Denial of Service (DoS) attack becomes an important security issue in the network service provisioning due to huge demand on internet services being provided by large application server. Recently, many research works have been developed for Distributed Denial of Services (DDoS) attack model to avoid flooding attack in the Internet Service Provider. However, DDoS attacks still causes demanding issues in Internet infrastructure and IT environment. In order to overcome such limitations, Fair Scheduling among the Multiple Flows (FSMF) scheme is proposed in this paper. FSMF scheme increases the system defenses thereby it efficiently eliminates the unconstitutional attack in internet service provisioning. FSMF scheme ensures immunity from misbehaving flows and allows for better congestion control in wireless network. In FSMF scheme, all the attack process and their general characteristics are initially analyzed to design a general DDoS defense technology. Then, location of network topology is analyzed depends on the each attack phases by assigning rules to packets. Experimental evaluation of FSMF scheme is done with the performance metrics such as attack resistance rate, vulnerability ratio and flow correlation coefficient. Experimental analysis shows that the FSMF scheme is able to improve the attack resistance rate by 9% and also reduce the vulnerability ratio of attacker by 38% when compared to the state-of-the-art works.

1. INTRODUCTION

Distributed Denial of Service (DDoS) attack has caused serious damage to the server using more resources in the hands of the Attacker and bullying is even more for the extension of the new Internet. The common DDoS attacks caused in the network layer are ICMP flood, SYN flood, UDP floods, which are called networks of DDoS attacks. The objective of these DDoS attacks is to use more bandwidth of the network and disallow service to users of the victim's system. Recently, most of the research works have been for designed for DDoS attack resistance and prevention. For example, Adaptive Probabilistic Filter Scheduling (APFS) architecture was designed in [1] using Probabilistic Packet Marking (PPM) and a filter scheduling policy to defeat DDoS attacks. But, it is not able to control the multiple flows of packets. Backbone traffic mining model to detect application-layer DDoS attack was introduced in [2] for identifying the malicious sources and to stop the abnormal traffic. However, attack resistance remained unsolved.

Trackback method for DDoS attacks was designed in [3] depends on entropy differences among normal and DDoS attack traffic. Trackback method for DDoS attacks was employed for information theoretical parameters. Therefore, Trackback method eliminates the inherited defects of the package identification mechanisms. Flow similarity-based approach was presented in [4] with aiming at avoiding DDoS attacks from flash crowds’ discrimination algorithm.

Mobile ad hoc network's routing vulnerability and the network performance under Distributed Denial of Service MANETS was analyzed in [5]. Supportive Bit-Compacted Authentication (SBA) was introduced in [6] to provide protection against DOS attacks and to identify malicious packets at intermediate nodes. A new mechanism was presented in [7] for detection and prevention of DDoS attacks on a web server where incoming traffic to the server was monitored and any abnormal rise in the inbound traffic was identified.

Application based Polynomial Distribution (A-PD) model was developed in [8] for reducing the difficulties associated to application oriented DDoS attack. A-PD model effectively reduces the abnormality of service or the attack rate thereby it increases the security. Analytical approach was designed in [9] to deal with the DDoS attacks problem. Analytical approach effectively reduces the flow of malicious packets from DDoS attacks.

Two different types of DDoS attacks like flooding attack and black hole attack was analyzed in [10] for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

2. RELATED WORKS

Gaussian distribution factor was introduced in [11] to improve the attack resistance scheme for achieving enhanced detection rate in the application DDoS attack. Survey of various DDoS attack prevention mechanism and detection mechanism are explained in [12] for effectively prevent and detect the DDoS/DoS attacks.

Dynamic resource allocation strategy was designed in [13] to oppose DDoS attacks against individual cloud customers. An analytical queueing model depends on the embedded Markov chain was developed in [14] to examine the performance of rule-based firewalls while focused to normal traffic flows with DoS attack flows targeting dissimilar rule positions. Privacy-preserving universal authentication protocol termed as Priauth was presented in [15] for providing strong user secrecy against eavesdroppers and foreign servers, session key establishment.

