Prevention of Black Hole Attack on MANET Using Trust Based Algorithm

Apurva Jain and Anshul Shrotriya

ABSTRACT

Mobile ad-hoc network (MANET) consists of wireless mobile nodes that are capable of communicating with each other without any centralized administration, due to this it is a self-organized network. The black hole problem is one of the security attacks that occur in mobile ad hoc networks (MANETs). In Black hole attack, a malicious node falsely advertise shortest path to the destination node with an intension to disrupt the communication. In this paper we simulate the black hole attack with the proposed Trust-based algorithm by the help of network simulator (NS-2). We analysed that the quality of services degrade due to Black hole so by using trust based algorithm the quality of services are improved.

Index Terms - MANET, Black hole attack, AODV, Trust-based algorithm, NS-2.

I. INTRODUCTION

Mobile ad-hoc network (MANET) consists of wireless mobile nodes that are capable of communicating with each other without any centralized administration, i.e., MANET is a self-organized network.

Communication in mobile ad-hoc network is done via multihop path. If two mobile nodes are inside each other's transmission range, they communicate directly; otherwise, in-between nodes forward the packet for them. In such a scenario, every node in the network should have the capability to function as a host as well as function as a router to forward the packet. In MANET, each node is free to join, leave, and move independently. As a result, the network topology changes rapidly and unpredictably, and connectivity among the terminal vary with the time. Due to inherent characteristics, MANETs are more vulnerable to attacks.

These attacks are generally classified as

1. Active attacks

2. Passive attacks.

A passive attack does not influence the normal functioning of a network. An adversary aims to capture the data without changing it. Therefore, it is difficult to recognize passive attack as the network operates normally. In general, encryption is used to combat such attacks.

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. The active attacks are further categorized as external attacks and internal attack. When the attack is from foreign network it is known as external attack whereas an attack from the node within the network is termed as internal attack. Internal attack, a malicious node falsely advertises a good path (e.g., shortest path or more stable path) to the destination node without really having one. There are different type of internal attack like black hole attack, Worm hole attack, Byzantine Attack, Jellyfish attack etc.

1. Wormhole attack:

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole.

2. Byzantine Attack:

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or

- *Apurva Jain is currently pursuing ME from Electronics & Communication from Medicaps Institute of Technology & Management Indore (M.P.), India, PH-919424009904. E-mail: apurvajain859@gmail.com*

- *Anshul Shrotriya is an Assistant Professor in Electronics & Communication department of Medicaps Institute of Technology & Management Indore (M.P.), India, PH-919993556641. E-mail: shrotriya_anshul@yahoo.com*

degradation of the routing services. It is hard to detect byzantine failures.

3. Jellyfish attack

In jellyfish attack, the attacker attacks in the network and introduce unwanted delays in the network. In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are propagated then packets are released in the network.

4. Black Hole Attack:

A packet drop attack or black hole attack is a type of denial-of-service attack accomplished by dropping packets. Black holes refer to places in the network where incoming traffic is silently "dropped", without informing the source that the data did not reach its intended recipients shows the black hole attack. Black Hole attacks effects the packet delivery and to reduce the routing information available to the other node

II. AODV ROUTING PROTOCOL

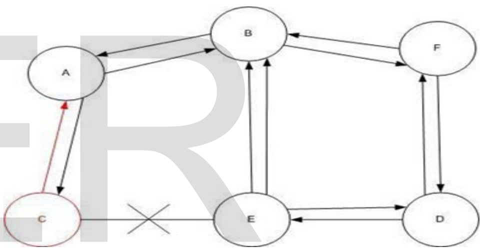
Ad-Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol discovers routes as when it is necessary does not maintain routes from every node at every time. Routes are maintained just as long as necessary. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node is the destination, it generates Route Reply (RREP). As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen.

III. BLACK HOLE ATTACK

In this type of attack, one malicious node uses routing protocol to claim itself of being shortest path to destination node but drops routing packets and doesn't forward packets to its neighbours. . The Black hole attack at network layer is the most attention seeking attack in ad hoc networks. In Black hole attack the situation can become worse if the black hole node declares itself as having shorter path to almost all nodes.

The black hole attack has two properties. First property is, the node exploits the MANET protocol, such as AODV (Ad hoc On-demand Distance Vector) to advertise itself as having a valid path to a destination node, even though the path is invalid, with the intention of intercepting packets. Second property is, the attacker consumes the intercepted packets without forwarding to any other node.

Following Fig shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process to find out the valid route. 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 Route Request 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.



