CHAPTER 6

PERFORMANCE AND RESULTS

In this chapter, the proposed methodologies are implemented with the network simulator (NS-2). Due to the impossibility to execute the defense mechanism in a real time scenario. It will be a great economic loss when the defense mechanism is not an effective one. Therefore, the network simulator has been used to predict the effectiveness of the defense mechanism with the scenario similar to real time. In the first section, the simulation scenario and simulation parameters are discussed, followed by the evaluation of primary performance metrics such as victim fraction, attack fraction, and victim trace fraction in the second phase. It also discusses other performance metrics viz., gain, effectiveness, false positive of spoofed packets. The performance metrics of Ex-IDPF is compared with performance of the existing systems such as RBF, HCF and IDPF. Finally, the basic parameters of Extended Inter Domain Packet Filter Architecture and other techniques are listed out.

6.1 NS-2 SIMULATOR

In order to evaluate the network performance various simulation tools were available to accomplish and a smooth journey with network research. The NS-2 simulator is the most standard open source network simulator in which its behavior is highly
trusted by the research community. It is a dependable, realistic discrete event based simulation tool which proves its efficiency. The primary design of the simulator is based on the OSI model to support wired networks and also facilitates open source code for prominent routing protocols used in the network. With this simulator the source code can be easily extended to support a new future in a wide range of realistic mobility models with finest granularity. It has various set of protocols, extensions and continuous contribution of researchers through the world. It is an integrated working environment to write code extensions, network animations, network traces, and plotting graphs. Thus, NS-2 is highly desirable one to complete this research work more successfully.

6.2 SIMULATION SCENARIO

Simulation scenario and their screenshots for the connection of nodes in AS at border routers, key replacement, key substitution, attack launch, attack detection and filtering is given in the following output nam screens. Each autonomous system has autonomous server. The initial node set up of autonomous systems that are connected each with 200 nodes through border routers are given in the figure 6.1.
Figure 6.1 Autonomous Systems each connected with 200 nodes through border routers

Security keys are placed at the border routers at the source AS, and it is verified at each border routers before entering into the network. At the instant of security key substitution, every router holds two security keys, old/previous and new. As a result, each router contains the key validation table with two keys corresponding to the source address. The screen shot for the security keys placed at the border routers is shown in the figure 6.2.
Figure 6.2 The security key placement at border routers for the source AS

Screen shorts of attackers launching the DDoS attack by flooding and make the link to jam which leads to high latency and low packet delivery ratio. Attackers disrupt the normal data transfer by the genuine nodes by this attack. The attack launch for 5 Autonomous Systems that are connected to each with 200 nodes through border routers are shown in figure 6.3.
Figure 6.3 The attack launch for 5 Autonomous Systems with 200 nodes

The screen shorts of attackers launching the DDoS attack by flooding and make the link to jam. The presence of attackers and the destination nodes that disrupt the normal data transfer by the genuine nodes by this attack for single AS server among the attack launch for 5 Autonomous Systems that are connected to each with 200 nodes through border routers are shown in figure 6.4.
Filters are placed effectively with the information in FR table checks for mode of each packet. Filter checks for mode in each packet which is explained in chapter 5. If the mode is four means it is valid key and come from correct feasible route and the packet is marked as genuine and forwarded to the destination. The relevant screen shot is given in the figure 6.5
Figure 6.5 Filters placement

In the figure 6.6 the network consists of nodes. The duplex links. It is used to create a graph to identify the how many data were sent, how many data were buffered, how many packet were sent, forward received and forward sent, how many data were dropped and so on, it is separated by the different colors.
Figure 6.6 Status of Data sent Vs Data dropped

6.3 IMPLEMENTATION METHODOLOGY

There are several ASes in the internet in which most of them are vulnerable to IP spoofing attack. Our aim is to protect almost 100% ASes on using Ex-IDPF. It is not possible to deploy Ex-IDPF in all available AS. For implementation purpose consider an 200 ASes assuming 5000 users or participants over 200 ASes. Therefore, Ex-IDPFs are deployed at 35-45 selectively chosen ASes. The ASes are chosen based on two criteria as follows, AS should be highly connected and should actively participate in the routing process and it should be present on numerous source destination routes when compared to other AS.
Autonomous Systems that satisfies these two criteria are selected to deploy Ex-IDPF. Ex-IDPF deployed AS experiences more profits than its customers. To achieve goal is to set up the filters at the AS level as per the optimal filter deployment schemes. After the routing process, the tables are populated according to the node’s performance. All sender nodes (s) generate traffic towards their corresponding receiver nodes (t) through several routes (r). On generating the traffic, they are aggregated at AS level in all aspects of (s, t and r) to mitigate the computational complexity. The proposed work supports optimal deployment schemes and does not require any modifications to existing IP protocol. Ex-IDPFs are deployed at border routers and our scheme does not modify any characteristics of BGP.

