DETECTING AND PREVENTING THE PACKET FOR TRACE BACK DDoS ATTACK IN MOBILE AD-HOC NETWORK

M.Yasodha\textsuperscript{1}, S.Umarani\textsuperscript{2}, D.Sharmila\textsuperscript{3}

\textsuperscript{1}PG Scholar, Maharaja Engineering College, Avinashi, India.
\textsuperscript{2}Assistant Professor, Maharaja Engineering College, Avinashi, India.
\textsuperscript{3}Professor & Head, Bannari Amman Institute of Technology, Sathyamangalam, India.

Abstract:

Mobile Ad hoc Network (MANET) is the sort of wireless networks that use multi-hop relaying and is an infrastructure less Network because of its potential of operating without the aid of any fixed network. Because of open nature of the system, it is vulnerable against several attacks. The key security risk on MANET is a Distributed Denial of Service (DDoS) attack. DDoS attack has the potential to create a huge measure of undesirable traffic. It is hard to identify and control the DDoS attack because of large scale and complex system environments. In this paper, an analytical technique that utilizes Reactive Defense Mechanism to mitigate the DDoS attack has been proposed. The proposed approach enhances network performance in terms of low delay and less packet drop. Further the simulation result shows the efficiency of the proposed methodology.

Keywords: Mobile Ad Hoc Network (MANET), Distributed Denial of Service (DDoS), Reactive Defense mechanism.

I. Introduction

Ad-hoc network is the network consisting of wireless nodes. It is essentially infrastructure less network which is self-organized i.e. the connections are created without any centralized management [1],[2]. A Mobile Ad hoc Network (MANET) is a unstructured network that can be made without fixed infrastructure. This implies that all its nodes act as routers and participate in its discovery and maintenance of routes to different nodes in the network i.e. nodes inside one another's radio extent communicate directly through wireless links, while those that are further separated use different nodes as relays. Its routing protocol must have the capacity to adapt to the new challenges that a MANET makes, for example, nodes versatility, security support, and quality of service, limited power supply and bandwidth.

These challenges set demands on routing protocols. There are distinctive key issues and sub-issues, for example, routing, multicasting/broadcasting, clustering, location service, mobility management, IP addressing, multiple access, radio interface,
TCP/UDP, power and bandwidth management, security, QoS/multimedia and fault tolerance.

Recent wireless research shows that the MANET presents a major security issue than traditional wired and wireless networks. DDoS attacks are accounted for as one of the greatly occurring attack over a recent decade. Numerous service providers and legitimated users have experienced a terrible experience from these attacks. A DDoS attack is large scale, facilitated attack on the availability of services at the target system or network asset. The DDoS attack is propelled by sending large measure of packets to the target node through the coordination of vast measure of nodes which are circulated all over the network. At the target side this traffic consumes the bandwidth and does not permit other critical packet to reach the system.

Though different security measures have been adopted broadly in wired networks, they cannot be utilized in MANETs. It is extremely challenging in MANETs to meet the regular security requirements, for example, data privacy, information trustworthiness, and service availability. Research has been directed in past decades that attempt to incorporate security arrangements on top of secure routing protocols. To date, on the other hand, it is still a continuous research on techniques to defend against DDoS attack. In this paper, we propose a novel a analytical method that uses Reactive Defense Mechanism to mitigate the DDoS attack in MANET.

II. Related Work

Several research works has been carried out to defend against DDoS attack in MANET [3], [4], [5]. In [6], the authors proposed a defense approach which contains flow monitoring table (FMT) at every node. FMT consists of flow id, source and destination id and packet sending rate. Data transfer rate is computed for each flow at intermediate nodes. With each one flow, the upgraded FMT is sent to the destination. After monitoring the MAC (Media Access Control) layer, the target node sends the Explicit Congestion Notification (ECN) bit to caution the sender nodes about the congestion. After receiving ECN, the sender reduces their sending rate. In the event that the channel gets to be congested persistently because of some sender nodes don't decrease their sending rate, it can be found by the target node utilizing the upgraded FMT. It checks current sending rate with the past sending rate of a stream. At the point when both the rates are same, the corresponding sender of the flow is considered as an attacker. Once the DDoS attackers are discovered, all the packets from those nodes will be rejected. Advantage of this approach is to enhance the performance of the Ad hoc system in terms of bandwidth, packet delivery ratio, and packet drop.

