLetEn algorithm. This section also explains how it foils DoS attacks in an infrastructure network and deployment strategy of algorithms in start and logoff frame attacks. The comparison of TPF with TPatLetEn is discussed in Section IV. This section also describes the functioning of TPatLetEn against DoS attacks. Finally, Section V concludes the paper.

II. RELATED WORK

Thuc D. Nguyen et al., [5] developed a light weight solution to defend against attacks on Management Frames. It is based on the factorization problem.

Mina Malekzade et al., [6] developed an experimental framework to measure the possible attacks using unprotected EAP frames against wireless communication.

Chibiao Liu et al., [7] presented a solution to detect and resolve AuthRF and AssRF attacks based on an experimental framework. It quantifies both the attacks against TCP and wireless voice over communication.

Manish Garg et al., [8] discussed the methodology of initiating DoS attacks and to create threats to security with the effect of DoS on WLAN. It is demonstrated that the attacks can be easily initiated and the difficult task is to prevent those attacks.

Tenatat Saelim,et. al.[9], provided a MAC spoofing detection algorithm for IEEE 802.11 networks. To differentiate an attacker station from a genuine station, this algorithm utilizes Physical Layer Convergence Protocol (PLCP) header of IEEE 802.11 frames. Experimental results showed that a cent percentage of MAC spoofing DoS detection when two monitoring stations are located at an appropriate location.

III. TRAFFIC PATTERN FILTERING WITH LETTER ENVELOP PROTOCOL (TPATLETEN)

Management Frames are easily susceptible to attacks, hence MFssent as unauthenticated. The solution proposed

in this paper is to protect the Management Frames (MF) against attacks. The Letter Envelop Protocol (LEP) [5] is proposed to prevent Request Flooding Attacks. The LEPis based on the Factorization problem. The Letter Envelop protocol works as follows:

- The client randomly generates two prime numbers p1 and q1. Then N1 is computed as N1=p1*q1. In the same way, access point (AP) generates p2, q2 and computes N2.
- During the authentication, the client sends an "envelop" containing N1 to the AP. The AP stores N1 and sends N2 to the client. The N2 sent by AP is common for all clients.
- When the client wants to disconnect, it sends the De-authentication Frame to the AP, along with the p1. Then, the AP computes p1/N1 and finds whether it corresponds with the already stored N1.
- If the value corresponds with the q1 it already sent, the client gets disconnected from the network. Otherwise, the frame is rejected as it is from the hacker.
- Similar procedure is followed for AP when it wants to disconnect from the client.
- If AP wants to de-authenticate from the network, it sends p2 to all the clients in the network.
- The N2, which is sent by AP, is common for all the clients. Clients check the received p2 with N2.
- If the clients received q2 from AP during the checking process, they infer it as the request from the AP and disconnect AP from the network.
- In such a case, when an AP is disconnected, the clients have to search for another APand start from the authentication process.

This solution is found to be effective in preventing MAC spoof DoS attack. Even though the hacker succeededto spoof the MAC Address, this will not make any effect to the legitimate client. The authentication process is progressed based on envelop-protocol. The hacker can generate prime numbers and communicate with AP, but hacker cannot generate the same prime numbers as the client. Generating the same numbers as the legitimate client is quite impossible. Since, attacking the client or spoofing the MAC address of AP is not possible. The LEP is used only to avoid slow Request Flooding attacks. In the case of vigorous attacks, AP uses TPF along with LEP [10, 11]. The TPF works as follows:

- AP counts the number of management frames per second when it receives from any particular address.
- If a request from any client is received more than 5 times or exceeds the desired limit within a time frame, the request is inferred as it is from the hacker and TPF ignores the request.

Hence, TPF is employed to prevent such type of continuous Resource Flooding Request from the attacker. In this paper, TPF is employed to defend against start frame and logoff frame attacks.

A. Architectural framework of TPatLetEn

Prior to sending authentication frame to AP, client sends N1 to AP. The N1 is computedusing two prime numbers p1 and q1. After receiving N1, AP sends N2 to the clients, which is common for all the wireless LAN users. During the authentication process, client sends authentication request to AP along with p1. The request is validated by checking with InT and BIC tables. Then, AP verifies N1 by computing N1/p1. The communication between client and AP starts if AP gets q1 using N1/p1. When the client wants to disconnect from the network, it sends de-authentication frame with p1. AP computes N1/p1 and gets q1, it ensures that the request can be processed. Otherwise, the request will be rejected and stores MAC address of the client in the InT table. If the number of start frame or logoff frame request received per second is greater than five, the received frames will be dropped and treated as a hacker; otherwise, it will be processed. The architectural framework of TPatLetEn is as illustrated in Figure 1.

