Analysis the Performance of MANET Protocol under Black Hole Attack for E-Mail Application

Lovepreet Singh
M.Tech Scholar ECE
Shaheed Bhagat Singh
State Technical Campus

Navdeep Kaur
Assistant Professor ECE
Shaheed Bhagat Singh
State Technical Campus

Gurjeevan Singh
DIC-ECE (P.W.)
Shaheed Bhagat Singh
State Technical Campus

ABSTRACT
A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes having ability to communicate with each other without any fixed network infrastructure. Due to the unavailability of controlling entity, routing and network management are done cooperatively by respective nodes. MANET is an autonomous system where each node act as an end system as well as a router to forward packets for other nodes., intermediate nodes are used to transmitting the packets from the source to the destination node, through different routing protocols i.e. AODV, DSR, GRP, OLSR etc. In this Paper the simulation analysis of the performance of AODV, DSR and TORA is compared for VOIP application under black hole attack. The performance is compared in terms of data dropped, network load, traffic sent and traffic received. The result shows that the overall performance of TORA is better than DSR and AODV.

Keywords
MANET, AODV, DSR, TORA, OPNET, E-mail

1. INTRODUCTION
MANETs are also called infrastructure less or non-infrastructure wireless networks. The term ad hoc implies that this network is established for a special, often extemporaneous service customized to specific applications. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others [1]. Routing and network management are done cooperatively by each other nodes. It is an autonomous system where each node operates not only as an end system but also as a router to forward packets for other nodes. A MANET consists of mobile nodes, a router with multiple hosts and wireless communication devices. The nodes of MANET are wireless radio type and they are mobile. The wireless communication devices are transmitters, receivers and smart antennas.To communicate with destination node, the other nodes must be lies in between the radio ranges of the source node; intermediate nodes are helpful to transmit data in-between the source and destination node [2]. Due to security provided by MANET it can be used in military battlefields, classrooms and rescue sites etc. [3]. The mobile nodes are connected to each other and data is route over the wireless network through intermediate nodes, to find out the route from source to destination MANET needs to routing protocols, which interchange the data between the nodes, these routing protocols are AODV, DSR, GRP, OLSR etc. [4][5].

2. RELATED WORK
Aujla [1] presented the performance analysis of five routing protocols (AODV, DSR, TORA, GRP, and OLSR) for two different applications (Videoconferencing and E-mail). Results showed that AODV and OLSR protocols are best suited for videoconferencing and E-mail respectively. Mohebi [2] has evaluated two MANET routing protocols (AODV and DSR) based on with/without black hole attack showing AODV performed better than under black hole attack. . Gupta [3] analysed the performance of three routing protocols (AODV, DSR and TORA) with respect to two performance metrics like end-to-end delay and packet delivery ratio (PDR) without black hole attack. Author concluded that the performance of AODV routing protocol is best in the network. DSR is suitable for network with moderate mobility and TORA is suitable for large dense mobile network. Saini [6] has analysed the performance of AODV routing protocol on various performance metrics like packet loss, packet delivery ratio (PDR) and average end-to-end delay. Paper concluded that the black-hole attack effect on packet loss is much lower as compare to effect on delay. Also, the packet delivery ratio (PDR) decreases when black hole node increases in network L. Geo [7] creating WMN by taking ftp traffic for two reactive protocols in which AODV performs better than DSR. In this paper we have evaluated the performance of three routing protocols (AODV, DSR and TORA) in MANET based on different scenarios of black hole attack for E-mail application.

3. ROUTING PROTOCOLS
An ad-hoc routing protocol is a standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network [8].The different protocols are proposed to deal with routing problem in the MANET. These routing protocols can be classified into two classes that are Reactive and Proactive. Reactive protocols are characterized by node acquire and maintain routes on demand, example is AODV. Proactive protocols are characterized by all nodes maintain routes to all destination in the network at all times. Thus using a proactive protocol, a node is immediately able to route (or drop) a packet, example is OLSR. In this Paper we have evaluated the performance of AODV, DSR and TORA routing protocols [9].

3.1 Ad Hoc On-Demand Distance-Vector Routing Protocol (AODV)
AODV is a reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route, AODV use control messages to find a route to the destination node in the network, it provide topology information for the node [1][4]. There are three types of control messages in AODV that are: Route Request Message (RREQ),Route Reply Message (RREP) and Route Error Message (RERR).

3.2 Dynamic Source Routing (DSR)
The Dynamic Source Routing protocol (DSR) [1] [10] is based on source routing, which means that the originator of each packet determines an ordered list of nodes through which

the packet must pass while travelling to the destination. The key advantage of a source routing design is that intermediate nodes do not need to maintain up-to-date routing information in order to route the packets that they forward, since the packet's source has already made all of the routing decisions [11]. This fact, coupled with the entirely on-demand nature of the protocol, eliminates the need for any type of periodic route advertisement or neighbor detection packets. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass; the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. There are two significant stages in working of DSR: Route Discovery and Route Maintenance. A host initiating a route discovery broadcasts a route request packet which may be received by those hosts within wireless transmission range of it. The route request packet identifies the host, referred to as the target of the route discovery, for which the route is requested. If the route discovery is successful, the initiating host receives a route reply packet listing a sequence of network hops through which it may reach the target. While a host is using any source route, it monitors the continued correct operation of that route. This monitoring of the correct operation of a route in use is called route maintenance. When route maintenance detects a problem with a route in use, route discovery may be used again to discover a new, correct route to the destination.

