International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

Performance Analysis of DSDV, AODV and ZRP under Blackhole attack

Neeraj Arora
M. E. Scholar, Computer Science Engineering Department,
M.B.M. Engineering College,
Jodhpur, India

Dr. N. C. Barwar
Associate Professor, Computer Science Engineering Department,
M.B.M. Engineering College, J.N.V. University,
Jodhpur, India

***Abstract*—A Mobile ad-hoc network (MANET) is a latest and emerging Research topic among researchers. Wireless mobile ad hoc network (or simply MANET) is a self-configuring network which is composed of several movable user equipment. These mobile nodes communicate with each other without any infrastructure, furthermore, all of the transmission links are established through wireless medium. Due to its unique characteristic like dynamic network topology, limited power and limited bandwidth for communication. MANET has more challenge compare to any other conventional network. One of the most challenging aspects is security and one of the most devastating attacks knows to MANET routing protocols is black hole attack. The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. This paper focus on analysis the performance of MANET Routing Protocols like DSDV, AODV and ZRP with or without malicious attack like black hole attack and the parameter used for performance analysis are packet delivery ratio, average throughput, average end to end delay and Packet Drop Rate using NS2.**

Keywords—MANET; DSDV; AOD;, ZRP; Blackhole attack

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. Nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages [1]. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the destination host.

In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on, unlike the conventional network. A MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [2]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network. Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task.

Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power. There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSDV, or AODV [3] [4]. More sophisticated and subtle routing attacks have been identified in recent published papers, such as the black hole (or sinkhole) [5], Byzantine [6], and wormhole [7] [8] attacks. Currently routing security is one of the hottest research areas in MANET.

II. MANET ROUTING PROTOCOLS

A. DSDV (Destination Sequence Distance Vector)

Destination-Sequenced Distance Vector (DSDV) routing protocol is a pro-active, table-driven routing protocol for MANETs. Every node will maintain a table listing all the other nodes it has known either directly or through some neighbors. Every node has a single entry in the routing table as shown in Figure.1 and Table 1. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node. Along with these details the table also keeps track of the Next-Hop neighbor to reach the destination node, the timestamp of the last update received for that node [9].

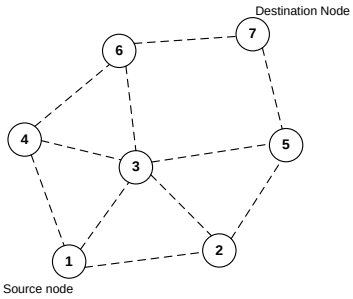

Fig. 1. Topology graph of the network

TABLE I. ROUTING TABLE FOR NODE 1

Destination	Next hop	Metric	Sequence number
1	-	0	S40_1
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	2	3	S94_7

B. *AODV (Ad-hoc On-Demand Distance Vector)*

AODV routing protocols is another reactive routing protocol, which consists of the following procedures [3]:

1. Path/Route Discovery
2. Path/Route Maintenance

AODV succeed to the concepts of Sequence number from DSDV protocols in order to retain the freshest route in the network. A RREQ (Route Request) [7] is broadcast throughout the network with a search ring technique. Upon receiving RREQ by a node which can be either destination node or an intermediate node with a fresh route to destination reacts with a RREP (Route Reply) uni- cast packet to the source node. As the RREP is routed back along the reverse path, the RREP has reach source node, a route is said to be established between source and destination node [6-7].

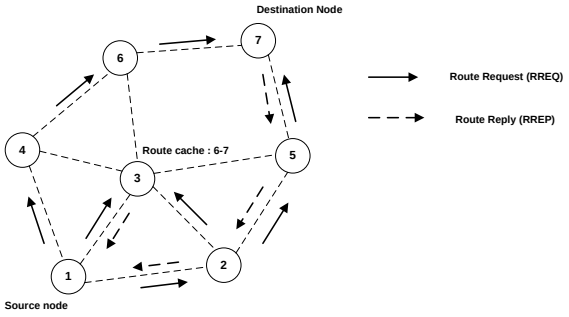

Fig. 2. Topology graph of the network

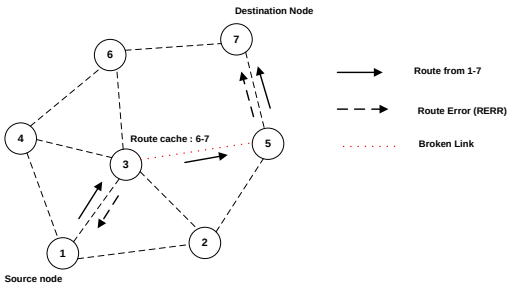

Fig. 3. Topology graph of the network

C. *ZRP (Zone Routing Protocol)*

In ZRP neighbor discovery may be implemented through a separate Neighbor 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 neighbor [12]. Neighbor 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) [13]. 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 [10] 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 behaviors that Black Hole attack possesses.

