International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 249 - 253

Effect of Black hole Attack on Mobile Ad-hoc Networks

Alphonsa George
Electronics and Communication dept.
College Of Engineering Kidangoor
Kottayam, India
11alphonsa@gmail.com

Dhanya Narayan, Cincy Mary Sebastian*
Electronics and Communication dept.
College Of Engineering Kidangoor
Kottayam, India
dhanyanarayan06@gmail.com
**junocincy@gmail.com*

***Abstract*—** Mobile ad hoc networks (MANETs) are obtaining popularity today, as it offers wireless connectivity to the users irrespective of their geographical position. Such networks are composed of a set of stations or nodes that communicating through wireless channels, without any fixed backbone support in which different nodes are allowed to join or leave the network at any time. MANETs are generally more vulnerable to information and physical security threats than wired networks, so security is a vital requirement in MANETs to provide secured communication between mobile nodes. Most of the routing protocols rely on the cooperation among the nodes for secure transmission due to lack of centralized administration. There is no general algorithm for security of principle routing protocols like AODV against various attacks. One of the most common attacks against routing in MANETs is the Black Hole attack. A black hole is a malicious node that uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In this paper, we examine the effect of blackhole node in adhoc networks using simulator tool NS2.

Keywords- *AODV; Black hole attack; MANET.*

*****

I. INTRODUCTION

Wireless network consists of mobile nodes without any physical connection to each other. Such networks do not have any physical media, rather they use radio frequency spectrum to send and receive data. Wireless networks have two basic architectures: - Fixed Backbone Network and Wireless Mobile Ad hoc Network. In fixed backbone network the infrastructure is fixed whereas in mobile networks it is variable. Hosts and routers together in combination create wireless networks. Wireless technology is used by Ad-hoc networks to pass messages from one node to another in order to communicate with each other. Typically Mobile Ad Hoc Networks refers to the networks which allow mobile wireless ad hoc architecture.

A Mobile Ad hoc network (MANET) is a self - configuring network that does not require any fixed infrastructure, which minimizes their cost as well as deployment time. The topology of the ad-hoc network changes dynamically and unpredictably. Also, the ad hoc network can be either constructed or destructed quickly and autonomously without any infrastructure. Without support from the fixed infrastructure, it is difficult for us to distinguish the insider and outsider of the wireless network. That is, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. MANETs require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, like battlefields, military applications, and other Emergency and disaster situations.

II. ROUTING IN MANET

The routing protocols are divided in to three categories based on management of routing tables. They are Proactive (Table-Driven) routing protocols, Reactive (On-Demand) routing protocols and Hybrid routing protocols.Table I shows the main features of all the three types of routing protocols.

Table: I Routing Protocols

Type	Features	Examples
Proactive Routing	• Routes are discovered and stored before the actual requirement. • Timely correction and distribution of routing information.	DSDV, OLSR
Reactive Routing	• Routes are discovered as and when required. • No distribution of information.	AODV, DSR
Hybrid Routing	• Combination of both reactive and proactive protocols. • Overcome the defects of both	ZRP, OORP

III. AODV ROUTING PROTOCOL

One of the most widely used routing protocol in MANETs is the Ad hoc on-demand distance vector (AODV)[1] routing protocol which is a reactive protocol[3]. In an Ad-hoc network each node maintains routing information in a table. This information contains the path to a specific destination. When the packet is to be sent for the very first time, the sending node checks the route in the routing table. If it is available then same route is used for sending the packets to the intended destination. If the route is not available then the node starts discovery of route by transmitting RREQ packet to its neighbours. All the nodes on receiving RREQ will verify whether they are the required destination node, if so then it sends the Route Reply (RREP) control message to the source else the node will check the routing table to determine if it has the active route to the destination node. If the active route is

