Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Investigation of E-mail Application based MANET routing protocols under black hole attack

Lovepreet Singh
Department of ECE
Shaheed Bhagat Singh State Technical Campus,
Ferozepur,India

Navdeep Kaur
Department of ECE
Shaheed Bhagat Singh State Technical Campus,
Ferozepur, India

Gurjeevan Singh
Department of ECE
Shaheed Bhagat Singh State Technical Campus,
Ferozepur, India

Abstract— In mobile ad-hoc networks, each routing protocol is anxious as it routes the packet to destination node safely depending upon topology. Three types of routing protocols are proactive, reactive and hybrid. Ad-hoc on-demand distance-vector (AODV), dynamic source routing (DSR) and temporally ordered routing algorithm (TORA) has been considered for investigation based on OPNET Modeler 14.5. The impact of black hole attack on these routing protocols has evaluated with respect to delay, retransmission attempts and throughput. The primary objective of research in this paper is to investigate the performance of popular MANET routing protocols by increasing the number of black hole nodes in network for E-mail application.

Keywords— MANETs; AODV; DSR; TORA; OPNET Modeler 14.5

I. INTRODUCTION

In wireless communication user can access the network by either point-to-point or point-to-multipoint methods [1]. MANETs are indeed a part of wireless communication which has ability to be self-configured without any centralized authority [2]. Mobile ad-hoc networks have large number of applications such as battlefield communication, public meetings, virtual class rooms etc. [3, 4, 5]. In such applications MANETs support videoconferencing, e-mail, VoIP etc. for communication. The limitations such as high error rate, power restrictions, and bandwidth constraints restrict the communication of networks [6]. There are several routing protocols in MANETs. When topology changes dynamically a special proposed protocol is engaged to establish a route between source and destination node using its own routing technique [7]. The important parameters (minimum overhead and bandwidth consumption) are involved during establishing a route [8]. The routing protocols are divided into three categories: Proactive, Reactive and Hybrid routing protocols. Due to dominant characteristics such as dynamically topology changes, lack of centralized authority the mobile ad-hoc networks are more vulnerable to various attacks. Security threats in an ad-hoc network can be classified into passive and active attacks. A passive attack does not disrupt operation of 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 by inserting false packet transition through the network. The black hole attack can occur at single or several nodes i.e. selective or cooperative black hole attack respectively [9, 10]. In black hole attack, a malicious node shows itself as a valid node. Once the route has been established through malicious node the data packets are drop or misuse by that node. In the following, related work discussed in section II, section III describes simulation setup, simulation results presented in section IV and finally conclusion is outlined in section V.

II. RELATED WORK

Aujla [6] 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 [11] 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. Saini [12] 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. Gupta [13] 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. L. Geo [1] 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.

III. SIMULATION SETUP

Optimized Network Engineering Tools (OPNET) version 14.5 has used to analyse the performance of three routing protocols in three different scenarios by varying the number of black hole nodes for E-mail application. The four different scenarios are as follow: first, in which 100 nodes are black hole nodes, second, 125 nodes are black hole nodes, and third and fourth, scenario has 150 and 175 black hole nodes respectively. The protocols used for research are AODV, DSR and TORA for all scenarios. The simulation has run for 60 sec with a seed value 128. Random waypoint mobility model is used in which node will move during simulation and randomly select a destination in the network and moves towards it at a specific or random chosen speed. The placement of WLAN nodes is random and the traffic flow in between nodes is also random as shown in Fig. 1. Table 1 show the performance metrics which were taken during simulation.

TABLE I: SIMULATION PARAMETERS

Simulation Parameters	**Values**
Routing protocols	AODV, DSR, TORA
Simulation time	60 sec
Simulation area	1000m x 1000 m
Total number of nodes	200
Number of Black hole nodes	100, 125, 150, 175
Data rate	18 mbps
PHY characteristics	PHY (802.11g)
Transmit Power	0.005 W
Application name	E-mail

