Design Implementation Framework for Intrusion Detection System for Mobile Adhoc Networks

Chilakalapudi Meher Babu¹, Dr. Ashish B. Sasankar²,
¹ASSISTANT PROFESSOR, DEPARTMENT OF CSE, MALINENI LAKSHMAIAH WOMEN’S ENGG COLLEGE, GUNTUR, INDIA
²PROFESSOR., HEAD, DEPT OF MCA, G.H. RAISONI INSTITUTE OF I.T, HARIGANGA CAMPUS, MIDC, NAGPUR, INDIA.

Abstract: The demand for speed in wireless networks is continuously increasing. Recently, most existent protocols, applications and services for mobile Adhoc networks (MANETs) assume a cooperative and friendly network environment and do not accommodate security. Cooperative communication has emerged as a new dimension of diversity to emulate the strategies designed for multiple antenna systems, since a wireless mobile device may not be able to support multiple transmit antennas due to size, cost, or hardware limitations. By exploiting the broadcast nature of the wireless channel, cooperative communication allows single antenna radios to share their antennas to form a virtual antenna array, and offers significant performance enhancements. This promising technique has been considered in the IEEE 802.16j standard, and is expected to be integrated into Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) multi-hop cellular networks.

Keywords: Wireless Sensor networks, Design issues, Routing protocols, Applications

I. INTRODUCTION

In MANETs, intrusion prevention (IPS) and intrusion detection (IDS) techniques need to complement each other to guarantee a highly secure environment, such as encryption and authentication, are more useful in preventing outside attacks. Once the node is compromised, intrusion prevention measures will have little effect in protecting the network. Therefore, an intrusion detection system is serving as the second line of defense in Adhoc network. In this first layer is a local intrusion detection module, which identifies the friends quickly and second layer is a global detection module in which intrusion behavior is checked rigorously before declaring the node as a trusted node or an intruder node. Finally, it adds a voting mechanism to generate the trust level for each node. This proposed model is fast responsive, light weighted and better than the conventional model available in Adhoc network environment. In this well-known security attacks are applied to the mobile Adhoc environment. Statistics are from raw data set, and rule sets are induced for well-known attacks like Denial of Service attack, Black Hole attack and Wormhole attack. Accuracy of the detection engine for Denial of Service (DoS) attack is observed to be 100%. For black hole attack observed accuracy is near to 99%, and for wormhole attack is 100% for given conditions and simulation environment. Observed accuracy of attacks is improved from the available conventional models. A detection engine based on statistics has been designed for Adhoc network environments.

II. STATEMENT OF THE PROBLEM

It is challenging to design an intrusion detection system for mobile Adhoc networks. The lack of pre-defined infrastructures and monitoring points make it difficult to collect data for the entire network. MANET’s should be considered while designing the IDS framework. In MANET it is more difficult to differentiate between false and true positives.

• Here problem can be divided into following sub problems:
• Design framework for monitoring the mobile Adhoc environment.
• To monitor the detection based on the statistical security features.
• MANET intrusion detection systems are to evaluate the performance of the validation.

III. ATTACK MODELS IN MOBILE ADHOC NETWORK

A node can prevent other nodes in the network from getting transparent share of the transmission channel. This activity can be considered as a denial of service (DoS) attack against the neighbors which are participating in a fair competition for allocation of transmission channels in a contention based network.
Design Implementation Framework for Intrusion Detection System for Mobile Adhoc Networks

a. Ignoring the MAC protocol:
Protocols like 802.11 uses request for transmission (RTS) and clear for transmission (CTS) mechanism to notify the neighbors that how long the transmission channel will be reserved by the node for successful transmission. This imposes along delay at the output queues of the nodes and finally packets are timed out and get removed.

b. Jamming the transmission channel with garbage
Garbage can consist of packets of unknown formats, violating the proper sequence of a transaction (e.g. sending a data packet without exchanging RTS and CTS) or simply random bits used as static noise by misbehaving nodes.

c. Ignoring the bandwidth reservation scheme
Nodes in a multi hop wireless network reserve a slot for transmission channel before initiating a flow. If enough bandwidth is not available, a new flow should not be admitted to avoid choking. A misbehaving node may not abide by this rule and try to push out packets when there is not enough bandwidth.

d. Malicious flooding
Deliver unusually large amount of data or control packets to whole network or some targeted nodes. We can distinguish two kinds of flooding attack. First one is the route request (RREQ) flooding attack. It ignores the network limitations for sending RREQ messages and sends a large number of RREQ packets with a maximum time to live (TTL) value addressing nodes that do not exist in the network. The second is called data flooding attack.