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 [10] 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 [10], 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 center 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].

A. 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.

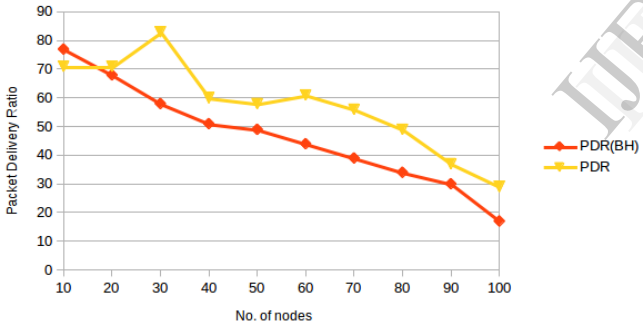

Fig. 4. DSDV: Packet Delivery Ratio with and without blackhole attack

Fig.4 shows that Packet Delivery Ratio of DSDV with blackhole attack and without blackhole attack. It is observes that blackhole attack decrease the performance of routing protocols because these malicious nodes drop the data packets.

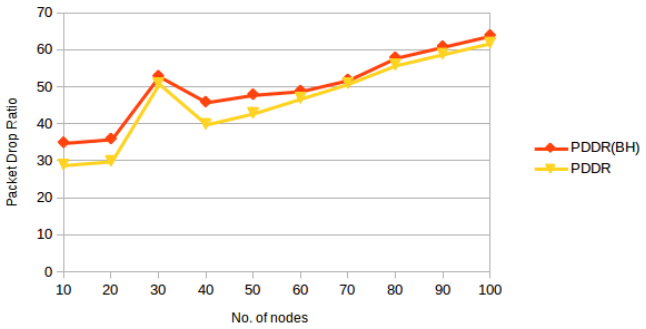

Fig. 5. DSDV: Packet Drop Ratio with and without blackhole attack

Fig.5 shows that Packet Drop Ratio of DSDV with blackhole attack and without blackhole attack. It is observes that Packet Drop Ratio is increases with number of nodes but with black hole it is much higher than without blackhole.

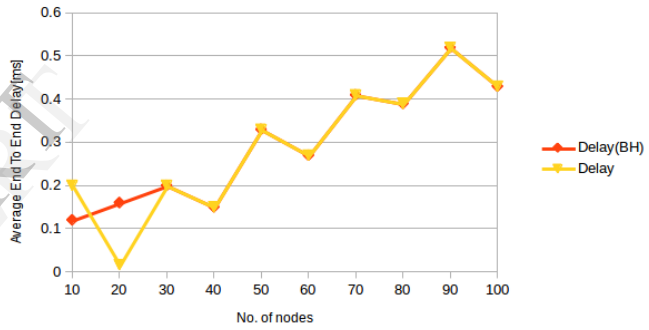

Fig. 6. DSDV: Average End to End Delay with and without blackhole attack

In case of end to end delay in Fig 6 shows that DSDV with blackhole attack have high end to end delay in presence of a malicious node as compare to that of DSDV without blackhole attack. As the routing protocols are able to adjust its changes in it during node restart and node pausing. As the number of source node increases end to end delay is also increases in routing protocols.

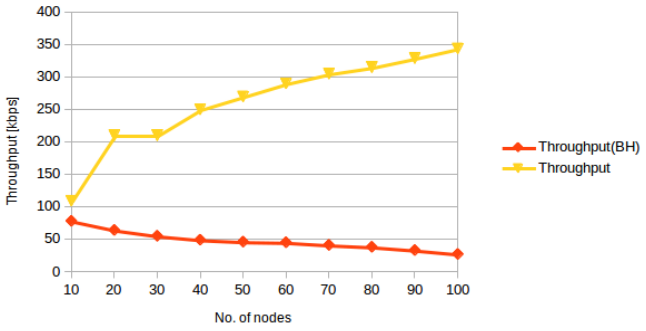

Fig. 7. DSDV: Average Throughput with and without blackhole attack

In Fig 7, it is obvious that the throughput for DSDV with blackhole is high compared to that of DSDV without attack, its throughput is higher han in the case with attack because of the packets discarded by the malicious node, Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput.

