Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack

Harmandeep Singh
RIMT-IET, Mandi Gobindgarh
Punjab, India

Gurpreet Singh
GNDEC, Ludhiana Punjab,
India

Manpreet Singh
GNDEC, Ludhiana Punjab,
India

ABSTRACT
There are several routing protocols that have been proposed for the possible deployment of MANETs in many fields like military, government and commercial applications. While the routing aspects of MANETs are already well understood but the research activities about the security in MANETs are still at their beginning. This paper focuses on the performance investigation of reactive and proactive MANET routing protocols, namely, AODV and OLSR, under Black-Hole Attack. The performance evaluations of metrics chosen are end to end delay, retransmission attempts, network load and throughput, when a percentage of nodes misbehave. It is evaluated that it is difficult to detect Black Hole attack, on the basis of the performance of the network.

Keywords
MANET, Black Hole attack.

1. INTRODUCTION
Mobile Ad Hoc Networks is a decentralized system in which every node is an autonomous entity. The movement of the nodes in MANETs is independent of each other, such that, every node can move anywhere in the network without any constraints imposed by any other node in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network. Every node in MANETs can act as host or router at the same time such that every node can receive the packets or sent the packets or re-route the packets if the received packets belongs to some other node. As the MANETs are expanding day by day security in MANETs is becoming the biggest concern for researchers. As in traditional networks MANETs are also vulnerable to various types of attack, such that active and passive attacks. In passive attacks, the attackers attempt to discover valuable information within their transmission range. On the other hand, active attacks attempt to disrupt the operation of communication attempt to disrupt the operation of communication [14]. Most of the research so far has been done in the area of routing protocols [4, 8]; although in recent year's security issues have also been explored. Some secure routing protocols have been proposed to protect routing messages and prevent attackers from either modifying these messages or injecting harmful routing messages into the network [3, 5, 8, 14].

2. MANET ROUTING PROTOCOLS
Several routing protocols have been proposed for the successful deployment of Mobile Ad Hoc Networks (MANETs). The protocols differ in terms of routing methodologies and the information used to make routing decisions. On the behalf of their different working methodologies, these routing protocols are divided into three different categories:

- Reactive Protocols
- Proactive Protocols
- Hybrid 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. When a route required by a source node to a destination for which it does not have route information, it starts a route discovery process, which goes from one node to another node until it arrives at the destination or a nodes in-between has a route to the destination. Reactive Protocols are generally considered efficient, where the route discovery is required to be less frequent. This makes the reactive protocols more suitable to the network with light traffic and low mobility. Normally, reactive protocols,

- Do not find routes until demanded.
- When tries to find the destination "on demand", it uses flooding technique to propagate the query.
- They consume bandwidth only, when the node start transmitting the data to the destination node.

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 keeping it simple, the whole network is known to all the nodes making that network. All the routing information is usually kept in number of different tables. Whenever, there is a change in the network topology, these tables are updated according to the changes. The nodes exchange topology information with each other, so that they can have route information any time when they needed. Proactive Protocols,

- Store all the routing information in the route cache in the form of tables.
- Maintain regular and up to date routing information about each node in the network by propagating route updation at fixed time intervals throughout the network or when there is a change in network topology.
-

2.3 Hybrid Protocols

Hybrid Routing Protocols combine proactive protocols with reactive protocols. They use distance-vectors for more precise metrics to establish the best paths to destination networks. Each node in the network has its own routing zone, the size of which is defined by a zone radius, which is defined by a metric, such as the number of hops. Each node keeps a record of routing information for its own zone. In Hybrid Protocols,

- Routers only maintain information about the adjacent routers.
- During reactive operation, sources initiate the establishment of routes to a given destination on demand.

