# DETECTION AND PREVENTION OF DENIAL OF SERVICE ATTACK

[1]Kalyani Ratnakant Pawar, [2]Mamta P. Mahajan, [3]Divya Dileep Vyas

Computer Engineering Department
SSBT COET Bambhori
Jalgaon, India

***Abstract*— Denial of Service (DoS) attacks is a major problem prevalent in Wireless Local Area Network. An attack occurs mainly because of Medium Access Control (MAC) address spoofing. MAC spoofing is a technique where an adversary pretends to be a legitimate client/Access Point (AP) and sends forgery frames to the victim client or AP. Most of existing solutions are prevent DoS attacks after an intruder sending forged frame by spoofing Client or AP's identity. Few solutions are exists to detect an attacker at the time of MAC address spoofing. None of the techniques such as wired enable protocol (WEP), Extensible Authentication Protocol (EAP) provides a complete solution. Intrusion Detection System (IDS) describes the existing solutions and drawbacks of the available solutions and also compares the existing technique with research work based on features, advantages and disadvantages.**

***Keywords*— Denial of Service (DoS), Intruder Detector and Manager (IDM), Wired Equivalent Protocol (WEP), Wireless Local Area Network (WLAN).**

## I. INTRODUCTION

Wireless Local Area Network (WLAN) is a kind of network in which the single access point can communicate with number of clients using wireless media. But sometimes intruder occurs means a client machine acts as an intruder which interferes as attacker. There are some existing systems that are used to secure system but they cannot secure the management frames hence network is susceptible to denial of service attack. Denial of Service attack is an attack which is aimed to make network resources unavailable to legitimate users and to affect throughput of network [1]. An authentication flooding Denial of Service attack occurs when an intruder attacks the victim AP with large number of spoofed authentication request frames. The AP cannot handle the barrage of spoofed authentication request frames, and eventually becomes un-responsive to handle the legitimate requests. To avoid such situation and to detect the attack activities may detection techniques are proposed one of the technique is Letter Envelope protocol which uses Intrusion Detection System to detect the intruder.

### A. Motivation

The increasing number of attacks and the effects of these happenings invoked our interest in this subject. This unresolved issue is actively present in the IT world for nearly a decade and there has never been an ultimate solution for this. The magnitude of damage caused by DoS is the motivation to learn more about this topic and urged us to do our contribution. Attacks have got businesses down, crippled the economy of a nation and even changed government. Experts [3] also predict that the future wars are going to be with IP packets as missiles since they are capable of bringing down a nation. The attack which was carried out in Burma [1] had kept the nation out of internet for several months. The traffic sent were unstoppable ranging from 10 to 15 Gbps which was several folds more than what the nation's network could withstand. The whole nation was devoid of internet and the e-commerce industry came to a standstill condition. Nevertheless, there are effective solutions that are suggested in order to survive these attacks even though complete removal is not possible. Allocating extra bandwidth, tracing back the attacker, identifying and stopping the fake packets are few of the general suggestions widespread amongst experts [4]. But the exact solution varies with the severity of the attack and the value of data that the company is trying to protect. Thus, the ultimate motivation arose with a desire of stopping DoS attacks that could lead to safe and secure IT world.

### B. Problem Definition

A wireless LAN (Local Area Network) is a type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. WLANs introduce the concept of complete mobility; communication is no longer limited to the infrastructure of wires. WLAN are popular today because of its exibility, easy installation and portability. Providing a secure communication to transfer data in a wireless medium is a challenging task. Security techniques in Wireless computer networks have been increasingly needed. There are many basic risks associated with the WLAN such as insertion attacks, interception and unauthorized monitoring of wireless traffic, jamming, and denial of service [3]. Many security techniques already exists such as WEP, Virtual Private Networking (VPN), 802.1X, the Extensible Authentication Protocol (EAP) and Remote Authentication Dial In User Service (RADIUS). These security techniques tried to solve the security bugs in WLAN. However, there are still some problems in the security that are not solved yet. In WLAN infrastructure network, WLAN offers increased

