CHAPTER - 4

LETTER ENVELOP PROTOCOL WITH TRAFFIC PATTERN FILTERING TO PREVENT RESOURCE FLOODING DoS ATTACKS (LEPT DoS)

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”

- Bruce Schneier

4.1 Background

A wireless infrastructure network is formed with legitimate stations and an Access Point (AP). The stations communicate with each other with the IEEE 802.11 defined protocols. In a WLAN infrastructure networks, Medium Access Control (MAC) layer communicates using three types of messages namely, management, control and data [Sus, 10]. The management frames are not encrypted and are vulnerable to DoS attacks. The MAC layer DoS attacks are classified into three types namely, masquerading DoS, resource flooding DoS and media access DoS attacks [Kem, 08]. These attacks make the legitimate users to be disconnected from the WLAN environment.

This chapter focuses on the prevention of resource flooding or depletion DoS attacks from entering into wireless networks. The probe request flood, authentication/deauthentication request flood and association/disassociation request flood are the various resource flooding DoS attacks. Resource depletion attacks target the shared resources such as AP to exhaust its processing and memory power so that, it is no longer able to provide services to other legitimate stations. These attacks could be accomplished as more sophisticated attacks such as introducing rouge APs to...
hijack the abandoned stations. In the deauthentication/disassociation DoS flooding attacks, an attacker transmits spoofed frames with the source address of the AP. When the targeted clients receive the frames, they are disconnected from the network and attempt to reconnect. When the attack is continued, the authenticated clients are unable to maintain connection to the wireless network. The deauthentication/disassociation DoS flooding attacks target one or all the users on a specific BSSID (Basic Service Set Identifier). In these sorts of attacks, the intruder uses spoofed source MAC address that are used to authenticate and associate to a target AP. The attacker repeatedly makes the authentication/association requests, so that the processing and memory capacity of the AP gets exhausted and the AP leaves the clients with little or no connection to the wireless network [Chi, 07]. Some common resource depletion attacks as discussed in the literature are described below [Tai, 10]:

- **Probe Request Flood**
  
  Stations in IEEE 802.11 wireless networks use probe requests to scan the wireless environment for the available connectivity with the APs. APs respond to these requests with information about the wireless network to allow wireless clients to associate with it. An intruder transmits bursts of such probe requests with different random fake MAC addresses to simulate the presence of large number of scanning stations. This attack consumes all of the memory and processing resources of an AP, preventing them from responding to legitimate clients’ requests [Ber, 08].

- **Authentication Request Flood (AuthRF)**
  
  During an authentication request flood attack, an intruder transmits authentication request frames with spoofed MAC addresses that attempt to authenticate to the AP.
The intruder floods the AP with such frames to exhaust its processing and memory resources. In response to authentication request frames, the AP has to allocate memory to keep information about each new station that successfully authenticates. An AP which is under attack will not be able to allow legitimate clients to connect with the wireless network [Ber, 08].

- **Association Request Flood (AssRF)**

  AP inserts the data supplied by a station into a table called, the association table that was maintained in its memory. IEEE 802.11 standard specifies a maximum value of 2007 concurrent associations to an AP. The actual size of this table varies among different models of APs. When this table overflows, AP would refuse further clients to be connected. Having cracked WEP, an attacker can authenticate several non-existing stations using legitimate-looking, using randomly generated MAC addresses. The intruder then sends a flood of spoofed association requests, so that the association table overflows. If an access control list is not in place for MAC address filtering, then the authentication and association request flood attacks are considerably easier for an intruder to launch. According to MAC protocol, an AP will not accept an association request sent by a station in an unauthenticated and unassociated state. However, it is surprising to see that contrary to the specification, many APs also respond to association requests in their initial states [Tai, 10].

- **Disassociation Request Flooding (DisRF)**

  Dissociation request flooding attacks are made by sending spoofed dissociation frames targeting the wireless clients. An intruder would repeatedly spoof the dissociation frames to keep the clients out of service.
Deauthentication Request Flooding (DeAuthRF)

In deauthentication request flooding attacks, an intruder transmits spoofed frame with the source address to AP. When AP receives such frames, it disconnects the client from the network. After crossing the 2 states, client communicates with the AP. The intruder spoofs client’s MAC address and send it to AP. AP disconnects the client from its network as shown in Figure 4.1.

