Anticipation of Wormhole Attacks by Selective Routing in Wireless Sensor Networks

D. Nanthiya, Dr. P. Keerthika, S. B. Gopal, V. Karthick, J. Kabish, S. Arish

Abstract: Mobile Ad hoc Network is a type of network, where all the nodes always move dynamically, geographically distributed, autonomous and doesn’t have any infrastructure. Each node in the MANET behaves like router and forwards the packet to other nodes. But this Wireless network is highly prone to attacks like eavesdropping, jamming, black hole, worm hole, gray hole, link spoofing and so on. Among these, the worm hole attack has severe impact against routing protocols of the network. To transfer the data packet from one node to another node, any one of the routing protocols such as DSR, AODV, ZRP and so on can be used. In this paper, the impact of worm hole attack against AODV routing is discussed. A Trust Enhanced Ad hoc On demand Distance Vector Routing protocol is proposed to detect the worm hole nodes and their link in the network. The worm hole attack commonly target to banks, government, private sector, public sectors, etc. The attacked node will be detected by combining Round Trip Time Technique with trust model. After the identification of malicious node, the node will be skipped and another shortest path will be identified by using AODV protocol. The proposed technique provides loop free operation and increased scalability. The proposed algorithm is simulated in network Simulator2 tool.

Index Terms: Wireless network, wormhole attack, Round Trip Time, Promiscuous mode.

1 INTRODUCTION

MANET stands for Mobile Ah Hoc Network. It is a wireless network and consists of mobile nodes. The mobile nodes doesn’t have any infrastructure. The characteristics of MANET are dynamic topology, bandwidth constrained variable capacity links, autonomous behavior, and energy constrained operation, limited security, less human intervention. Each node in the network behaves as router because they forward the received packets to the destined node. In this network, the nodes does not know the topology of their network. They have to discover by themselves. If any new node arrives, it must publicize itself into the network. It must also listen to similar other announcements given by other nodes. Since the nodes were unaware about the topology, the routing protocol helps to find the routes between the nodes. The information will be broadcasted on that route. So many routing protocols are exist in existence. They are broadly classified into 3 categories namely proactive routing protocol, reactive routing protocol and hybrid routing protocol.

Proactive routing protocol: It is also named as table driven routing protocol because each node has a routing table that contains the information of the routes to reach remaining destination nodes. Since the environment is dynamic nature, the routing table has to be updated periodically. This periodic update incurs additional overhead to the network. Some of the proactive routing protocols are DSDV, GSR, OLSR, Babel, and WRP. The major disadvantage is it is unfit for large networks. Because the entries in the routing table becomes large and tedious to maintain and update it.

Reactive routing protocol: It is also called as on demand routing protocol. This protocol maintains the routing table only on demand. It involves 2 phases namely route discovery and route maintenance. If any node wants to send any data packet then it checks its cache for the availability of route to reach the destination node. If route exists then it reuses the same route else it initiates the route discovery process. In route maintenance phase, the link failures can be predicted. It uses acknowledgement mechanism for route maintenance. Examples of this protocol are AODV, DSR, ABR and SSA.

Hybrid routing protocol is the combination of both reactive and proactive routing protocol. It tries to overcome the shortcomings of the reactive and proactive routing protocol. It incorporates the route discovery process of reactive protocol and routing table maintenance from proactive routing table. This helps to route the packets in larger networks. Examples of hybrid routing protocol are ZRP, SHARP and soon.

Fig. 1 MANET environment

The network suffers from many attacks such as black hole attack, worm hole attack, black mail, traffic analyze attack and so on. Among these attacks, the worm hole attack has serious impact over network performance. In the work hole attack, some nodes will be malicious and may present
sparsely. These malicious nodes have secret tunnel between them. Using this tunnel

2 RELATED WORK

Ankita et al.[2] has present an approach about Wormhole and Black hole attack on AODV Routing protocol in MANET. In this paper they analysed the basic characteristics of Black hole attack and Wormhole attack in the wireless decentralized network. In this network the nodes can communicate on the basis of mutual trust. Parag Kumar Guha Thakurta et al.[3] proposed an approach for detecting Wormhole attacks in AODV Routing protocol. In this paper, they proposed a two phase. The Wormhole link detection procedure in AODV Routing protocol identified the malicious link for avoiding unsecure packet transfer. They considered Round Trip Time and Round Trip Bit transfer of each node to identify the malicious link. Tao Yang et al.[6] proposed an approach for a secure Routing in wireless sensor networks based on trust evaluation model. In this paper they proposed an Energy Optimized Secure routing(EOSR) based on distributed trust evaluation model to identify the malicious node. They not only ensures the data is passing through the trusted nodes, but also balances the energy consumption among the trusted nodes. Neeraj Arya et al.[4] proposed a technique for detecting and avoiding wormhole attack and collaborative Blackhole attack on MANET using Trusted AODV routing algorithm. In this paper they categorize about wormhole attack and collaborative Blackhole attack and also proposed a trust based mechanism to detect and avoid these attacks.