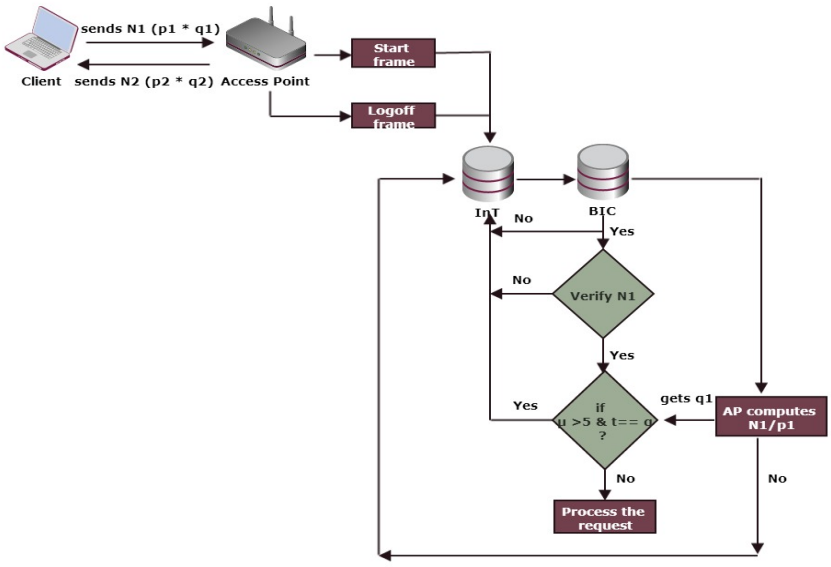

Fig. 1. Architectural framework of TPatLetEn

B. Preventing DoS attacks using TPatLetEn

In this work, we propose TPatLetEn to effectively defend against start frame and logoff frame DoS attacks. The effectiveness of TPatLetEn algorithm is discussed in this section. The TPatLetEn algorithm is simulated on NS2 [11] for experimental purpose. The scenario of experimental setup is consists of four nodes such as client, AP, intruder and TPatLetEn, where TPatLetEn is functioning as a monitoring node. The performance of TPatLetEn algorithm is tested on start frame and logoff frame attacks.

1) TPatLetEn on Start frame attack

Client and AP are configured fortesting the authentication. Factorization based authentication algorithm TPatLetEn is implemented. The client send N1 to AP, the N1 is computed by multiplying two prime numbers p1 and q1. Then, AP sends N2 to client,which is computed using p2 and q2. After AP receives logoff request from client along with p1, AP computes N1/p1, gets q1 and process the de-authentication frames. Similar procedure is followed for logoff frame over client attack. If an AP wants to disconnect from the network, it sends logoff request along with p2. If client gets q2 by computing N2/p2, that will be considered as a legitimate request. Otherwise it will be treated as a spoofed frame. If the number of requested packet is more than 5 within a second, it is considered as a spoofed frame. N2 is common for all wireless clients. During authentication process, client send authentication frame to AP along with p1. If AP receives p1, it computes N1/p1. The computed value N1/p1 is corresponding to q1, the request is considered from legitimate frame.

In case of vigorous attack, TPat takes over the control. The hacker is identified when the AP receives more than five start frame and logoff frame request within one second. The functioning of TPatLetEn algorithm over start frame attack is given below as algorithm 1.

TPatLetEn - Algorithm for Start frame attack
Step 1: Step 1: initialize $\alpha = 4ms$, $\mu = 1$, $t = 0$
Step 2: Let p1,q1,p2,q2 be a prime
Step 3: Client computes N1
Step 4: N1= p1 × q1
Step 5: AP computes N2
Step 6: N2 = p2 × q2
Step 7: Client sends N1 to AP
Step 8: AP stores N1 and sends N2 to client
Step 9: Client and AP gets connected
Step 10: Spoofs intruders MAC address and store it in InT
Step 11: if If $\mu > 5$ && $t == \alpha$ then
Step 12: Reject, spoof and store it in InT
Step 13: else
Step 14: Process the request

Algorithm 1: Algorithm for Start frame attack

2) TPatLetEn on logoff frame attack

When a client wants to disconnect from the network, it sends p1 to AP. The MAC address of the requesting client is checked in InT and BIC tables. If the MAC address of the client is presented in InT, the request will be rejected, else, the request is redirected to BIC table. If MAC address of the client is presented in BIC, the control will be redirected to TPatLetEn. The TPatLetEn algorithm over Logoff frame attack on given below as algorithm 2.

