IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. IV (Mar – Apr. 2015), PP 89-93
www.iosrjournals.org

Performance measurement of MANET routing protocols under Blackhole security attack

Md. Humayun Rashid[1], Md. Rashedul Islam[2]

[1]*Lecturer, Department of Computer Science &Eng, IUBAT-International University of Business Agriculture & Technology, Bangladesh.*

[2] *Lecturer, Department of Computer Science &Eng, IUBAT-International University of Business Agriculture & Technology, Bangladesh.*

Abstract: *Unlike wired networks or other wireless networks, where the nodes communicate with each other via an access point or a base station, wireless Mobile ad hoc network is an infrastructure less network where the network is formed out of randomly moving nodes. The nodes in a Mobile ad hoc network work as a host as well as a router. Since there is no centralized management and the network is formed only by the participating node's cooperation, Mobile ad hoc network (MANET) faces numerous security challenges. Out of many security attacks Blackhole attack is one of the severe one. A Blackhole attack is a Denial-of-service attack. In a request response based route discovery method, a Blackhole node advertises itself as a node that has the shortest route to the destination. It can drop all the packets that it is supposed to relay to the destination. In this paper, we evaluate the performance of one reactive protocol (AODV), one proactive protocol (OLSR) and a hybrid protocol (ZRP). In order to find out the intensity of Blackhole attack on MANET, we take these three routing protocols and check the performance of these protocols with and without attack. We compare the resultto see which class of protocol is more challenged by the attack. We used OPNET 15.0 simulator to measure the performance of these routing protocols in different performance metrics. After the simulation was run, we found that the performance of these protocols get worse under Blackhole attack and the performance of AODV outweigh both OLSR and ZRP.*

Keywords:*MANET,AODV,OLSR,ZRP,BLACKHOLE,Security*

I. Introduction

Mobile Ad-Hoc network is an autonomous system where nodes/stations are connected with each other through wireless links [2]. Nodes are free to join or leave the network at any time. Main reasons behind the popularity of MANET are infrastructure less design approach, active nature and effortlessness in deployment. Analyzing, reading and researching on routing in networks are the key investigation fields. Routing protocols of MANET is deriving the attraction of researchers because of their challenging behavior in terms of security and ability of performing smart responsibilities.

Protocols in MANET are classified into i. Reactive ii. Proactive iii.Hybrid [2]. Reactive protocols do not commence route discovery until they are requested i.e. AODV [1].Proactive protocols works other way of reactive protocol and it constantly maintain the updated topology of the network i.e. OLSR. On the other hand, the hybrid routing protocols combine the advantages of both reactive routing protocols and the proactive routing protocols i.e. ZRP. In this paper we are going to work with one reactive protocol (AODV) one proactive protocol (OLSR) and one hybrid protocol (ZRP).

1.1 Ad Hoc On-Demand Vector Routing (AODV)

This protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only between nodes which need to communicate [3]. It allows its nodes to find routes rapidly for the entire unidentified and newer ends which are not in the existing communication or navigation of the packets. This entire operation mechanism is loop free. Nodes are allowed to response in other links breakages. Whenever the link broken is reported the AODV cause the affected set of the nodes to be notified so that they avoid the node which is not in the communication cycle [4]. In order to detect and manage neighboring nodes a simple hello message [4] is used. Whenever there is no "fresh enough" route is detected it broadcast a route request (RREQ) [3] to its neighbors. When neighboring node get RREQ then they reply through route reply (RREP) [3]. RREQ and RREP help AODV to establish bidirectional route and the shortest path between the nodes are updated. The AODV routing protocol builds on the DSDV algorithm [3] which minimizes the number of required broadcast by creating routed on an on demand basis.

DOI: 10.9790/0661-17248993

1.2 Optimized Link State Routing (OLSR) Protocol

Optimized link state routing protocol [10] is a proactive routing protocol where the routes are immediately available when needed. In OLSR any changed occurred in topology than it causes topological information flooding to all available hosts in the network because it is an optimization version of pure link state protocol. By reducing the maximum time interval for periodic message transmission OLSR may optimize the reactivity to topological changes. As OLSR maintains routes to all destinations to network, traffic patterns are benefited by the protocol where a large subset of nodes are communicating with another large subset of nodes and where source and destination changes over time. The application does not permit delays for a long time for in transmission of data packet is well suited for OLSR. A dense network is the perfect environment for OLSR because on dense network most communication determined between the large numbers of nodes.

1.3 Zone routing protocol (ZRP)

The Zone routing protocol is a hybrid protocol that is composed of the nature of the reactive protocol that seeks the routes towards the destination out of the zone [11] and of the proactive link state routing protocol that works within the zone and manages the entire route in it. The hybrid nature of this protocol allows it to use both reactive protocols and proactive protocols for sending information throughout the network.

