DISTRIBUTED DENIAL OF SERVICE ATTACK PREVENTION USING CRITICAL LINK METHOD IN MANET


Abstract— Mobile Ad hoc Network (MANET) is self configuring network of mobile node connected by wireless links and considered as network without infrastructure. Routing protocol plays a critical role for efficient communication between mobile nodes and operates on the basic assumption that nodes are completely supportive. Because of open organization and restricted battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. After becoming part of active path, these nodes start denying forwarding or dropping data packets thereby degrades the performance of network. In this paper, Intrusion prevention system against distributed denial of service attack (DDoS) were proposed, so that our network gets more secure through attack and detect malicious node and malicious behavior through the Intrusion prevention system (IPS) and detect via Intrusion Detection System.

Index Terms—MANET, Routing, Malicious, DDOS, IPS.

I. INTRODUCTION

A mobile ad-hoc network is a group of devices which are connected without a predetermined infrastructure such as access points or independent base stations. This lack of infrastructure supposes the devices in the routing system, creating multi-hop wireless paths linking nodes with those which are out of their wireless range. This kind of networks without fixed infrastructure and high mobility are ideal for places such as battlefield, and for establishing communications after natural disasters. However, in these environments network security becomes critical [1].

Each node in the network also acts as a router, forwarding data packets to other nodes [2]. Many routing protocols are used to manage the ad-hoc networks. These protocols are categorized into three categories: flat, hierarchical, and geographic position assisted routing [3]. There are two types of flat routing protocols: reactive and proactive. The Ad-hoc On-Demand Distance Vector (AODV) protocol is a reactive protocol designed for ad-hoc networks [4]. AODV uses a broadcast route discovery mechanism which relies on dynamically established routing table entries at intermediate nodes. AODV floods the whole network with Route Request packets (RREQ) and Route Reply (RREP) packets. This flooding leads to high overhead.

A. DDoS Attacks

DoS attack causes either disruption or degradation on victim’s shared resources, as a result preventing legitimate users from their access right on those resources. DoS attack may target on a specific component of computer, entire computer system, certain networking infrastructure, or even entire network / Internet infrastructure. Attacks can be either by exploits the natural weakness of a system, which is known as logical attacks or overloading the victim with high volume of traffic, which is called flooding attacks [5].

A distributed form of DoS attack called DDoS attack, which is generated by many compromised machines to coordinately hit a victim. DDoS attacks are adversarial and constantly evolving. Once a particular kind of attack is successfully countered, a slight variation is designed that bypasses the defense and still performs an effective attack. In this paper, overview of the DDoS problem, available DDoS attack tools, defense challenges and principles, and a classification of available DDoS prevention mechanisms is covered. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat [6].

The current prevention mechanisms reviewed in this paper are clearly far from adequate to protect network/Internet from DDoS attack. The core problem is that there are still lots of insecure machines over the network/Internet that can be compromised to commence large-scale coordinated DDoS attack. One talented direction is to develop a comprehensive solution that encompasses several defense actions to trap variety of DDoS attack. If one level of protection fails, the others still have the opportunity to defend against attack. A victorious intrusion requires all defense planes to fail [7].

A. Intrusion Detection System

Zhang and Lee [8] present an intrusion detection technique for wireless ad hoc networks that uses cooperative statistical anomaly recognition techniques. The use of anomaly based detection techniques results in number of false positives. Stamoulis proposes architecture for Real-Time Intrusion Detection for Ad hoc Networks (RIDAN) [9]. The detection process depends on a state-based misuse detection system. Therefore, each node needs extra processing power and sensing capabilities.
In [10], the method requires the intermediate node to send Route Confirmation Request (CREQ) to next hop in the direction of the destination. This operation can amplify the routing overhead resulting in performance poverty. In [11], source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination, so that it can distinguish the safe route to destination. This method can origin the routing delay, since a node has to wait for RREP packet reach to destination from more than two nodes. In [12], the feature used is dest_seq_no, which reflects the trend of updating the threshold and hence reflecting the adaptively change in network surroundings.

Therefore, a method that can prevent the attack without rising routing overhead and delay is requisite. All the above mentioned techniques except [12] use static value for threshold. To determine the problem, threshold value should be reflecting current network environment by enhancing its value. And also, this solution ensures that a node once detected as malicious cannot participate in forwarding and sending of a data packet in the network.

II. RELATED WORK

According to [1] proposes a way or place where security application can track more traffic instead of applying to all nodes that can save much more cost as compared to provide security for every node. Critical link are that place, from where maximum traffic can travel and monitoring of those nodes are easy.

According to [13], DoS attack can be launched in two forms. The first form aims to break down the target by sending one or more carefully constructed control packets that make use of the protocol or operating system vulnerabilities. The second form is to overflow the target with a huge amount of rubbish data, which leads to exhaustion of network bandwidth or computer resources.

In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes [14], [15]. As a consequence, routing loops may appear and introduce severe network congestion. Multiple attackers may completely isolate a victim, by preventing it from finding performed via network-layer packet blasting [16]. The attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET. In a SYN flooding attack, the attacker creates a large number of half-opened Transmission Control Protocol (TCP) connections with a target node, but never completes the handshake to fully open the connection [13], [14].