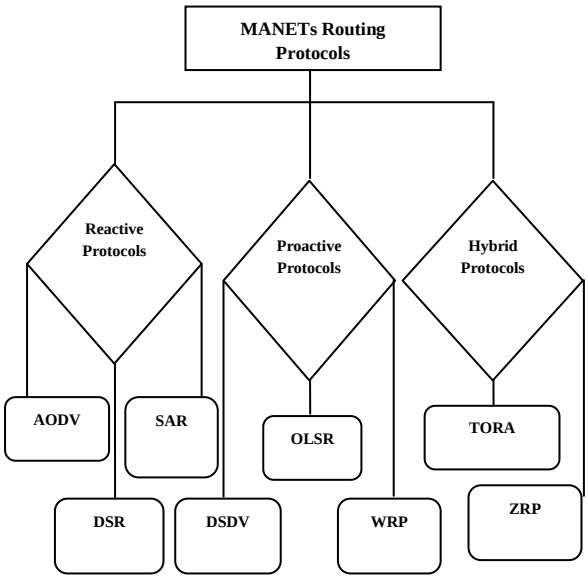

Fig. 1 Categories of MANET routing protocols

3. POSSIBLE ATTACKS ON ROUTING PROTOCOLS

In this paper, we are primary concerned about the security attacks that jeopardize the normal working of the MANET Routing Protocols. These attacks are classified in two different categories:

1. Active Attacks
2. Passive Attacks

3.1 Active Attacks

Active attacks are the attacks that 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. 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. ROUTING MISBEHAVIORS

Misbehavior of nodes has been used to distinguish nodes in a network that are under security attack. Previous work was pointed out only one type of misbehavior: selfish behavior [16]. Selfish nodes use the network but do not cooperate, such that, saving battery life for their own communication. These nodes do not intend to directly damage other nodes. In the previous paper [16], three types of behaviors of the nodes are defined:

1. Type 0 well-behaving nodes: Nodes behave nicely according to a routing protocol, including, route discovery, route maintenance, and packet forwarding and receiving.

2. Type 1 selfish nodes: In this type, a selfish node does not perform packet forwarding. So, every packet sent to these nodes to forward is dropped. Thus, it disables the packet forwarding function for all packets.

3. Type 2 selfish nodes: In this model, a node does nothing with the packet sent to it; thereby no execution function is performed. The selfish node can be considered as a rest node inside the network, since it stops contributing to the network maintenance, routing discovery, nor packet forwarding and receiving.

New type of nodes are defined as the type 3 nodes [3] showing malicious behavior. Malicious nodes aim at damaging the working of other nodes by causing network outage by partitioning the network, by flooding the network, by sending forged routing packets, by replication of stale packets, etc. In this paper, new type of node, type 4 is introduced. These nodes are also showing a kind of malicious behavior caused by Black Hole attack. A type 4 node, advertises itself for having the shortest path to the destination node. This attacker node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.

5. NETWORK SIMULATION

Simulation Modeling is becoming an increasingly popular method for network performance analysis. The research is carried out using discrete event simulation environment software, known as OPNET (Optimized Network Engineering Tool) Modeler version 14.5. It is one of the most widely used commercial simulators based on Microsoft Windows platform. The simulation focused on the performance of the routing protocols under security attacks. Two types of network scenarios are designed: high density and low density networks. In the case of Black Hole attack, low density network consist of 80 nodes and high density network consist of 150 nodes. In the case of low density network, 10 nodes are misbehaving and for high density network 20 nodes are

misbehaving. Fig. 2 shows the scenario of low density network under Black Hole attack.

The nodes are randomly placed within certain gap from each other in 800×800 m campus. The constant File Transfer Protocol (FTP) and video conferencing traffic was generated in the network explicitly i.e. user defined via Application and Profile Configuration. The transmitter and receiver parameters are configured with defining RX-Group in the network. The simulation time was set to 600s and used optimized kernel to make the simulation faster.