Packet destined for a node in the same zone as the originator, are sent with the help of the proactive protocol where an existing routing table is used for immediate packet delivery. Whereas, a reactive protocol is used to confirm if a destination is outside the originating zone. The reactive protocol does it by checking every successive zone in the route in order to see whether the destination node is outside or inside the zone. Is this way the processing overhead is reduced for those routes. Also, the control overhead is reduced for longer routes which would be an issues if the proactive routing protocols were used, while the routing delay is eliminated with in a zone that would arise from the route discover process of the reactive routing protocols.

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Different types of attacks effects tremendously on their performance. Basically attack in MANET is classified [5] as

I. Active attack
II. Passive attack

In this paper we are going to discuss about the effect of one active attack (Black hole attack) over AODV, OLSR and ZRP protocols.

1.4 Black Hole Attack

Black hole attack is a denial of service attack [8] in which malicious node sends fake information by claiming that it has a fresh or shortest route to destination route. Result of selecting this path for sending data packets by the source node is data misuse or discarded. One RREQ message is broadcasted by the source node, the black hole node immediately response with RREP message and source assume that the destination is behind the black hole and avoids other RREP packets coming from other trusted nodes [7]. By assigning a high sequence number malicious node performs this task [6]. Now attacker will drop the received message and will not broadcast according to protocols need. Therefore the quantity of information on other nodes is reduced. This malicious node is called black hole node [9].

II. Methods:

The aim of this project is to analyze the performance comparison of the chosenrouting protocols under Blackhole attack and to see which protocol is more affected by the attack and results in less data delivery when there's a variation in node mobility speed. Also, we needed to see the effect of the presence of the malicious node on the network and how it disrupts the normal operation of the network. To achieve the desired goals, the basic method was to create three scenarios with normal operational parameters for the reactive, proactive and hybrid routing protocols. And then, each of the scenarios was duplicated and few malicious nodes were added in the duplicated scenarios. The whole idea was to check the performance of the reactive protocol (AODV), the pro-active routing protocol (OLSR) and the hybrid protocol (ZRP).

2.1 Performance Metrics

To evaluate the performance of the Routing protocols, the following quantitative metrics were chosen.

2.1.1 Network load: It is the total amount of traffic received by the network, from the MAC layer, which is queued for transmission. It represents the data traffic in bits/sec.

2.1.2 End to End delay: End to end delay is the time that a packet takes to reach the destination from the sender. Delay occurs from the source throughout the intermediate nodes towards the destination. For example, route discovery process, queuing at the interfaces, buffering, retransmission etc.

2.1.3 Packet delivery ratio: It is the ratio of the successful data received at the destination over the number of data packets generated. It measures the reliability of the protocol in action.

III. Simulation environment setup and Study

In this section, the total description of how the simulation was carried out and how the different scenarios were created with their associated parameters were given. We used OPNET network simulator 15.0 to carry out our tasks. Simulation was run for 1000 seconds of simulation time. The nodes were made to form Ad hoc networks in a 1000 × 1000 m rectangular area. Six scenarios of the same measurement were created with 40 mobile nodes in each of them. In order to find out the effect of mobility on the protocols, each node's speed was varied using seven values of 10, 20, 30, 40, 50, 60, 70m/s. The node mobility speed depends on the increase in the speed value. Each node was assigned with a pause time of 1 second. We usedFTP application for heavy file transfer in the network. At first, three scenarios were created to see the normal operation of each protocol. Then, each of the three scenarios was duplicated and malicious nodes were injected with the properties of a Blackhole node in each of the duplicated scenarios. In this simulation, the Blackhole nodes generate a number between 15 and 150 randomly. The Blackhole node adds the generated random value in to the sequence number of RREQ and then it also generates the sequence number in RREP.

Table-1: The different parameters used in the network simulation

Model family	MANET
Routing protocols	AODV, OLSR,ZRP
Network scale	Campus
Technology	WLAN(Ad HOC)
Operational mode	802.11b
Simulation area	1000 × 1000 m
Simulation time	1000 seconds
Number of scenarios	6
Number of nodes in each scenario	40
Attacker nodes	10
Node speed/mobility	10-70 m/s
Pause time	1 sec
Trajectory	Vector
Packet inter arrival time	Exponential(1)
Packet size(bits)	Exponential (1024)
Data rate	15 Mbps
Default transmitting power	.005 watts

IV. Result analysis

In this section the results based on the simulations have been shown. The results are given in the following figures were evaluated using OPNET.