A packet may refer to the routing table and take a path from s to r and unfortunately, it may be filtered out. Deploying filters at AS level has a major drawback such as it cannot find the spoofing attack that occurs within the AS. This technique is not effective when both the sender and receiver reside at the same AS because routing table is maintained at only AS level and exclude this drawback on calculating the filter effectiveness.

The proposed work is executed in NS-2 simulator to observe the security key validation and execution time for each packet is less than 6 ns. The marking block verifies the correctness of the source IP address. The filtering component is placed followed by the detecting
component. The path history table is maintained and updated in BGP. The key validation table also validated in BGP and they need at least one lookup operation. During the lookup operation, the key validation table validates each packet.

Security key is 16 bit random number and it includes the source and target AS number. The security key is altered for every 2-3 hours in a random manner to disable the spoofing capability of an attacker. During the lookup operation, the border router validates the security key for all incoming packets. The essential operations of the proposed system are executed in this operating system. The filters are deployed according to the deployment scheme. During the security key replacement, each packet header holds both old and new keys. The time estimated for the detection of a spoofed packet is less than 6 ns. Table 6.1 presents the simulation parameter of the proposed system.

<table>
<thead>
<tr>
<th><strong>Table 6.1 Simulation Parameter</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Number of ASes</td>
</tr>
<tr>
<td>Number of users per AS</td>
</tr>
<tr>
<td>Per packet estimation time</td>
</tr>
<tr>
<td>Number of feasible routers</td>
</tr>
<tr>
<td>Number of feasible path</td>
</tr>
<tr>
<td>Key replacement</td>
</tr>
<tr>
<td>Size of security key</td>
</tr>
<tr>
<td>Simulation run time</td>
</tr>
</tbody>
</table>
6.4 PERFORMANCE METRICS

AS graph can be represented as \( G (V, E) \) in which \( V \) represents
the nodes and \( E \) represents the edges. Let ‘\( u \)’ and ‘\( s \)’ be any pair of
ASes in the network such that \( |S (u, s)| \) represents a set of ASes
from which an attacker in AS ‘\( u \)’ can spoof addresses to attack ‘\( s \)’.
For
any pair of ASes, ‘\( a \)’ and ‘\( s \)’, \( |T (a, s)| \) is the set of ASes from which
attackers can attack ‘\( s \)’ using addresses corresponding to ‘\( a \)’, before
they reach ‘\( s \)’. The performance level of Ex-IDPF is measured using
three performance metrics. The basic performance metrics used are
Victim Fraction (VF), Attack Fraction (AF) and Victim Trace Fraction
(VTF).

6.4.1 Victim Fraction

Victim fraction specifies the number of nodes that could be
attacked by an attacker that spoofs the IP address of almost \( n \) nodes.
It is computed by applying the following equations.

\[
\text{Victim fraction} = \frac{|s: \forall u, |S (u, s)||}{|V|} \quad \ldots (6.1)
\]

From the equation 6.1 the victim fraction for the number of
nodes that an attacker could attack is identified .Here \( V \) represents
the nodes, ‘\( u \)’ and ‘\( s \)’ be any pair of ASes in the network such that \( |S \)
(u, s) represents a set of ASes from which an attacker in AS ‘u’ can spoof addresses to attack the victim.

6.4.2 Attack Fraction

Attack fraction is the percentage of nodes among which the zombies cannot attempt any IP spoofing attacks over other nodes except its own. It is computed by applying the following equations.

\[
\text{Attack fraction} = \frac{|u: \forall s, |S(u, s)||}{|V|} \quad \text{... (6.2)}
\]

From the equation 6.2 attack fraction is calculated. Here V represents the nodes, ‘u’ and 's' be any pair of ASes in the network such that |S(u, s)| represents a set of ASes from which an attacker in AS ‘u’ can spoof addresses to attack 's'.

6.4.3 Victim Trace Fraction

The victim trace fraction represents percentage of nodes that are capable to identify the spoofed packets and locate the origin of the spoofing process. It is computed by applying the following equations.

\[
\text{Victim trace fraction} = \frac{|s: \forall a, |T(a, s)||}{|V|} \quad \text{... (6.3)}
\]
From the equation 6.3 victim trace fraction is calculated for any pair of ASes, ‘a’ and ‘s’, \( |T(a, s)| \) is the set of ASes from which attackers can attack s using addresses corresponding to ‘a’, before they reach ‘s’.