3.3 Temporally Ordered Routing Algorithm (TORA)

TORA is Temporally Ordered Routing Algorithm which is the one algorithm from basic link reversal algorithm. Basic functionality of TORA can be divided into three main processes: Creating Routes can be created by assigning the directions to the links for whole network or sometimes to the part of the network as desired. Maintaining routes refers to the topological changes which are always expected in the mobility environment where MANETs are worked on. By this, it means that when there is a topological change, all the routes to the destination have to be re-established and redefined within a finite time. Erasing route is one process to erase the other routes from the network and is done by clear (CLR) messages [12].

4. MISBEHAVIOUR NODES

Misbehavior nodes are those nodes having different behavior with respect to other nodes. Misbehavior nodes reduce the performance of network because they drop the packet at the time of communication, and it is always the intermediate nodes along a path, they do not forward packets to others because of negative effect on the performance of the network. This issue has been considered by many researchers that shown a small percentage of selfish nodes can significantly reduce the overall performance of the network. One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission. A misbehavior node may refuse to forward data packets for other node in order to conserve its own.

5. SECURITY IN MANET

Security is the most important concern for the basic functionality of network, due to features like open medium, changing its topology dynamically, lack of central monitoring management, cooperative algorithms and no clear defense mechanism in MANET [13]. Security threats in an ad hoc network can be classified into passive and active attacks. A passive attack does not disrupt operation of a routing protocol, but only attempts to retrieve valuable information by listening to routing traffic, which makes it very difficult to detect. An active attack is an attempt to improperly modify data, gain authentication, or procure authentication by inserting false packet transition through the network. A black hole attack can be achieved by a single-node or by several nodes in collusion.

5.1 Routing table overflow attack

A misbehavior node advertises routes that go to non-existent node to the authorized nodes, present in the network. An attacker can simply send excessive route advertisements to overflow the victim's routing table.

5.2 Routing cache poisoning attack

In this attackers take advantages of the promiscuous mode of routing table updating, in which a node overhearing any packer may add the routing information contained in that packet header to its own route cache, even if that node is not on the path.

5.3 Black Hole attack

Its effect on MANET in two ways, firstly a misbehavior node advertises the route with less hope count for a given destination. Once route is established via misbehavior node then it will drop all the data packets, Secondly once route is established via misbehavior nodes then it will drop the data packets selectively [13].

6. SIMULATION ENVIRONMENT

In carrying out the performance of AODV, DSR and TORA in the presence of black hole attack for applications E-mail application we have performed four different the following experiments in which 100, 125, 150 and 175 black hoe nodes are considered in first, second, third and fourth scenario respectively. In each scenario the placement of nodes is random over an area of 1000*1000. The simulation was run for 300s with a seed value of 128. OPNET Simulator 14.5 [8] was used to analyze the performance of AODV, DSR and TORA protocol. We used OPNET modeler, as OPNET modeler provides a comprehensive development environment supporting the modeling of communication network and distributed systems and it also support the both applications. OPNET modeler provides better environment for simulation, data collection and data analysis [14]. The Simulation parameters used in our scenario are shown in Table 1.

Table 1 Simulation Parameters

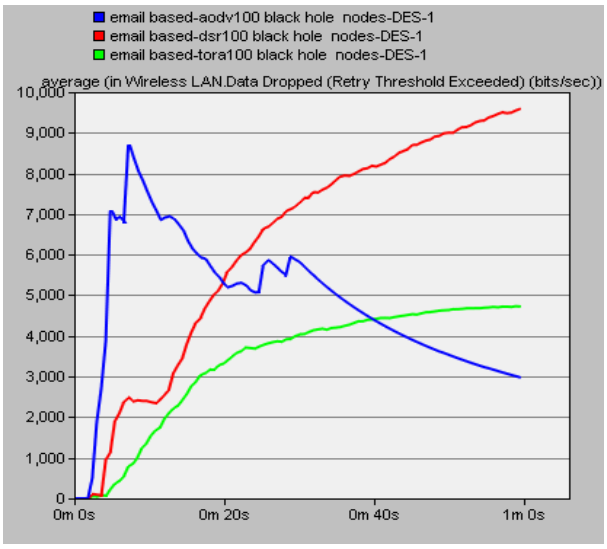
Network Parameters	Values
Number of Nodes	200
Number of Black Hole Nodes	100, 125, 150, 175
Simulation Time	60 sec (1 min)
Simulation Area	1000 m X 1000 m
Routing Protocols	AODV, DSR, TORA
Data Rate	18mbps
PHY Char.	PHY 802.11g
Application Name	E-mail
Simulator	Opnet Modeler 14.5