Figure 4.1 Deauthentication Frame by the Faked Client

There are certain existing countermeasures for MAC layer resource flooding DoS attacks. The resource flooding attacks which are taken into study are deauthentication request flooding, authentication request flooding and association request flooding. These attacks cause the WLAN or some of its wireless nodes to be out of services. Chibiao liu et al. [Chi, 07] proposed a solution to detect and resolve Authentication Request Flooding (AuthRF) and Association Request Flooding.
Letter Envelop Protocol with Traffic Pattern Filtering to Prevent Resource Flooding DoS Attacks (LEPT DoS)

(AssRF) attacks based on an experimental framework. This method quantifies both the attacks against TCP and wireless voice over IP communication. There are two countermeasures, namely, MAC Addressing Filtering (MAF) and Traffic Pattern Filtering (TPF) which are used against both the attacks.

In the IEEE 802.11 standard, whenever a wireless station wants to leave a network, it sends a deauthentication or disassociation frame to the AP. But, the frames are not encrypted and not authenticated by AP. Hence, attacker easily spoofs the frame and launches resource flooding DoS attack. Thuc D. Nguyen et al. [Thu, 08] presented an algorithm called, Letter Envelop Protocol (LEP) based on a hard function. The deauthentication and disassociation attacks are called as farewell attacks. These attacks disconnect the authenticated client from the network. They follow the ‘Open Authentication’ or ‘Shared Key Authentication’. The farewell attacks are simple, but, cause serious damages. This existing algorithm is effective against farewell attacks, but, works only with specific platforms, like Atheros Chipset running on Linux and it needs hardware upgradation as stated by the authors. Hence, a solution is needed to detect and prevent the resource flooding DoS attacks, which is applicable to all the platforms and requires no hardware upgradations.

This chapter discusses the issue addressed in identifying the resource flooding DoS attacks. Finding the best solution to resource depletion DoS attacks are still in research. Hence, Letter Envelop Protocol with Traffic pattern Filtering (LEPT DoS) security algorithm is proposed to mitigate the resource flooding DoS attacks. This algorithm increases the throughput value to a greater extent.
4.2 Objectives

Objectives of this chapter are listed below:

- To propose an algorithm to prevent the resource depletion DoS attacks on the WLAN infrastructure environment.
- To increase the throughput value in order to achieve improved WLAN performance.

4.3 LEPT DoS Algorithm

According to the frame format, management frames are more vulnerable to MAC layer DoS attacks, since, they are sent unencrypted. The proposed work is based on the LEPT DoS algorithm, which is used to prevent the resource flooding or resource depletion DoS attacks by increasing the packet send rates.

Algorithm 4.1 LEPT DoS

Start

Event-type (Login, Logout)

integer :

N1 be a semiprime from p1 and q1;

N2 be a semiprime from p2 and q2;

C1 be the client;

AP1 be the Access Point;

If (event_Request_C1 = login) then

compute N1 = p1 * q1; /*C1 generates and stores N1 value*/

store N1 in C1;

compute N2 = p2 * q2; /*AP1 generates and stores N2 value*/

store N2 in AP1;
get_N1() value from C1 store into AP1;

get_N2() value from AP1 and store into C1; start communication;

If (event_Request_C1 = logout) then

C1 sends logout request to AP1 with p1; logout_Req_C1+=1;

If ((logout_Req_C1<=5) && (p1 corresponds to N1))

then Accept the logout request;

Else

Reject the request assuming that it is from the intruder

endif

endif

 endors

/*When AP1 wants to logout from the Network*/
If (event_Request_AP1 = logout)

AP1 sends p2 value to all clients;

logout_Req_AP1+=1

If ((logout_Req_AP1 <=5) && (p2 corresponds to N2)) then /*

C1 computes p2/N2 and verifies whether p2 corresponds to N2*/

Accept the logout request

else

Reject the request assuming that it is from the intruder who attacks

AP1 endif

endif

endif

Stop
The procedure of LEPT DoS algorithm is explained below:

1. This algorithm takes Login and Logout as the event type. N1 is a semi prime number calculated by multiplying p1 and q1 values, which should be prime numbers. C1 and AP1 are the variables assigned for the client and AP.

2. When login request is made by client, N1 value is computed as p1 * q1, this N1 value is stored in the client C1.

3. Now, N2 is computed as p2 * q2, which is generated by AP and stored in AP1.

4. The value of N1 and N2 are received and stored in AP1 and C1 respectively.

5. When this exchange of N1 and N2 values are over, communication between the AP and client begins.

6. When client C1 wants to logoff from network, it sends one logoff request to AP1 along with p1 value.

7. A counter is opened for counting the number of times the logout request are made as logout_Req_C1 and assigned 1 as its initial value.