In [7], the authors introduced a system for determining misbehave or intrusion in MANET utilizing intrusion detection system and secure the network from Distributed Denial of Service (DDOS) and examined the result on the basis of real TCP flow routing.
packet delivery ratio and average end-to-end delay in typical DDoS attack and IDS time. This defense mechanism comprises of a Flow Monitoring Table (FMT) of every mobile node. It consists of sender_id, time, receiver_id, transport_info, protocol_type, node coordinate axis and event_type. They capture the data of all nodes till specific time. The normal and abnormal behavior of the network is watched. If network contamination was recognized, they identify the attacker node and it will be obstructed from the network.

In [8] a confidence based filtering method (CBF) has been proposed to identify the DDoS attack in cloud. Here, anomaly detection is utilized and the normal profile of the network is created during non-attack period and CBF is employed to identify the attacker in attacker period. In [9] DDoS flooding attack detection is done by a step-by-step investigation approach in which entropy based detection technique to defend against DDoS attack, to prevent flooding of abnormal traffic and ensure the transmission of normal traffic.

In [10], the authors introduced a quantitative model to describe the DDoS flooding attack and its traffic detail. They likewise proposed an analytical model for searching for particular patterns of the attack traffic, targeting to attain: Decide if there is aberrance in the activity and whether the peculiarity is the DDoS attack. Decide the time when the attack is dispatched. Network forensics is the procedure of capturing, recording, and analysis of network actions to find the source of security attacks. The flooding attack is considered in this work. It plans to incapacitate the whole network, instead of any specific node, by infusing overwhelming attack traffic (e.g. RREQ broadcast) into the MANET. Since all or the majority of key assets of mobile nodes are pointlessly expended on handling and transmitting the attack activity, real users traffic is denied.

In [11] a novel defense mechanism has been presented that utilizes the medium access control (MAC) layer information in order to identify the attackers. This defense mechanism comprises distributed rate control and bandwidth reservation. Once the attackers have been identified, the packets from those nodes are blocked.

III. Proposed DDoS Mitigation Technique

This section present an analytical approach to identify the number of malicious packets and a modified hop count inspection technique to alleviate the malicious packets being sent that causes serious threat to the network performance.

A. Probabilistic Approach to Compute Malicious Packet Count

Let us consider that the packets arrive at a node with a Poisson distribution λ and let n be the number of malicious packets, r be the number of legitimate packets, N is the total number of packets arrived with λ and p be the probability that the packet is malicious and (1-p) be the probability that the packet is legitimate.
The conditional probability that the packet being malicious is given by

\[ p(n, r) = p(n + r, n) \cdot p(n + r) \]  

(1)

Here \( p(n + r, n) \) is the probability that \( n \) occurrences are success and can be expressed in binomial form as given below

\[ p(n + r, n) = \binom{n + r}{n} p^n q^r \]  

(2)

\[ p(n + r, n) = (n + 1)! \frac{p^n q^r}{(n! r!)} \]  

(3)

The Poisson distribution of \( p(n + r) \) is given by

\[ p(n + r) = e^{-\lambda} \frac{\lambda^{n+r}}{(n+r)!} \]  

(4)

Then using eq (3) and (4), eq (1) becomes

\[ p(n, r) = (n + 1)! \frac{p^n q^r}{(n! r!)} \cdot e^{-\lambda} \frac{\lambda^{n+r}}{(n + r)!} \]  

(5)

\[ = p^n(1-p)^r \cdot e^{-\lambda} \frac{\lambda^{n+r}}{(n! r!) \cdot (n + r)!} \]  