7. RESULTS

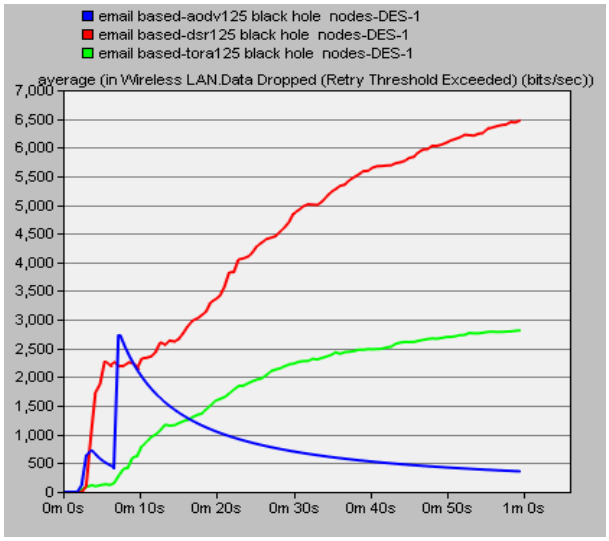
Simulation is conducted to evaluate the performance of Mobile Ad Hoc Network using OPNET version 14.5. All the result is clarified in the presence of AODV, DSR and TORA routing protocols. The result is evaluated by varying the number of black hole nodes for E-mail application. We analyzed the performance in the terms of data dropped; network load, traffic sent and traffic received using different range of scenario.

7.1 Data Dropped

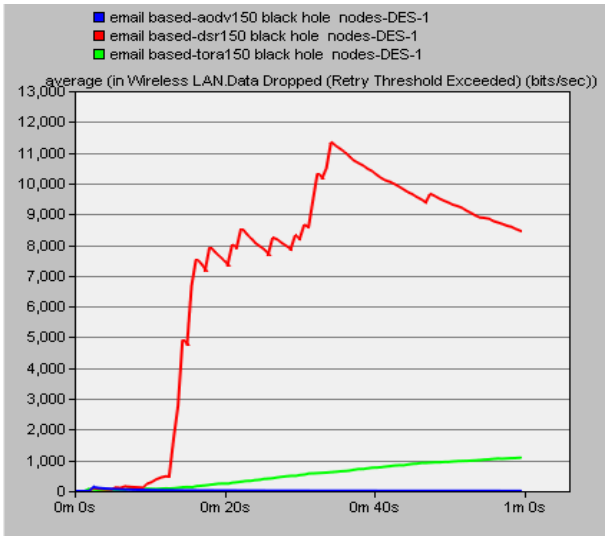
The traffic (bits/sec) received by the higher layer of all WLAN nodes in the network dropped as a result of consistently failing retransmissions. The number of higher layer packets is dropped because the node could not receive any ACKs for the retransmissions of those packets or their fragments, or the packets reached to the transmit lifetime limit. Figure 1 and Table 2 shows the data dropped for E-mail application. For AODV routing protocol, at the end of simulation time 60 sec traffic (bits/sec) received by higher layer of all WLAN nodes in the network is dropped i.e. 2,987.666, 358.4 and 6.4 (bits/sec) in first, second and third scenario respectively. Figure 1 (a-c) and Table 2 show that DSR protocol has maximum data dropped at 60 sec of simulation time i.e. 9,587.2, 6,469.333 and 1,085.333 in first, second and third scenario respectively. TORA shows 4,722.666, 2,813.333 and 8,460.8 (bits/sec) data dropped in first, second and third scenario respectively which, is less than DSR protocol but more than AODV protocol. Results show that in the fourth scenario data dropped by each routing protocol is 0. The simulation results show that AODV has least data dropped as compared to DSR and TORA routing protocols.



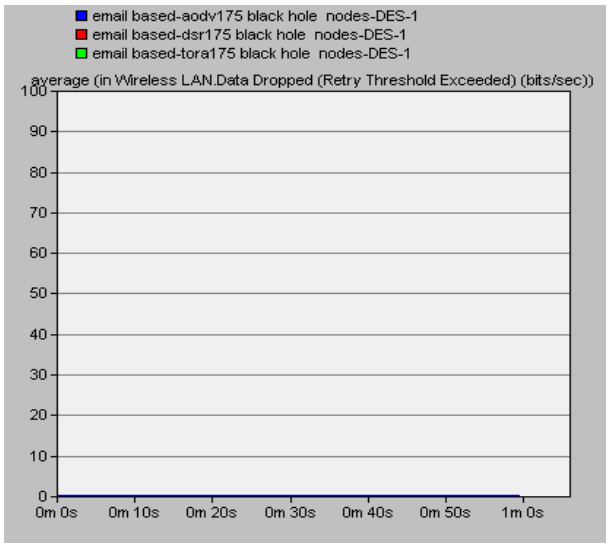
(a)