6.5 PERFORMANCE EVALUATION

This section deals with the performance evaluation of Ex-IDPF on considering the attack scenario. Various performance metrics are compared with the proposed and existing schemes.

6.5.1 Victim Fraction

The figure 6.7 represents the victim fraction of nodes that participates in Ex-IDPF and those participate in IDPF. VF is considered in percentage and it is plotted against number of filters. Here, considered 200 ASes on which 35-45 filters are deployed according to filter deployment scheme. When there are no filters in the system, it has VF of 92%. On deploying the filters VF decreases with increase in number of filters. Ex-IDPF protects the victim from the attack in an effective manner.
6.5.2 Attack Fraction

Impact of attack fraction in Ex-IDPF and IDPF filter is shown in Figure 6.8. From the Figure, it is clear that the attack fraction of the Ex-IDPF is up to 91% while the attack fraction of IDPF is only up to 87% and deploy up to 35-45 filters among 200 ASes. The system performance remains the same even after deploying more filters. This specifies that the Ex-IDPF is more efficient in controlling the IP spoofing. The accuracy of attack fraction is much greater in the proposed Ex-IDPF than that of already existing IDPF. The packets are now protected from the attacker with the use of Ex-IDPF. From the above Figure, it is clear that, the probability of attacking node is well decreased with the use of the proposed filter.
Figure 6.8 Attack Fraction of Ex-IDPF and IDPF

6.5.3 Victim Trace Fraction

Victim trace fraction represents percentage of nodes that are capable to identify the spoofed packets and locate the origin of the spoofing process. Figure 6.9 indicates the comparison of correlation between the number of nodes and victim trace fraction in the proposed Ex-IDPF system and the existing IDPF system. VTF is expressed in percentage and plotted against number of filters. In Extended Inter Domain Packet Filter 91% of nodes can identify the attackers whereas in IDPF only 83% of nodes can identify the attacking nodes. According to optimal filter deployment scheme, 35- 45 filters are enough to provide an efficient defense mechanism.
6.6 GAIN

This parameter deals with the gain that detection method (marking) offer to its users. The users with marking scheme achieve more gain than the others. A sample of 200 users per AS is considered. The user with security key achieves almost 97.01% of gain and hence this method is considered as beneficial method. User per AS’s gain with and without marking block is shown in the Figure 6.10
6.7 FILTER PERFORMANCE OVER SPOOFING ABILITY OF THE ATTACKER

Filter must be designed such that it should greatly reduce the spoofing ability of the attackers regardless of number of attackers. Spoofing ability is defined as the ability of the attacker to spoof the IP address regardless of filtering. Figure 6.11 represents the spoofing ability of attackers in RBF and Ex-IDPF with the deployment of 35-45 filters. The attacker has 75% of ability to spoof the IP address in the absence of defense mechanism. The spoofing ability of the attacker is reduced to 2% with 45 filters. The filtering process does not get affected even when BGP path explores.
Figure 6.11 Spoofing ability Vs Number of filters

6.8 NETWORK ROUTERS

Figure 6.12 illustrates the presence of number of participating router over a part of internet. There may be 24772 internet routes but it contains only hundreds of feasible routes. The routers numbered from 10-18 has highest number of feasible paths. Figure 6.26 explains that only small number of internet routes comprise of more than 36 participating routers.
6.9 PERFORMANCE MEASUREMENT OF EX-IDPF DEPLOYMENT SCHEME

In the optimal filter deployment scheme, 35-45 filters provide 85% effectiveness measure for all participating modes. The Ex-IDPF makes 30% of attacker locality very impaired and 40% fairly impaired. The total time taken for per packet estimation is approximately 6 ns. The per packet estimation time represents the period of storing its details in the FR table. The storage cost is nearly 5-8 times greater than HCF’s and RBF’s as numerous feasible neighbors have to maintain a table of record for each parameter entry.

Let us consider the feasibility of each node is represented by 1 bit and thus, 40 bytes is needed for storing each neighbor’s parameter value and additionally 5 bytes are required to store all
prefixes. Since Ex-IDPF is vulnerable to “path all” attack, it is unable to filter out the packets that comes from a different route other than source node but reaches the destination through feasible route. In Ex-IDPF, the value of parameter table changes whenever a change occurs in the routing process, it must be updated in FR table.