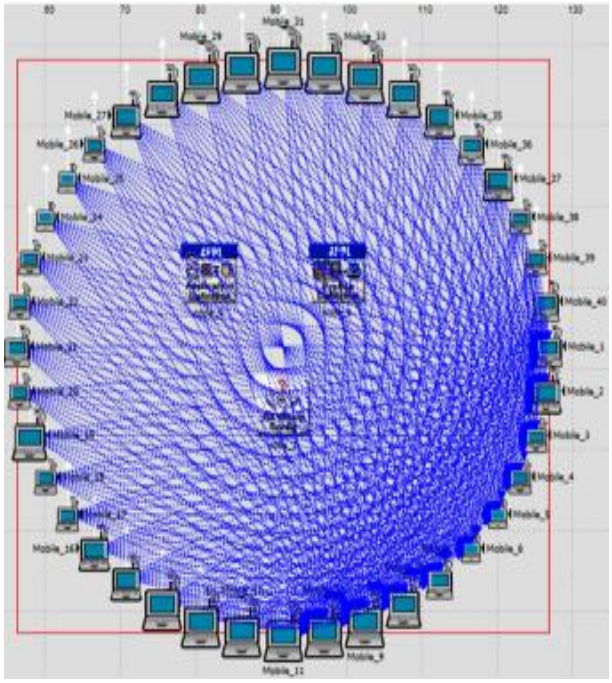

Fig. 2 Black Hole Attack Scenario

5.1 Application Configuration

A heavier application traffic flow in the network was generated, which each node will be processing from the respective application server in the network. The application traffic generated was as, FTP Application: High Load and Video Conferencing: High Resolution Video.

Table 1. FTP Application Parameters [15]

Command Mix (Get/Total)	0%
Inter Request Time (seconds)	Constant (3600)
File Size (bytes)	Constant (15000000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort (0)
RSVP Parameters	None
Back End Custom Application	Not Used

In addition, to allow more traffic flow in the network, video application was also configured using default values available in OPNET for higher resolution video.

5.2 Profile Configuration

The profile configuration for each application was defined as, Operation Mode: Serial (Ordered) and Start Time: 55 seconds. In addition, the FTP application start time, was set to constant 5 seconds of time period and the video application start time, was set to constant 75 seconds. The constant mode of application traffic was selected so as to generate Constant Bit Rate (CBR) traffic flow in the network.

5.3 Wireless parameters

The wireless parameters are common to all of the two routing protocols as shown in table 2

Table 2. Wireless LAN Parameters

Wireless LAN MAC Address	Auto Assigned
BSS Identifier	Auto Assigned
Physical Characteristics	Direct Sequence
Data Rate (bps)	11 Mbps
Channel Settings	Auto Assigned
Transmit Power	0.030
RTS Threshold	None
Buffer Size (bits)	102400000
Large Packet Processing	Fragment

6. PERFORMANCE METRICS

For the comparison of protocols under the various security attacks, four different metrics have been chosen:

6.1 Delay (sec)

This is the average end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network. The lost packets are not included in this measurement because the delay of the lost packets is infinity.

6.2 Network Load (bits/sec)

Represents the total load (in bits/sec) submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network.

6.3 Retransmission attempts (packets)

Total number of retransmission attempts by all WLAN MACs in the network, until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit.

6.4 Throughput (bits/sec)

Also known as packets delivery ratio or normalized throughput. It is the ratio of the number of packets received by the CBR sink to the number of packets sent by the CBR source.

7. SIMULATION RESULTS AND ANALYSIS

7.1 Delay

Fig. 3 shows the end to end delay in a low density network (80 nodes) under black hole attack configured by using AODV protocol and OLSR protocol. It is concluded that in the case of AODV protocol, delay is decreased by 68.26% while in the case of OLSR protocol this decrement is of 20% because in black hole attack, the malicious nodes sit in between the actual sender and receiver and creating the illusions to each

other. So during the path creating process, the malicious node sends reply quickly than the real destination and pretends to be a real destination. So, sender begins to send the data which is received by the malicious node. That's why; the average end to end delay of the network is decreased for both high density and low density network cases. But in both cases AODV protocol shows more end to end delay than OLSR due to its route search and reactive nature. Fig. 4 shows the end to end delay in a high density network (150 nodes) under black hole attack. In this case, end to end delay is decreased by 32.7% for AODV protocol but the change in OLSR protocol is negligible.