(6)

\[ = p^n (1-p)^r \left( e^{-\lambda p} e^{-\lambda(1-p)} \frac{\lambda^n \lambda^r}{(n + r)!} \right) \]  

(7)

\[ = e^{-\lambda p} (p^n \lambda^n) / n! \cdot e^{-\lambda(1-p)} (1 - p)^r \lambda^r / r! \]  

(8)

The probability of malicious packets in the traffic is given as

\[ p(N = n) = \sum_{n=0}^{\infty} e^{-\lambda p} (p^n \lambda^n) / n! \]  

(9)

By using the above equation, the number of malicious packets can be found with packet arrival rate \( \lambda \) and the joint probability \( p \) (\( p=1 \)). After obtaining the number of malicious packets modified hop count approach is used to alleviate these malicious packets.

**B. Modified Hop Count Approach**

The modified hop count approach defends against DDoS attack based on the value stored in the TTL field. The algorithm first initializes a counter to one and for the number of malicious packets found it extracts the final and initial time to live value for every packet and computes the hop count value from the extracted value. If the computed hop count of the packet is not equal to the retrieved hop count then the packets are considered as malicious and discarded, otherwise packets are considered legitimate.

| Initialize count=1 |
| Tf= final value of TTL |
| Ti= Initial value of TTL |
| Hs= Stored hop count |
| Let H= Tf-Ti |
for count= 1 to n
Begin
If(H!=Hc)
Discard the packet
Else
Allow the packet
End if
End

Fig 1 Modified Hop Count Algorithm

IV. Simulation Study

A. Simulation Setup

Simulations are carried out to evaluate the performance of the proposed approach. NS2 is used a simulation environment consisting of 60 mobile nodes. The nodes move randomly at an average speed m/s. Simulation time is 100secs. The routing protocol utilized is AODV that integrates the proposed mitigation technique. Table 1 shows parameters considered for simulation.

<table>
<thead>
<tr>
<th>Simulation Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Area</td>
</tr>
<tr>
<td>Routing Protocol</td>
</tr>
<tr>
<td>No. of Mobile Nodes</td>
</tr>
<tr>
<td>Network Topology</td>
</tr>
<tr>
<td>IEEE Standard</td>
</tr>
<tr>
<td>Broadcasting Range</td>
</tr>
<tr>
<td>Application Type</td>
</tr>
<tr>
<td>Application rate</td>
</tr>
<tr>
<td>Simulation Time</td>
</tr>
<tr>
<td>Data Transfer Protocol</td>
</tr>
<tr>
<td>Connection Type</td>
</tr>
</tbody>
</table>

Table 1 Simulation Parameters

Here, three nodes 5, 9, 15 send malicious traffic at the same time. Then node 25 send malicious traffic after 60 secs. The destination node for the entire traffic is node 6.

B. Performance Analysis

The proposed approach is evaluated in terms of the performance metrics: delay and drop rate. Fig 2 shows the delay in case of the proposed mitigation strategy. It is shown that the delay is low when compared to that of the normal AODV protocol. Fig 3 shows the drop ratio of the proposed approach. It is shown that only minimum packets are dropped in case of the proposed approach. In conventional AODV when the number of malicious node increases more number of legitimate packets is dropped.

Fig 2 Average Delay
V. Conclusion

MANET is an infrastructure less network because of its potential to operate without the help of fixed infrastructure. These networks are more vulnerable than wired counterpart and security plays a major role because of lack of limited resources and trusted centralized authority. The key security risk is a Distributed Denial of Service (DDoS) attack. It is hard to identify and control the DDoS attack because of large scale and complex system environments. In this paper, an analytical technique that utilizes Reactive Defense Mechanism to mitigate the DDoS attack has been proposed. Simulations are carried to evaluate the performance of the proposed approach and the results shows that this approach enhances network performance in terms of low delay and less packet drop.

References


