A SECURE INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORK

M.Vallinayagam¹ S.Sasikala ²
¹Research Scholar of Computer Science, Sree Saraswathi Thyagaraja College
Pollachi – 642 107, Coimbatore, Tamil Nadu, India

²Head of UG Computer Science, Sree Saraswathi Thyagaraja College
Pollachi – 642 107, Coimbatore, Tamil Nadu, India

Abstract— Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance, MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc also contains wireless sensor network so the problems is facing by sensor network is also faced by MANET. While developing the sensor nodes in unattended environment increases the chances of various attacks. The Intrusion Detection is one of the possible ways in recognizing a possible attacks before the system could be penetrated. The encryption and authentication solution, which are considered as the first line of defense, are no longer sufficient to protect MANETs. Therefore, Intrusion Detection Systems (IDSs) is needed to be the second line of defense to protect the network from security problem. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. “A Secure Intrusion Detection System against DDoS attack in MANET” in this project discussed on the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this paper we discussed some attacks on MANET and DDoS also and provide the security against the DDoS attack.

Keywords— Put your keywords here, keywords are separated by comma.

1. INTRUDCTION

1.1 Intrusion Detection

As defined by Heady et al., an intrusion is any set of actions that attempt to comprise the integrity, confidentiality or availability of a resource. Intrusion leads to violations of the security policies of a computer system, such as unauthorized access to private information, malicious break-in into a computer system, or rendering a system unreliable or unusable.

The focus of this thesis is on the intrusion detection subsystem, which constitutes the first line of defense for a computer network system. There are a number of approaches in this field. Most of them fall into three primary categories: anomaly detection, misuse detection and hybrid schemes.

The anomaly detection approach is based on a model of normal activities in the system. This model can either be predefined or established through techniques such as machine learning. Once there is a significant deviation from this model, an anomaly will be reported. By contrast, a misuse detection approach defines specific user actions that constitute a misuse and uses rules for encoding and detecting known intrusions. The hybrid detection approach uses a combination of anomaly and misuse detection techniques.

Mobile ad hoc network (MANET) is a group of two or more devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other. As we know that there is no any centralized system so routing is done by node itself. Due to its mobility and self-routing capability nature, there are many weaknesses in its security. To solve the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection [1] and anomaly-based intrusion detection.

In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base 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[2] 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.

One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack 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 huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

1.2 DENIAL-OF-SERVICE

DoS (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. These are the nastiest, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service.

The premise of a DoS attack is simple: send more requests to the machine than it can handle. There are toolkits available in the underground community that make this a simple matter of running a program and telling it which host to blast with requests. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests (hits on the web site running there, for example).

2. RELATED WORK

The new DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV & DSR. Wei-Shen Lai et al [3] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuzul et al [4] 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 [5] 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 [6] have presented the important problem of detecting pulsing denial of service (PDos) attacks which send a sequence of attack pulses to reduce TCP throughput. Xiaoxin Wu et al [7] proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification Ping. S.A.Arunmozhi and Y.Venkataraiman [8] proposed a defense scheme for DDoS attack in which they use MAC layer information like frequency of RTD/CTS packet, sensing a busy channel and number of RTS/DATA retransmission. Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim [9] 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 the flood of abnormal traffic. Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu [10] 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.

Mobile ad hoc network has a tremendous popularity in the domain of networking. A mobile ad hoc network (MANET) is a collection of mobile hosts. It can be rapidly deployed as a multi hop packet radio network without the aid of any existing network infrastructure or centralized administration. Nodes within each other's radio range communicate directly via wireless links. The applications of MANET range from a one-off meeting network to emergency operations such as disaster recovery to military applications due to their easy deployment. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. MANET does not have any concentration points where IDS can collect audit data for the entire traffic monitoring process in network. The wireless links between nodes are highly susceptible to link attacks, which include passive eavesdropping, active interfering, and leakage of secret information, data tampering, impersonation, message replay, message distortion, and denial of service. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, inject erroneous messages, modify messages, and impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Every node in the MANET must be prepared for encounter with the adversary [21].

Due to the nature of mobility for mobile networks needs additional mechanism for providing security. These vulnerabilities do not exist in a fixed wired network. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. So there is need to develop new architecture and mechanisms to protect the wire-less networks and mobile computing applications.

Intrusion detection is an important part of computer security. It provides an additional layer of defense against computer is use after physical, authentication and access control. Generally, there are two intrusion detection techniques: misuse based detection and anomaly based detection. Misuse based detection exploits the signatures of known attacks whereas anomaly based techniques allow detection of unknown attacks by measuring deviations from a normal behavior.