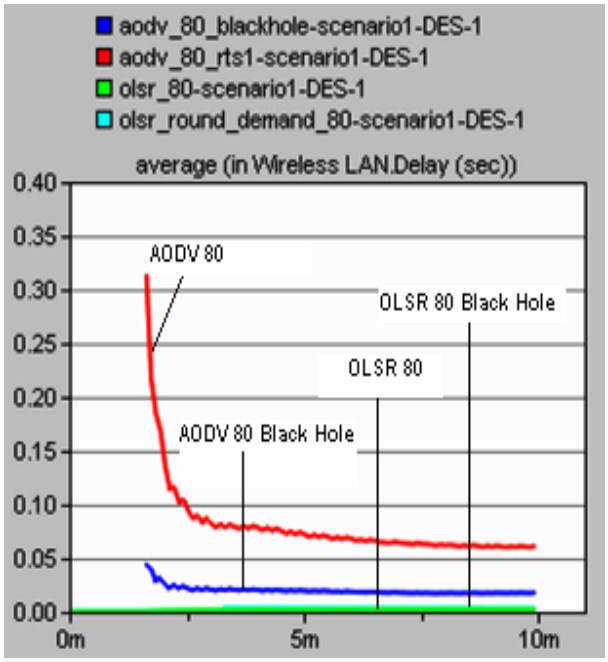

Fig. 3 Delay for low density network, Black Hole Attack

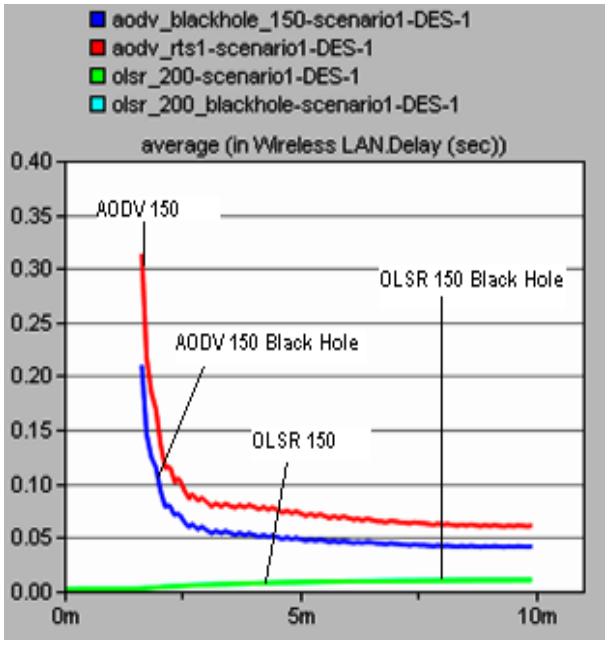

Fig. 4 Delay for high density network, Black Hole Attack

7.2 Network Load

The network load graph of OLSR and AODV with and without presence of a malicious node in a low density network (80 nodes) has been shown in the Fig. 5. In low density network under black hole attack, the network load is decreased by 41.65% for AODV protocol while the change in network load for OLSR protocol is negligible. Changes in the network load for high density networks are shown in Fig. 6. In the case of high density network (150 nodes) under black hole attack configured by using AODV protocol, the network load reduced by 20.21 % while for OLSR protocol, the statistics are same as seen in the low density network. It has been concluded that AODV performs better in the low density networks because AODV generates low routing over head than OLSR. Things change drastically, as the network size increases. In the large network, the offered load increases and the AODV overhead increases considerably with the increase in the traffic load. In this case, OLSR completely outperforms the AODV.