(b)



(c)

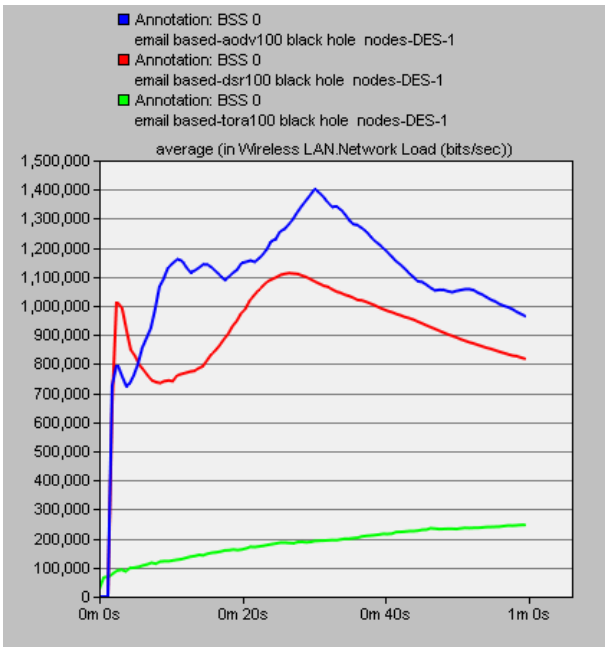


(d)

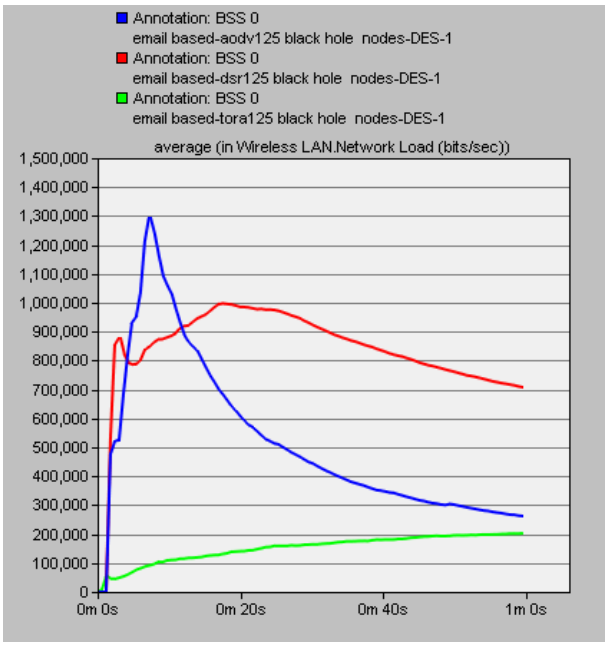
Fig 1: Data Dropped for different black hole nodes (a) 100 (b) 125 (c) 150 and (d) 175 nodes.

7.2 Network Load

The total end-to-end delay received by the higher layer of all WLAN nodes affects the overall load of the network depending on routing protocols used in MANETs. Figure 2 and Table 3 shows the network load for E-mail application. TORA routing protocol shows lowest network load i.e. 246,688, 202,773.333 and 176,729.066 bits/sec in first, second and third scenario compared to AODV and DSR. This is due to reason that depending on TORA routing protocol the higher layer of all nodes in the network received lowest end-to-end delay that affects the overall load of the network. But in fourth scenario both AODV and DSR routing protocols have same network load i.e. 60,678.933 bits/sec at 60 sec of simulation time which is less than TORA i.e. 120,762.133 bits/sec. The overall performance of TORA routing protocol shows less network load than AODV and DSR.



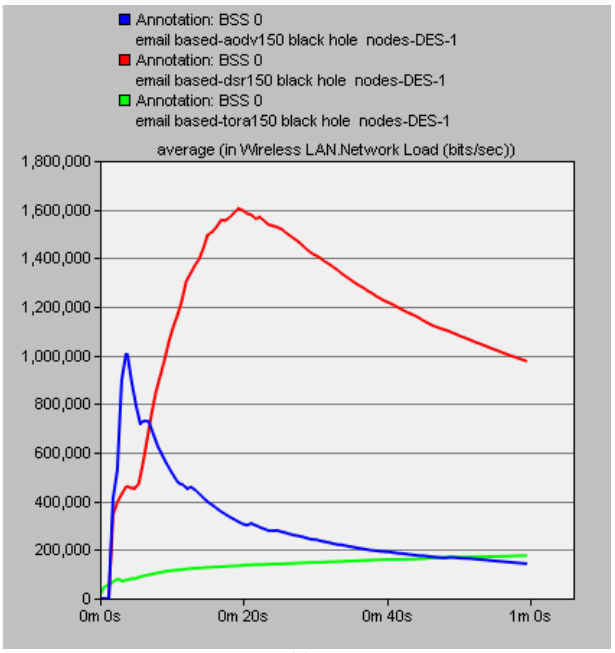
(a)



