



Impact of Black Hole Attack at Different positions in Trust Implemented AODV routed MANETs

¹Gayathri.D

Research Scholar, Department of Computer Science,
Bharathiar University,
Coimbatore, Tamil Nadu, INDIA.

²Dr.S.JanakiRaman

Assistant Professor,
Department of Banking Technology, Pondicherry University,
Pondicherry, INDIA.

Abstract: MANETs are Mobile Ad hoc Networks that comprise complex distributed system that have dynamic topology and no fixed infrastructure. These make them to become very privileged in disaster recovery environments. But their routing protocols have no security related issues and they are vulnerable to many attacks. Here in this paper we have taken AODV protocol implemented with a metric called Trust to ensure secure and reliable transmission of packets and study is made by implanting Black Hole Attack in the network at different positions.

Keywords: MANETs, AODV, Trust, Black Hole Attack, Positions.

I. Introduction

MANETs are group of mobile nodes which get in to communication where there is no pre-existing infrastructure, this nature has made MANETs to gain momentum as they help realize network services in places with no basic or fixed infra-structure. These nodes in MANETs act both as host as well as routers in forwarding packets for each other in a multi-hop fashion. So it is necessary of the MANETs that all the nodes are reliable which made security an essential requirement even here. Trust is a metric and a measure of reliability which is implemented in AODV, Ad hoc On demand Distance Vector Protocol and a remarkable enhancement in Packet Delivery Ratio is got when compared to Black Hole Attack implemented AODV in [12]. In this paper, the Black Hole Attack is implemented and its impact is studied at different position in the network.

II. Over view of AODV protocol

AODV, Ad hoc On Demand Distance Vector Protocol is a type of reactive routing protocol for MANETs. It makes use of Destination Sequence Number to prevent loops in Network. AODV uses HELLO packets and floods it in order to indicate its presence in the network. It uses the RRER, Route Repair messages to indicate Link Failure. To start a communication it uses RREQ, Route Request packets and RREP, Route Reply Packets. These two help in getting a fresh route to the destination. The actual data packets are forwarded in the fresh route sought. To start with, the source floods RREQ packets to the neighbors. If the neighbors are the destination or if they have route to the destination they send RREP messages to the source. If the neighbors do not have they forward it to their neighbors. By this way route is found. By the time RREP messages reach the source all the intermediate nodes know the route to the destination as well as the route to the source. Now the source on getting the RREP packets checks for the highest Destination Sequence Number in them to forward the data packets to ensure the freshness of the route.

III. Black hole attack

Black Hole is a type of Active Attack and as the name suggests, packets received by the attacker disappears. The attacker introduced in the network's active path and advertises itself having the shortest path to the destination or advertises itself to be the destination by spoofed IP address of the destination. Black Hole Attack drastically reduces the efficiency of the network. Packet Delivery Ratio is dropped drastically by this type of attack. In Ad hoc On Demand Distance Vector protocol black hole Attacker sends fake RREP, Route Reply messages to the source with highest Destination Sequence Number and gets the data packets for itself and then drops it. Hence drastically affecting the Packet Delivery Ratio.

Figure 1 Source sending RREQ.