Application-based attacks force the victim to perform CPU and memory-intensive database operations and leave few resources to serve legitimate users. This type of attack may be closely related to the sleep deprivation attack, which aims to consume the energy of a victim node [13].

The study presented in [15] investigates the influence of flooding attacks with Dynamic Source Routing (DSR) protocol messages to network performance. The packet delivery ratio and packet delay have been evaluated under different flooding frequencies and different numbers of attack nodes. The analysis assumes only the random waypoint mobility model.

In [17], a notion of dynamic DoS attack has been introduced and analyzed, considering Ad hoc On-demand Distance Vector (AODV) routing protocol. The attack propagation has been modeled by a semi-Markov process. The analysis indicates that the impact of DoS attack may be spread by the mobility of malicious nodes; this is faster in dense networks than in sparse networks.

A simulation study on anonymity threats against MANETs [18] considers a sparse mode inference attack where a target node moves straightly across a network from the left side to the right.

Solutions to locate malicious packet dropping using an unobtrusive monitoring technique have been proposed in [19]. Performance evaluation has indicated that the detection effectiveness depends on the node speed and the applied mobility model.

III. PROPOSED SCHEME

A. Problem Definition

In the field of mobile ad hoc networks routing protocols, there are lot of problems to be tackled such as Quality of service, routing optimization and security issues. My main interest is in the security issues related to routing protocols in MANETs. The work is done through Network simulator-2 and measures network performance. Our aim to apply Intrusion prevention system against distributed denial of service attack so that our network totally secure through attack and detect malicious node and malicious activity through the Intrusion prevention system and detect via Intrusion Detection System.

B. Data Collection and Implementation Strategy

For data collection and implementation we will use Network Simulator- 2 (NS-2). The description about simulation environment is as follows:

Network simulator 2 (NS2) is the result of an ongoing effort of research and development that is administrated by researchers at Berkeley [20]. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multipath protocol.

The simulator is written in C++ and a script language called OTcl2. Ns use an Otcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called Network Animator.

C. Simulation Parameter

We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc. According to table-1 shown below, we simulate our network.
Table 1: Simulation parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>50</td>
</tr>
<tr>
<td>Dimension of simulated area</td>
<td>800×600</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Simulation time (seconds)</td>
<td>35</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR, FTP</td>
</tr>
<tr>
<td>Packet size (bytes)</td>
<td>1000</td>
</tr>
<tr>
<td>Number of traffic connections</td>
<td>10</td>
</tr>
<tr>
<td>Maximum Speed (m/s)</td>
<td>Random</td>
</tr>
</tbody>
</table>

IV. RESULT ANALYSIS

A. TCP Analysis

In this simulation, three TCP connections with TCP normal case, TCP at Malicious case and TCP at IPS (Intrusion Prevention System) were created and analyze the comparative result between them. In graph result shows x-coordinate as simulation time in seconds and y-coordinate represents window size (No. of Packets), according to result output it is observed that maximum window size which TCP normal case reached is 40 units, TCP Malicious Case reached till 12 packets and TCP IPS time reached maximum 55 packets. As per result shows, there is much more variation in data transfer. According to simulation result it is observed that the performance of TCP window at IPS case is much higher while it is medium at normal case and too less at malicious time.

B. UDP Packet Receive Analysis

According to graph shown below, x axis shows simulation time in sec. and y axis shows total UDP packet according to our representation red line show total number of UDP packets received by receiver in normal case with respect to time, green line shows total number of UDP packets receives by the receiver in Malicious case and blue line shows UDP packet receives by receiver in IPS case, according to graph in IPS case Maximum UDP Packets were successfully received as compared to another cases.

C. Misbehavior Analysis

This graph shows misbehavior analysis of system. X - Axis represents percentage of attack infection and Y- axis shows time in seconds. In graph red line shows DoS attack infection and green line shows normal routing misbehavior. According to result obtained in simulation it is observed that routing misbehavior is affecting system slowly with maximum of 4 %. After 18 seconds when DoS attack introduced it infect the system rapidly up to 36 %.
D. Packet Delivery Ratio Analysis

Packet delivery fraction (ratio) is a ratio of no of receives packets from no of packets transmitted per time unit. We formulize that

$PD = \left(\frac{Rx}{Send}\right) \times 100$

According to graph shown below, PDF of normal case shown by red line, PDF of malicious case shown with green line and blue line shows PDF of IPS time. As per result obtained higher PDF value of Normal case is nearly 74 %, higher PDF value of malicious case is nearly 76 % but only for a moment after that performance was degraded rapidly. While higher PDF value of IPS case is 78 %. As per graph IPS case shows better result than other two cases.

![Figure 4: Packet Delivery Ratio Analysis](image)

V. 5. CONCLUSION

Intrusion prevention system against distributed denial of service attack were proposed, so that our network totally secure through attack and detect malicious node and malicious activity through the Intrusion prevention system and detect via Intrusion Detection System. As per result observed in simulation, Intrusion Prevention System (IPS) shows better performance and enhances the reliability of network. This Scheme is also gives better result in case of Denial of Service (DoS) attack.

REFERENCES