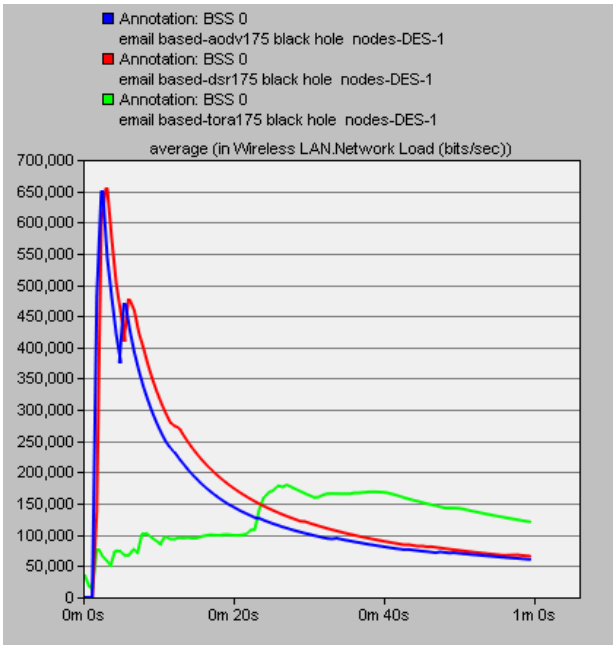
(b)

7.3 Traffic Sent

Average number of packets per second submitted to the transport layers by all email applications in the network. Figure 3 and Table 4 shows traffic sent (packets/sec) for E-mail application. TORA routing protocol shows lowest traffic sent i.e. 0 (packets/sec) in first, second and third scenario compared to AODV and DSR. In fourth scenario TORA has 3.13 (packets/sec) traffic sent which is also less from both AODV and DSR routing protocols at 60 sec of simulation time. Traffic sent by AODV protocol is 10.66, 12.13, 7.53 and 3.78 (packets/sec). AODV is better than other routing protocols.



(c)



(d)

Fig 2: Network Load for different black hole nodes (a) 100 (b) 125 (c) 150 and (d) 175 nodes.

Table 2 Data Dropped of AODV, DSR and TORA

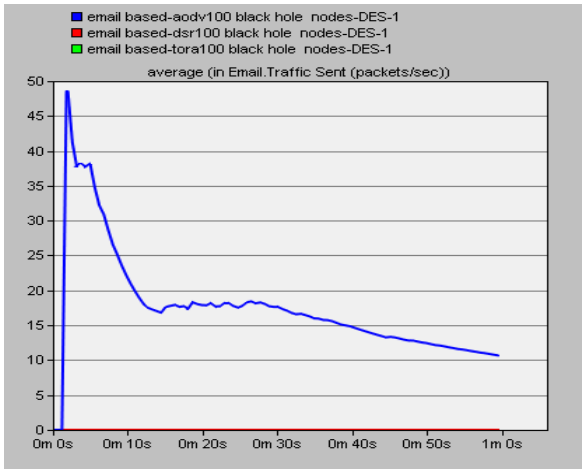
Data Dropped (bits\sec) for 100 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	7,087.719	2,367.407	1,555.555
20	5,197.714	5,589.333	3,398.095
30	5,815.424	7,286.797	4,036.601
40	4,298.357	8,170.196	4,440.597
50	3,496.784	8,998.901	4,655.686
60	2,987.666	9,587.2	4,722.666
Data Dropped (bits\sec) for 125 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	1,991.111	2,325.925	800
20	1024	3,422.476	1,622.857
30	689.230	4,862.745	2,237.908
40	527.058	5,674.975	2,488.888
50	421.647	6,123.921	2,701.176
60	358.4	6,469.333	2,813.333
Data Dropped (bits\sec) for 150 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	35.55	296.296	35.55
20	18.28	7,352.380	243.809
30	12.30	8,193.464	522.875
40	9.41	10,179.710	764.705
50	7.529	9,307.607	963.137
60	6.4	1,085.333	8,460.8
Data Dropped (bits\sec) for 175 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	0	0	0
20	0	0	0
30	0	0	0
40	0	0	0
50	0	0	0
60	0	0	0