wireless access to the client with the help of AP. The clients are connected with one or more Access Points (AP). There are three types of frames, namely, management, control and data frames used in the IEEE 802.11 networks. Data frames carry higher-level protocol data in the frame body. Control frames are used to deliver the data frames by area clearing operations, channel acquisition and carrier sensing maintenance functions. Management frames act as supervisory functions by joining and leaving the wireless networks and move association from one AP to other AP. Authentication/association frames are used when the authenticator (i.e. AP) and supplicant (i.e. STA) want to authenticate/associate with each other. De-authentication/disassociation messages are used when the authenticator and supplicant want to de-authenticate/ disassociate with each other. Authentication / association De-authentication /dis-association frames are frames belong to the management frames which are defined in IEEE 802.11i standard [2], and all the management frames are sent in clear without any protection as these frames will be used before the authenticator and supplicant are mutually authenticated. Hence, an adversary can easily forge these frames. Cryptographic protection is not implemented yet for management frames in the 802.11 standard. Therefore, by listening to the traffic and learning the MAC addresses of the station and the AP, an attacker can forge a de-authentication or a disassociation frame and transmit it either to the station or to the AP to knock the station off the network [5]. These is accomplished through spoofing legitimate client (STA)/APs medium access control (MAC) address. Less protection in MAC address led to get easy spoofing. Since the management frame is un-encrypted; adversary sends the management frame to the victim using spoofed MAC address. De-authentication attacks are more efficient than disassociation attacks because they require more work for the station to return back to the associated state. If the attack is repeated persistently, the station is kept from accessing the network indefinitely. The attacker targets an individual station not the whole network [6]. DoS attacks benefit from a central basic vulnerability, which is the easiness of MAC-address spoofing. All the nodes are connected through a central device called an Access Point (AP). The Access Point vulnerabilities make the DoS attack more serious. When the DoS attack is made the authenticated/associated user is denied from service by getting de-authentication/dis-association message. In proposed system Letter Envelope Protocol (LEPT)[2] is non-cryptographic method to detect MAC spoofing[7] attack. LEPT at association level prevents request flooding attacks. But the attacker can do his work or attack at the authentication level itself. Since the authentication process is carried out with \Open Shared" or \Pre Shared key" authentication, it cannot have a secure authentication. If the communication is stopped or hacked at the authentication level, the request flooding attacks are very easy to make. To overcome such disadvantage, LEPT [2] is used at the authentication level itself. So, from the initial state itself, the LEPT starts functioning and the network is secured from flooding DoS attacks. When LEPT is sent along with authentication frame, the spoofing possibilities are minimized and it prevents vigorous resource flooding attacks. When continuous flooding DoS attacks are experienced, the LEPT procedure is suitable for having a good throughput. The traffic pattern filtering [8] method sets a threshold value of maximum five attempts to request for authentication or de-authentication. When the threshold value exceeds the limit, the request is ignored by the network [2]. The envelop value generated by AP and client are mutually verified and the authentication and de-authentication processes are followed after that. AP stores the `N' generated by clients [2] and if the intruder tries to de authenticate/disassociate legitimated clients after spoofing their MAC addresses; it becomes difficult due to the LEPT algorithm. So, when the intruder tries to de-authenticate, the intruder itself will be disconnected from the network. The client continues its original state.

## II. RELATED WORK

Neveen I. Ghali in [1], have stated that 7 features are enough to detect DoS attack with high accuracy. This reduction in number of attributes for detection process reduces Intrusion Detection system (ID). The drawback of this approach is a lengthy detection process and degrading performance of an ID system.

Imen Brahmi et al. in [4], have proposed \Hybrid (Misuse-Anomaly) IDS" using data mining and mobile agent technology to detect known and novel attacks. A weakness of these systems is that they are not effective against naval attacks that have no matched signatures.