TPatLetEn - Algorithm for Logoff frame attack
Step 1: initialize $\alpha = 4ms$, $\mu = 1$, $t = 0$
Step 2: Let p1,q1,p2,q2 be a prime
Step 3: Client computes N1
Step 4: N1= p1 × q1
Step 5: AP computes N2
Step 6: N2 = p2 × q2
Step 7: Client sends N1 to AP
Step 8: AP stores N1 and sends N2 to client
Step 9: Client and AP gets connected
Step 10: Client sends p1 to AP
Step 11: AP computes N1/p1 and checks q1
Step 12: If yes, client gets disconnected
Step 13: else
Step 14: Spoofs intruders MAC address and store it in InT
Step 15: if If $\mu > 5$ && $t == \alpha$ then
Step 16: Reject, spoof and store it in InT
Step 17: else
Step 18: Process the request

Algorithm 2: Algorithm for Logoff frame attack

C. Experimental Results of TPatLetEn over DoS Attacks

This section discusses the experimental results on testing effectiveness of TPatLetEn over logoff frame and start frame attacks. This section briefs how far the proposed TPatLetEn detects and prevents the DoS attacks. This section alsodescribes the comparison results of the proposed TPatLetEn with existing Traffic Pattern Filtering (TPF) and Letter Envelop Protocol (LEP). The results show that the effectiveness of TPatLetEn against MAC spoof DoS attacks, which is better than the other existing solutions TPF and LEP. Experimental test bed is as given in table 1.

TABLE I Experimental Setup

Area	500 × 500
Packet type	CBR
Packet Size	1000
CBR interval	0.008
Duration of Simulation	50 secs
Nodes	4 nodes (1 Client, 1 AP, 1 Attacker and 1 Monitoring node)
Queue type	Drop tail
Queue limit	10
MAC type	MAC 802.11
Channel	Wireless
Bandwidth	1.7 Mb
Agent	TCP

D. Start frame and Logoff frame attacks over AP/Client

For experimentation, 80 CBR packets in average were taken to evaluate the proposed solution TPatLetEn during the start frame and logoff frame attacks. The experimental setup is created on NS2 simulator to test TPatLetEn. The attacks scenario were created and evaluated the performance of TPatLetEn based on networks throughput, packet delivery ratio, packet drop, control overhead, normalized routing overhead and delay time. Start frame and logoff frame attacks were simulated and the above mentioned parameters were measured during the attacks and after applying the solution.

In Table 2 and 3, the results obtained during the start frame and logoff frame attacks over AP/client and after applying TPatLetEn algorithm.

TABLE II Result of Start frame over AP/Client

Parameter	Over AP		Over Client	
	Attack Scenario	TPatLetEn	Attack Scenario	TPatLetEn
Packet Delivery Ratio	61.53	82.71	73.03	89.87
Control Overhead	81	109	101	66
Normalized Overhead	1.687	1.62	1.55	0.92
Delay	0.16	0.18	0.25	0.01
Throughput	177688	444088	429829	537315
Packet drop	30	14	24	8

TABLE III Result of Logoff frame over AP/Client

Parameter	Over AP		Over Client	
	Attack Scenario	TPatLetEn	Attack Scenario	TPatLetEn
Packet Delivery Ratio	79.48	79.26	89.15	79.26
Control Overhead	98	108	108	109
Normalized Overhead	1.58	1.66	1.5	1.67
Delay	0.34	0.18	0.22	0.18
Throughput	554613	471917	495437	414307
Packet drop	16	17	9	17

IV. Result and Discussion

Performance of TPatLetEn is evaluated based on packet delivery ratio, packet drop, throughput, control overhead, normalized routing overhead and delay time in start frame and logoff frame attacks.