Table 3 Network Load of AODV, DSR and TORA

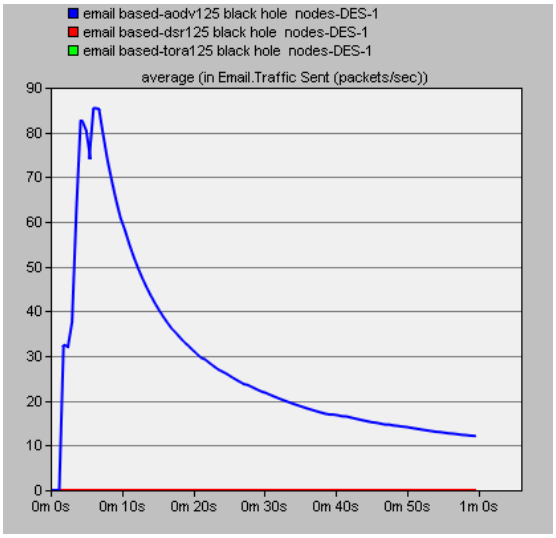
Network Load (bits\sec) for 100 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	1,147,454.814	740,657.777	124,429.629
20	1,151,155.809	992,019.809	165,782.852
30	1,401,616.732	1,076,480	191,179.084
40	1,166,812.753	977,745.314	216,780.676
50	1,054,327.215	884,828.235	234,694.901
60	964,766.4	817,719.466	246,688
Network Load (bits\sec) for 125 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	978,899.649	893,549.473	110,266.666
20	529,789.476	985,159.619	140,929.523
30	435,725.128	916,285.128	164,348.717
40	343,694.685	824,503.188	180,931.400
50	298,400.627	757,132.549	195,811.705
60	262,418.666	707,708.8	202,773.333
Network Load (bits\sec) for 150 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	500,918.518	1,120,788.148	115,585.185
20	301,962.666	1,583,850.666	137,935.238
30	237,384.615	1,400,644.102	148,712.820
40	188,510.917	1,207,666.086	160,350.862
50	165,083.607	1,076,089.098	165,083.607
60	143,092.266	976,163.733	176,729.066
Network Load (bits\sec) for 175 black hole nodes			
Simulation Time (sec)	AODV (bits\sec)	DSR (bits\sec)	TORA (bits\sec)
10	264,059.259	295,337.543	85,460.740
20	141,060.571	170,558.476	99,184.761
30	100,851.241	118,796.339	163,094.379
40	79,247.149	87,805.990	165,920
50	69,835.294	69,835.294	141,338.980
60	60,678.933	60,678.933	120,762.133

Table 4 Traffic Sent of AODV, DSR and TORA

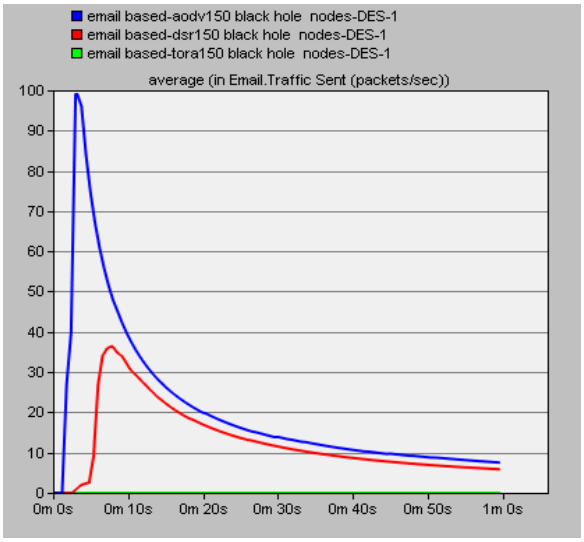
Traffic Sent (Packets\sec) for 100 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	19.91	0	0
20	17.85	0	0
30	17.61	0	0
40	14.42	0	0
50	12.29	0	0
60	10.66	0	0
Traffic Sent (Packets\sec) for 125 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	58.42	0	0
20	30.87	0	0
30	21.79	0	0
40	16.74	0	0
50	13.96	0	0
60	12.13	0	0
Traffic Sent (Packets\sec) for 150 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	35.78	29.56	0
20	19.61	16.57	0
30	13.85	11.47	0
40	10	8.60	0
50	8.76	6.88	0
60	7.53	5.86	0
Traffic Sent (Packets\sec) for 175 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	17.80	19.29	4.0
20	9.8	10.66	2.4
30	6.79	7.45	5.35
40	5.29	5.58	4.60
50	4.44	4.44	3.73
60	3.78	4.2	3.13



(a)



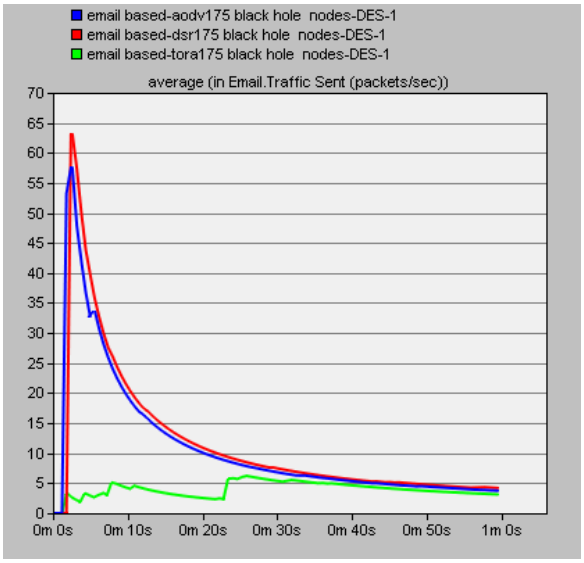
(b)