Zhenwei Yu et. al., in [9], has proposed a \Automatically Tuning Intrusion Detection System" used to identify abnormal activities in a computer system. The proposed system will automatically tune the detection model on-the-y according to the feedback provided by the system operator when false predictions are encountered.

Jiwu Shu, Bigang Li et al., in [10] has proposed \Design and Implementation of a Storage area Network System". Based on the Faber Channel Protocol introduces some of The key techniques in the network storage system, including a SCSI simulating target, intelligent and uniform storage management architecture, and the processing flow of the read/write commands.

## III. PROPOSED SYSTEM

In Figure 3.1 Access Point is connected to wired backbone called distributed system which provides internet service. Stations requests to access point to get associated with it for data services. Intrusion Detection System (IDS) is intermediatory part that filters users requests by analyzing their behaviors. IDS provides access to valid requests and blocks intruders by identifying their malicious attempts.

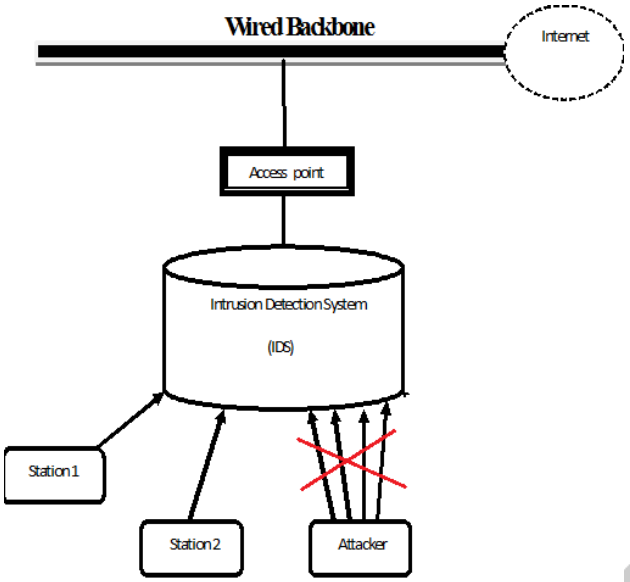


Fig 3.1 System Architecture

There are two algorithms in a proposed system, namely, the Intruder Detector and Manager (IDM) and Letter Envelop Protocol with Traffic pattern filtering (LEPT). The Intrusion Detector and Manager (IDM) algorithm detects and prevents the intruder entering into the network by maintaining tables in order to avoid the masquerading DoS attacks. When this procedure is followed, IDM increases the throughput by preventing intruders and maintains the history of intruders. This reduces the computational time of the AP and maintains the throughput and bandwidth. The LEPT algorithm is proposed to avoid the resource flooding DoS attacks.

*Algorithm of IDM*

START

Event_type (register, login, logout)
{
If (Event_request = register) then
string_mac_a = get_Mac_Address ()
If (string_mac_a is in intruder) then /*Check Intruders' List*/
(Ignore the request)
Else
If (string_mac_a is in registered) then /*Already registered*/
(Ignore register request)
Else
(Accept the register request) and
(Ask for login)
End if
End if
End if

If (Event_request = login) then
string_mac_a = get_Mac_Address ()
If (string_mac_a is not in registered) then /*Check Registers' List*/
(Print message "register first") and
(Ignore request)
Else
If (string_mac_a is in logged in) then /*Already logged in*/
(Ignore the login request)
Else
(Accept login request) and
(Ask for logout)
End if
End if
End if

If (Event_request = logout) then
string_mac_a = get_Mac_Address ()
If (string_mac_a is not in loggedin) then /*Check login' List*/
(Print message "login first " ) and
(Ignore request)
Else
(Accept log out request)
End if
End if

STOP
}

*Algorithm of LEPT*

START

Event-type (register, login, logout)
{
If (Event_request_C1 = register) then
(C1 sends registration request to AP1)
registration_req_C1+=1;
If (registration_req_C1>=10) then
(Mark C1 as an intruder) and
(Make access denied)
Else
If (Event_request_C1 = login) then
(Compute N1 = P2 * Q2)
/*AP1 generates and stores N2 value for C1*/
Get_P2 () value from AP1;
Get_N2 () value from AP1;
Start communication;