A. Packet delivery ratio

After instantiating the attacks targeted on AP and client, the TPatLetEn is applied. The packet delivery ratio measured after applying TPatLetEn is degraded. Packet delivery ratio is not increasing above 90% and decreased up to 79%, which is poorer than the attack scenario, whereas ThreV and ANM performs good in packet delivery ratio. These three algorithms combined together, hybridized, perform better and considered as an effective solution to detect and prevent the DoS attacks.

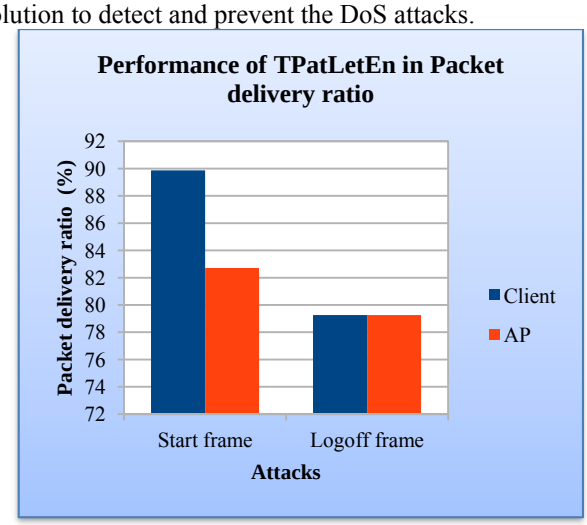

Fig. 2.Performance evaluation of TPatLetEn based on Packet delivery ratio

The Figure 2 shows that the performance of TPatLetEn is decreased considering Packet delivery ratio in logoff frame attack over AP /client.

B. Control overhead

Control overhead decreases when the performance of a network increases. In this experiment, the measured values show decreased control overhead which indicate enhanced performance of TPatLetEn. The TPatLetEn achieves good result on start frame over client in all four different types of attacks.The control overhead measurement is sustained in 108, which is considered as a better result. The performance evaluation over control overhead is illustrated in Figure 3.

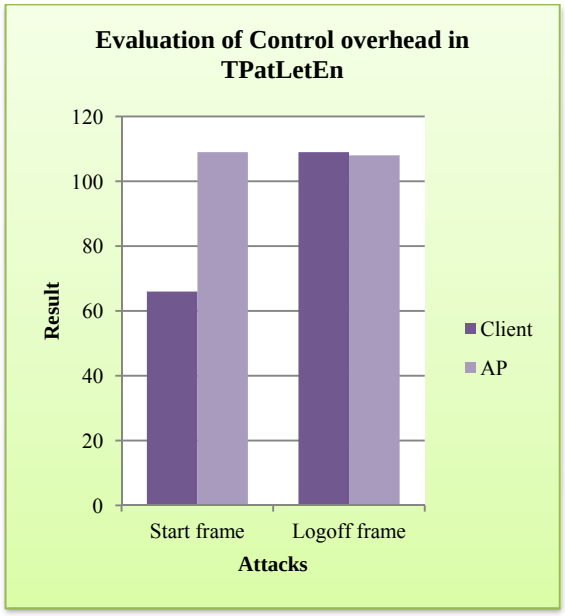

Fig. 3.Evaluation of Performance over Control overhead

C. Normalized routing overhead and delay time

In normalized routing overhead, the experimental result shows that the performance of proposed TPatLetEn is relatively good only in start frame over client than other three types of attacks. As control overhead, normalized routing overhead also maintains sustainability. Considering delay time, TPatLetEn works better in start frame attack. (See Figure 4)

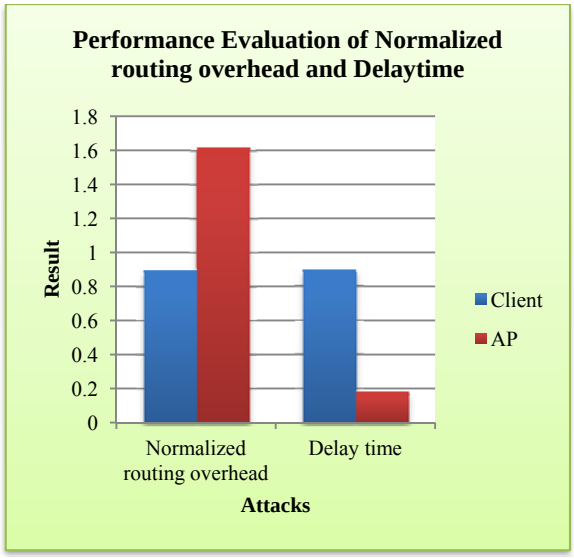

Fig. 4. Evaluation of Normalized routing overhead and Delay time

D. Comparison of TPatLetEn with TPF

The proposed algorithm TPatLetEn is compared with existing TPF mechanism. The comparison resultindicates the effectiveness of the algorithm over*delay time* and *throughput*.