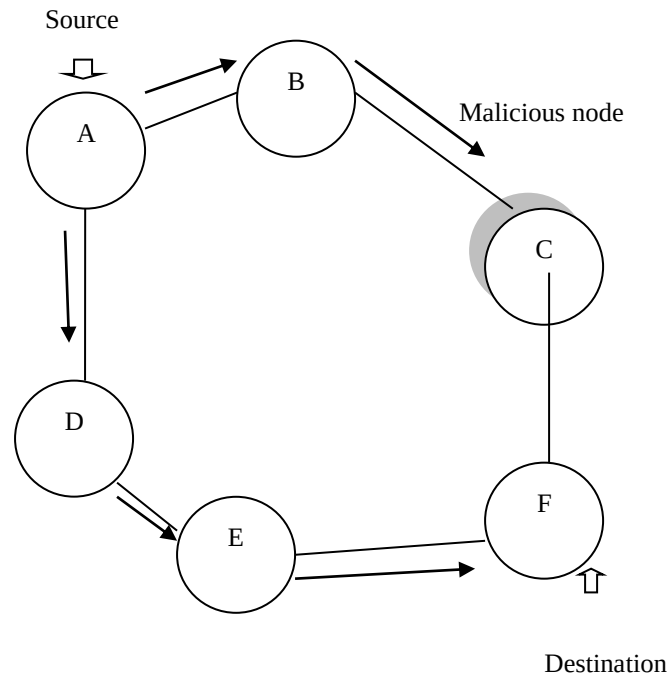
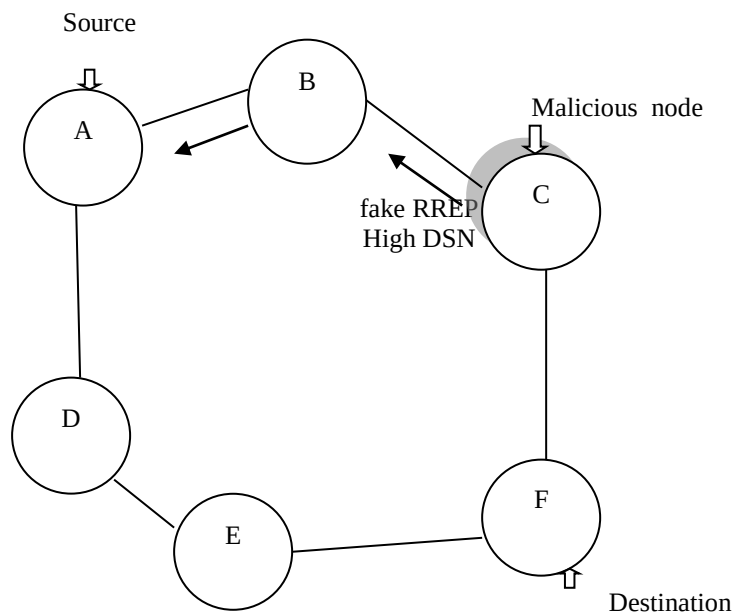


Figure 2 Attacker sending fake RREP



IV. Trust Implemented AODV

Trust is the reliability that a node has on another node and this implemented in AODV for secure routing in Mobile Ad hoc Networks. Trust is implemented in AODV in [12] by the following method. Initially all the nodes Trust Value is assigned to zero. First the nodes are said to watch promiscuously and a cyclic buffer is used to store the packets sent for forwarding. If the packets are forwarded then the cyclic buffer is recycled and the packet is deleted from the buffer and the corresponding nodes trust value is increased by one. If the packet is not forwarded or if the packet is delayed forwarding for a long time then the nodes Trust value is decreased by 1. When a node has a Trust value of -5 or below it is not included for routing.

V. Simulation Setup

A Mobile Ad hoc Network model has been created by using ns 2.34 simulator with 50- 100 nodes in a time duration of 30 seconds in a transmission range of 250 meters, with a data rate of 2 mbps, traffic type Constant Bit Rate (CBR) and a time interval set to 0.01 seconds with MAC layer 802.11. The comparison is performed in Trust based AODV, Ad hoc On Demand Distance Vector protocol under Black Hole Attack. The Attack positions vary and are near the source node, near the destination node and in the middle. The metric taken for comparison is Packet Delivery Ratio.

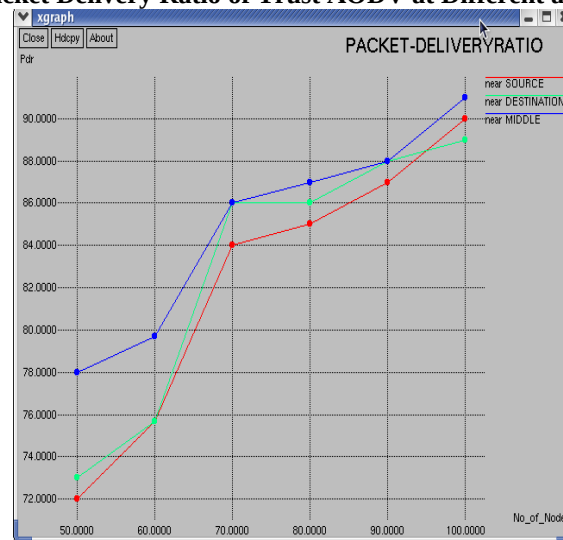
Table I Simulation parameters and values

