Prevention against DDOS in MANET Using IDS

Prof.AnkushPawar[1], Ms. Kshama Dwivedi[2]

[1] Head of Department (Computer Engineering), DRIEMS, Neral [MH], India

[2] Pursuing Master of Engineering in Computer Science, ARIET, Asangaon [MH], India

ABSTRACT

A MANET is a type of ad hoc network that can change locations and configure itself on the fly.Since the nodes are mobile, the network topology may change rapidly and unpredictably over time.The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. Since there is no centralized control, these nodes are prone to various attacks on network. Our main focus is expanding the effect of Distributed Denial of Service (DDoS) in routing packets, packet loss rate, end to end delay. Emphasizing on these factors we formulate a solution to figurea secure IDS to detect this attack and block it.

Keywords:- Intrusion Detection System, MANET, DDOS.

1.INTRODUCTION

Mobile Ad hoc Network (MANET), are infrastructure-less network comprising of an autonomous collection of mobile routers connected by wireless medium. These networks have dynamic and constantly varying topology. Nodes can join and leave the network any time and the links are created and broken dynamically. The distinctive attributes of MANET has made it useful for a large number of applications. These applications include various types of commercial (intelligent transportation system, ad hoc gaming, smart agriculture) and non-commercial applications (military applications, disaster recovery, wild life monitoring) etc. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoSattack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack targets a server or process at the victim making it unable to legitimate requests for service. Any amount of resources can be exhausted with a sufficiently strong attack. The only viable approach is to design defence mechanism that will detect the attack and respond to it by dropping the excess traffic. To solve the security issues there is a need of an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection and anomaly-based intrusion detection. In Signature-based intrusion detection there are some previously detected pattern or signature are stored into the database of the IDS. If any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory. To solve this problem anomaly based IDS is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network

2.RELATED WORK

The ad hoc networks have inherent vulnerabilities that are not easily preventable.Intrusion prevention measures, such as encryption and authentication, are required toprotect network operation. But these measures cannot defend compromised nodes, which carry their private keys. Intrusion detection presents a second wall of defense.It is a necessity in the ad hoc networks to find compromised nodes promptly and takecorresponding actions to against. A distributed and cooperative architecture for betterintrusion detection was proposed in [3]. Based on the proposed architecture, astatistical anomaly detection approach is used. The detection is done locally in eachnode and possibly through cooperation with all nodes in the network. But how todefine the anomaly models based on which trace data is still a main challenge. Wei-Shen Lai et al [4] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuz1 et al [5] have proposed a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms such as swarm intelligent technique. Giriraj Chauhan and Sukumar Nandi [6] proposed a QoS aware on demand routing protocol that uses signal stability as the routing criteria along with other QoS metrics. Xiapu Luo et al [7] have presented the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP. The security solution should protect each node in the network and the security of the entire networks relies on the collective protection of all the nodes. The security solution should not be for a single layer in the network. Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim [10] proposed DDoS flooding attack detection through a step-by-step investigation scheme in which they use entropy-based detection mechanism against DDoS attacks in order to guarantee the transmission of normal traffic and prevent theflood of abnormal traffic. Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu [11] proposed a Confidence-Based Filtering method (CBF) to detect DDoS attack in cloud computing environment. In which anomaly detection is used and normal profile of network is formed at non attack period and CBF is used to detect the attacker at attack period.

3.CLASSIFICATION OF ATTACK

The attacks in MANET can roughly be classified into two major categories, namelypassive attacks and active attacks. A passiveattack obtains data exchanged in the network without disrupting the operation ofthe communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET.Table 1 shows the general taxonomy of security attacks against MANET. Examplesof passive attacks are eavesdropping, traffic analysis, and traffic monitoring.Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.The attacks can also be classified into two categories, namely external attacksand internal attacks, according the domain of the attacks. External attacks are carried out by nodes that donot belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severewhen compared with outside attacks since the insider knows valuable and secretinformation, and possesses privileged access rights.Attacks can also be classified according to network protocol stacks. Some security attacks use stealth, whereby the attackers try to hide theiractions from either an individual who is monitoring the system or an intrusiondetection system (IDS). But other attacks such as DoS cannot be made stealth.

