ISSN:0975-9646

Performance Analysis of Black Hole Attack on different MANET Routing Protocols

Neeraj Arora[#1], Dr. N.C. Barwar[*2]

[#] *M.E. Scholar, Computer Science Department, M.B.M. Engineering College, J.N.V. University, Jodhpur, Rajasthan, India*
[*] *Associate Professor, Computer Science Department, M.B.M. Engineering College, J.N.V. University, Jodhpur, Rajasthan,*

***Abstract*— A Mobile Ad-hoc NETwork (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Due to the openness of its nature it is vulnerable to various kinds of threats and malicious nodes are difficult to detect since every node participates in the operation of the network equally. One of the security thread is Black hole attack in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. The scope of this paper is a study and analysis the performance of MANET Routing Protocols like DSDV, DSR, AODV, OLSR and ZRP with or without malicious attack like black hole attack and the parameter used to judge the performance analysis are packet delivery ratio, average throughput, average end to end delay and Packet Drop Rate using NS2 under different scenarios.**

***Keywords*— MANET, OLSR, AODV, ZRP, Black hole attack.**

I. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc. have reduced drastically whereas the performance of these devices have improved exponentially. Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. In MANET each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes. Security is a prime importance in scenarios of deployment such as battlefield in an ad hoc network. Since MANET has multi hop links, it is venerable against several attacks like black hole attack, Byzantine attack, wormhole attack etc. This paper shows the comparison of AODV, OLSR and ZRP under Black hole attack.

II. MANET ROUTING PROTOCOLS

There are three types of MANET Routing protocols: Reactive, Proactive and Hybrid. Some of the MANET Routing Protocols are explained as given below:

A. DSDV(Destination Sequence Distance Vector)

The Destination Sequenced Distance Vector (DSDV) protocol is a proactive routing protocol based upon the distributed Bellman Ford algorithm [1]. In this routing protocol, each mobile host maintains a table consisting of the next-hop neighbour and the distance to the destination in terms of number of hops. It uses sequence numbers for the destination nodes to determine "freshness" of a particular route, in order to avoid any short or long-lived routing loops. If two routes have the same sequence number, the one with smaller distance metric is advertised. The sequence number is incremented upon every update sent by the host. All the hosts periodically broadcast their tables to their neighbouring nodes in order to maintain an updated status of the network. The tables can be updated in two ways – either incrementally or through a full dump. An incremental update is done when the node doesn't observe any major changes in the network topology. A full dump is done when network topology changes significantly or when an incremental update requires more than one NPDU (Network Packet Data Unit).

B. OLSR (Optimized Link State Routing)

The Optimized Link State Routing (OLSR) protocol is described in RFC3626 [2]. OLSR is proactive routing protocol that is also known as table driven protocol by the fact that it updates its routing tables. OLSR has three types of control messages which are describe bellow.

(*a) Hello*: This control message is transmitted for sensing the neighbour and for Multi Point Distribution Relays (MPR) calculation.

(b) Topology Control (TC): These are link state signalling that is performed by OLSR. MPRs are used to optimize theses messaging.

(c*) Multiple Interface Declaration (MID):* MID messages contains the list of all IP addresses used by any node in the network. All the nodes running OLSR transmit these messages on more than one interface.

C. DSR(Dynamic Source Routing)

The Dynamic Source Routing Protocol [3] is an on-demand routing protocol which is based on the concept of source routing. In source routing, a sender node specifies in the packet header, the complete list of nodes that the packet must traverse to reach the destination node. This essentially means that every node just needs to forward the packet to its next hop specified in the header and need not check its routing table as in table-driven routing protocols.

D. AODV (Ad-hoc On-Demand Distance Vector)

The Ad hoc On-demand Distance Vector routing protocol [4] inherits the good features of both DSDV and DSR. The AODV routing protocol uses a reactive approach

to finding routes and a proactive approach for identifying the most recent path. More specifically, it finds routes using the route discovery process similar to DSR and uses destination sequence numbers to compute fresh routes.