8. When the counter value is <=5 times and p1 value corresponds to N1, then the logout request is accepted by AP1.

9. Otherwise, when counter value exceeds the threshold limit 5 and p1 does not correspond to N1, the logout request is rejected assuming that it is from the intruder.

10. Now, the procedure starts with logout request sent from AP1 to C1, when AP1 wants to leave from the network.

11. When event request of AP1 is logoff, it sends p2 value to all clients.

12. The counter for logout request of AP1 is assigned 1 initially.
13. When counter value of AP1 is \(<\text{or}=5\), which is the threshold value maintained by AP1, and p2 value corresponds to N2, the logout request is accepted by client C1. Here, C1 computes \(p2/N2\) and verifies whether \(p2\) corresponds to N2.

14. Otherwise the logout request is ignored assuming that it is from intruder who is trying to attack AP1.

The proposed LEPT DoS algorithm is found to be effective in preventing request flooding attacks, because, though the intruder spoofs the MAC address, legitimate clients or AP is not affected. The intruder generates prime numbers and communicates with AP. But, the intruder could not generate the same prime numbers as client. So, attacking the client or AP and spoofing the MAC address become difficult for the intruder. The existing LEP algorithm is used to avoid only slow request flooding attacks. When intruder aims resource flooding DoS attacks, the pattern filtering methods are found to be comfortable when combined with LEP. Hence, Traffic Pattern Filtering (TPF) is employed in such a case to prevent continuous resource flooding requests from the intruder. Threshold value is fixed as maximum five times and it may be minimized to 3, depending on the level of security required in the particular environment. When the request exceeds threshold limit and the prime numbers exchanged are not the same, the request is rejected. The proposed LEPT DoS algorithm is implemented using both a Java procedure and a simulation environment using NS2 (Network Simulator). The algorithm is validated by measuring the throughput before and after implementing the LEPT DoS algorithm.
4.4 Simulation Results

The experimental setup consists of one AP, one target client and one attacker. Wireless card is used for simulating AP. Configuration requirements are as follows:

- Two PCs (CPU: Intel I3, RAM 2 GB, HDD 80GB) as wireless client and AP.
- One PC (CPU: Intel I5, RAM 2 GB, HDD 80GB) as attacker.

The coding is based on Java NetBeans. At the initial stage, when a client wants to communicate with AP, it needs authentication. The algorithm generates N1, with p1 and q1 values, and sends it along with authentication frame to the AP. N1 value is stored in AP. AP again sends back N2, using p2 and q2 to the client. After storing N2, client and AP start their communication. Client moves to the state of association from authentication. When the client wants to deauthenticate or disassociate from AP, it sends p1 to AP along with the deauthentication/disassociation frame. AP checks p1/N1, and after confirmation, it sends response to the client. If the computed value doesn’t match, it ignores the request assuming that it is from the intruder. Intruder finds it impossible to predict the prime number generated by the client. Spoofed ‘p’ can be easily detected. Because , only the client or AP who generates the “envelop” N can prove that they are the legitimate owner of p. Initially, client sends authentication request to AP with the MAC address. The MAC address is checked and client is allowed to enter into the network. The second step is to associate with the other clients in the network as shown in Figure 4.2.
Figure 4.2 Clients Communicate with each Other

Now, the intruder enters into the setup by spoofing the MAC address of client 1. Intruder tries to make authentication request flooding attacks as depicted in the Figure 4.3.

Figure 4.3 Authentication Request Flooding Attack
Due to the authentication request flooding attacks, the legitimate client is disconnected from the network. Deauthentication flooding attacks are made in the same way by intruders with faked MAC address of clients.

Now, the proposed algorithm LEPT DoS is deployed in the AP. The envelop value generated by AP and client are mutually verified and the authentication and deauthentication process are followed after that. Figure 4.4 shows the generation of p1 and q1 values as 33 and 49 for example. Then N1 value is 1617.