3 SYSTEM MODEL

3.1 AODV working principle

The AODV is an ondemand protocol. It expects every node to maintain information about other nodes only when the communication. It has 2 major phases. The first phase is Route Discovery and second phase is route discovery phase. Route Discovery

In this phase, if the route is not available with the source node to reach destination, then the source node broadcasts route request packet (RREQ) to its neighbors. The neighbors checks if it is the destination node. If it is not the destination node, then it again broadcasts to its neighbors. The broadcasting continues until the destination is reached. The destination node at once after receiving the RREQ packet replies with RREP packet. The RREP packet is forwarded to the source in the reverse path. At sometimes some intermediate node may contain route to reach destination. In such cases the intermediate itself send the route reply packet RREP to the source in reverse path.

Route Request

Rupinder Sing et al.[8] proposed an approach an Hybrid technique for detection of Wormhole attack in Wireless sensor network. In this paper they examined about to detecting the wormhole attack .they use watchdog and Delphi schemes for detection. The special feature of this technique is that it can defend against all the categories of Wormhole attack without depending on any required hardware like global positioning system, etc. Hiteshwer et al.[1] present an approach for Network Security attacks in Ad-hoc wireless networks. In this paper they investigated about Wormhole attack and they present a general mechanism called packet leashes for detecting and defending against wormhole attacks and also they have proposed a protocol named TIK which is used to implement leashes.

the attacked node based on Round trip time variation technique. R.Arun Prakesh et al.[23] proposed an approach for detection, prevention and mitigation of Wormhole attack in wireless Ad-hoc network by coordinator. In this paper they detect to prevent and mitigate the wormhole attack by selecting a coordinator by wireless election algorithm.
The next node B receives the packet and it broadcasts to the other nearest nodes i.e. to node C. Node C updates its values in the routing table for every broadcast the routing table will be updated. Finally, the Request packet received by the Destination node E and it starts preparing the reply packet to its valid link.

**Route Reply**

<table>
<thead>
<tr>
<th>Destadd</th>
<th>Nexthop</th>
<th>Seqno</th>
<th>Hopcount</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>D</td>
<td>120</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>E</td>
<td>E</td>
<td>120</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>E</td>
<td>C</td>
<td>120</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td>E</td>
<td>B</td>
<td>120</td>
<td>4</td>
<td>-</td>
</tr>
</tbody>
</table>

Node E unicasts the reply packet to node D with its packet format Source address, destination address, Hop count, Lifetime.

Node D updates its routing table and send the message to Node C.

After receiving the message, the Node C updates its routing table and transfers the message to the next Node B.

Node B receives the message and finally the message will send to the Source Node A.

Finally, the link will be created to transfer the packets.

**Route Maintenance**

Generally the route maintenance is done with the help of RERR Route Error message packets. An active path is a path selected by source to transfer data to the destination. Since the nodes in the MANET are in moving state, the link and nodes in the active state may suffer from link failures. The RERR is initiated by the node which is upstream closer to source node. It lists all the nodes affected by the link failure. On receiving the RERR packet, every nodes updates this information as invalid for the route to reach destination.

The source node reinitiates the route discovery process to find the new route.

A path is established between A-B-C-D-E. But the link between d and E gets failed. Node D now updates this information in its routing table. Then it creates a RERR packet and lists all the destination that are unreachable to destination. Now node D forwards upstream i.e., to C first then to B and finally then to the source A. The nodes C and B invalids the route to D in its routing table. The source node also invalidates the path to D and then reinitiates the resource discovery process.

**3.2 RTT**

Round Trip Time Technique

The formula used for calculating the Round Trip Time (RTT) for a particular node.[3] It will be calculated with the time of Route request (RREQ) and Route reply (RREP). It will be calculated as

\[
RTT_{N1} = Y - X - RTT_{previous}
\]

Where

- \(X\) – Route request time
- \(Y\) – Route response time

RTT previous - Round Trip Time of the previous node

This formula is used to calculate the Round Trip Bit Transfer (RTBT) which is the parameter of a node while wormhole link is detected. Though it was calculated by the following formula

\[
RTBT\text{ of a node} = RREQ\text{ packet bytes} + RREP\text{ packet bytes}
\]

Where, \(RREQ\) packet bytes and \(RREP\) packet bytes are the size of the packets.