1) Delay time

Delay time is decreases in the experiment, which shows that the performance of TPatLetEn is improved. Based on delay time, the TPatLetEn performed better than TPF. The Figure 5illustrates that the TPatLetEn works out well in start frame and logoff frame attacks than TPF mechanism. In Start frame attack, delay time in TPF is 0.73 and TPatLetEn is 0.18. The delay time measured during TPatLetEn application is lesser than TPF, which shows the higher performance of TPatLetEn than TPF considering delay time on start frame attack.

Delay time measured during logoff frame attack in TPF is 0.69 and in TPatLetEn is 0.18. This shows the enhanced performance of TPatLetEn considering delay time during Logoff frame attack, which is better than TPF. The comparison result of TPF and TPatLetEn is illustrated in Figure 5.

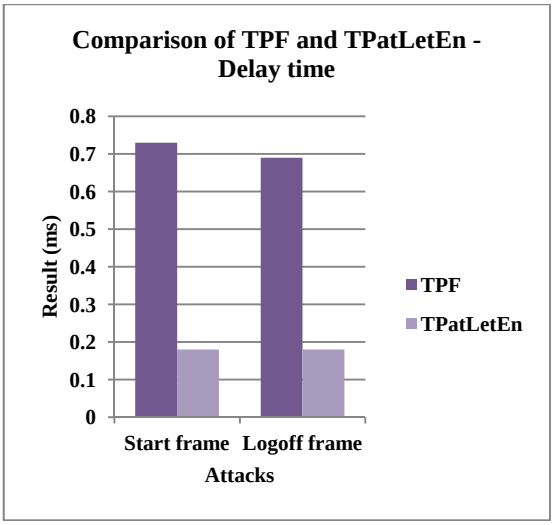

Figure 5 Comparison of TPF and TPatLetEn in Delay time

2) Throughput

Like delay time, the *throughput* is increased in TPatLetEn application. Increased throughput explains the increased performance of TPatLetEn than TPF. Throughput is drastically improved in TPatLetEn application, which proves that the effectiveness of the proposed algorithm.In Figure 6, the Comparison results of TPF and TPatLetEn based on *throughput* is illustrated.

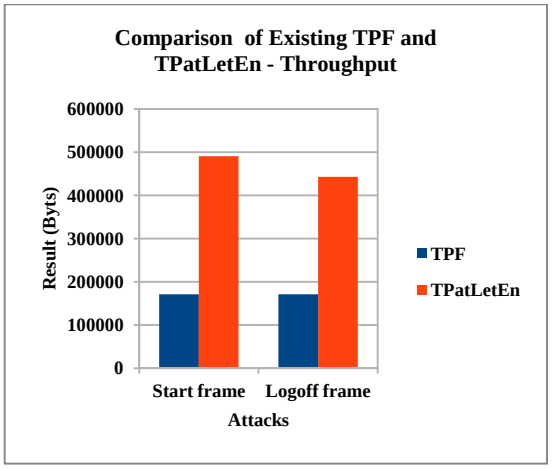

Figure 6.Performance Comparison of TPF and TPatLetEn based on Throughput

3) Packet drop

In TPatLetEn implementation, the packet drop measurement does not give any reasonable result. The packet drop in TPF is zeroduring start frame and logoff frame attacks. Whilepacket drop is 8 in start frame attack and 17 in logoff frame attack in TPatLetEn implementation. The experimental result shows that the TPatLetEn is found to be ineffective considering packet drop.