Software puzzle scheme was introduced in [16] for avoiding GPU-inflated DoS attack. Software puzzle scheme has utilized software protection technologies to make sure challenge data confidentiality. Protective framework was designed in [17] for avoiding HTTP based DoS/DDoS attacks such as the flexible, collaborative, multilayer, DDoS prevention framework (FCMDFP). The FCMDFP framework was evaluated on the basis of optimum specifications for a protective framework for the protection of web applications from HTTP-based DoS and DDoS attacks. In [18], a novel framework was presented for DDoS defense technique based on two filters such as simple filter and enhanced filter for detecting and avoiding attacks.

Mathematical model of total traffic was developed in [19] to reveal DoS / DDoS attacks and to raise the
network security level at the expense of the organization of multi-level of protocols routing. MOTAG framework was designed in [20] that employ dynamic, hidden proxy nodes as moving targets to mitigate insider-assisted network flooding DDoS attacks. On the basis of the above techniques and methods presented in this thesis we propose a new framework called fair scheduling under the multiple flows (FSMF) scheme for DDoS attack resistance and prevention in the wireless network. Proposed FSMF regime developed that removes the unconstitutional attack on the wireless network, which in turn increases the defenses (i.e. resist attack capability). FSMF scheme also ensures immunity (i.e. prevention) from misbehaving flows in wireless network. The paper is structured as follows. In chapter 2 we describe the design of the exhibition plans under the multiple flows (FSMF) scheme for DDoS attack resistance and prevention in the wireless network. Chapter 3 presents the different experimental settings in this work. We evaluate our algorithm for object detection and compare them with the state of progress of the work, discuss in detail in Chapter 4. Finally, the paper concludes in section 5.

3. FAIR SCHEDULING AMONG THE MULTIPLE FLOWS (FSMF) SCHEME FOR DDoS ATTACKS RESISTANCE AND PREVENTION

Fair Scheduling among the Multiple Flows (FSMF) scheme has to be developed based on an analysis of DDoS attack overall IT environment. In FSMF scheme, we propose a new fair scheduling for each attack phase and DDoS attack detection technologies. The main objective of FSMF scheme is to avoid DDoS attacks in wireless network. In FSMF scheme, Fair Scheduler has simple rules for controlling multiple packets flow with aiming at avoiding unconstitutional attacks and increasing system defenses in wireless network. Fair scheduling is a method of assigning rules to packets for controlling the multiple flows (i.e. speed of packet transmission in wireless network) such that all the packets flows get on average or an equal speed over time. As a result, FSMF scheme efficiently eliminates the unconstitutional attacks and ensures prevention from misbehaving flows in wireless network. The DDoS attack resistance and prevention using FSMF scheme is shown in Figure 1. From the Figure 1, proposed FSMF scheme is used fair scheduling algorithm for controlling the packet flows in wireless network thereby it eliminates the DDoS attacks and ensures immunity from the misbehaving flows. Fair scheduling scheme will assigns some rule for each packet in wireless network. During packet transmission, FSMF scheme completely block the sophisticated DDoS attacks from the client based on the rules formed in fair scheduling rule base. As a result, proposed FSMF scheme significantly eliminates the unconstitutional attack which results in improved system defenses in wireless network.

3.1 Analysis of DDoS Attack Process

Initially, the all attack process of DDoS attack should be evaluated in FSMF scheme with the aim of building an effective DDoS defense infrastructure. The analysis of attack process of BotNet comprises of four parts such as Attack agent development part, Attack agent distribution part, Attack agent control part, Attack phase. BotNet is a collection of cooperated computers which also termed as "zombies" infected with malwares that allows an attacker to manage them. The DDoS attack process of BotNet is demonstrated in below Figure 2.