IV. PACKET FORWARDING IN ANOMALIES
Anomalies in packet forwarding take the following forms:

a. Packet Drop
A malicious node may disrupt the normal operation of a network by dropping packets. This type of attack can be classified into two types: (a) Black hole attack and (b) Gray hole attack.

b. Blackhole Attack
In blackhole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [6], [10], and [7]. In this way attacker node will always have the availability in replying to the route request and thus attract the whole traffic on the network and intercept the data packet and further it may retain it or drop it.

c. Gray-Hole attack
An attacker selectively drops data packets.

d. Delay in Packet Transmissions
A node can give preference to transmitting its own or friend’s packets by delaying others’ packets. As a result some flows may not be able to meet their end-to-end delay and jitter requirements.

e. Wormhole Attack
A tunnel is created between two nodes that can be utilized to secretly transmit packets. In a MANET, wormhole [7] is a term adopted to describe an attack against the routing protocol in which two cooperating malicious nodes create a tunnel between two points of the network. The attack is possible even if none hosts were compromised and even attacked network introduced a strong authentication and encryption algorithms.

V. PROPOSED N - TIER ARCHITECTURE FOR IDS
We propose a N-tier Architecture for IDS in a MANET that improves the efficiency of existing MANET IDS architectures and is conceptually based on [4], [10] and [5]. The main idea of the system is to provide reliable IDS that can detect any kind of intrusion attempts and at the same time able to reduce the number of false alarms raised by the system. With the focus of improving the detection strategies, only a simple response mechanism is deployed in the system. In global IDS rules are applied to normal intruder detection threshold for rigorous checking before declaring the node as the trusted node.
VI. PERFORMANCE EVALUATION METRICS FOR NETWORK TRAFFIC

[BASED ON 10]

6.1 Throughput:
Throughput is the measure of sent packets through the number of packets delivered to the receiver provides the throughput of the network. The throughput is defined as the total amount of data a receiver actually receives from the sender divided by the time it takes for receiver to get the last packet [10].

\[
\text{Throughput} = \frac{Pr}{Pf}
\]

Where Pr is the total number of Received Packets and Pf is the total number of Forwarded Packets. [11].

<table>
<thead>
<tr>
<th>Pause time (sec)</th>
<th>Throughput (bits/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSR</td>
</tr>
<tr>
<td>0</td>
<td>12472</td>
</tr>
<tr>
<td>10</td>
<td>12769</td>
</tr>
<tr>
<td>20</td>
<td>14261</td>
</tr>
<tr>
<td>30</td>
<td>14841</td>
</tr>
<tr>
<td>40</td>
<td>14203</td>
</tr>
<tr>
<td>100</td>
<td>14641</td>
</tr>
</tbody>
</table>

6.2 Packets Dropped:
Some of the packets generated by the source will get dropped in the network due to high mobility of the nodes, congestion of the network etc.

<table>
<thead>
<tr>
<th>Pause time (sec)</th>
<th>Packets Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSR</td>
</tr>
<tr>
<td>0</td>
<td>2885</td>
</tr>
<tr>
<td>10</td>
<td>2270</td>
</tr>
<tr>
<td>20</td>
<td>720</td>
</tr>
<tr>
<td>30</td>
<td>148</td>
</tr>
<tr>
<td>40</td>
<td>769</td>
</tr>
<tr>
<td>100</td>
<td>386</td>
</tr>
</tbody>
</table>

Packet Loss % = (1-Pr/Ps)*100

Where Pr is total number of Received Packets and Ps is total number of Sent Packets.

6.3 Packet Delivery Ratio:
The ratio of the data packets delivered to the destinations to those generated by the CBR sources. It is the fraction of packets sent by the application that are received by the receivers [6].