![Graph showing effectiveness of optimal deployment scheme](image)

**Figure 6.13 Effectiveness of optimal deployment scheme**

The effectiveness of optimal deployment scheme is shown in Figure 6.13. It is clearly shown that 35-45 filters provide 85% of effectiveness for all nodes. The effectiveness of filtering node is little bit higher than that of all nodes.

### 6.10 FALSE POSITIVE

When a packet reaches the filter, it should decide whether to accept or discard the packet. In case if filter accepts a packet, it is
forwarded to the destination through the filter. There are some considerable issues in determining the correctness of the filters. It is mainly estimated using a parameter called false positive. False positive can be defined as the probability of filter which accepts the spoofed packets. The chief goal of the filter is to maintain the false positive value smaller. The number of false positive and false negative for 2300 attackers is shown in the Figure 6.14. The Ex-IDPF maintains lower false positive value than TPM technique.

![Figure 6.14 Number of false positive](image)

### 6.11 PARAMETERS OF VARIOUS DEFENSE MECHANISMS

Various defense schemes and their defense parameters are listed in table 6.2. The IDPF uses group of previous hop as its defense parameter while Ex-IDPF uses group of feasible path. HCF uses hop count as its parameter and RBF uses single previous hop
as its defense parameter. All these techniques involve in constructing tables and updating the entries based on the routing information.

**Table 6.2 List of defense schemes with their parameter**

<table>
<thead>
<tr>
<th>Defense scheme</th>
<th>Parameter used</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBF</td>
<td>Single previous hop</td>
</tr>
<tr>
<td>IDPF</td>
<td>Group of previous hop</td>
</tr>
<tr>
<td>HCF</td>
<td>Hop count</td>
</tr>
<tr>
<td>Ex-IDPF</td>
<td>Group of feasible path and key marking</td>
</tr>
</tbody>
</table>

6.12 COMPARISON OF SUCCESS OF EX-IDPF WITH EXISTING SYSTEMS

Table 6.3 represents the comparison of the proposed and existing schemes such as RBF, IDPF and HCF are compared to the proposed system. The Ex-IDPF is the only scheme in which almost all users attain maximum gain. The per packet estimation time in Ex-IDPF is much less than the IDPF and comparatively less than the RBF and HCF. The existing IDPF does not use any marking scheme so it has low storage value. Victim fraction is much less for the proposed system and it is high for RBF. The proposed system protects about 97.3% of the target from the attacker. The proposed system can trace the location of the true origin of attack about 98.64%. Comparison can also be made on the basis of type of defense mechanism such as active or passive.
Table 6.3 Parameter metrics comparison of Ex-IDPF with existing Schemes

<table>
<thead>
<tr>
<th>Factor</th>
<th>RBF</th>
<th>IDPF</th>
<th>HCF</th>
<th>Ex-IDPF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet estimation time</td>
<td>3 ns</td>
<td>22 μs</td>
<td>3 ns</td>
<td>6 ns</td>
</tr>
<tr>
<td>Gain (%)</td>
<td>63</td>
<td>57</td>
<td>96.2</td>
<td>97.33</td>
</tr>
<tr>
<td>Victim Fraction (%)</td>
<td>92.8</td>
<td>80.03</td>
<td>74.1</td>
<td>57</td>
</tr>
<tr>
<td>Attack Fraction (%)</td>
<td>81.21</td>
<td>86.32</td>
<td>90</td>
<td>92.14</td>
</tr>
<tr>
<td>Victim Trace Fraction (%)</td>
<td>30.05</td>
<td>33.6</td>
<td>95.42</td>
<td>96.21</td>
</tr>
</tbody>
</table>

6.13 CONCLUSION

This chapter provided us the implementation of proposed work. The attack scenario is simulated using network simulator. 200 ASes are considered with 5000 users and users are distributed in a random manner. The basic parameters to evaluate the Ex-IDPF performances are attack fraction, victim fraction and victim trace fraction. Secondary parameters are gain, effectiveness and false positives. These parameters conclude that the probability of attacking node is well decreased with the use of Ex-IDPF. The spoofing ability of the attacker is reduced to 2% with 45 filters. The Ex-IDPF maintains lower false positive value than TPM technique.

Performance of Ex-IDPF is compared with that of other prominent existing IP spoofing defense mechanisms such as RBF, IDPF and HCF. Their performances are compared in terms of per packet estimation time, gain, attack fraction, victim fraction and victim trace fraction. Ex-IDPF follows optimal deployment schemes and advantages of optimal filter deployment scheme have been
proved. The effectiveness of the marking block is also high compared to other marking systems. This implementation section concludes that Ex-IDPF is an effective defense mechanism against IP spoofing based DDoS attack.