E. ZRP (Zone Routing Protocol)

In ZRP neighbour discovery may be implemented through a separate Neighbour Discovery Protocol (NDP). Such a protocol typically operates through the periodic broadcasting of "hello" beacons. The reception of a "hello" beacon can be used to indicate the status of a connection to the beaconing neighbour [5]. Neighbour discovery information is used as a basis for the Intra-zone Routing Protocol (IARP). IARP can be derived from globally proactive link state routing protocols that provide a complete view of network connectivity. Route discovery in the Zone Routing framework is distinguished from standard broadcast-based route discovery through a message distribution service known as the Border-cast Resolution Protocol (BRP) [6]. On availability of BRP, the operation of Zone Routing's global reactive Inter-zone Routing Protocol (IERP) is quite similar to standard route discovery protocols. An IERP route discovery is initiated when no route is locally available to the destination of an outgoing data packet

III. BLACK HOLE ATTACK

Black Hole attack [7] is a kind of active attack. In this attack, Black Hole waits for neighboring nodes to send RREQ messages. When the Black Hole receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, gives a high sequence number to make entry in the routing table of the victim node, before other nodes send a true RREP. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Black Hole attacks all RREQ messages this way and takes access to all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. There are two major behaviours that Black Hole attack possesses.

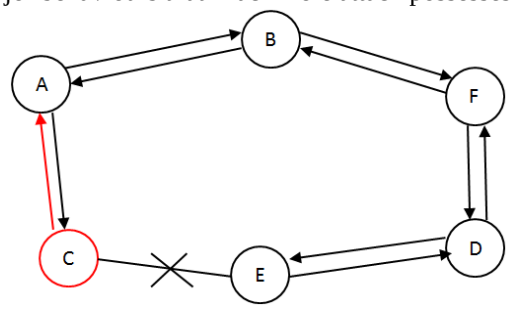

Fig. 1 Black Hole Problem

They are as follows:-

1. Black Hole node advertise itself by showing larger or highest possible destination sequence no. as we know larger the sequence [8] no. means the route is fresh and latest for a particular destination. This way malicious node bluffs the source node, who wants to initiate communication.

2. It is an active DoS attack in MANET [9], which intercepts all incoming packets from an intended source. A black hole node absorbs the network traffic and drops all packets.

The malicious node is supposed to be positioned in centre of the wireless network.

IV. NS2 SIMULATION

Ns2 is most widely used simulator by researchers; it is event driven object oriented simulator, developed in C++ as backend and OTcl as front end. If we want to deploy a network then both TCL (Tool Command Language) as scripting language with C++ to be used [11].

F. Performance Metrics

The following performance parameters are consider during the simulation of MANET routing protocol under malicious attack:

1) Packet Drop Ratio: It is the ratio of the data lost at destination to those generated by the CBR sources. The packets are dropped when the node is not able to find the valid route to the node specified as an intermediate node in the route to reach the destination node.

2) Average Delay: Represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination.

3) Throughput: This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps.

4) Packet Delivery Ratio: The ratio between the amount of incoming data packets and actually received data packets

Table I shows mobility scenarios in which we simulate MANET Routing Protocol. This simulation uses random way point model with varying number of nodes among 10 to 100. This simulation used the following parameters.

TABLE I
SIMULATION PARAMETERS

Simulator	NS-2 (version 2.35)
Simulation Time	500 (s)
Number of Nodes	10, 20, 30,.…100
Simulation Area	1000 x 1000m
Routing Protocols	DSDV, OLSR, DSR, AODV and ZRP
Traffic	CBR(Constant Bit Rate)
Pause Time	10 (m/s)
Max Speed	20(m/s)

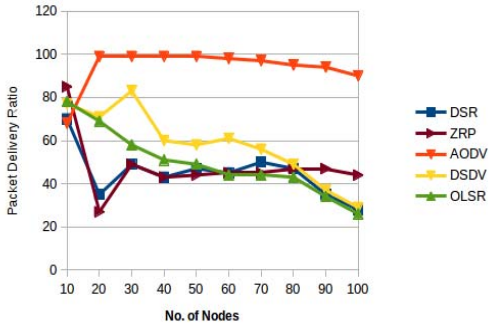

Fig. 2 Packet Delivery Ratio of DSDV, DSR, AODV, OLSR and ZRP with black hole attack

Fig. 2 shows the Packet Delivery ratio of DSDV, DSR, OLSR and ZRP under black hole attack. In this graph packet delivery ratio is highest in AODV Routing Protocol.