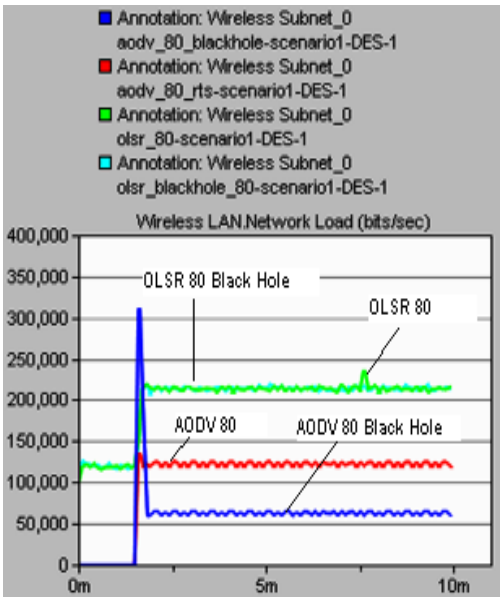

Fig. 5 N/W Load for low density network Black Hole Attack

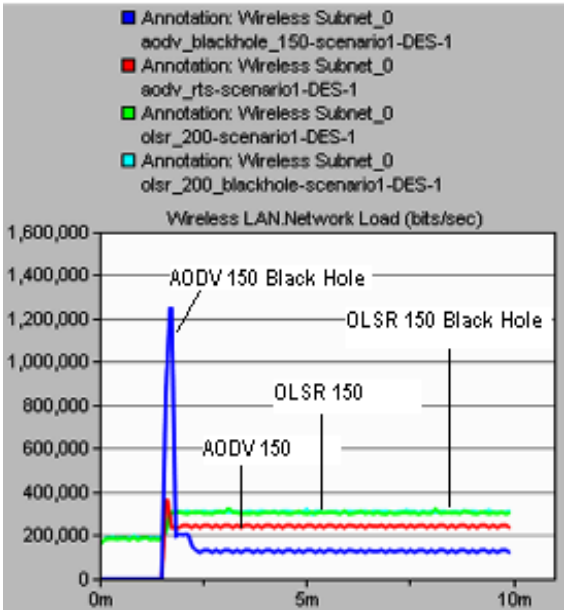

Fig. 6 N/W Load for high density network Black Hole Attack

7.3 Retransmission Attempts

Figure 7 shows the retransmission attempts to send the data in OLSR low density network under black hole attack is decreased by 11.23 % while in the case of AODV protocol, these attempts are decreased by only 2%. While for high density network, the retransmission attempts for OLSR protocol has been changed minutely but increased with respect to low density network. But in the case of AODV protocol, the whole situation is vice-versa of OLSR. In this case, the retransmission attempts are increased by 3.3% as shown in the figure 8.

