ISSN No. 2278-3091
Volume 2, No.3, May - June 2013
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://warse.org/pdfs/2013/ijatcse02232013.pdf

Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs

Harmandeep Singh[1], Manpreeet Singh[2]
[1]Research Scholar, Department of IT, GNDEC, Ludhiana, INDIA, harmandeol2003@yahoo.co.in
[2]Assistant Professor, Department of IT, GNDEC, Ludhiana, INDIA, mpreet78@gmail.com

ABSTRACT
MANET Routing protocols suffer from different kind of attacks on all the layers of its protocol stack. One of such attack which occurs at the network layer is Black Hole attack and the aim of this paper is to analyze the affect of Black Hole Attack under three different categories of MANETs Routing Protocol i.e. Reactive, Proactive and Hybrid namely as AODV, OLSR and ZRP. We have analyzed the performance degradation on these above mentioned protocols The performance evaluations of metrics chosen are end to end delay, throughput, when a percentage of nodes misbehave.

Keywords: MANETs AODV, OLSR, ZRP.

1. INTRODUCTION

In Mobile Ad Hoc Networks every node is an autonomous entity. In MANETs the movement of the nodes is independent of each other i.e. without any constraints imposed by any other node every node can move anywhere in the network. Nodes participating in the network are the systems or devices i.e. mobile phone, laptop, personal digital assistance, and personal computer. In MANETs[6] every node can act as host or router at the same time such that every node can sent the packets or received the packets or re-route the packets if the received packets belongs to some other node. MANETs are also vulnerable to various types of attack, such that active and passive attacks. In passive attacks, within the transmission range the attackers attempt to discover valuable information. On the other hand, active attacks attackers attempt to disrupt the operation of communication [13]. Most of the research so far has been done in the area of routing protocols [14, 9], But these routing protocols suffer from different kind of attacks one of such attack is Black Hole Attack.

2. MANET ROUTING PROTOCOLS

For deployment of MANETs several routing protocols have been proposed. The protocols differ in terms of routing methodologies and the information used to make routing decisions[6]. On the behalf of their different working methodologies, these routing protocols are divided into three different categories:

- Reactive Protocols
- Proactive Protocols
- Hybrid Protocols

Classification of these MANET Routing protocol is shown in Figure.1

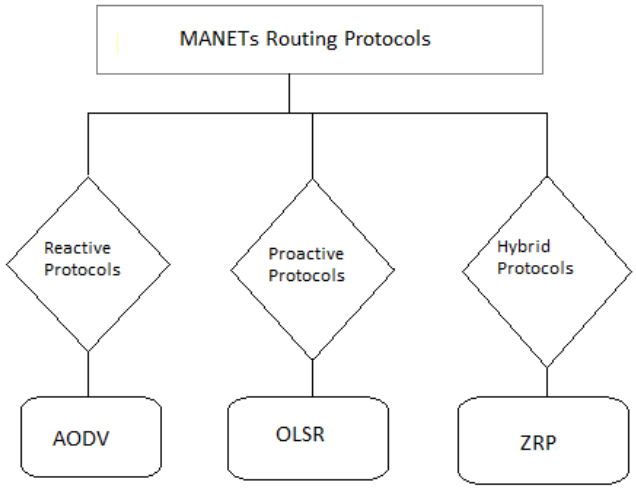

Figure 1: Categories of MANETs Routing Protocols

2.1 Reactive Protocols

Reactive Protocols are also known as, On Demand Routing Protocols because they establish routes between nodes only when they are required to route data packets.

Working of Reactive Protocol (AODV): Ad-hoc On Demand Distance Vector (AODV)[1],[2] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination, sent using UDP/IP protocols. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message[2]. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their

neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination.

2.2 Proactive Protocols

Proactive Protocols are also known as Table Driven Protocols. These protocols maintain constantly updated topology of the network. Every node in the network knows about the other nodes in advance the routing information is usually kept in number of different tables. These tables are updated according to the changes in the network.

Working of Proactive Protocol (OLSR): Optimized Link State Routing Protocol, OLSR[4] is developed for mobile ad hoc 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.

2.3 Hybrid Protocols

Hybrid Routing Protocols combine proactive protocols with reactive protocols. To provide the best path to destination network it uses the distance-vectors techniques.