The \(RTBTTH\) which is the threshold value for the Round Trip Bit Transfer which will be obtained as following

\[
RTBTTH = max\ (RTBTTH)
\]

**3.3 Trust**

For each node in the network, the promiscuous mode is enabled. This node makes every node to monitor the activities of its neighbor. This mode can be used to predict the trust value of a node. The trust value is calculated based on the successful proper forwarding of packets. The threshold value for trust is maintained. If the trust value reached its threshold, then this information is broadcasted among remaining nodes.

**4 PROPOSED APPROACH**

Algorithm: Phase 1

1. From the source, broadcast the Route Request packet (RREQ) to the neighboring nodes and check
whether the node is destination otherwise node will broadcast the packet.
2. When the request packet reached the destination it will send the Route Reply packet (RREP) with the shortest path to the source.
3. Finally the route will be created with that shortest path.

**Algorithm: Phase-2**

1. Initialize the variable tot and store the size of both RREQ and RREP packets.
2. Set a variable named previous_rtt and initialize as 0.
3. Count the number of nodes in the selected path.
4. Starting from the source to destination node the Round Trip time(RTT) and Round Trip Bit transfer time(RTBT) will be calculated
   i. RTT = time of a node getting a RREP packet – time of a node getting a RREQ packet – Previous RTT value.
   ii. RTBT = tot / RTT
   iii. Previous_rtt = RTT
5. Calculate the threshold value RTBT
6. If RTBT < RTBT TH then the link is wormhole attacked
   Else
   The link is well founded.

**Algorithm: Phase-3**

1. Enable the promiscuous mode in NS2.
2. Update the trust level for each node.

5 EXPERIMENTAL RESULTS

5.1 Simulation parameters

The area will be in the radius of 1440m x 1200m, the simulation time will be of 10 seconds, there will be 16 number of nodes, the CBR traffic model is used. Number of wormhole tunnels is 1/2/3/4 (up to 8 wormhole peers maximum). Value of Mac protocol is MAC/802.11. The data rate will be of 256 kbps, data packets will be in 1024 Bytes/packets. AODV protocol is used and the source type is UDP, the channel type is channel/wireless channel. Radio propagation model value is propagation/two-ray round wave. Value of interface queue type is queue/drop tail. Link layer type is LL and the antenna used is antenna/omni antenna.

5.2 Simulation Studies

**Packet delivery ratio:** Packet delivery ratio (PDR) can be measured as the ratio of number of packets delivered in total to the total number of packets sent from source node to destination node in the network.

\[
PDR = \frac{\text{number of packet received by destination node} \times 100}{\text{number of packets send by source node}}
\]

**Drop Rate:** number of packets dropped by nodes is said to be as Drop Rate.

\[
\text{Drop Rate} = \frac{\text{number of packet send} - \text{number of packet Received}}{100}\times\text{(number of packet send)}
\]

**End-to-End delay:** End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination.

\[
\text{End-to-end Delay} = \frac{\sum (\text{arrive time} - \text{send time})}{\text{(Number of connections)}}
\]

**Throughput:** Throughput is a measure of how many units of information a system can process in a given amount of time.

\[
\text{Throughput} = \frac{\text{(Total bytes received by destination node)}}{\text{Total simulation time}}
\]

All these parameter metrics are pictorially represented by bar graph and the outcome is compared with the existing approach and the nodes without detecting the wormhole.

**Throughput chart**

From this chart it is clear that our proposed algorithm is getting more throughput when compared with the existing technique and without detecting the wormhole in nodes.

**Packet drop ratio**

From the above chart it is clear that the packet drop ratio is less when compared with the existing system and without detecting the wormhole in nodes.
The above chart shows that our proposed algorithm has high packet delivery ratio when compared with the existing approach and without detecting the wormholes in nodes.

The above chart shows that the end to end delay between the packets sending from source to destination is high when compared with other two attributes.

6 CONCLUSION
This paper proposed an extension of AODV protocol to detect the wormhole attack in wireless networks. The protocol first identifies the route from source to destination and then verifies the trust of the chosen route based on trust value and RTT metrics. The presence of wormhole nodes by any node are then broadcasted in the network. This algorithm shows significant performance improvement in sending the data packets to destination. The algorithm can be extended in future work by enhancing data security and also it can be implemented in real time prototype to evaluate its efficiency.

REFERENCES