![Figure 4.4 AP at the Initial State](image)

AP stores the ‘N’ generated by the clients and it becomes impossible for the intruder to deauthenticate/disassociate the legitimate client after spoofing the MAC address due to the usage of proposed LEPT DoS algorithm. When intruder tries to deauthenticate, intruder itself is disconnected from the network and client continues its original state.
A simulation environment is setup with the Network Simulator 2 (NS2) tool to validate the performance of the proposed LEPT DoS algorithm. The attacks which are taken for simulation are authentication request flooding (AuthRF), association request flooding (AssRF), deauthentication request flooding (DeAuthRF) and disassociation request flooding (DissRF). NS is a discrete event simulator targeted at networking research. It provides substantial support for TCP routing and multicast protocols over wired and wireless networks. Using X graph (A plotting program), graphical representations of simulation results are generated and Linux platform, preferably Ubuntu is used. Simulation scenario is set by assigning nodes as AP, clients and intruder. At the beginning of the simulation, AP and client are in communication. The intruder enters into the network by spoofed MAC address. During DoS attack, the throughput value is dropped to zero. This is observed through the graphs generated by NS2 by taking time/second in X axis and throughput along Y axis. After implementing the solution, intruder could not make the attack, because, client authentication is based on the prime number generated and exchanged with AP. Hence, LEPT DoS algorithm prevents the intruder from entering into the network. Intruder spoofs the MAC address of the authenticated client and sends association request to the AP as depicted in Figure 4.5 and client is disconnected from the network as shown in Figure 4.6.
Figure 4.5 Intruder Spoofs MAC Address of the Authenticated Client

Figure 4.6 Client is Disconnected
While using LEPT DoS algorithm in the AP, intruder fails to establish connection with legitimate client. Through the LEPT DoS algorithm, AP verifies that the client is already in connection, which is shown in Figure 4.7.

![Figure 4.7 AP Checks and Found that the Client is already Authenticated](image1)

Figure 4.7 AP Checks and Found that the Client is already Authenticated

Figure 4.8 shows that communication with the original client is not affected as intruder fails to associate with AP because of LEPT DoS algorithm.

![Figure 4.8 Intruder Fails to Associate](image2)
The same procedure is applied for deauthentication and dissociation request flooding attacks. It is found that throughput drops to zero during the attack. With LEPT DoS algorithm, throughput of the WLAN is increased to a greater extent.

### 4.5 Findings and Interpretations

The existing LEP algorithm, when used at association level, prevents request flooding attacks. But the intruder makes intrusion at the authentication process itself. Since, the authentication process is carried with “Open Shared” or “Pre Shared key” authentication and it does not provide a secure authentication. If communication is stopped or hacked at the authentication level, request flooding attacks are very easy to make. To overcome such disadvantage, LEPT DoS algorithm is used along with the authentication process. So, from the initial process of communication, LEPT DoS starts functioning and the network is secured from resource flooding DoS attacks. The procedure follows Traffic Pattern Filtering by maintaining the threshold value less than or equal to five. This prevents the vigorous DoS attacks and improves security.

**Figure 4.9 Comparison of Throughput**
Figure 4.9 shows comparison of throughputs during the resource flooding attack and with LEPT DoS algorithms. It is observed that throughput is dropped during the resource flooding attack. But, after implementing LEPT DoS, it is found that throughput has been increased. The existing LEP invoked at association level which minimizes the request flooding attacks. But, before association, the client has to authenticate itself to AP. Since, the authentication frame is sent unencrypted, it is easily spoofed by intruders. When LEPT DoS algorithm is applied along with authentication frame, the spoofing possibilities are minimized. Figure 4.10 generated by NS2, shows that the LEPT DoS increases the throughput level to a greater extent.

![Throughput Comparison before and after LEPT DoS](image)

**Figure 4.10 Throughput Comparison before and after LEPT DoS**

Figure 4.11 shows the comparison between existing LEP algorithm and proposed LEPT DoS. When continuous flooding DoS attacks are experienced, LEPT
DoS algorithm is suitable for having a good throughput. The traffic pattern filtering method sets a threshold value of maximum five attempts to request for authentication or deauthentication. When threshold value exceeds the limit, the request is ignored by the network. The solution needs no firmware upgradation. It is a cost effective method to be adopted by WLAN users in order to enhance the security of the network from the resource depletion DoS attacks made at the MAC layer.

