Implement of AODV, SAODV and ASODV Routing Protocols for Black Hole in Ad Hoc Networks and Optimized Performance

1Mukesh Yadav, 2Kamlesh Singh, 3Surendra Kumar
1Research Scholar & Asst Professor of Computer Science Engineering in Dr.K.N.Modi University, Newai, Rajasthan, INDIA
2Assistant Professor of Computer Science Engineering in Dr.K.N.Modi University, Newai, Rajasthan, INDIA
3Assistant Professor of Computer Science Engineering in Dr.K.N.Modi University, Newai, Rajasthan, INDIA

ABSTRACT:
A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form an arbitrary topology. The routers are free Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load). Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. Besides the general security objectives like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. During the last few years, continuously increasing growth in the deployment of wireless and mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist. Therefore, a network layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols. Unfortunately all of the widely used ad hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic. This assumption can prove to be disastrous for an ad hoc network that relies on intermediate nodes for packet forwarding. HERE WE presented performance impacts faced by the ad hoc network environment using different routing protocols. This study is made to compare the performance between three routing protocols, original AODV (Ad hoc On Demand Distance Vector), Secure AODV, Adaptive (A-SAODV).

I. INTRODUCTION
Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an
attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

II. CURRENT SENIORIO

2.1 Black Hole Attack

In black hole 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. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address.

The method how malicious node fits in the data routes varies. Fig. 4.1 shows how black hole problem arises, here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node “A” before any other node. In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start seeding data packets to node “C”. In this way all the data packet will be lost consumed or lost.

2.2 Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

Fig. 2.2 Black hole attack specification

2.3 Secure AODV (SAODV)

Secure AODV (SAODV) is a security extension of the AODV protocol, based on public key cryptography. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed to guarantee their integrity and authenticity. Therefore, a node that generates a routing message signs it with its private key, and the nodes that receive this message verify the signature using the sender’s public key. The hop count cannot be signed by the sender, because it must be incremented at every hop. Therefore, to protect it (i.e., not allow malicious intermediate nodes to decrement it), a mechanism based on hash chains is used. In its basic form, this makes it impossible for intermediate nodes to reply to RREQs if they have a route towards the destination, because the RREP message must be signed by the destination node. To preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the double signature: when a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message towards itself.

2.4 SAODV Hash Chains

Hash chains are used in SAODV to authenticate the hop count of the AODV routing messages (not only by the end points, but by any node that receives one of those messages. Every time a node wants to send a RREQ or a RREP it generates a random number (seed). Select a Maximum Hop Count. Maximum Hop Count SHOULD be set to the TTL value in the IP header, and SHOULD never exceed its configuration parameter NET_DIAMETER. The Hash field in the Signature Extension is set to the seed. The Top Hash field is set to the seed hashed Max Hop Count times. Every time a node receives a RREQ or a RREP it verifies the hop count by hashing Max Hop Count Hop Count times the Hash field, and checking that the resultant value is the same than the Top Hash. If the check fails, the node SHOULD drop the packet. Before rebroadcasting a RREQ or forwarding a RREP, a node hashes one time the Hash field in the Signature Extension.

2.5 Adaptive Secure AODV (A-SAODV)

Adaptive Secure AODV (A-SAODV) is a prototype implementation of SAODV, A-SAODV is a multithreaded application: cryptographic operations are performed by a dedicated thread to avoid blocking the processing of other messages.

Figure 2.5: A-SAODV Route Request and Route Reply Processing

Figure 2.5.1: Multithreaded Architecture of A-SAODV
III. RELATED WORKS AND PROPROSED SCENARIO

A black hole attack happens when a malicious node D' intercepts the data traffic from the source node S to the destination node D. D' may misbehave by agreeing to forward packets but fail to do so, because it is overloaded, selfish, malicious, or broken. This kind of black hole attack can be detected by setting the promiscuous mode of each node. Another type of black hole attack is that D' claims to have the IP address of D, thus leads S to form the path to D', instead of D.

3.1 Neighborhood based method by metric

In neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to establish the path to the true destination such that the impact of the black hole attack can be mitigated. They first introduce a metric, the neighbor set of nodes. Neighbor set is defined as all the nodes that are radio transmission range of the node. Because of the mobility of nodes, the neighbor set of a node keeps changing and it is expected that the neighbor set changes faster when mobility increases. The chance that two mobile nodes have the same neighbor set at the same time is very small. So the neighbor set provides a good “identity” of a node, i.e., if the two neighbor sets received at the same time are different enough, they conclude that they are generated by two different nodes. They use two sets of experiments to demonstrate that the neighbor set of a node is a good attribute to identify a node.

3.1.1 Detection

In order to collect neighbor set information, they introduce two types of control packets in the detection phase: Request Neighbor Set (RQNS) and Reply Neighbor Set (RPNS). The packet format of RQNS is as follows:

\{SrcAddr, DesAddr, RequestNeighborSeq#, NextHop\}

SrcAddr is the IP address of the source node S, and DestinationAddress is the IP address of the destination D. Each node is responsible for maintaining one counter: the sequence number of the RQNS, which unicasts to the destination using the underlying AODV routing protocol. D or D', after receiving RQNS, replies a message RPNS. The message format of RPNS is as follows:

\{SrcAddr, DestAddr, RequestNeighborSeq#, Neighbor Set\}

The first three items, i.e., SmAddr, DesAddr, RequestNeighborSeq#, identify to which RQNS this RPNS corresponds. Neighbor Set contains the current neighbor set of D or D'.

IV. IMPLEMENTATION

4.1 Protocol implementation

The algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP).