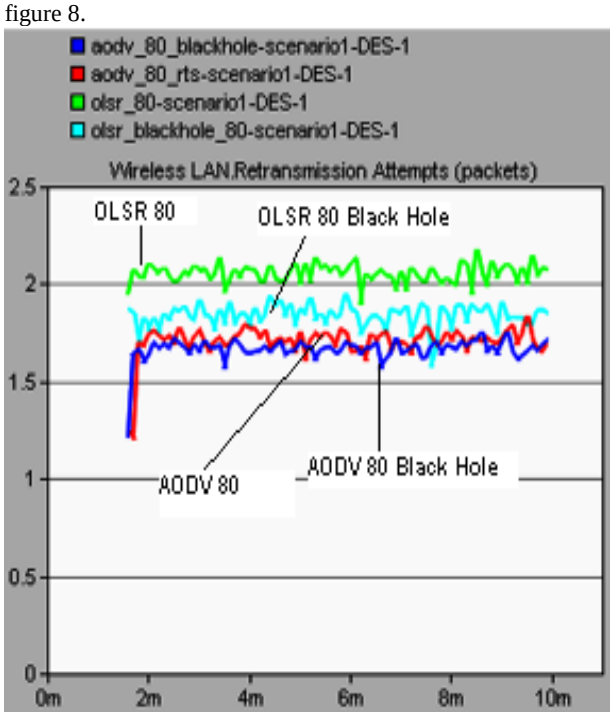

Fig. 7 Retrans. Att. for low density n/w, Black Hole Attack

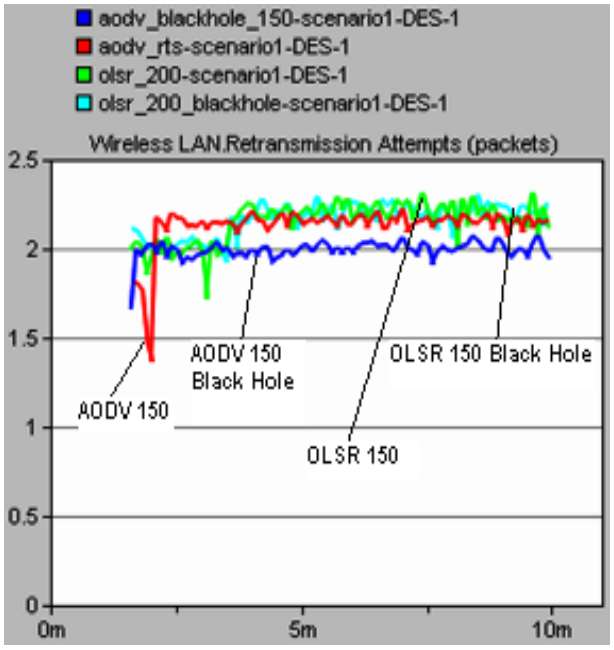

Fig. 8 Retrans. Att. for high density n/w, Black Hole Attack

7.4 Throughput

In communication networks, throughput is defined as, the average rate of successful message delivery over a communication channel. Figure 9 shows, the throughput of AODV and OLSR protocol with and without the presence of malicious nodes in the low density network under black hole attack. In this case, low density network configured by using OLSR protocol, the throughput is increased by only 1.1% while in the case of AODV protocol throughput is changed by only 2%. It can be said that in the low density network changes are very minute. In a network under the black hole attack, the malicious nodes creating the illusion to the sender that the packets are delivered to the destination node and malicious node sends the acknowledgements to the sender. Figure 10 shows the changes in the throughput of AODV and OLSR protocol under high density (150 nodes) network. It is observed that the throughput for high density (150 nodes) AODV network under black hole attack is increased by 26.24 % from a normal behaving network while in the case of OLSR protocol, this increment is of 4.42%.

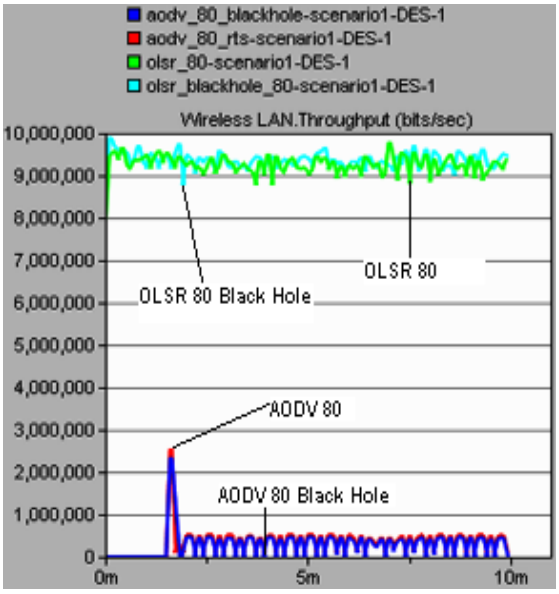

Fig. 9 Throughput for low density n/w, Black Hole Attack

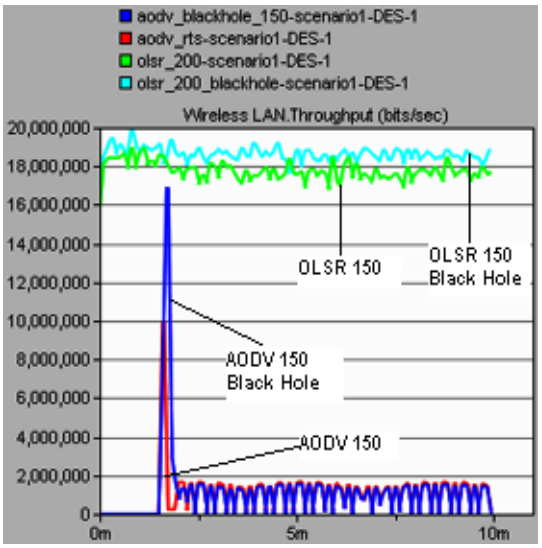

Fig. 10 Throughput for high density n/w, Black Hole Attack

8. CONCLUSION

In this study, the performance of one reactive protocol, AODV and one proactive protocol, OLSR is compared under security attack black hole attack. Network performance is evaluated in terms of end to end delay, retransmission attempts, network load and throughput. In the case of Black Hole attack, it is concluded that it is difficult to detect the passive attacks i.e. Black Hole attack, on the basis of the performance of the network. So to prevent the success of such passive attacks, we have to adopt some type of prevention measures like encipherment, digital signature etc.

