International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 4, April 2014 ISSN 2319 - 4847

Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack

Neeraj Arora[1] and Dr. N.C. Barwar[2]

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

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

Abstract

Mobile adhoc networks (MANETs) are extensively used in military and disaster management applications. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks. One of the most devastating attacks knows to MANET routing protocols is black hole attack. This paper focus on evaluation of MANET Routing Protocols like AODV, OLSR and ZRP with black hole attack and the parameters used for this study are packet delivery ratio, average throughput, and average end to end delay using NS2 to evaluate the behaviors of these protocols under the black hole attack .

Keywords: MANET; OLSR; AODV, ZRP; Black hole attack

1. Introduction

The increasing use of mobile devices such as laptops, PDAs and mobile phones have helped in exciting applications such as virtual classrooms, rescue missions, virtual conferences, etc. Mobile ad-hoc Networking is a technology which makes all these applications anywhere. The requirement of MANET is a group of mobile nodes to self-configure and constitute a network without the need of any fixed infrastructure or a centralized controlling authority [1]. In this network, a mobile node behaves as a host and a router at the same time.

The 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.

2. MANET Routing Protocols

2.1 AODV (Ad-hoc On-Demand Distance Vector)

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

a. Path/Route Discovery b. 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].

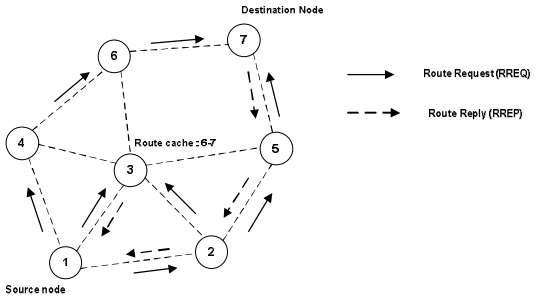

Figure 1 Topology graph of network

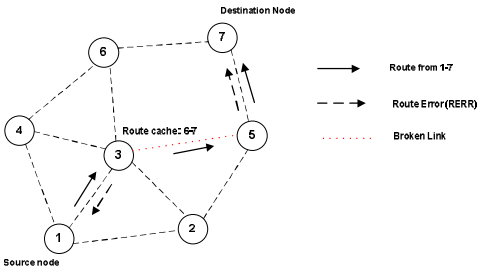

Figure 2 Topology graph of network

2.2 OLSR (Optimized Link State Routing)

Optimized Link State Routing Protocol, OLSR [4] is developed for mobile adhoc networks. It is well suited to large and dense mobile networks. It operates as a table-driven, proactive protocol, that is, it exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as "multipoint relays" (MPR) [2], [6]. MPRs, are responsible for forwarding, control traffic, declaring link state information in the network, provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required.

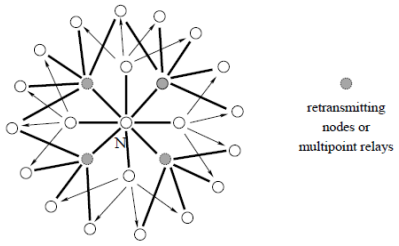

Figure 3 Topology graph of network

2.3 ZRP (Zone Routing Protocol)

ZRP routing protocol is implemented through a separate Neighbor Discovery Protocol (NDP) using neighbor discovery. This protocol typically operates 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.

3. 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 as given under.

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

4. NS2 Simulation

Ns2 is most widely used simulator by researchers; it is event driven object oriented simulator, developed in C++ as back end 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].

4.1 Simulation parameters

For simulation, we have used NS-2[2.35] network simulator [14]. Mobility scenarios are generated by using a random way point model by varying 10 to 60 nodes moving in simulation area of 1000m x 1000m. We have used the following parameters.

Table 1: Simulation parameters [14]

Simulator	NS-2 (version 2.35)
Simulation Time	500 (s)
Number of Nodes	10 to 60
Simulation Area	1000 x 1000m
Routing Protocols	AODV, OLSR & ZRP
Traffic	CBR(Constant Bit Rate)
Pause Time	10 (m/s)
Max Speed	20(m/s)

4.2 Performance Metrics

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

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

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.

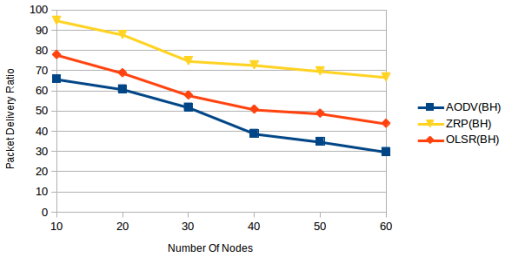

Figure 4 Packet Delivery Ratio of AODV, OLSR, ZRP under Black hole attack

Figure 4 shows the packet delivery ratio of AODV, OLSR and ZRP under Black hole attack. Simulation result shows the packet delivery ratio is decreases with increasing number of node and AODV has least packet delivery ratio under black hole attack.

Figure 5 shows the average end to end delay of AODV, OLSR and ZRP under Black hole attack. Simulation result shows OLSR routing protocol has highest delay in comparison to ZRP and AODV under black hole attack.

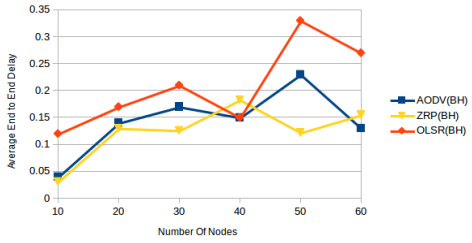

Figure 5 Average End to End delays of AODV, OLSR, ZRP under Black hole attack

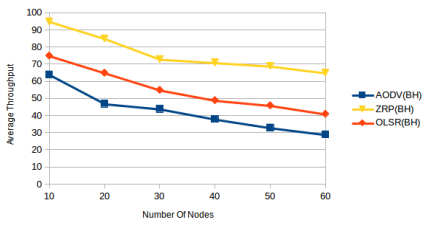

Figure 6 Average Throughput of AODV, OLSR, ZRP under Black hole attack

In Figure 6 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.

5. Conclusion

In this paper, analysis and evaluation of AODV, OLSR and ZRP protocols have been considered with respect to different performance parameters such as Average end-to-end delay, throughput and packet delivery ratio. It is noted that the performance of AODV protocol adversely affect as compared to others in different scenarios. In future work we can implement some security algorithm on these protocols to analyze the performance of these protocols to minimize attacks and make more secure under the 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. IEEE 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 Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.
[12] Haas ZJ, Pearlman MR, Samar P, The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft, 2002
[13] Zone Routing Protocol Group [Online] Available: http://tools.ietf.org/html/draft-ietf manet-zone-zrp-04
[14] 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.

AUTHORS

Neeraj Arora is currently a M.E. Scholar in Computer Science Engineering at M.B.M Engineering College. He received B.Tech in Computer Science Engineering from Jodhpur Institute of Engineering and Technology in 2011. He has published more than 5 in national and international conference and journal .His field of interest is Computer Network, Image Processing, Database Management System etc.

Dr. N.C. Barwar is currently working as an Associate Professor in M.B.M Engineering College. He received B.E. from M.N.I.T. Bhopal, M.E. in Digital Communication from M.B.M. Engineering College and PhD from J.N.V. University. He has published more than 40 papers in national and international conferences and journals and having teaching experience of more than 20 years at PG and UG levels. His field of interest is Computer Networks, Multimedia, VOD, and Information theory etc.