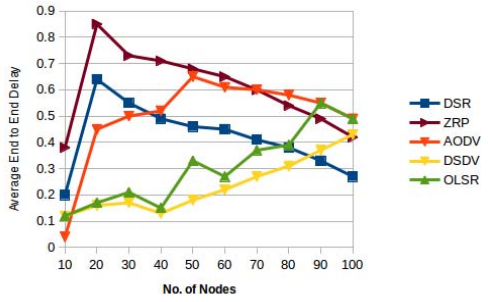

Fig. 1 Average End to End Delay of DSDV, DSR, AODV, OLSR and ZRP with black hole attack

Fig 3 shows average End to End Delay of MANET Routing Protocols. Initially ZRP has highest delay but as the number of nodes get increased the Average End to End Delay got decreases.

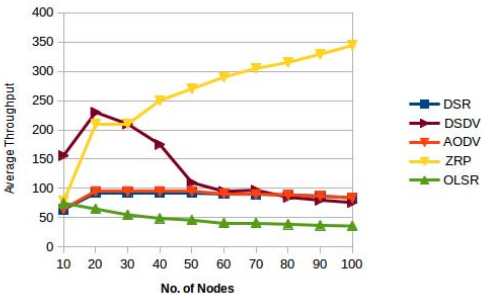

Fig. 4 Average Throughput of DSDV, DSR, AODV, OLSR and ZRP with black hole attack

In Fig 4 the throughput for ZRP with black hole is highest compared to that of AODV and ZRP. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput.

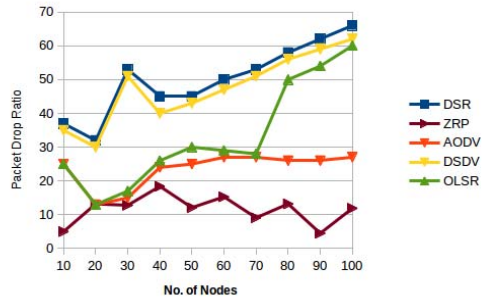

Fig.5 Packet Drop Ratio of DSDV, DSR, AODV, OLSR and ZRP with black hole attack

The Packet Drop Ratio of DSR, ZRP, AODV, DSDV and OLSR Routing Protocols under black hole attack are shown in fig 5. According to this graph ZRP has lowest Packet Delivery Ratio because ZRP has advantage of both the table driven and on demand routing protocol.

V. CONCLUSIONS

Initially when number of nodes is less the Average End to End delay is highest in ZRP and lowest in DSDV but as the number of nodes get increased ZRP has lowest End to End Delay and DSDV has highest. Average Throughput is highest in ZRP in comparison to other MANET Routing Protocols under black hole attack. When MANET Routing Protocols are compared Packet Drop Ratio is lowest in ZRP Routing Protocol. Hence ZRP is given better performance when test cases are performed on MANET Routing Protocols under Black Hole Attack.

REFERENCES

[1] E. Çayırcı, C.Rong, “Security in Wireless Ad Hoc and Sensor Networks,” vol. I. New York, Wiley, pp. 10, 2009.

[2] S. Ci et al., “Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,”IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.

[3] Zaid Ahmad, Jamalul-lali Ad Manan, Kamarularifin Abd Jalil,“Performance Evaluation on Modified AODV Protocols”, IEEE Asia-Pacific Conference on Appiled Electromagnetics, Dec. 11-13, 2012.

[4] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing. IEE Security & Privacy, pp. 28-39, 2004.

[5] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[8] Kitisak Osathanunkul and Ning Zhang” A Countermeasure to Black Hole Attacks in Mobile Ad hoc Networks” 978-1-4244-9573-3/11/$26.00 ©2011 IEEE.

[9] Hizbullah Khattak, Nizamuddin, Fahad Khurshid, Noor ul Amin,”Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash” 978-1-4673-5200-0/13/$31.00 ©2013 IEEE

[10] Ming-Yang Su, “Prevention of Selective Black hole Attacks on Mobile Ad hoc Network through Intrusion Detection Systems”, Computer Communications, 2010, pp. 21-26

[11]] Neeraj Arora, Dr. N.C. Barwar, “Performance Analysis of DSDV, AODV and ZRP under Black hole attack”, International Journal of Engineering Research & Technology (IJERT), Volume 3, Issue 04, April 2014.