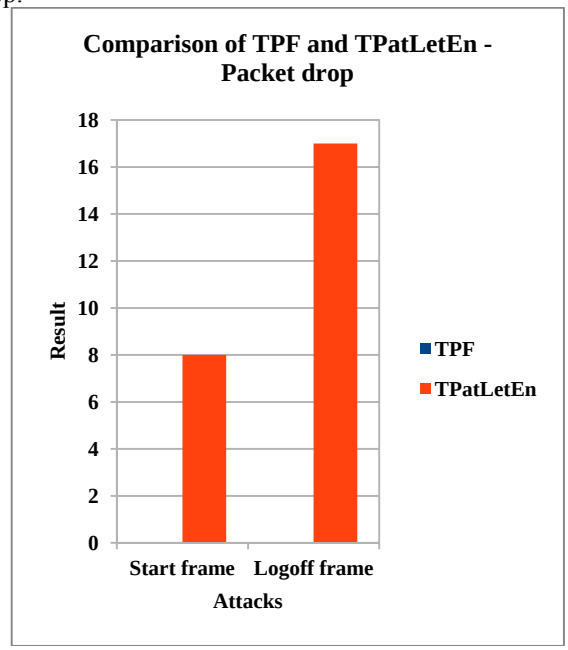

Figure 7 Comparison of TPF and TPatLetEn in Packet drop

V. CONCLUSION

This paper deliberates the proposed TPatLetEn algorithm in perceiving and thwarting MAC spoof DoS attacks, and compares TPatLetEn with existing TPF and LEP. The TPatLetEn is derived as a hybrid mechanism from the existing TPF and LEP mechanism. To overcome the deficiency of TPF and LEP algorithm, TPatLetEn is devised and tested. The experimental result clearly shows that the performance of TPatLetEn is increased than TPF during start frame and logoff frame attacks considering the network throughput and delay time.

REFERENCES

[1] ArashHabibiLashkari, Mir Mohammad SeyedDanesh, BehrangSamadi, "A Survey on Wireless Security protocols (WEP,WPA andWPA2/802.11i)", *2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT),Beijing, China,* pp. 48-52, August 8-11,2009.

[2] Nancy Cam-Winget, Russ Housley, David Wagner and Jesse Walker, "Security flaws in 802.11 data linkprotocols", *Communications of the ACM,* Vol.46, Issue. 5, May 2003.

[3] http://en.wikipedia.org/wiki/IEEE_802.11w-2009

[4] Kai Tao, Jing Li, and SrinivasSampalli"Detection of Spoofed MAC Addresses in 802.11 Wireless Networks", Springer-Verlag Berlin Heidelberg pp. 201–213, 2008.

[5] ThucD.Nguyen, "A lightweight solution for defending against Deauthentication/disassociation attaks on 802.11 networks", *IEEE,* pp. 1-6, August 2008.

[6] JalilDesa, Mina Malekzadeh, Abdul Azim Abdul Ghani and ShamalaSubramaniam: An Experimental Evaluation of DoS Attack and Its Impact on Throughput of IEEE 802.11 Wireless Networks, International Journal of Computer Science and Network Security, Vol. 8, No. 8, pp. 1-5, August 2008.

[7] Chibiao Liu, and James Yu, "A Solution to Wireless LAN Authentication and Association DoS Attacks", *IAENG International Journal of Computer Science,* 34:1, IJCS_34_1_4, August 2007.

[8] Abhishek Gupta and ManishGarg, "DoS Attacks on IEEE 802.11 Wireless Networks and its Proposed Solutions", http://ssrn.com/abstract, April 2010.

[9] TanatatSaelim, PrawitChumchu and ChunyamonSriklauy, "A New MAC Address Spoofing Detection Algorithm using PLCP Header" *IEEE, ICOIN*, 48-53, 2011.

[10] Sivagowry S, Persia A, Vani B and Arockiam L, "A Solution to Prevent Resource Flooding Attacks in 802.11 WLAN", *Lecture Notes in Computer Science Communication in Computer & Information Science(CCIS 269).*Springer-Verlag, Berlin Heidelberg, 607-616, 2012.

[11] Durairaj, M., and A. Persia. "Comparison of ICM with TPF-LEP to Prevent MAC Spoof DoS Attack in Wireless Local Area Infrastructure Network.",*Research Journal of Applied Sciences, Engineering and Technology*, 2040-7459, Vol 7(19), pp. 4162-4170, May 2014.

[12] The ns Manual (formerly ns Notes and Documentation), The VINT Project a Collaboration between researchers at UC Berkeley, LBL,USC/ISI and Xerox PARC. Kevin Fall hkfall@ee.lbl.govi, Editor Kannan Varadhanhkannan@catarina.usc.edui, Editor, May 9, 2010, pp: 73.