I. Attack agent development part

Initially, the attack agent should be developed. The attack agent can include a lot of functionalities likes various attack methods, control mechanisms, self-destruction function and information leak functions.

II. Attack agent distribution part

By using the developed attack agents, attackers have to collect the BotNet PCs. For the BotNet PCs register of agents should distribute. There are many ways to share the agents to vulnerable PCs. Initially, it can employ the vulnerabilities of PCs for agent sharing. It also can be downloaded from a web page by normal users. One of the most popular methods for agent sharing is deceiving the users and let them download the agent by means of Web page or P2P network by themselves. This download process is a legitimate activity as a result it is difficult to prevent the agent sharing by network level attack detection and prevention systems.

C. Attack agent control part

Once the attack agents are established in a BotNet PC then it should be controlled by the attacker. For that, attackers developed their own communication protocols to control the agents. Though, malware control protocol could be without difficulty detected and blocked. As a result, agents use legitimate
application protocols like HTTP, IRC, P2P, etc. By using these protocols agents communicate with Command and Control server (C&C server). When an attacker attacks specific target to C&C server then the server sends the command to BotNet PCs. The attackers can update the agents and destruct them as well by using this method.

D. Attack part
Presently attempted attacks are very complicated attacks. In fact, it is very difficult to detect those attacks. Besides, attackers cause different types of attacks at the same time and the bandwidth of each attack are not that big enough to be detected easily. If only the attack packet is investigated, it is perfectly normal. Definitely, other types of attacks such as massive traffic generation attack are also still tried.

3.2 Fair Scheduling among the Multiple Flows for avoiding the DDOS attacks
Fair Scheduling is used to control the flow of packets (i.e. packets with different arrival rates and are packets controlled by assigning some rules to packets while during the packet transmission for avoiding the DDOS attacks) in wireless network for avoiding DDOS attacks. In FSMF scheme, Fair Scheduling can be subjected to multiple flows with each flow targeting the same or different rule. In this section, we model and analyze the performance of a Fair Scheduling to multiple packet flows in wireless network. In FSMF scheme, we define a flow in a moving term so that an incoming flow is always triggers a rule. If a trigger more than one rule, then was defined as several flows.

The previously described analytical model for a flow can also be used to study the performance, even with multiple incoming flows with corresponding arrival prices \[\lambda_j, 1 \leq j \leq \delta\] such that each individual flow \(\lambda\) triggers a particular rule in \(\{\lambda_j: 1 \leq j \leq \delta\}\) of the Fair Scheduling rule base as illustrated in Figure 3.

![Figure 3 multiple incoming flows with each flow matching a different rule using FSMF scheme](image)

Multiple incoming flows with each matching a different rule with FSMF scheme is shown in figure 3. Where \(\delta\) represents the total number of incoming flows and \(\lambda\) refers to the size of a Fair Scheduling rule base. It is to be noted that more than one flow can trigger the same rule \(\lambda\). A solution for this case is estimated by means of aggregating all flows into one aggregated flow and evaluating the average matching rule position for the aggregated flow. The aggregated flow rate \(\lambda\) is mathematically formulated as follows,

\[\lambda = \sum_{i=1}^{\delta} \lambda_i \] \hspace{1cm} (1)

From (1), \(\lambda_i\) denotes the flow rate of multiple packets in wireless network whereas \(i = 1, 2, \ldots, \delta\) The average position of all matching rules for the aggregated flow can be mathematically formulated as below,

\[P = \left[\sum_{i=1}^{\delta} \left(\frac{\lambda_i}{\lambda} \right) \right] \] \hspace{1cm} (2)

From (2), \(P\) refers the matching rule position of flow \(\lambda\), \(\lambda_i\) denotes the arrival rate of packet and \(\lambda_i\) is defined as the flow rate of multiple packets. Then, the individual throughput of \(\tau\) (i.e. rate of successful packet delivery over a wireless network) can be mathematically formulated as

\[\text{Individual throughput } \tau_i = \frac{\lambda_i}{\lambda} \times P \] \hspace{1cm} (3)