![Figure 4.11 Comparision of LEP and LEPT DoS](http://www.novapdf.com/)

**Figure 4.11 Comparision of LEP and LEPT DoS**

Table 4.1 compares the existing and proposed methods based on various measures and it is found that the proposed LEPT DoS algorithm works well compared with the existing methods.
Table 4.1 Comparisons of Existing and Proposed Algorithm

<table>
<thead>
<tr>
<th>Existing Methods</th>
<th>Proposed Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>The existing algorithm is able to prevent slow DoS attacks used at association level.</td>
<td>When continuous flooding DoS attacks are experienced, the LEPT DoS algorithm is suitable for having a good throughput.</td>
</tr>
<tr>
<td>The intruder starts his entry during the authentication process itself. Since the authentication process is carried with “Open Shared” or “Pre Shared key” authentication, it cannot have a secure authentication.</td>
<td>LEPT DoS algorithm is used at the authentication level. So, authentication level DoS attacks are prevented.</td>
</tr>
<tr>
<td>If the communication is stopped or hacked at the authentication level, the request flooding attacks are very easy to make.</td>
<td>The Traffic Pattern Filtering (TPF) method sets a threshold value of maximum five times to make request for authentication or deauthentication.</td>
</tr>
<tr>
<td>This existing algorithm is effective against farewell attacks, but works only with specific platforms like Atheros Chipset running on Linux and needs hardware upgradation</td>
<td>LEPT DoS prevents vigorous resource flooding DoS attacks and does not require any firmware upgradation.</td>
</tr>
</tbody>
</table>

4.6 Mathematical Generalization

The resource flooding or depletion DoS attacks namely, authentication request flood, association request flood, deauthentication request flood and disassociation request flood are discussed in this chapter. From experimental results, throughput values before and after the proposed solution are compared. The results are depicted in the form of graphs. The experimental results proved that the proposed algorithm LEPT DoS works well and, increases throughput value and, thus performance of WLAN is enhanced. A mathematical generalization is used to support the findings which is given below with reference to Figure 4.10.
During the DoS flooding attacks, the packet transfer rate falls to zero value, but, after the implementation of the proposed LEPT DoS algorithm, the throughput is raised to a greater extent.

Before the implementation of the proposed LEPT DoS algorithm,

\[
\text{Current\_LEPT\_DoS(throughput)} = \text{LEPT\_DoS(throughput)} - C_1 \quad \text{Eqn. (1)}
\]

Where, \(C_1\) is the fall of packet transfer rate.

After the implementation of the proposed LEPT DoS algorithm,

\[
\text{Current\_LEPT\_DoS(throughput)} = \text{LEPT\_DoS(throughput)} + C_2 \quad \text{Eqn. (2)}
\]

Where, \(C_2\) is the increased packet transfer rates with respect to the proposed LEPT DoS algorithm. From Figure 4.10, \(C_1 = 0.99765\) bytes and \(C_2 = 0.9997\) bytes. Approximately, throughput is increased to 20.5 bytes during DoS flooding attacks, after applying the proposed LEPT DoS algorithm. The packet transfer rates are increased to a significant amount and remains greater than zero, after the proposed algorithm LEPT DoS is adopted.

4.7 Chapter Summary

This chapter has summarized the serious effects of resource flooding or depletion DoS attacks in WLAN infrastructure environment. With the resource flooding requests, intruder takes control of WLAN. The legitimate clients had to unknowingly wait for reconnection with the network. LEPT DoS has been proposed for preventing the resource flooding DoS attacks which includes probe request flooding, authentication/deauthentication request flooding and association/disassociation flooding attacks. This algorithm has been found to be effective in preventing request flooding attacks, because, though the intruder spoofs the MAC address, the legitimate
clients or the AP is not affected. The authentication is progressed based on envelop-protocol. The intruder generates prime numbers and communicates with AP. But, the intruder does not generate the same prime numbers as the client. Hence, attacking the client or AP and spoofing the MAC address become difficult for the intruder.

The existing algorithm has been used to avoid slow request flooding attacks. When the intruder aims vigorous resource flooding DoS attacks, the pattern filtering methods have been found to be comfortable when combined with LEP. There is no hardware upgradation is needed for the implementation of LEPT DoS algorithm. The existing LEP algorithm works only with specific platforms like Atheros chipset running on Linux and needs hardware upgradation. With the proposed LEPT DoS algorithm, the throughput has been increased as validated by both NS2 and Java procedures. Both ways showed the same results, they are prevention of resource flooding DoS attacks and better performance of WLAN by increasing throughput value without the need for any hardware upgradations. The solution is a cost effective one to be used along with the wireless networks.