(c)

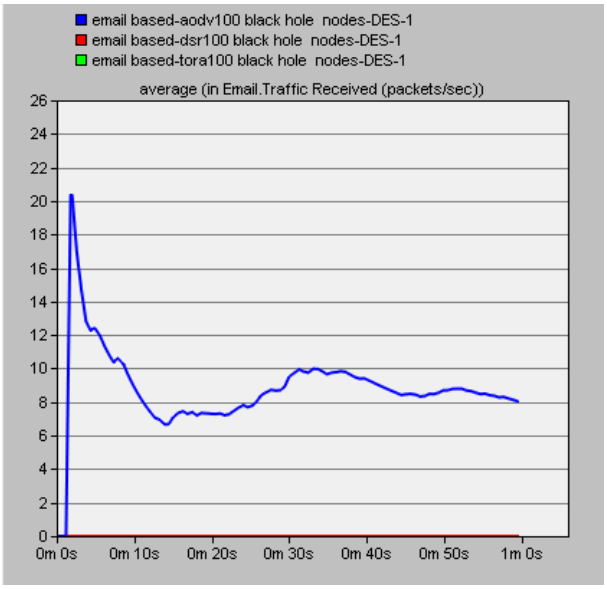
7.1 Traffic Received

Average number of packets per second submitted to the transport layers by all email applications in the network. Figure 4 and Table 5 shows traffic sent (packets/sec) for E-mail application. TORA routing protocol shows lowest traffic sent i.e. 0 (packets/sec) in first, second and third scenario compared to AODV and DSR. In fourth scenario TORA has 3.13 (packets/sec) traffic sent which is also less from both AODV and DSR routing protocols at 60 sec of simulation time. Traffic sent by AODV protocol is 10.66, 12.13, 7.53 and 3.78 (packets/sec). AODV is better than other routing protocols.



(d)

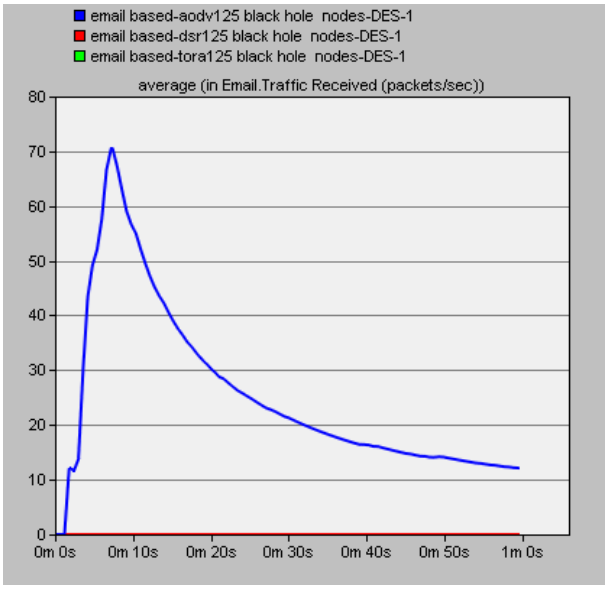
Fig 3: Traffic Sent for different black hole nodes (a) 100 (b) 125 (c) 150 and (d) 175 nodes.



(a)

8. CONCLUSION

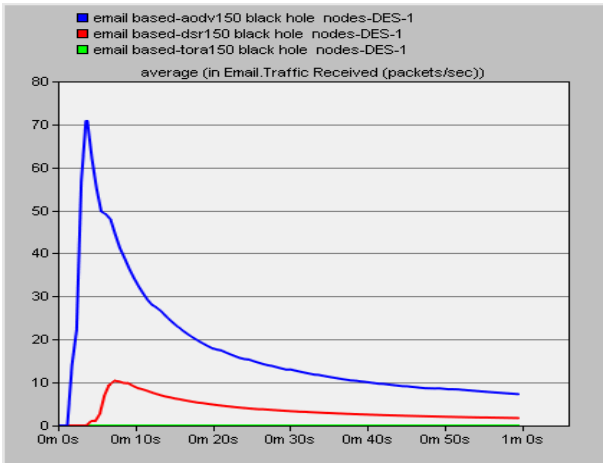
We have considered the black hole attack in MANET to analyze the performance of AODV, DSR and TORA by varying no. of black hole nodes for E-mail application using OPNET 14.5. The results are carried out in terms of data dropped, network load, traffic sent and traffic received. Simulative results showed that AODV has least data dropped as compared to DSR and TORA routing protocols. The Investigation also showed that the overall performance of TORA routing protocol shows less network load than AODV and DSR. Also AODV has maximum traffic sent and received, as compared to other routing protocols.