not available then the intermediate node will broadcast the RREQ packet in search of the destination node on behalf of the original source node. If active route is available i.e. on receiving RREP from its adjacent nodes, the intermediate node will compare the Destination Sequence Number (DSN) from the routing table to the one present in RREQ packet. DSN is nothing but the sequence number of last packet which destination sends to the source. If this DSN is equal to or less than the sequence number of RREQ packet then further RREQ is broadcasted to its neighbours. If the DSN from the routing table of one of the neighbours is greater than the sequence number in the packet then the path/route is accepted as it contains the 'fresh route' and the data will be sent through this route to the destination. During this process if link failure is detected by any of the nodes then Route Error (RREP) message is sent to all of its neighbours who are using this link [4] [6]. This is demonstrated in the Figure. 1.

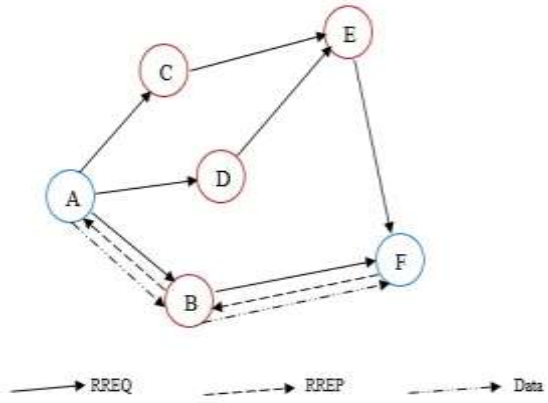

Figure: 1 AODV communication

IV. TYPES OF ATTACKS

Some of the unique characteristics that exist in the ad hoc networks are dynamic topology, distributed operation, and resource constraints, which inevitably increase the vulnerability of such network. Many characteristics are used to classify attacks in the ad hoc networks like the behaviour of the attacks (passive vs. active) and the source of the attacks (external vs. internal).

Passive Attacks

A passive attack does not change the valuable information transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Here, attacker does not disrupt the operation of a routing protocol but it attempts to discover the important information from routed traffic. Detection of these type of attacks is difficult since the operation of network itself doesn't get affected.

Active attacks

Active attacks are severe attacks that prevent message flow between the nodes. Active attacks actively modify the data with the intention to stop the operation of the targeted networks. Examples of active attacks consists of actions like message modifications, message replays, message fabrications and the denial of service attacks. Active attacks may be internal or external.

External Attacks

External attacks launched by adversaries who are not initially authorized to be involved in the network operations. These attacks usually aim to cause network congestion, denying access to specific network function or to interrupt the whole network operations. External attacks prevent the network from normal communication and generating additional overhead to the network.

Internal Attacks

Internal attacks are initiated by the authorized nodes in the networks, and might come from both misbehaving and compromised nodes. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the ad hoc networks. Security requirements such as authentication, confidentiality and integrity are severely vulnerable in these networks with the compromised internal nodes because communication keys used by these nodes might be steal and passed to the other colluding attackers.

Black hole Attacks

The black hole attack is one of the severe network layer attack in MANETs. In a black hole attack[12], the attacker swallows (i.e. receives but does not forward) all the messages he receives, just as a black hole absorbing everything passing by. Black hole node does not forward any of the message he receives, it simply drops all data packets.

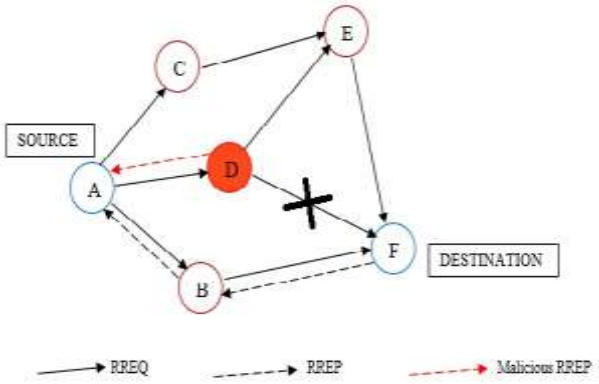

Figure: 2 Black hole Attack

Figure 2 shows black-hole attack. In black hole attack, malicious nodes trick all their neighbouring nodes to attract all the routing packets to them. When the malicious node insert itself between communication route, it is able to drop the packet, it is retrieve information from the data packet and can be modify it. Here, node F is the destination. Node D will send fake RREP to source showing it has routing to node F with higher sequence number. Source transmits data packet to D before waiting other RREPs. Node D is a black-hole, so it simply drops data.