BLACK HOLE ATTACK

IV. TRUST BASED ALGORITHM

In trust based algorithm firstly increase the monitoring without transmitting the packet. This allows nodes to obtain trust information about nodes without transmitting packets, by monitoring of other nodes packets. The Trust Nodes now store packets that have been sent out for forwarding as well as general packets that have been promiscuously seen that are expected to be forwarded. The two sets of packets are stored separately in cyclic buffers packet Buffer and general Packet Buffer to detect if a packet has been forwarded successfully a buffer of packets that have been recently sent for forwarding is stored. This is stored in a cyclic buffer, defined in the class Circular Buffer and instantiated within that nodes Trust Node. Using a circular buffer means that if packets are not removed frequently enough it will cause the buffer to cycle erasing the last element. This means that if a node is dropping packets then the buffer will start to cycle. Been forwarded, the packet can be found and removed from the buffer, increasing the trust in that node. Increase the trust Value the amount associated with seeing one of the nodes own packets forwarded and Decrease the trust Value the amount associated with one of the nodes packets not being forwarded timely.

V. SIMULATION AND RESULT

We used the network simulator (ns-2).A network is constructed for the simulation purpose and then monitored for a number of parameters. We simulate our model for 20 nodes. We set the parameters for our simulation as shown in Table 1

Table 1: Simulation Parameters

Simulator	Ns-2 (version 2.35)
Simulation duration	30 sec
Number of Mobile Nodes	19
Number of Black hole Nodes	1
Topology	750*750
Transmission Range	250m
Routing Protocol	AODV
Traffic	Constant Bit Rate (CBR)
Packet Size	512 bytes

Protocols can be compared by evaluating various performance metrics as shown below:

5.1. Packet Delivery Ratio:

It is calculated by dividing the number of packet received by destination through the number packet originated from source.

$$PDF = (Pr/Ps)$$

Where Pr is total Packet received and Ps is the total Packet sent. Simulation results of figure 1(a) show that Packet Delivery Ratio increases using TAODV as compare to BAODV.

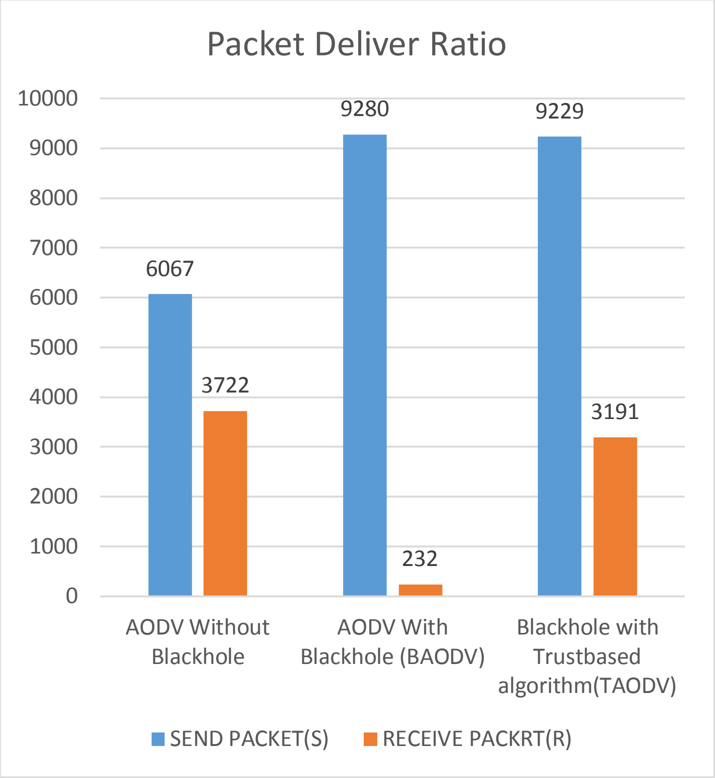


Figure 1(a): Impact of Black hole Attack on Packet Delivery Ratio.

5.2. Average end-to end delay:

It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination.

$$D = (Tr - Ts)$$

Where Tr is receive Time and Ts is sent Time.

Simulation results in figure 1(b) show that TAODV has high end to end delay than AODV routing protocol under black hole attack.

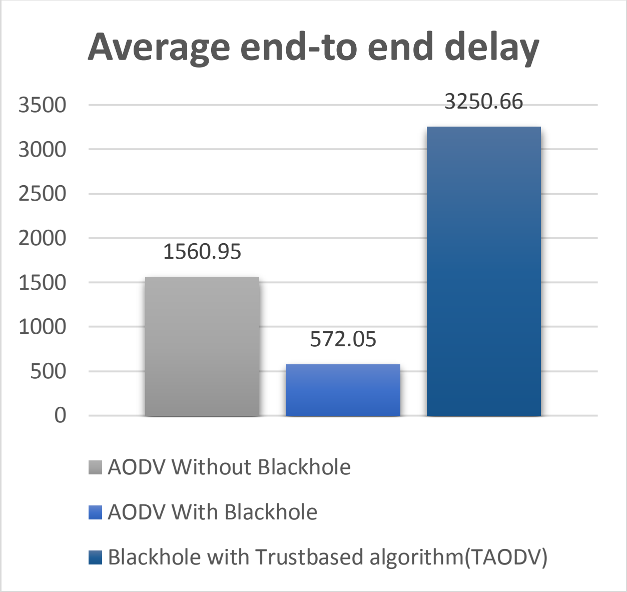


Figure 1(b): Impact of Black hole Attack on Average End to End Delay

5.3. Energy:

Simulation results in figure 1(c) show that BAODV has high energy consumption than TAODV.