Working of Hybrid Protocol (ZRP): Zone Routing Protocol Hybrid protocols exploit the strengths of both reactive and proactive protocols, and combine them together to get better results[16]. The network is divided into zones, and use different protocols in two different zones i.e. one protocol is used within zone, and the other protocol is used between them. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. ZRP uses proactive mechanism for route establishment within the nodes neighborhood, and for communication amongst the neighborhood it takes the advantage of reactive protocols. The local neighborhoods are known as zones, and the protocol is named for the same reason as zone routing protocol[16]. Each zone can have different size and each node may be within multiple overlapping zones. The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius r. The nodes whose minimum distance is less than r are interior nodes.

3. ATTACKS ON MANET ROUTING PROTOCOLS

The security attacks that jeopardize the normal working of the MANETs Routing Protocols are classified in two different categories:

1. Active Attacks
2. Passive Attacks

3.1 Active Attacks

Active attacks affect the normal operation of the network. In Active attacks, attacker actively participates in disrupting the normal operation of the network services by act as an internal node in the network[4]. Being an active part of the network, it is easy for the node to exploit and hijack any internal node to use it for malicious packets injection or denial of service. The attacker drop packets, modify packets, replay packets, fabricate messages or impersonates as some other nodes, nodes rush packets or tunnel them over high speed private networks to an accomplice in other part of the network, etc.

3.2 Passive Attacks

In Passive attack, the attacker listen to network in order to get information, what is going on in the network? In passive attacks, the attacker does not actively participate in bringing the network down. It listens to the network in order to know and understand, how the nodes are communicating with each other, how they are located in the network? Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network[4].

4. Black Hole Attack

In a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one[12]. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes[6]. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network[8]. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack

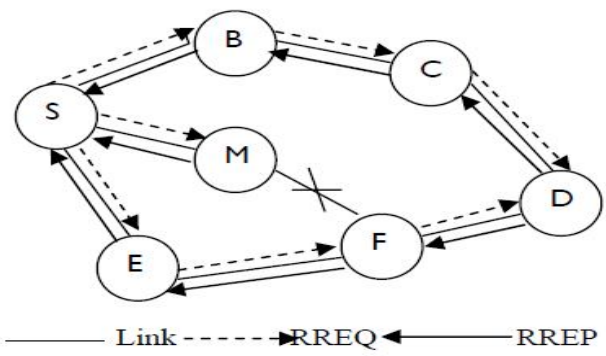

Figure 2: Black Hole Attack

In above figure 2, S and D are assumed to be source and destination nodes respectively. Let M be the malicious node. S being the source node would initiate the route discovery process and broadcasts a RREQ that is received by the nodes B, M and E being the neighbours of node S. Upon receiving the RREQ from the node S, node B and E makes a search to their cache for a fresh route to the destination. Non-availability or older entry in their route table causes nodes to rebroadcast the RREQ and this process is continued till the RREQ arrives at node D[12].

But node M claims to have the fresh route to destination and sends RREP packet to the source node S. The reply from the malicious node reaches the source node much earlier than other legitimate nodes, as the malicious nodes does not have to check its routing table[15]. Nodes those have route to the destination would update their route table with the accumulated hop count and the destination sequence number of the destination node and generate a RREP control message. The destination sequence number that determines the freshness of a route is a 32-bit integer associated with every route [8]. The malicious node claims to have a fresher route by including a very high destination sequence number in RREP packet. The source node chooses the path provided by the malicious node and starts sending the data packets, which are dropped by the malicious node.

5. SIMULATION ENVIRONMENT

For simulation, we have used NS-2[2.34] network simulator[10]. Mobility scenarios are generated by using a random way point model by varying 10 to 100 nodes moving in simulation area of 1000m x 1000m. We have used the following parameters.

Table 1: Simulation Parameters.

Simulator	NS-2 (version 2.34)
Simulation Time	500 (s)
Number of Nodes	10 to 60
Simulation Area	1000 x 1000m
Routing Protocol	AODV, OLSR & ZRP
Traffic	CBR (Constant Bit Rate)
Pause Time	10 (m/s)
Max Speed	20 (m/s)

The metrics used to evaluate the performance are given below.

i) *Packet Delivery Ratio:* The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

ii) *Throughput:* It is the total number of received packet per unit time. In another term, throughput is the packet size (in term of bits) that is going to be transmitted divided by the time that is used to transmit these bits.

iii) *Average End to End Delay:* This is defined as the delay between the time at which the data packet was originated at the source and the time it reaches the destination.

6. SIMULATION RESULTS

After taking into consideration the simulation parameters mentioned in Table 1 we came across the following results:

Table 2: Simulation Results of AODV under Black Hole attack.