Fig 8 show that under blackhole attack the packet delivery ratio of AODV is far less than normal AODV, as compared to AODV under black hole attack.this is beacause the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination and hence it affesct Packet Delivery ratio.

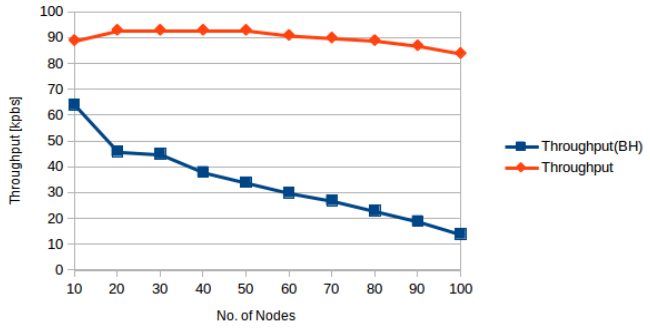

Fig. 8. AODV: Packet Delivery Ratio with and without blackhole attack

It is observed from the fig.9 that, the impact of the Black hole attack to the Networks throughput. The throughput of the network also decreases due to black hole effect as compared to without the effect of black hole attack.

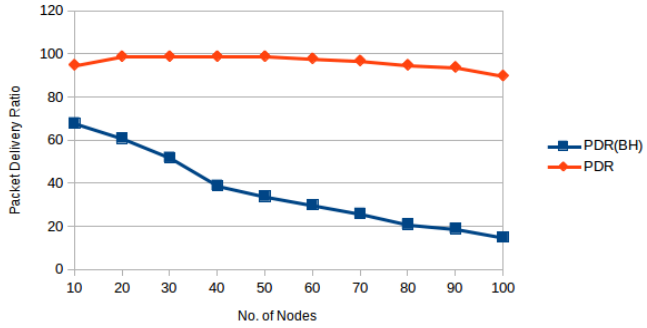

Fig. 9. AODV: Average Throughput with and without black hole

Fig.10 shows that with increasing number of nodes the Packet Drop Ratio is normally same in both case i.e. with and without blackhole, but the Packet Drop Ratio is much higher in case of blackhole attack with comapre to without blackhole.

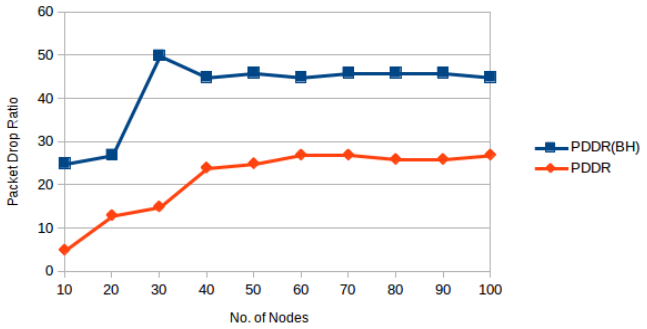

Fig. 10. AODV : Packet Drop Ratio with and witout blackhole attack

In Fig 11. Average End to End Delay of AODV routing protocol is shown. The following figure shows that the delay with blackhole is much higher than without blackhole because

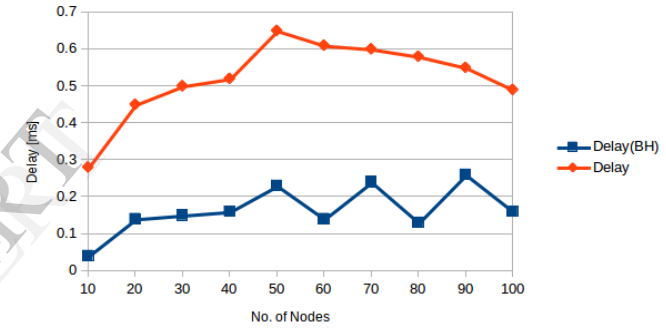

Fig. 11. AODV: Average End to End Delay with and without black hole

the packet are dropped by malicious node and AODV adjust its changes in it during node restart and node pausing thus increases the delay.