Table 1 : General taxonomy of security attacks

Active Attacks	Jamming, Spoofing, Modification, Replaying, DOS
Passive Attacks	Eavesdropping, Traffic Analysis, Monitoring

Denial of Service (DOS) and Distributed Denial of service (DDOS) being more focused in this paper, they are described below:

Denial of Service

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

Distributed Denial of Service

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

4.ATTACK DETECTION

DDOS attack is the main problem in all ad hoc scenarios as well as in wireless sensor networks. IDS uses two intrusion detection parameters, packet reception rate (PRR) and inter arrival time (IAT). But only these two parameters are not completely sufficient for intrusion detection in wireless sensor network and as well as in MANET. If we also add other parameters into it to make it works more accurately. So we use additional intrusion detection parameters.We have considered that mobile ad hoc network contains 9 mobile devices that are communicate from each other through intermediate nodes, each node contain routing table.

Normal Case

We set number of sender and receiver nodes and transport layer mechanism as TCP and UDP with routing protocol as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the result through our simulator.

Attack Case

In Attack module we create one node as attacker node whose set the some parameter like scan port , scan time , infection rate , and infection parameter , attacker node send probing packet to all other neighbour node whose belongs to in radio range, if any node as week node with nearby or in the radio range on attacker node agree with communication through attacker node, so that probing packet receive by the attack node and infect through infection, after infection this infected node launch the DDOS (distributed denial of service) attack and infect to next other node that case our overall network has been infected.

IDS Case-I

In this case of IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behaviour comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack.

IDS Case-II

In our simulation result we performed some analysis in terms of routing load, UDP analysis, TCP congestion window, Throughput Analysis and overall summary. It includes the detection of following attacks:

Fraggle Attack

A Fraggle Attack is a denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router’s broadcast address within a network. It is very similar to a Smurf Attack, which uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal. In a fraggle attack, a spoofed broadcast packet is sent to port 19. The spoofed address is the address of the victim. Since it is broadcast, it goes to every system on the network. If port 19 is open and the character generator service is running on these systems, they will send a stream of characters to the victim.

Smurf Attack

A smurf attack uses Internet Control Management Protocol (ICMP) to send a broadcast ping with a spoofed source address. It’s easier to understand this by looking at one step at a time.

- Normal ping. A regular ping sends one or more ICMP echo requests to a system and the system responds with one or more ICMP echo replies. This provides verification the remote system is operational. A regular ping uses unicast. In other words, the ICMP packet is addressed to one system from one system.
- Broadcast ping. A broadcast ping is not normal. It sends the ICMP echo request to a broadcast address sending it to virtually all systems on the network. Each system will then respond to the system that sent it flooding this system with ICMP echo replies.
- Spoofed source broadcast ping. The smurf attack spoofs the source address with the address of the victim, and then sends it out as a broadcast ping. Each system on the network will then respond, and flood the victim with echo replies.

SYN Flood Attack

SYN flooding is an attack vector for conducting a denial-of-service (DoS) attack on a computer server.The attack involves having a client repeatedlysend SYN (synchronization) packets to every port on a server, using fake IP addresses. When an attack begins, the server sees the equivalent of multiple attempts to establish communications. The server responds to each attempt with a SYN/ACK (synchronization acknowledged) packetfrom each open port, and with a RST (reset) packet from each closed port.

5.ALGORITHM

```
Create node =ids;
Set routing = AODV;
If ((node in radio range) && (next hop! =Null)
{
Capture load (all_node)
Create normal_profile (rreq, rrep, tsend, trecv, tdrop)
{
pkt_type; // AODV, TCP, CBR, UDP
Time;
Tsend, trecv, tdrop, rrep, rreq
}
```

```
Threshold_parameter ()
If ((load<=max_limit) &&
(new_profile<=max_threshold) &&
(new_profile>=min_threshold))
{
No any attack;
}
Else
{
Attack in network;
Find_attack_info ();
}
Else
{
“Node out of range or destination unreachable”
}
Find_attack_info ()
{
Compare normal_profile into each trace value
If (normal_profile! = new trace_value)
{
Check pkt_type;
Count unknown pkt_type;
Arrival time;
Sender_node;
Receiver_node;
Block_Sender_node(); //sender node as attacker
}
```