From (3), \(\tau\) denotes the aggregated throughput, \(\lambda_i\) is referred as the flow rate of multiple packets. Determining the \(\tau_i\) can be used to compute other performance measures of flow \(\lambda_i\). For instance, the CPU utilization per flow \(\tau_i\) is mathematically formulated as below,

\[U_{util_i} = \frac{\tau_i}{\lambda_i} \] \hspace{1cm} (4)

From (4), \(\tau\) represent the mean service time that defined as the sum of mean service time of all stages. The average packet delay \(\tau_i\) is same as average packet delay for aggregated flow \(\tau\) which is mathematically formulated as,

\[\tau = \sum_{i=1}^{\delta} \tau_i \] \hspace{1cm} (5)

From (5), \(\tau\) refers the mean of packets in the system and \(\tau\) represents the aggregated throughput. The same is also true for the packet loss per flow being equivalent to the packet loss of aggregated flow. The algorithmic process of Fair Scheduling using FSMF scheme is explained in below figure.

![Figure 4 Fair Scheduling Algorithm for Controlling Multiple Packet Flows in Wireless Network](image)
As shown in Figure 4, in FSMF scheme, Fair Scheduling Algorithm initially assigns some rule for each packet in wireless network. Then, it calculates the aggregated flow of all packages for the control of multiple streams in the wireless network. Subsequently, it evaluates the average position of all matching rules for the aggregated flow to avoid the DDoS attacks in wireless network. After that, Fair Scheduling Algorithm estimates the rate of successful packet delivery over a wireless network (i.e. individual throughput) to ensure the immunity from the misbehaving flows in wireless rate. Finally, this algorithm evaluates the CPU utilization per flow with aiming at eliminating the unconstitutional attack in internet service provisioning which increases the system defenses in wireless network.

4. Experimental Evaluation
In order to test proposed method, FSMF scheme is implemented using NS-2 simulator with the network range of 1000*1000 m size. The number of sensor nodes selected for experimental purpose is 40 nodes. The resources are allocated effectively for node ‘1’ to ‘n’ nodes. The simulation results show that it takes 500 sec to transmit the packet securely from source to destination without DDoS attack. The parametric values for performing experiments are illustrated in table 1.

Table 1 Simulation setup

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>DSDV</td>
</tr>
<tr>
<td>Network range</td>
<td>1000 m * 1000 m</td>
</tr>
<tr>
<td>Simulation time</td>
<td>50 ms</td>
</tr>
<tr>
<td>Number of mobile nodes</td>
<td>10, 20, 30, 40, 50, 60, 70</td>
</tr>
<tr>
<td>Mobility model</td>
<td>Random Way Point</td>
</tr>
<tr>
<td>Network simulator</td>
<td>NS 2.34</td>
</tr>
<tr>
<td>Mobility speed</td>
<td>10 m/s</td>
</tr>
<tr>
<td>Pause time</td>
<td>15 s</td>
</tr>
<tr>
<td>Packets</td>
<td>7, 14, 21, 28, 35, 42, 49</td>
</tr>
</tbody>
</table>

In the Random Way Point (RWM) model, each node shift to an erratically chosen location with randomly selected speed between a predefined smallest amount and highest speed. The standard of the total number of mail sent or received per node using RMW is evaluated for the communication requirements, and alternately measure resiliency by counting the number of times must it should run the protocol in order to detect a single node replication. The performance of FSMF scheme is tested with metrics such as attack resistance rate, vulnerability ratio, and flow correlation coefficient. The result of the FSMF scheme is compared against with existing methods such as Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2] respectively.

4. DISCUSSION
In this section, the result analysis of FSMF scheme is evaluated. Comparison is made with the two existing methods namely Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2]. To estimate the efficiency of FSMF scheme, the following metrics like attack resistance rate, vulnerability ratio, and flow correlation coefficient are measured.