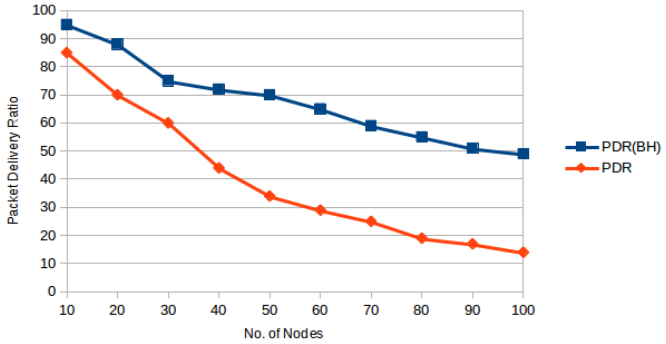

Fig. 12. ZRP: Packet Delivery Ratio with and without black hole attack

Fig 12 show two things first is as the number of nodes increase packet delivery ratio of ZRP with malicious node and without malicious node is decrease and second is the

packet delivery ratio under black hole is less than that of without blackhole.

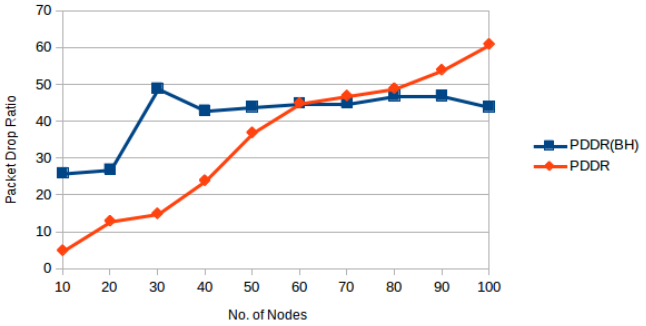

Fig. 13. ZRP: Packet Drop Ratio with or without blackhole attack

Fig.13 shows that Packet Drop Ratio of ZRP with blackhole attack and without blackhole attack. It is observes that initially Packet Drop Ratio of network under blackhole is more than without blackhole but with the increasing number of nodes the Packet Drop Ratio is just reverse of the previous case.

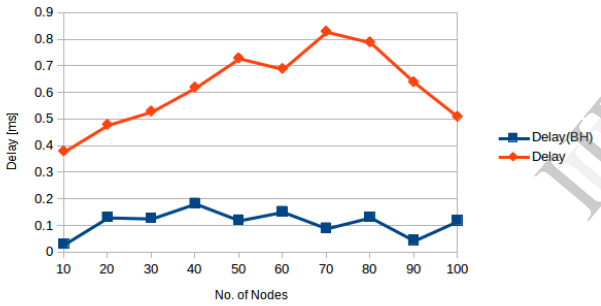

Fig. 14. ZRP: Average End to End Delay with and without blackhole attack

Simulation results in Fig 14 show that ZRP without malicious node has less end to end delay than ZRP under black hole attack. The Average End to End Delay is also incerases with increasing number of nodes in the network.

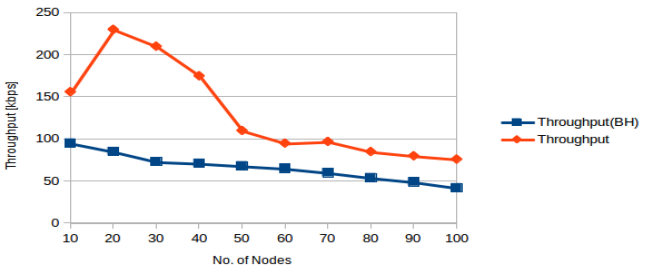

Fig. 15. ZRP: Average Throughput with and without blackhole

It is observed from the fig.15 that, the impact of the Black hole attack to the Networks throughput. The throughput of the network also decreases due to black hole effect as compared to without the effect of black hole attack

CONCLUSION

According to performance analysis of MANETS routing protocols like DSDV, AODV and ZRP with respect to different performance metrics like Packet Delivery Ratio (PDR), Packet Drop Ratio (PDRR), Throughput (Th), and End-To-End delay both with and without Black Hole attack in the network. Finally, these simulations conclude the effect of Black Hole is more on AODV protocol as compared to DSDV and ZRP.

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]] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Jtheynal of Engineeri ng Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[12] Haas ZJ, Pearlman MR, Samar P (2002) The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft

[13] Zone Routing Protocol Group [Online] Available: http://tools.ietf.org/html/draft-ietf manet-zone-zrp-04