V. PERFORMANCE METRICS

The performance of a MANET can be analyzed using metrics like packet delivery ratio, end to end delay etc. The characteristics of different performance metrics are explained in this section.

A. *Packet Delivery Ratio (PDR)*

PDR is the proportion of total number of packets/messages received by the intended destination to the total number of packets/messages transmitted by the source. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means better performance of the protocol [11].

Packet Delivery Ratio = Total Packets Received / Total Packets Sent.

B. *End to End Delay*

It is the delay required to deliver the packets from source to destination. This includes all possible delays caused by buffering during routing discovery latency, queuing at the interface queue, and retransmission delays at the MAC, propagation and transfer times The lower value of end to end delay means the better performance of the protocol. End to End Delay must be low to get better performance of AODV. It is measured in milliseconds[11].

End to end delay = _(arrive time - send time).

C. *Throughput*

Average packets sent successfully over a communication channel is throughput. Throughput is expressed as bytes or bits per sec (byte/sec or bit/sec).

D. *Routing Overhead*

The number of routing packets transmitted per data packet delivered at the destination. This metric gives an idea of the extra bandwidth consumed by overhead to deliver data packet.

VI. SIMULATION RESULTS

The network simulation is carried out using NS-2[8]. MANET performance is evaluated with black hole nodes in the ad-hoc network and compared the results with secure ad-hoc networks. The simulation parameters are provided in table II.

Table II: simulation parameter

Parameters	Value
Simulator	NS-2.35
Area	750*1000
Routing Protocol	AODV
Simulation Time	100s
Application Traffic	CBR
Number of Nodes	5, 10,15,20
Malicious Nodes	01-May
Packet Size	512 Bytes
Transmission Rate	2 Packets/s
Movement Model	Random Waypoint

MANET with black hole attack using AODV protocol is simulated. Figure 3 shows Packet Delivery Ratio is decreased up to 20% with black hole attack and as number of nodes increases PDR slightly increases.

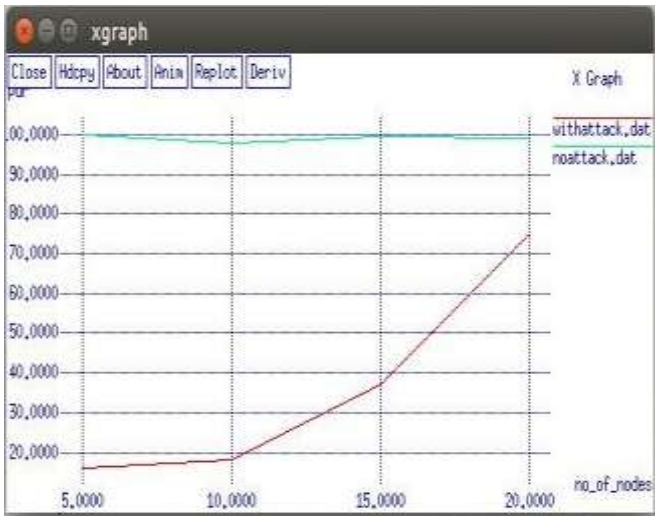

Figure: 3 PDR vs No of nodes

Figure: 4 Throughput vs No of nodes

Figure 5: Routing overhead vs No of Nodes

 ISSN: 2321-8169
249 - 253

In our particular network around 100 packets are sent per second, but after addition of black hole to this network it is shifted to 15 packets. From Fig: 4 it is clear that when there is 20 nodes found throughput is improved.