4.1 Measurement of Attack Resistance Rate
Attack Resistance Rate ($ARR$) using FSMF scheme is defined as ratio of number of nodes restricted by attackers to the threshold number of nodes in the network path. Attack Resistance Rate is measured in terms of percentage (%) and formulated as below,

$$ARR = \frac{\text{No. of nodes restricted by attackers}}{\text{total no. of nodes}} \quad \ldots \quad (6)$$

Higher the Attack Resistance Rate, the method is said to be more efficient.

Table 1 Tabulation for Attack Resistance Rate

<table>
<thead>
<tr>
<th>No. of nodes</th>
<th>Attack Resistance Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FSMF scheme</td>
</tr>
<tr>
<td>10</td>
<td>84.36</td>
</tr>
<tr>
<td>20</td>
<td>86.33</td>
</tr>
<tr>
<td>30</td>
<td>87.25</td>
</tr>
<tr>
<td>40</td>
<td>88.14</td>
</tr>
<tr>
<td>50</td>
<td>89.47</td>
</tr>
<tr>
<td>60</td>
<td>90.12</td>
</tr>
<tr>
<td>70</td>
<td>92.78</td>
</tr>
</tbody>
</table>

Table 1 represents the Attack Resistance Rate of FSMF scheme with respect to different number of nodes in the range of 10-70 and comparison is made with existing methods such as Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2] respectively. From the table value, it is clear that the proposed FSMF scheme increases the Attack Resistance Rate than the other state-of-art methods.

Figure 5 Measurement of Attack Resistance Rate
Figure 5 shows the impact of Attack Resistance Rate using proposed FSMF scheme, Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2] versus different number of nodes in the range of 10 to 70. As illustrated in Figure, the proposed HGRSD method performs relatively well when compared to existing methods [1], [2]. From the figure, while increasing the number of nodes, the Attack Resistance Rate is gets also increased. But comparatively Attack Resistance Rate using FSMF scheme is higher. This is because of the application of Fair Scheduling algorithm in FSMF scheme. Fair Scheduling algorithm efficiently block the sophisticated DDoS attacks from the client based on the rules formed in fair scheduling rule base. Therefore, FSMF scheme is improved the Attack Resistance Rate by 12% when compared to the existing Adaptive Probabilistic Filter Scheduling (APFS) [1] and 6% when compared to the Backbone traffic mining model [2] respectively.

4.2 Measurement of Flow Correlation Coefficient
In FSMF scheme, Flow correlation coefficient is calculated for two different network flows in each node. Each node contains input network packet flows. Higher the Flow correlation coefficient, the method is said to be more efficient.
The Flow correlation coefficient for FSMF scheme is elaborated in Table 2. We consider the framework with different number of nodes in the range of 10 to 70 for experimental purpose using NS-2. The performance of proposed FSMF scheme is compared with existing methods such as Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2] respectively.

Table 2 Tabulation for Flow correlation coefficient

<table>
<thead>
<tr>
<th>No. of nodes</th>
<th>Flow correlation coefficient</th>
<th>FSMF scheme</th>
<th>Adaptive Probabilistic Filter Scheduling</th>
<th>Backbone traffic mining model</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>75</td>
<td>47</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>79</td>
<td>51</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>82</td>
<td>55</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>85</td>
<td>56</td>
<td>79</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>88</td>
<td>59</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>89</td>
<td>68</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>91</td>
<td>73</td>
<td>85</td>
<td></td>
</tr>
</tbody>
</table>

Figure 6 demonstrates the impact of Flow correlation coefficient versus different number of nodes in the range of 10 to 70 using FSMF scheme. As illustrated in Figure, the proposed FSMF scheme performs well when compared to existing methods such as Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2] respectively. From the figure, while increasing the number of nodes, the Flow correlation coefficient is gets also increased. But comparatively Flow correlation coefficient is improved by using FSMF scheme. This is because of the application of Fair Scheduling algorithm in FSMF scheme. With the help of Fair Scheduling algorithm, FSMF scheme efficiently eliminates the misbehaving flows in wireless network. As a result, FSMF scheme is improve the Flow correlation coefficient by 17% when compared to the existing Adaptive Probabilistic Filter Scheduling (APFS) [1] and 9% when compared to the Backbone traffic mining model [2] respectively.