Due to vulnerabilities introduced by mobility, anomaly based detection techniques are more crucial in mobile networks than misuse based detection techniques.
However, designing them is challenging because normal profiles are usually very hard to build and maintain due to the mobility of nodes. It is generally acknowledged that the main limitation of an anomaly based detection technique is that it generates a higher false positive rate than the misuse based detection technique. Therefore, establishing and maintaining normal profiles for nodes and improving the detection performance are crucial in designing an efficient anomaly detection algorithm in mobile networks [21].

2.1. NEED OF INTRUSION DETECTION SYSTEM

The nature of mobility creates new vulnerabilities due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management points and up till now many of the proven security measures turn out to be ineffective. So there are needs more security mechanisms in mobile ad hoc network. The wireless channel is accessible to both legitimate network users and malicious attackers. Attackers may intrude into the network through the subverted nodes. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network. Despite such dynamics, mobile users may request for anytime, anywhere security services as they move from one place to another.

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. The security solution should protect the network from both the inside and outside intruders into the system.

The security solution should encompass all three components of prevention, detection, and reaction that work in concert to guard the system from collapse. The security solution should be practical and inexpensive in a highly dynamic and resource constrained networking scenario. However an attacker succeeds in infiltrating the security system and causes them to misbehave. Node misbehaviour can result in degradation of network performance. Therefore there is need of intrusion detection system for monitoring the anomalies and take necessary actions if an anomaly is detected. In the next session different types of attack in MANET are discussed.

2.2 TYPES OF ATTACKS IN MANET

There are various types of attacks based on behavior of nodes in mobile ad hoc network are classified as follows:

- Unfair use of transmission channel
- Anomalies in packet forwarding

2.2.1 Unfair Use of Transmission Channel or Misbehavior

In this attack a node can prevent other in its neighborhood from getting fair share of the transmission channel. This misbehavior can be considered as DoS attacks against the competing neighbors in a contention-based network since the competing neighbors are deprived of their fair share of the transmission channel. Some of the possible methods for unfair use of the transmission channel are ignoring the MAC protocol, jamming the transmission channel with garbage, ignoring bandwidth reservation scheme, malicious flooding, and network partition.

2.2.2 Anomalies in Packet Forwarding

In this attack anomalies in packet are forwarded such as packet dropping, delay packet transmissions, wormhole, routing loop, DoS, fabricated route messages, rushing, spoofing. Any type of attacks which may be either unfair use of transmission channel or misbehavior, anomalies in packet forwarding, it must be detected. So the next session focuses on intrusion detection techniques in MANET.

2.3 ATTACK ON AD HOC NETWORK

There are various types of attacks on ad hoc network which are describing following:

2.3.1 Wormhole

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [11]. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunnelled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet shortages.

2.3.2 Blackmail

This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [12]. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated [13].

2.3.3 Routing Table Poisoning

Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [14]. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

2.3.4 Replay

A replay attack is performed when attacker listening the conversation or transaction between two nodes and put important message like password or authentication message from conversation and use this in future to make attack on the legitimate user pretending as real sender.

2.3.5 Location Disclosure

Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [15] or with simpler probing and
monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

2.3.6 Black Hole

In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination [16]. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

2.3.7 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 [14]. 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.

2.3.8 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.

2.3.9 Rushing Attack

Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols [17]. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

2.3.10 Masquerade

It is an intruder who gain the privilege of any one system as an authenticate user by stolen user password, through finding security gaps in programs, or through bypassing the authentication mechanism.

2.3.11 Passive Listening and traffic analysis

The intruder could passively gather exposed routing information. Such an attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol.

2.4 INTRUSION DETECTION TECHNIQUES IN MANET

According to the detecting attack intrusion detection system is classified into two types:

- Misuse or signature based intrusion detection
- Anomaly based intrusion detection

2.4.1 Misuse or Signature Based Intrusion Detection

In Misuse detection searches for the traces or patterns of well-known attacks which are stored as signatures. These signatures are provided by human expert based on their extensive knowledge of intrusion techniques. In this process if a pattern matched is found, this signals an event for which an alarm raised. After that security analyst evaluate the alarms to decide what action to take for e.g. shutting down part of the system, alerting the relevant internet service provider of suspicious traffic, or simply nothing unusual traffic for future reference. In misuse intrusion detection system only known attacks are detected.

2.4.2 Anomaly Based Intrusion Detection

In Anomaly detection uses a model of normal user or system behaviour and flags significant deviations from this model as potentially malicious. In anomaly detection novel attacks are detected. Designing the anomaly detection is difficult because normal profiles are usually hard to build and maintain due to mobility of nodes [21].

PROBLEM STATEMENT

DDOS attack is the main problem in all ad hoc scenario i.e. in MANAT and as well as in wireless sensor networks. In the Paper with reference no. [18] Has an intrusion detection system in wireless sensor network which uses the anomaly intrusion detection system in which 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 in our proposal we use different intrusion detection parameters in mobile Ad hoc networks. We assume that a mobile ad hoc network contains two or more than two mobile devices that are communicate from each other through intermediate nodes, each node contain routing table, in our proposal we use AODV routing protocol in all normal module attack module and IDS (intrusion detection system) for prevention through attack. In this paper we simulate the three different condition results normal time, Attack time and IDS module time through NS-2 simulator.