9. FUTURE WORK

In future, the performances of other reactive and proactive protocols under other security attack [7] can be evaluated, to make these results more justified and scope of suitable detection and prevention techniques [1,6,10] will always be there.

10. REFERENCES

[1] Alfawar, M. Z., Alzoubi, S. 2009. A Proposed Security Subsystem for Ad Hoc Wireless Networks. In: International forum on Computer Science technology and Applications. (2009), 1-4.

[2] Ali, F., Khaldown A. A. 2008. A Shared Secret based Algorithm for securing the OLSR Routing Protocol. In: IJCSNS International Journal of Computer Science and Network Security, Vol. 8 No. 6, (2008), 337-343.

[3] Bo, M. S., Xiao, H., Adereti, A., Malcolm, A. J., Christianson, B. 2007. A Performance Comparison of Wireless Ad hoc Network Routing Protocols under Security Attack. In: Third International Symposium on Information Assurance and Security. UK (2007), 50-55.

[4] Candolin, C., Kari, H. H. 2002. A Security Architecture for Wireless Ad Hoc Networks. (2002), 1095-1100.

[5] Deng, H., Li, W., Aggarwal, P. D. 2002. Routing Security in Wireless Ad Hoc Networks. In: IEEE Communication Magazine. (2002), 70-75.

[6] Hu, C. Y., Perrig, A., Johnson, B. D. Aridane. 2002. A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: Proceeding of the 8th Annual International Conference on Mobile Computing and Networking. Atlanta, Georgia, USA (2002)

[7] Hu, C. Y., Perrig, A., Johnson, B. D. 2002. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In: IEEE Workshop on Mobile Computing Systems and Applications. (2002), 3-13.

[8] Li, H., Singhal, M. 2006. A Secure Routing Protocol for Wireless Ad Hoc Networks. In: HICSS' 06: Proceedings of the 39th Annual Hawai International Conference on System Sciences. (2006) , 1-10

[9] Padilla, G. E., Aschenbruck, N., Martini, P., Jahnke, M., Tolle, J. 2009. Detectine Black Hole Attacks in Tactical MANETs using Topology Graphs. In: 32nd IEEE Conference on Local Computer Networks. (2009), 1043—1050.

[10] Papadimitratos, P., Haas, J. Z. 2003. Secure Link State Routing for Mobile Ad Hoc Networks. In: Proceedings of IEEE Workshop on Security and Assurance in Ad Hoc Networks in Conjunction with the 2003 International Symposium on Applications and the Internet.. Orlando, FL (2003), 1-7.

[11] Papadimitratos, P., Haas, J. Z. 2002. Secure Routing for Mobile Ad Hoc Networks. In: Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference. San Antonio, TX (2002)

[12] Tseng, Y. C., Balasubramanyam, P., Ko, C., Limprasittiporn, R., Rowe, J., Levitt, K. 2009. A Specification based Intrusion Detection System for AODV. (2009), 1-10.

[13] T. P. Singh, Neha and V. Das, 2012. Multicast Routing Protocols in MANETs. In: International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 2, and (JAN. 2012).

[14] Westhoff, D., Paul, K. 2002. Context Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks. In: IEEE GLOBECOM. Taipei, Taiwan (2002), 178-182.

[15] W.R. Salem Jeyaseelan and Shanmugasundaram Hariharan. 2011. Investigation on Routing Protocols in MANET" In : International Journal of Research and Reviews in Information Sciences (IJRRIS), Vol. 1, No. 2, (2011), 80-84.

[16] Y. Sharma and J. Sengupta. 2010. Performance Evaluation of MANET routing protocols under various security attacks. In the proceedings of International Conference Methods and Modeling in Computer Science, new delhi. (2010), 117-124.