4.3 Measurement of Vulnerability ratio

In FSMF scheme, Vulnerability is the ability where a node’s quality gets easily attacked by the attackers. Lower the Vulnerability ratio, the method is said to be more efficient.

Table 3 Tabulation for Vulnerability ratio

<table>
<thead>
<tr>
<th>Methods</th>
<th>Vulnerability ratio (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSMF scheme</td>
<td>28.68</td>
</tr>
<tr>
<td>Adaptive Probabilistic Filter Scheduling</td>
<td>41.35</td>
</tr>
<tr>
<td>Backbone traffic mining model</td>
<td>37.86</td>
</tr>
</tbody>
</table>

Table 3 represents the Vulnerability ratio of FSMF scheme versus different number of nodes in the range of 10 to 70. To determine the performance of FSMF scheme, comparison is made with existing methods such as Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2] respectively. From the table, it is illustrative that the Vulnerability ratio using the proposed FSMF scheme is reduced when compared to other methods [1], [2].

Figure 7 Measurement of Vulnerability ratio

Figure 7 illustrates the impact of Vulnerability ratio for FSMF scheme versus different number of nodes. As illustrated in Figure, the proposed FSMF scheme performs well when compared to existing methods such as Adaptive Probabilistic Filter Scheduling (APFS) [1] and Backbone traffic mining model [2] respectively. From the figure, while increasing the number of nodes, the Vulnerability ratio gets also increased. But comparatively Vulnerability ratio is reduced by using FSMF scheme. This is due to the application of Fair Scheduling algorithm in FSMF scheme. With the support of Fair Scheduling algorithm, FSMF scheme evaluates the CPU utilization per flow with aiming at eliminating the unconstitutional attack in internet service provisioning which in turn increases the system defenses in wireless network. Therefore, FSMF scheme is reduced the Vulnerability ratio by 44% when compared to the existing Adaptive Probabilistic Filter Scheduling (APFS) [1] and 32% when compared to the Backbone traffic mining model [2] respectively.

5. CONCLUSION

In this paper, an effective novel framework is designed called as Fair Scheduling among the Multiple Flows (FSMF) scheme for DDOS attack resistance and prevention. The main goal of FSMF scheme is to avoid the DDOS attack and to ensure immunity from the misbehaving flows in wireless network. FSMF scheme is initially analyzes the all attack process and their general characteristics. Then, location of the network topology is analyzed, depends on the individual phases of attack by assigning fair planning rules for packages for the control of several flow rates in the wireless network. With the help of fair scheduling algorithm, FSMF scheme effectively block the sophisticated DDoS attacks from the client based on the rules formed in fair scheduling rule base. Besides, FSMF scheme efficiently eliminates the unconstitutional attack in internet service provisioning which in turn increases the system defenses. In addition, FSMF scheme ensures immunity (i.e. prevention) from misbehaving flows and allows for better congestion control and rate-adaptive applications. The proposed FSMF scheme is conduct experimental work on NS 2 simulator. With the experiments conducted for FSMF scheme, it is observed that the attack resistance rate for different number of nodes in wireless network provides more accurate as compared to existing...
methods. The experimental results show that FSMF scheme provides better performance with an improvement of attack resistance rate by 9% and also reduced the vulnerability ratio of attacker by 38% when compared to state of the art works.

REFERENCES


15. Dajiao He, Jiajun Bu, Sammy Chan, Chun Chen, and Mingjian Yin, “Privacy-Preserving Universal Authentication Protocol for Wireless Communications”