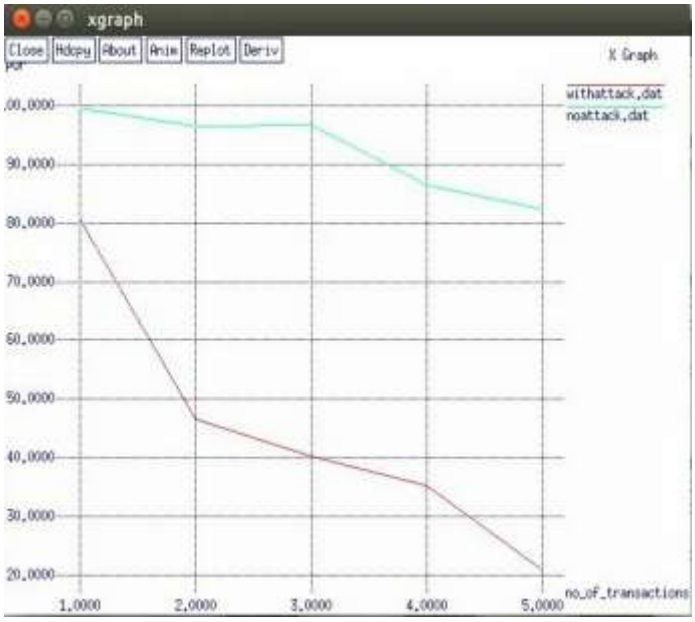

Figure 6: PDR vs No of Transactions

Routing overhead is another performance metric which indicates control messages. Figure 5 shows how it varies in network with black holes.

Number of connections between different nodes affects the performance of mobile ad-hoc networks. Figure 6 to 8 analyzes the effect of transactions in ad-hoc network as well as black hole network. Packet delivery ratio decreases as transactions increases.