3. METHODOLOGY

CRITERIA FOR ATTACK DETECTION

Here we use thirteen mobile nodes and simulate through three different criteria NORMAL case, DDOS attack case and after IDS intrusion detection case.

3.1 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.

3.2 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 neighbor 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.

3.3 IDS Case

In IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behavior 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. In our simulation result we performed some analysis in terms of routing load, UDP analysis, TCP congestion window, Throughput Analysis and overall summery.

In our algorithm firstly we create 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. Else there is an attack in the network and find the attack. For doing it compare normal profile with each new trace value i.e. check packet type, count unknown packet type, arrival time of packet, sender of packet, receiver of packet. And after detection of any anomaly in that parameters then block that packet sender node (attacker node).

4. SIMULATION ENVIROMENT

The simulation is implemented in Network Simulator 2.31[19], a simulator for mobile ad hoc networks. The simulation parameters are provided in Table 1. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen 35 m/s. A packet size of 512 bytes and a transmission rate of 4 packets/s.

- Performance Metrics: In our simulations we use several performance metrics to compare the proposed AODV protocol with the existing one [20]. The following metrics were considered for the comparison were
  - a) Throughput: Number of packets sends in per unit of time.
  - b) 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.
  - c) End to End delay: - Measure as the average end to end latency of data packets.
  - d) Normalized routing load: Measured as the number of routing packets transmitted for each data packet delivered at the destination.

### TABLE 1 Simulation Parameters for Case Study

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Examined Protocol</th>
<th>AODV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Dimension of simulated area</td>
<td>800x600</td>
<td></td>
</tr>
<tr>
<td>Simulation time (sec)</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Radio range</td>
<td>250m</td>
<td></td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR, 3pkts/</td>
<td></td>
</tr>
<tr>
<td>Packet size (bytes)</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>Number of traffic connections</td>
<td>TCP/UDP</td>
<td></td>
</tr>
<tr>
<td>Maximum Speed (m/s)</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Node movement</td>
<td>random</td>
<td></td>
</tr>
<tr>
<td>Types of attack</td>
<td>DDOS</td>
<td></td>
</tr>
</tbody>
</table>

5. RESULTS AND DISCUSSION

### TABLE II Overall summary of Results in Cases

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Normal Case</th>
<th>Attack Case</th>
<th>IDS Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEND</td>
<td>828</td>
<td>533</td>
<td>844</td>
</tr>
<tr>
<td>RECEIVE</td>
<td>804</td>
<td>482</td>
<td>812</td>
</tr>
<tr>
<td>ROUTING PACKETS</td>
<td>99</td>
<td>219882</td>
<td>174</td>
</tr>
<tr>
<td>PACKET DELIVERY FRACTION</td>
<td>97.1</td>
<td>90.43</td>
<td>96.21</td>
</tr>
<tr>
<td>THROUGHPUT</td>
<td>107.815</td>
<td>58.13</td>
<td>87.57</td>
</tr>
<tr>
<td>NORMAL ROUTING LOAD</td>
<td>0.12</td>
<td>456.19</td>
<td>0.21</td>
</tr>
<tr>
<td>AVERAGE ENE TO END DELAY</td>
<td>852.04</td>
<td>751.64</td>
<td>830.31</td>
</tr>
<tr>
<td>No. Of dropped data(packet)</td>
<td>23</td>
<td>51</td>
<td>29</td>
</tr>
<tr>
<td>No. Of dropped data(bytes)</td>
<td>23852</td>
<td>44556</td>
<td>28628</td>
</tr>
</tbody>
</table>

According to performance analysis in normal case, in attack case and in IDS case we observe that DDOS attack definitely affected the network and our scheme is successfully defend the network and also provides the protection against them. In case of attack we observe that the routing load is very high because attacker node are continuously transmit the routing packets to their neighboured and every node in network are reply to attacker node by that heavy congestion is occur. Packet delivery fraction and end to end delay are also goes low, which shows that packets are not deliver accurately and number of dropped data is goes high approximately twice to the normal condition.

6. CONCLUSION AND FUTURE WORK
The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self-organizing nature. The results demonstrate that the presence of a DDoS increases the packet loss in the network considerably. The proposed mechanism protects the network through a self-organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbours. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. We believe that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks. We have also emphasized the need of providing concrete steps towards appliance of proper forensic analysis, with an aim to more efficiently discourage all future attacks. Besides, it is explicitly pointed out to the need of maintaining node anonymity, protecting privacy of mobility patterns, and integrating adequate mechanisms to applied IDS in way to assure network survivability in the attack occurrences.

REFERENCES