<table>
<thead>
<tr>
<th>Pause time (sec)</th>
<th>Packet Delivery Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSR</td>
</tr>
<tr>
<td>0</td>
<td>0.8324</td>
</tr>
<tr>
<td>10</td>
<td>0.84911</td>
</tr>
<tr>
<td>20</td>
<td>0.9533</td>
</tr>
<tr>
<td>30</td>
<td>0.99905</td>
</tr>
<tr>
<td>40</td>
<td>0.94869</td>
</tr>
<tr>
<td>100</td>
<td>0.97698</td>
</tr>
</tbody>
</table>

PDF = (Pr/Ps)*100
It is calculated by dividing the number of packet received by destination through the number packet originated from source. Where Pr is total Packet received & Ps is the total Packet sent.

6.4 Normalized Routing Overhead:
The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission. The routing overhead describes how many routing packets for route discovery and route maintenance need to be sent in order to propagate the data packets [7].

<table>
<thead>
<tr>
<th>Pause Time (sec)</th>
<th>DSR</th>
<th>DSDV</th>
<th>AODV</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2805</td>
<td>4319</td>
<td>2328</td>
</tr>
<tr>
<td>10</td>
<td>2270</td>
<td>4224</td>
<td>1884</td>
</tr>
<tr>
<td>20</td>
<td>720</td>
<td>2206</td>
<td>692</td>
</tr>
<tr>
<td>30</td>
<td>148</td>
<td>1898</td>
<td>594</td>
</tr>
<tr>
<td>40</td>
<td>769</td>
<td>2566</td>
<td>783</td>
</tr>
<tr>
<td>100</td>
<td>386</td>
<td>756</td>
<td>885</td>
</tr>
</tbody>
</table>

6.5 End-to-End Delay:
End-to-End delay indicates how long it took for a packet to travel from the source to the application layer of the destination. [7], i.e. the total time taken by each packet to reach the destination. Average End-to-End delay of data packets includes all possible delays caused by buffering during route discovery, queuing delay at the interface, retransmission delays at the MAC, propagation and transfer times.

6.6 Optimal Path Length:
It is the ratio of total forwarding times (depends on number of hops) to the total number of received packets. Optimal path length increases as the number of hops on optimal path increases.
VII. CONCLUSION

We recap the thesis contributions as follows:

(a) We identified that Incentive based approach is best suited for the mobile Adhoc environment.
(b) The model proposed is incentive based, fast responsive and light weighted which is independent from any central authority and easy to detection for individual nodes.
(c) Incremental approach is used for designing the detection system as soon as any specific attack is identified. It is easy to add additional attacks in the detection engine.
(d) This work is not only based on specific kinds of attack but also all known attacks possible in the network layer for Adhoc environment are investigated including packet drop, false cache poisoning, delay in packet transmissions, routing loop and selfishness.
(e) For the network layer denial of service (DoS) attack, The black hole, The wormhole attacks are investigated. From raw dataset important features are extracted. The accuracy of the detection engine is observed to be 99.20%, and this is better than the detection engines available for DoS attack in Adhoc network.

REFERENCES


AUTHOR PROFILE

Chilakalapudi Meher Babu did his M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh (INDIA) and pursuing Ph.D in R.T.M. Nagpur University, Nagpur (India). He has 9 National and International Journal Publications to his credit. Currently he is working as Assistant Professor in the Department of CSE of Malineni Lakshmi Women’s Engineering College, Guntur, AP (India). His area of interest in research includes Network Intrusion Detection System on Wireless Lan’s, IP Address, Routing Algorithms etc.,

Dr. Ashish B. Sasankar did his M.CA, M.tech (CSE), M.Phil. (Computer Science) & Ph.D in Computer Science from R.T.M. Nagpur University (India). He has a rich experience of 16 years in the field of Education. Currently, he is the Head of the Department of MCA in the most prestigious G.H. Raisoni Institute of Information Technology [GHRIIIT], Nagpur [India]. He is a Ph.D Guide for Computer Science in the Faculty of Science in R.T.M. Nagpur University, Nagpur (India) and guiding many of his research scholars doing their Ph.Ds in Computer Science in R.T.M. Nagpur University, Nagpur. He has 40 National & International Journal Publications to his credit. He is a Member of the IEEE and CSI.