Protocol	Number of Nodes	Packet Delivery Ratio	Average End to End Delay	Throughput %
AODV	10	66	0.04	64
	20	61	0.14	47
	30	52	0.17	44
	40	39	0.15	38
	50	35	0.23	33
	60	30	0.13	29

Table 3: Simulation Results of OLSR under Black Hole attack.

Protocol	Number of Nodes	Packet Delivery Ratio	Average End to End Delay	Throughput %
OLSR	10	78	0.12	75
	20	69	0.17	65
	30	58	0.21	55
	40	51	0.15	49
	50	49	0.33	46
	60	44	0.27	41

Table 4: Simulation Results of ZRP under Black Hole attack.

Protocol	Number of Nodes	Packet Delivery Ratio	Average End to End Delay	Throughput %
ZRP	10	95	0.031	95
	20	88	0.13	85
	30	75	0.126	73
	40	73	0.183	71
	50	70	0.122	69
	60	67	0.155	65

7. CONCLUSION

In this paper, we have analyzed the Black hole attack on AODV, OLSR and ZRP with respect to different performance parameters such as Average end-to-end delay, throughput and packet delivery ratio. We conclude the effect of black hole attack is more on AODV protocol as compared to others. In future work we can implement some security algorithm on these protocols to avoid the black hole attack.

ACKNOWLEDGEMENT

I express my sincere gratitude to my guide Mr. Manpreet Singh, for his valuable guidance and advice. Also I would like to thanks all the faculty members and colleagues for their continuous support and encouragement.

REFERENCES

1. Mohammad Ilyas, **The Handbook of Ad Hoc Wireless Networks**.
2. Amitabh Mishra, **Security and Quality of service in Ad Hoc Wireless Networks (chapter 1, 3)**, *Handbook* ISBN- 13 978-0-521-87824-1.
3. T. P. Singh, Neha and V. Das, **Multicast Routing Protocols in MANETs**, *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, Vol. 2, JAN. 2012.
4. Harmandeep Singh, Gurpreet Singh and Manpreet Singh, **Performance Evaluation of Mobile Ad Hoc Network Routing Protocols Under Black Hole Attack**, *International Journal of Computer Applications*, Vol. 42(18):1-6, March 2012..
5. W.R. Salem Jeyaseelan and Shanmugasundaram Hariharan, **Investigation on Routing Protocols in MANET**, *International Journal of Research and Reviews in Information Sciences (IJRRIS)*, Vol. 1, No. 2, pp. 80-84, 2011.
6. Priyanka Goyal, Vinti Parmar, Rahul Rishi, **MANET: Vulnerabilities, Challenges, Attacks, Application**, *International Journal of Computational Engineering & Management (IJCEM)*, pp. 32-37, 2011.
7. LathaTamilselvan, Dr.V.Sankarayanan, **Prevention of Black hole Attack in MANET**, *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, IEEE*, 2007.
8. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, **Detecting Blackhole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method**, *International Journal of Network Security*, Vol.5, No.3, PP.338–346, Nov 2007.
9. Li, H., Singhal, M., **A Secure Routing Protocol for Wireless Ad Hoc Networks**, *HICSS' 06: Proceedings of the 39th Annual Hawai International Conference on System Sciences*, page 1-10, 2006.
10. Al-Shurman, M., Yoo, S., Park, S., **Black hole Attack in Mobile Ad Hoc Networks**, *ACM Southeast Regional Conference*, pp. 96-97, 2004.
11. H. Deng, W. Li, Agrawal, D.P., **Routing security in wireless Ad-Hoc networks**, IEEE *Communications Magazine*, Vol.40, pp.70- 75, ISSN: 0163-6804, Oct. 2002.
12. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, **Detecting black hole attack on AODV based mobile Ad hoc networks by dynamic learning method**, *International Journal of Network Security*, Vol. 5, no. 3, pp. 338–346, 2007.
13. Westhoff, D., Paul K, **Context Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks**, *IEEE GLOBECOM. Taipei, Taiwan*, pp. 178-182, 2002.
14. Candolin, C. Kari, H. H., **A Security Architecture for Wireless Ad Hoc Networks**, 1095-1100, 2002.
15. Bo, M. S., Xiao, H., Adereti, A., Malcolm, A. J., Christianson, B., **A Performance Comparison of Wireless Ad hoc Network Routing Protocols under Security Attack**, *Third International Symposium on Information Assurance and Security*, pp. 50-55, 2007.
16. Ravilla Dilli, Putta Chandra Shekar Reddy, **Energy Management in Zone Routing Protocol (ZRP)**, *International Journal of Emerging Technology and Advanced Engineering*, Volume 2, Issue 5, May 2012.