If (Event_request_C1 = logout) then
(C1 sends logout request to AP1 with P2 and N2)
If (P2 corresponds to N2) then
(Accept the logout request)
Else
(Reject the request)
End if
End if
End if

STOP

## IV. RESULT

In table 4.1 is for sample results. The parameters are Register, Login and Logout respectively. The input given for registration is pwd=1234 then it shows output as "Registered

Successfully", else when the request is more than ten then it shows output as "Flooding detected". For login P1=3 and Q2=10 are password given as an input, then the output shown as "Logged in successfully P2=5, N2=120" and Access Point generates P2=5, N2=120 for client. P2=5, N2=120 are password provided as input for logout, then output is given as "Logged out successfully". If the input for logout request is incorrect i.e. P2=4, N2=123 which does not match with Access Point generated P2 and N2, then output is shown as "Incorrect P2 and N2".

| Parameter | Input | Output |
|---|---|---|
| Register | pwd=1234 | Registered Successfully |
| Register | Register request more than 10 | Flooding detected |
| Login | P1=3, Q1=10 | Logged in successfully P2=5, N2=120 |
| Logout | P2=5, N2=120 | Logged out successfully |
| Logout | P2=4, N2=123 | Incorrect P2 and N2 |

Table 4.1: Sample Results

## V. CONCLUSION

A wireless network is affected due to Denial of Service Attacks because management frames are sent over network un-encrypted. In such case, proposed Intrusion Detection System (IDS) makes it possible to detect denial of service attacks. The Intruder Detector and Manager (IDM) used in IDS has been improved the WLANs performance apart from preventing the masquerading DoS attacks. The added advantage in IDM was that it has been spoofed and stored the intruders Medium Access Control (MAC) address. It suggested that the usage of duplicate IDM to manage in case of failures. The maintenance of duplicate IDM will increase the traffic overhead. But, it prevents the WLAN from the unauthorized users. Letter Envelop Protocol (LEPT) in IDS is used at the authentication level itself. So, from the initial state itself, the LEPT starts functioning and the network is secured from flooding DoS attacks. With LEPT used in IDS, the throughput becomes unaffected and the performance, confidentiality and availability of WLAN is maintained without insisting changes in existing protocols.

## REFERENCES

[1] N. I. Ghali, \Feature selection for effective anomaly-based intrusion detection." International Journal of Computer Science and Network Security, vol. 9, no. 3, pp. 285{289, 2009.

[2] A. L and V. B, \Security algorithms to prevent denial of service (dos) attacks in wlan." International Journal, vol. 2, no. 1, 2012.

[3] A. Mohammed and R. M. J, \Methodologies for detecting dos/ddos attacks against network servers." in The Seventh International Conference on Systems and Networks Communications, ICSNC Semi-Markov models, 2012.

[4] B. Imen, Y. S. Ben, and P. Pascal, \Mad-ids: novel intrusion detection system using mobile agents and data mining approaches." in Intelligence and Security Informatics. Springer, 2010, pp. 73{76.

[5] P. A and S. R, \Detection and prevention of denial of service attacks using distributed denial-of-service detection mechanism."

[6] Z. S. Taghavi, J. Jyoti, and T. David, \A survey of defence mechanisms against distributed denial of service (ddos) flooding attacks." Communications Surveys & Tutorials, IEEE, vol. 15, no. 4, pp. 2046{2069, 2013.

[7] F. Paul, \Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," 2000.

[8] H. Ahsan, H. Mohamed, and B. B. K, \Detecting service violations and dos attacks." in NDSS, 2003.

[9] Y. Zhenwei, T. J. JP, and W. Thomas, \An automatically tuning intrusion detection system." Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on,vol. 37, no. 2, pp. 373{384, 2007.