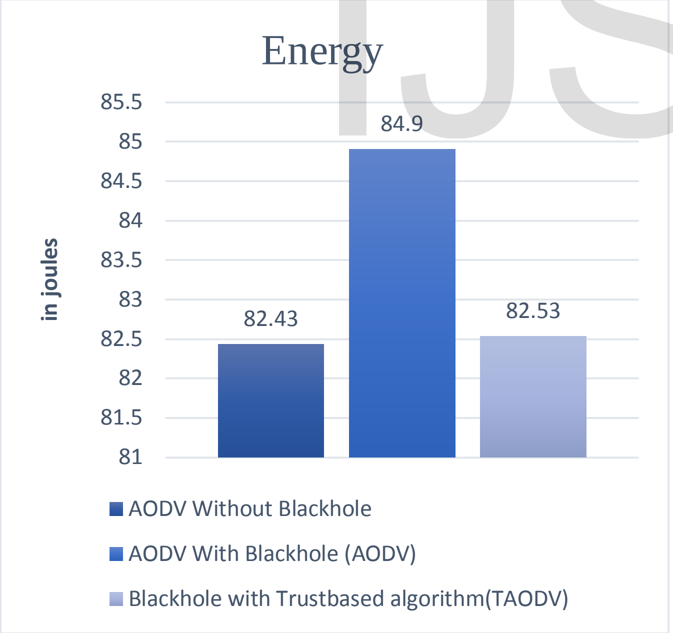


Figure 1(c): Impact of Black hole Attack on Energy

5.4. Throughput:

It is the amount of data receive at destination.figure1 (d) show that TAODV has high throughput than BAODV

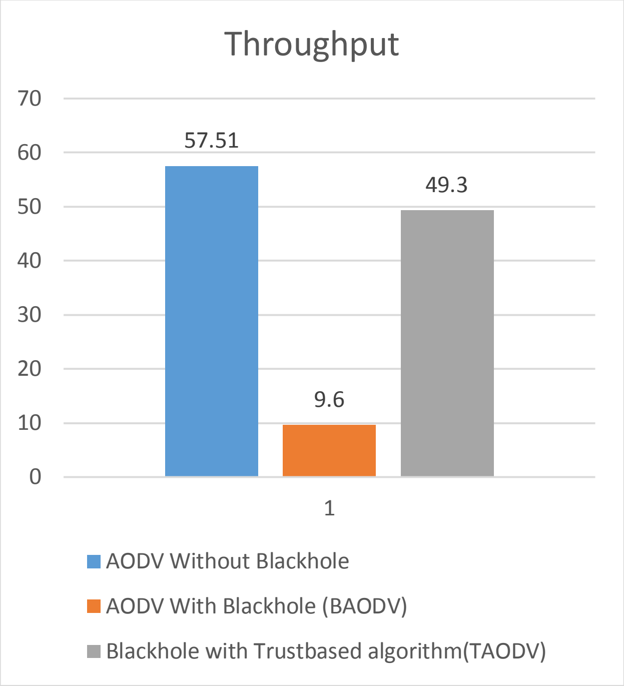


Figure 1(d): Impact of Black hole Attack on Throughput

VI. CONCLUSION

In this paper, we studied AODV with black hole attack. We evaluate the effects of black hole attack on AODV in MANET. We simulate the black hole behaviour with the help of Network Simulator 2 and compared the performance of black hole AODV with the original AODV and trust based algorithm in terms of different parameter metrics. The simulation results show that the packet loss and Energy increases in the network with a black hole node. We observed that the End-to-end Delay and Throughput of the network is decreased due to black hole attack .So to prevent black hole attack we proposed Trust based algorithm and observe that the packet loss and energy is decreases. Throughput and End to End delay increases.

REFRENCES

[1] P.Singh and G.Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[2] N. Sharma and A.Sharma “The Black-hole node attack in MANET”, 2012 Second International Conference on Advanced Computing &Communication Technologies.

[3] V. Palanisamy, P. Annadurai, and S.Vijayalakshmi. “Impact of Black Hole Attack on Multicast in Ad hoc Network (IBAMA)”, 2010 IEEE.

[4] Mohana, N.K. Srinath, and Amit L.K,”Trust Based Routing Algorithms for Mobile Ad-hoc Network”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2.

[5] J. Kumar, M. Kulkarni, and D. Gupta” Effect of Black Hole Attack on MANET Routing Protocols”, I.J. Computer Network and Information Security, 2013.

[6]M.Shurman and S.Yoo“Black Hole Attack in Mobile Ad Hoc Networks “ACMSE’04.