Figure 7: Routing overhead vs No of Transactions

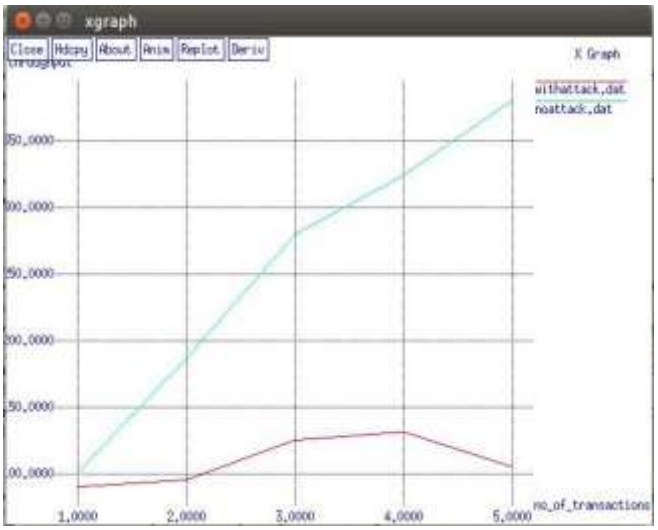

Figure 8: Throughput vs No of Transactions

Figure 9: PDR vs Node Mobility

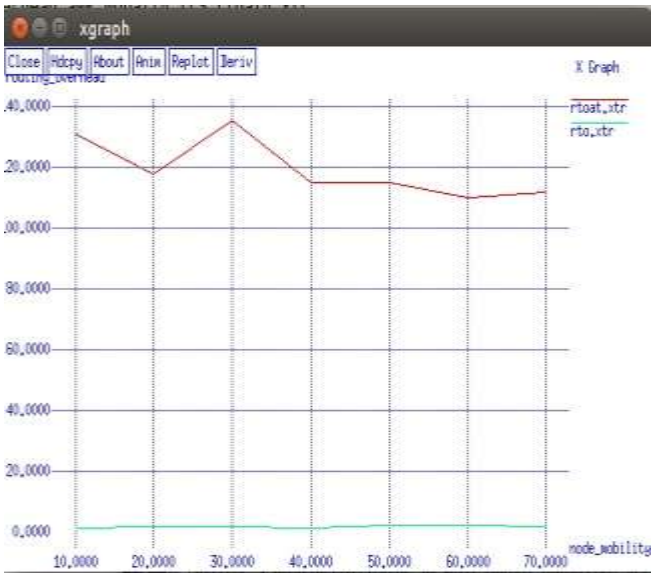

Figure 10: Routing overhead vs Node Mobility

Figure 9 shows how packet delivery ratio of both AODV network and AODV under attack varies with various node movements. Normal AODV network keeps PDR in maximum itself even the node mobility reaches to 70m/s. AODV under attack undergoes shows some variations but does not improved much even if mobility increases. Routing overhead of black hole network possess so big value than AODV network as in figure 10.

Figure 11: End to End delay vs Node Mobility

End to end delay is increases from very low value of normal network to 400ms for network with black hole attack. Figure 11 shows variation of end to end delay as node mobility increases. Average end to end delay is actually the total time taken to complete the journey for a data packet. In an ad-hoc network as the total number of mobile nodes increases this time duration is also slightly increases. With black holes end to end delay increases sharply since it is impossible for a packet to catch its destination.

VII. CONCLUSION

The performance of mobile ad-hoc networks under black hole attack using different metrics are evaluated. The packet delivery ratio of AODV network under black hole attack is very small. End to end delay and routing overhead are sharply increases with black holes. Many detection mechanisms are there to detect black holes like DRI mechanism, but overall performance is still need to be improved. As a future work, an efficient detection as well as prevention mechanism can be proposed to satisfy all the performance metrics.

REFERENCES

[1] C.E.Perkins and E.M.Royer, ”Ad Hoc On Demand Distance Vector Routing,” Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.

[2] Pradish Dadhania, Sachin Patel “Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks” in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 1, pp.1487-1491, January - February 2013.

[3] N.Mistry,D.C.Jinwala and M.Zaveri, “Improving AODV protocol against black hole attacks”, international multiconference of engineers and computer scientists 2010, vol 2, IMECS 2010, march 17-19 2010, Hong Kong.

[4] Janne Lundberg, Helsinki University of technology, "Routing Security in Ad hoc Networks", Seminar on National Security, http://citeseer.nj.nec.com/ 400961.html.

[5] Sherin Abdel Hamid “Routing for Wireless Multi-Hop Networks: Unifying Features” http://www.springer.com/978-1-4614-6356-6.

[6] Chuck Perkins “Request for Comments: 3561” Nokia Research Center, University of California, Santa Barbara, July-2003. http://www.ietf.org/rfc/rfc3561.txt

[7] Renu Mishra, Dr.Sanjeev Sharma. “Vulnerabilities and security for adhoc networks“, IEEE International Conference on networking and information technology, pp. 192-196, May 2010.

[8] The network simulator-ns 2.35. http://www.isi.edu/nsnam/ns/1997

[9] Ei Ei Khin1, Thandar Phyu. ”Impact of Blackhole attack on AODV routing protocol,” International Journal of Information Technology, Modeling and Computing (IJITMC), Vol. 2, No.2, May 2014.

[10] Vikas Solomon Abel ” Survey of Attacks on Mobile AdhocWireless Networks”, International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 2 Feb 2011

[11] AliffUmairSalleh, ZulkifliIshak, Norashidah Md. Din, and MdZainiJamaludin, "Trace Analyzer for NS-2", IEEE, pp. 29-32, Student Conference on Research and Development (SCOReD), Malaysia, 2006.

[12] Rusha Nandy, Debndutta Barman Roy, "Study of various attacks in MANET and elaborative discussion of rushing attack on DSR with clustering scheme," Int. Journal on Advanced Journal and Applications, vol. III, 20ll.