This algorithm creates an IDS node in which we set AODV as a routing protocol. Then after the creation, our IDS node check the network configuration and capture lode by finding that if any node is in its radio range and also the next hop is not null, then capture all the information of nodes. Else nodes are out of range or destination unreachable. With the help of this information IDS node creates a normal profile which contains information like type of packet, in our case (protocol is AODV, pkt type TCP, UDP, CBR), time of packet send and receive and threshold. After creating normal profile and threshold checking is done in the network i.e. if network load is smaller than or equal to maximum limit and new profile is smaller than or equal to maximum threshold and new profile is greater than or equal to minimum threshold then there is no any kind of attack present.

6.PERFORMANCE EVALUATION

In this section, we present results of our experiment by using NS-2 simulator for an Ad Hocnetwork consisting of 9 nodes. We assume that there is one intruder sending a sequence ofconsecutive packets constituting an attack to the destination. The intrusion isconsidered detected if the attack packets pass through any of the nodes that constitute theintrusion detection system.We use a randomly selected set of 9 nodes and considera packet as constituting the attack signature. Wefound the accuracy of detection. Performance Metrics: In our simulations we use several performance metrics to compare the proposed AODV protocol with the existing one. The following metrics were considered for the comparison were

a) Throughput: Number of packets sends in per unit of time.

b) Normalized routing load: Measured as the number of routing packets transmitted for each data packet delivered at the destination.

c) Throughput: Number of packets sends in per unit of time.

d) End to End delay: - Measure as the average end to end latency of data packets.

e) Packet delivery fraction (pdf): The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.

1. UDP Packet Analysis.

In UDP packet analysis we observe that the packet loss is more in the time of attack. But after applying IDS again the number of packets delivery increases. At the time of attack number of UDP packet received is near about 24 but at the time of normal and IDS time it is 37, 35 respectively.

2. UDP Packet loss Analysis

At the normal time UDP packet loss is near about negligible and at the time of attack it goes very high, where at the time of IDS it only goes to 2 packets.

3. TCP Packet Analysis

After applying IDS the packet loss is minimizes and packet delivery increases. At normal time receiving of TCP packet is near about 34 packet and at IDS time it goes to near about 27 packets but at the time of attack it goes very low i.e. 2 packets.

4. Throughput Analysis

At the time of attack throughput decreases due to congestion in network. This graph represents after applying IDS throughput increases. At the normal time and at IDS time throughput is near about 107 and 85 respectively. But at attack time it goes down near about 50.

5. Routing load Analysis.

In case of attack it is very high this is the main reason of congestion occurs in the network. After applying IDS routing load is in under control. At normal and IDS time routing load is approximately negligible but at the time of attack it goes to near about 15000 packets.

7.CONCLUSION

With sufficient run time andfully random mobility, the algorithm results are close and show the commonperformance of the proposed prevention system. When the normal operation network isunder DDoS data flooding attacks, the network resources and functionalities aretremendously impacted and damaged. The proposed IDS may effectivelydetour and filter the network traffic at the guard nodes.

REFERENCES

[1] F. Anjum, D. Subhadrabandhu and S. Sarkar.Signaturebased intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[2] D. E. Denning, An Intrusion Detection Model," IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222- 232, USA, 1987.

[3] Yongguang Zhang, Wenke Lee. Intrusion Detection in Wireless Ad-Hoc Networks. Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11 Aug. 2000.

[4] Wei-Shen Lai, Chu-HsingLin , Jung-Chun Liu ,Hsun-Chi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)

[5] ShabanaMehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008)

[6] GirirajChauhan,Sukumar Nandi: QoS Aware Stable path Routing (QASR) Protocol for MANETs, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).

[7] Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009)

[8] Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game theoretic Approach, in Proceedings of the 2nd ACM symposium on Information, computer and communication security, pp 365-367 (2006)

[9] S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312.

[10] Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim "DDoS flooding attack detection through a step-by-step investigation" 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications, ISBN: 978-1-4673-0495-5,2011

[11] Qi Chen ,Wenmin Lin , Wanchun Dou , Shui Yu " CBF: A Packet Filtering Method for DDoS Attack Defence in Cloud Environment", 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. ISBN:978-0-7695-4612-4.2011