Network load:

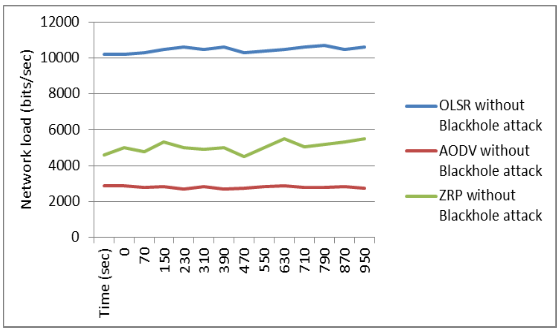

Fig-2: Network load of AODV, OLSR & ZRP (without attack).

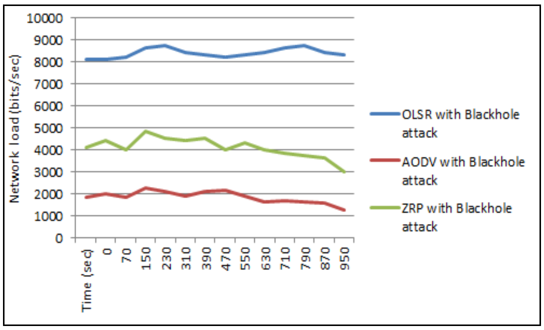

Fig-3: Network load of AODV, OLSR & ZRP (with attack).

End to End delay:

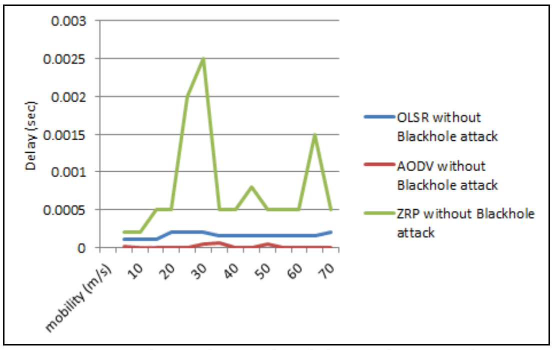

Fig-3: Delay with varied mobility without attack.

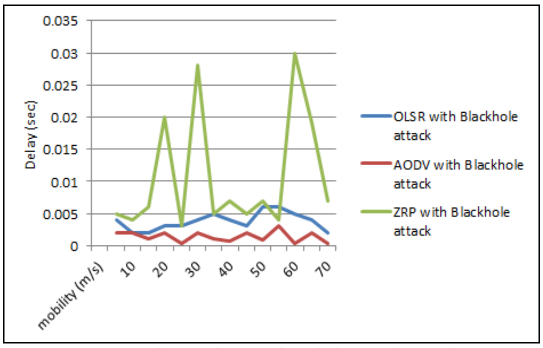

Fig-4: Delay with varied mobility with attack.

Packet delivery ratio:

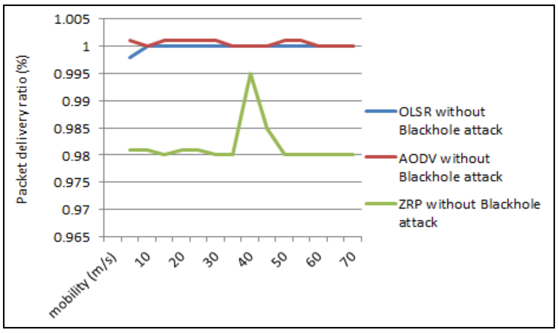

Fig-5: Packet delivery ratio without attack.

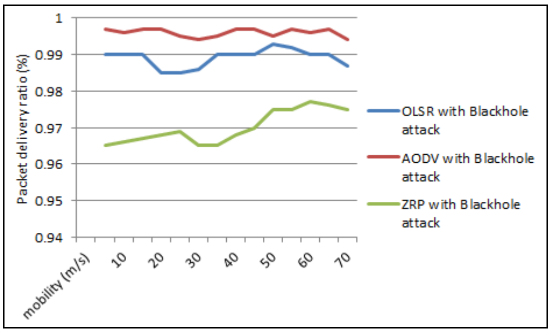

Fig-6: Packet delivery ratio with attack.

4.1 Network load:

As can be seen from the figures above, without the Blackhole attack in the network, OLSR outperforms both ZRP and AODV in terms of network load. AODV shows the least network load in the network. Since the mobile network influences change in link state and results in broadcasting of Topology control (TC) messages and Hello messages for finding neighboring hosts and link status, OLSR has highest load comparing to the other two protocols. Also OLSR's table driven approach also puts pressure on the network load as its frequent update and maintenance of the network increases overhead. While comparing to the other two protocols, AODV shows minimum load.