PARAMETERS	VALUES
SIMULATOR	NS 2.34
NODES	50 – 100
ATTACK	BLACK HOLE ATTACK
SIMULATION AREA	1500 * 1000
ROUTING PROTOCOLS	TRUST IMPLEMENTED AODV
TRAFFIC	CBR (CONSTANT BIT RATE)
ATTACK POSITION	NEAR SOURCE, NEAR DESTINATION AND CENTER
DATA RATE	2 MBPS
INTERVAL	0.01 SECONDS
SIMULATION TIME	30 SECONDS
ANTENNA	OMNI DIRECTIONAL
PACKET SIZE	512 BYTES
TRANSMISSION RANGE	250 M
NUMBER OF ATTACKERS	ONE
PROPAGATION	TWO RAY GROUND

VI. Results and Discussion

The measured metric is Packet Delivery Ratio. Packet Delivery Ratio is the ratio of packets forwarded by the source to the packets received by the destination. The Trust implemented AODV gives a very higher performance than AODV under Black Hole Attack in [12]. The Black Hole Attacker is placed near the source, destination and in the middle of the network and the Packet Delivery Ratio investigated.

Figure 3 Packet Delivery Ratio of Trust AODV at Different attack position



From the graph the near source node position and the near destination position are more attack prone position. The center position is not as vulnerable as compared to the near source and near destination position.

VII. Conclusion

The vulnerability increases when the attackers are near the source and when they are near the destination which is due to the fact that when near the source they become neighbors and tend to get the packets and drop the packets. When near the destination chances of passing through them remains high being dropped. The different attack position can be studied by implementing other attacks and in other protocols as well.

References

- [1] S.Corson, J.Marker, "Mobile Ad hoc Networking", RFC-3651.
- [2] C.Perkins, E.Royer and S.Das, "Ad hoc On demand Distance Vector Routing", RFC-3651.
- [3] Hoang Lan Nguyen, Uyen Trang Nguyen, "A Study of Different Types of Attacks on MANETs" Elsevier – Ad hoc Networks 6(2008)32-46.
- [4] Pradip M.Jawandhiya, Mangesh M.Ghonge, Dr.M.S.Ali, "A Survey of Mobile Ad hoc Network Attacks", International Journal Of Engineering and Technology vol 2(9),2010, 4063-4071.
- [5] Monika Roopa K, Prof. BVR Reddy, "Blackhole implementation in AODV Routing Protocol" International Journal of scientific and Engineering Research, vol 4, Issue 5, May-2013 ISSN 2229-5518.
- [6] Fan-Hsun tseng, Li-Derchou, han-chieh Chao, "a Survey of blackhole Attacks in wireless mobile ad hoc Networks" Human Centric Computing and Information Sciences, a Springer open journal.
- [7] Harjeet Kaur, Manju Bala, Varsha Sahni, "Study of Black hole Attack using Different Routing Protocols in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , ISSN : 2278-8875, vol 2, Issue-7, July 2013.
- [8] Bo Sun, Yong Guan, Jian Chen and Udo W.Pooch, "Detecting Black-hole Attack in Mobile Ad hoc Networks" The Institution of Electrical Engineers, 2003.
- [9] Kamal Deep mekha, Mohit Virendra, Shambhu Upadhaya, "Trust Based Routing Decisions in Mobile Ad hoc Networks"
- [10] Mohmood Salehi, Hamed Samvati, "Injection and Evaluation of New Attacks on Ad hoc proactive Routing algorithms", international journal of information Security Research, vol 2, Issue 2, March-june-2012.
- [11] Harmandeep Singh, Gurpreet Singh, Manpreet Singh, "Performance Evaluation of Mobile Ad Hoc Network Routing protocols under Black hole Attack", International Journal of Computer applications, 0975-8887, vol.42- No-18, March 2012.
- [12] Gayathri. D, S. Janakiraman, "Comparison of the performance of TRSAODV with AODV Under blackhole attack in manets", International journal of research in engineering and technology, 2319-1163, vol.5-no.6, jan-2016.