4.2 Data routing information table

Each node maintains a data routing information (DRI) table. This table keeps track of whether or not the node did data transfers with its neighbors. This table contains one entry for each neighbor and indicates whether the node has sent data through this neighbor and whether the node has received data from this neighbor. Table entry contains node id, from and through as shown in Table 1. The field from stands for information on routing data packets from the node (in the node id field) while the field through stands for information on routing data packets through the node (in the node id field). Values of from and through fields will be 0 or 1 to represent false and true respectively. Table 1 shows the sample DRI table for a node. The entry 1, 0 for node 3 implies that this node has routed data packets from node 3 but has not routed any data packet through node 3.

**TABLE 1: SAMPLE DRI TABLE**

<table>
<thead>
<tr>
<th>NODE ID</th>
<th>From</th>
<th>Through</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

4.3 Algorithm

In our new technique, we rely on reliable nodes (any node is reliable to the source node if it has successfully routed data through that node) to transfer data packets. The modified AODV routing protocol and the algorithm for our proposed methodology are described below.

In this protocol, if the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (Route Request) message to discover a secure route to the destination node same as in the AODV. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes.
between source and the destination. If the intermediate node (IN) generates the Route Reply (RREP), it has to provide its next hop node (NHN) and its DRI entry for the next hop node. When the reply comes back, it collects the IP addresses of all nodes between source and the intermediate node but no intermediate node updates the route entry for the destination. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node or not. If the source node has used IN before to route data, then IN is a reliable node and source will first send a route establishment message to IN node along the path that RREP comes according to the information contains in the RREP message. Upon receiving this message all nodes between the source and the intermediate node will update or insert route entry for the destination. Then source node starts sending data through the IN and updates the DRI table with nodes between source and IN node. If the source has not routed data through IN before, IN is not a reliable node. Then source first stores the information about IN and the nodes between the source and IN, and sends Further Request (FREQ) message to NHN of the IN to verify the reliability of the IN and ask NHN:
1) Whether the IN has routed data packet through NHN.
2) Who is the current NHN’s next hop to the destination?
3) Has the current NHN routed data through its own next hop?

Then NHN in turn responds with Further Reply (FREP) message which includes:
1) DRI entry for IN.
2) The next hop node (NHN) of current NHN, and
3) The DRI entry for the current NHN’s next hop.

4.4 Wait and try method:

In the paper “Prevention of Black hole Attack in MANET” by the author Latha Tamilselvan and Dr. V Sankaranarayanan proposed a wait and try method. To reduce the probability of black hole attack, it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. They use GLOMOSIM to shows that their protocol provides better performance than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

They propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hop details from the other neighboring nodes. After receiving the first request it sets timer in the ‘Timer Expired Table’, for collecting the further requests from different nodes. It will store the ‘sequence number, and the time at which the packet arrives, in a ‘Collect Route Reply Table’ (CRRT).

M- Malicious
S-Source
D- Destination

V. MY OBSERVATION

The comparisons of three routing protocol have been measured between AODV, Secure AODV and Adaptive Secure AODV to study the performance of each routing protocols in a free-attack simulation environment using different performance metrics

5.1 Scenario and Environment Settings

The scenario and the environment settings are fixed. It is purposely done to see the fair results between the routing protocols. These routing protocols AODV, Secure AODV and Adaptive Secure AODV are fairly compared in a chosen free-attack simulation environment. Here are some of the details on the setup:-
- Number of Nodes = 50 nodes
- Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment
  - Maximum connections = 40 traffic sources
  - Mobility Model = Random Waypoint
  - Mobility Speed = 40 m/s
  - Rate = 8kbps (2 packets per load)
  - Topology Size = 500m x 500m
  - Time = 100 seconds (results are collected every 10s of pause time)

5.2 Performance Metrics and Evaluation

For the simulation results, there are 6 performance metrics that have been used in my simulations as shown below:-

5.3 Packet Delivery Fraction (in percentage)

The ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources. PDF shows how successful a protocol performs delivering packets from source to destination.
Higher value (nearest to 1.0) means the better the results. It describes the loss rate that will be seen by the transport protocols, which in turn, affect the maximum throughput that the network can support. As the calculation, Packet Delivery Fraction (pdf %) = (received packets / sent packets) * 100.

Figure: 5.3 packet delivery (fraction)% vs pause time

VI. CONCLUSION

AODV is perhaps the most well-known routing protocol for a MANET. It is a reactive protocol node in the network exchanging routing information only when a communication must take place and keep this information up-to-date only as long as the communication lasts. Real network test based. Ad Hoc On-Demand Distance Vector (AODV) routing protocols was selected as the basis of the entire simulations. Due to the needs of securing the routing in the wireless ad hoc networks, Secure AODV (SAODV) was developed to add security to original AODV which includes cryptographic operations that can have a significant impact on the routing performance. To get better performance while maintaining the secure routing, Adaptive SAODV (A-SAODV) was developed based on the SAODV implementation, which was claimed to introduce some improvement on the routing compared to the SAODV. Based on this justification, some analysis and studies are made on the performance and impacts using AODV, Secure AODV (SAODV) and Adaptive Secure AODV (A-SAODV) in a free-attack simulation environment to analyze these routing protocols and make some comparisons on the performance. The collection of simulation results will show the performance impact of security implementation into the original AODV after the implementations of SAODV and A-SAODV into the networks.

VII. FUTURE WORK

Here I have done the performance and implementation comparisons studies on different routing protocols; AODV, SAODV and A-SAODV. For the future research, a research must be put on the presence of attacks inside the routing environment. From there, we could see the differences in term of performances between these three routing protocols or other routing protocols in ad hoc networks. The outputs and findings will be much different and the usage of security methods to be in place should be looked again to get better performance or to get better security. And finally, the best routing protocol could be chosen, but still totally depends on the requirements of that routing environment or systems; either to have best performance or best security.

REFERENCES