The performance of all three protocols in terms of network load gets affected by the presence of the malicious nodes in the network. OLSR shows a little drop in network load that is because some of the traffic it sends and receives for maintenance of the network is diverted to the Blackholenodes.The order of the network load remains the same with OLSR having the maximum network load and ZRP having more network load than AODV. Even though both AODV and ZRP have less network load, their network load tends to drop with time.

4.2 Delay:

From the above figures for End-to-End delay, it is clear that without the Blackhole nodes in the network, delay of both AODV and OLSR is around only 0.1 millisecond and 0.25 milliseconds respectively, since, AODV and OLSR use HELLO messages to determine any link outages. AODV also takes less connection setup time comparing to the other protocols. Whereas ZRP actually shows more delay variation than AODV and OLSR as the node mobility increases.

In the presence of Blackhole nodes in the network,all the protocols exhibit more delay. The AODV protocol starts its operation at a fluctuating 2ms delay whereas the OLSR protocol reaches more than 5ms as the node mobility increases. The ZRP protocol takes the most delay at approximately 50ms.

4.3 PDR:

As seen from the above results, without the Blackhole attack taking place in the scenario, AODV and OLSR maintain a packet delivery rate that is almost 100% even thought there was an increased mobility. With a packet delivery rate of a staggering 98% packet delivery rate ZRP comes behind. This is because in order to maintain neighbor connectivity both AODV and OLSR use HELLO message and to maintain links. Therefore they have such impressive results.

On the other hand the packet delivery ratio for all the three protocols drops in presence of the malicious nodes in the network. The packet delivery ratio drops, as some traffic is misled towards the Blackhole nodes. It is also noticed that even though AODV and OLSR had almost the same performance without the presence of the malicious nodes in the network, but with the malicious nodes disrupting, AODV does better at delivering packet comparing to OLSRwhereas, packet delivery ratio of ZRP increases slightly as the node mobility increases.

In terms of the performance of individual routing protocols it can be said that in terms of Network load, End-to-End delay and Packet delivery ratio, AODV is a better protocol because of its nearly consistent performance under attack.

V. Conclusion

To get a more accurate result, the same performance comparison can be done using different node density. Different performance metrics can be chosen to identify the better performing protocol under attack. The simulation study on more pro-active, reactive and hybrid protocols can be done for a better comparison. The other attack such as Wormhole attack, jellyfish attack, routing table overflow attack can be studied to see the effects of them routing protocols and to find out which protocol is more harmful than the other. In future we wish to come up with algorithms for all three protocols that will ensure performance consistency under attack.

References

[1]. Esmaili H.A., KhalijiShoja M. R, Gharaee "Performance Analysis of AODV under Black Hole attack through use of OPNET simulator", World of Computer Science and Information Technology Journal (WCSIT), ,ISSN: 2221-0741,Vol. 1, No. 2, 49-52, 2011

[2]. Ullah I.,Rehman S. "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis, Electrical Engineering, Thesis no: MEE 10:62,June, 2010

[3]. Das R. Dr. Purkayastha B.S., Dr. Das P. "Security Measures for Black Hole Attack in MANET: An Approach" International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 4 Apr 2011

[4]. Chowdhury A.,Kunal "Performance Evaluation of AODV under Blackhole Attack", International Journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN 2250-2459,Volume 2, Issue 5, May 2012

[5]. Singh H., Singh G., Singh M., "Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack" , International Journal of Computer Applications (0975 – 8887), Volume 42– No.18, March 2012

[6]. Roopak M, Dr. Reddy B., "Performance Analysis of Aodv Protocol under Black Hole Attack", International Journal of Scientific & Engineering Research, ISSN 2229-5518 Volume 2, Issue 8,August-2011

[7]. Dokurer, S.; Ert, Y.M.; and Acar, C.E. (2007). "Performance analysis of adhoc networks under blackhole attacks". SoutheastCon, 2007, Proceedings IEEE, 148 – 153.

[8]. Kaur H., Bala M., Sahni V., " Study of Blackhole Attack Using Different Routing Protocols in MANET" , International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, July 2013

[9]. Bhole A. T., Patil P. N., "Study Of Blackhole Attack In MANET", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754,Volume 2, Issue 4, October 2012

[10]. Ade S. A., Tijare P. A.," Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks", International Journal of Information Technology and Knowledge Management,July-December 2010, Volume 2, No. 2, pp. 545-548

[11]. J Hsu, S Bhatia, M Takai, R Bagrodia "Performance of mobile ad hoc networking routing protocols in realistic scenarios, Military Communications Conference". MILCOM '03. IEEE (Volume:2), 2003