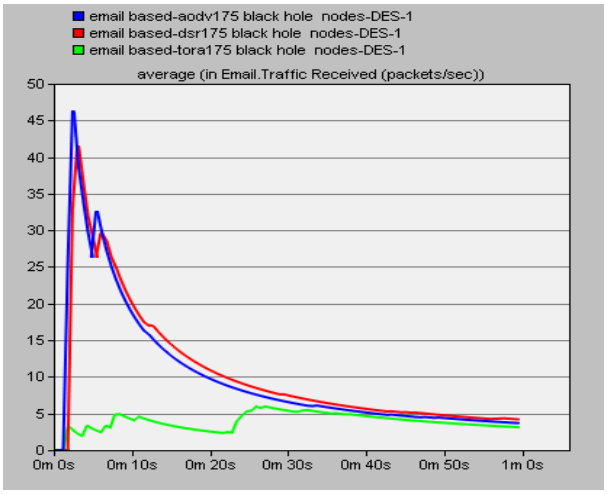
(b)

Table 5 Traffic Received of AODV, DSR and TORA

Traffic Received (Packets\sec) for 100 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	8.15	0	0
20	7.28	0	0
30	9.54	0	0
40	9.15	0	0
50	8.70	0	0
60	8.05	0	0
Traffic Received (Packets\sec) for 125 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	55.0	0	0
20	29.61	0	0
30	20.83	0	0
40	16.32	0	0
50	13.96	0	0
60	12.13	0	0
Traffic Received (Packets\sec) for 150 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	30.87	8.77	0
20	17.66	4.76	0
30	12.75	3.26	0
40	10	2.52	0
50	8.43	2.01	0
60	7.3	1.73	0
Traffic Received (Packets\sec) for 175 black hole nodes			
Simulation Time (sec)	AODV (Packets)	DSR (Packets)	TORA (Packets)
10	17.19	18.42	4.56
20	9.52	10.66	2.47
30	6.41	7.30	5.25
40	5.0	5.5	4.60
50	4.33	4.70	3.68
60	3.68	4.2	3.13



(c)



(d)

Fig 4: Traffic Received for different black hole nodes (a) 100 (b) 125 (c) 150 and (d) 175 nodes.

9. REFERENCES

[1] Aujla, Gagangeet Singh and Kang, Sandeep Singh, "Comprehensive Evaluation of AODV, DSR, GRP, OLSR and TORA Routing Protocols with Varying number of nodes and traffic applications over MANETs," Department of CSE, Chandigarh Engineering College, India, April 2013.

[2] Mohebi, Amin and Kamal, Ehsan and Scott, Simon, "Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack," International Journal of Modern Education \& Computer Science, vol. 5, 2013.

[3] Gupta, Sorabh and Gill, Sumeet and Joshi, Anil, "Analysis of Black Hole Attack on AODV and OLSR Routing Protocols in MANET," IJCA, vol.1, pp.11-19, october 2011.

[4] Ramaswamy, Sanjay and Fu, Huirong and Sreekantaradhya, Manohar and Dixon, John and Nygard, Kendall E, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," International Conference on Wireless Networks, 2003.

[5] Su, Ming-Yang, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, pp. 107-117, 2011.

[6] Saini, Akanksha and Kumar, Harish, "Effect Of Black Hole Attack On AODV Routing Protocol In MANET," IJCST, vol. 1, pp. 57-60, 2010.

[7] Guo, Lei and Peng, Yuhuai and Wang, Xingwei and Jiang, Dingde and Yu, Yinpeng, "Performance evaluation for on-demand routing protocols based on OPNET modules in wireless mesh networks," Computers \& Electrical Engineering, vol. 37, pp. 106-114, 2011.

[8] Saxena, Nidhi and Kumar, Sanjeev and Saxena, Vipul, "Performance Analysis of AODV Routing Protocol under the Different Attacks Through The Use Of OPNET Simulator," International Journal of Innovative Research and Development, vol. 2, pp. 244-248, 2013.

[9] Tamilarasan, Santhamurthy, "A Quantitative Study and Comparison of AODV, OLSR and TORA Routing Protocols in MANET," International Journal of Computer Science Issues(IJCSI), vol. 9, pp. 364-369, January 2012.

[10] Vats, Kuldeep and Sachdeva, Monika and Saluja, Krishan, "Simulation and performance Analysis of OLSR, GRP, DSR Routing Protocol using OPNET," IJETED volume 2, Issue 2, March 2012.

[11] Gupta, S Balaji and Navneeth, T and Sundar, S and Vidhyapathi, CM, "Performance Evaluation of MANET Routing Protocols under Varying Node Mobility," International Journal of Engineering \& Technology (0975-4024), vol. 5, 2013.

[12] Tamilarasan, S and Sivaram, Dr R, "An Analysis and Comparison of Multi-Hop Ad-Hoc wireless Routing Protocols for Mobile Node," International Journal of Science and Applied Information Technology, vol. 1, pp. 1-5, march-April 2012.

[13] Singh, S. (2014). Maodv: To identify a secure route selection in manet under blackhole. Master's thesis, Shaheed Bhagat Singh State Technical Campus.