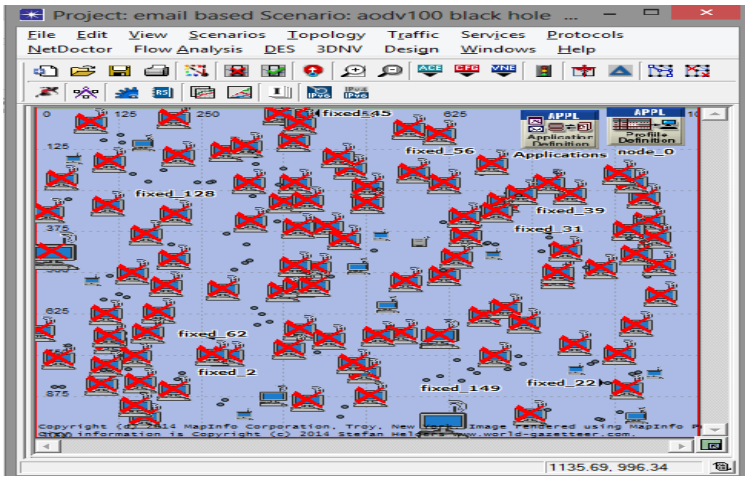


Fig. 1 Snapshot of research scenario

IV. RESULTS AND DISCUSSIONS

Simulation results showed the performance comparison of three different MANET routing protocols AODV, DSR and TORA. To evaluate the overall performance we have determined the various performance parameters such as delay, retransmission attempts and throughput by varying the number of black hole nodes in three different scenarios for E-mail application.

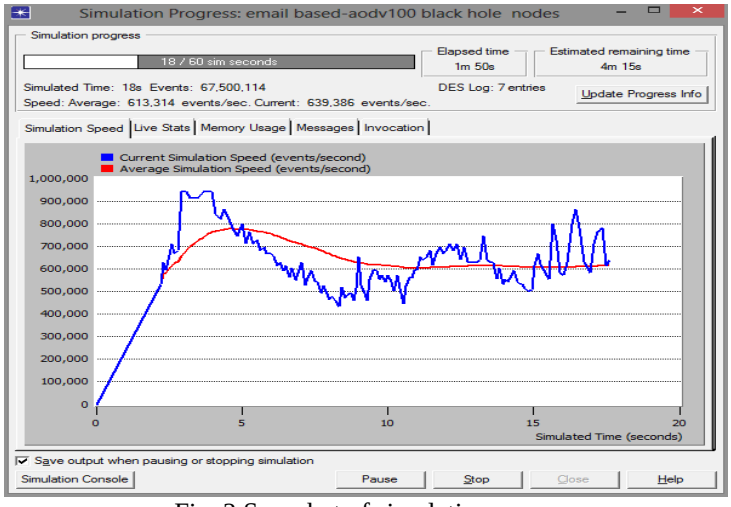
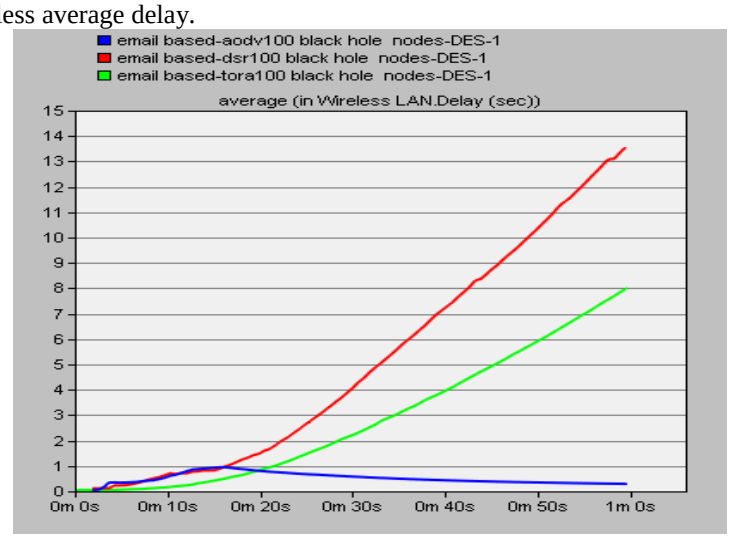


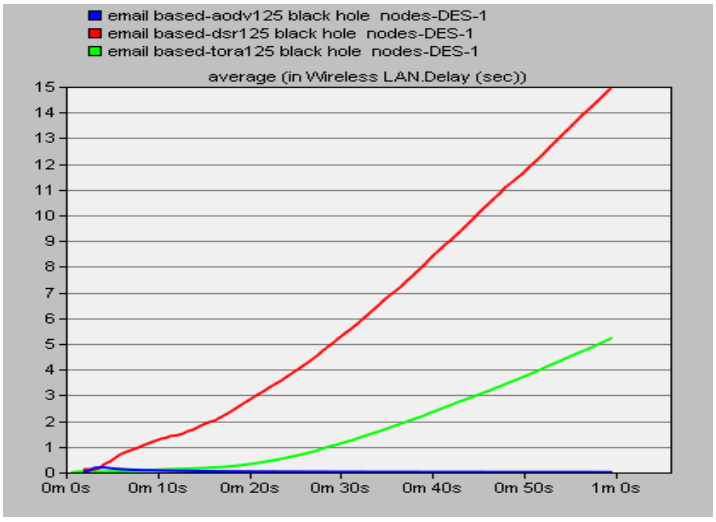
Fig. 2 Snapshot of simulation progress

A. Delay

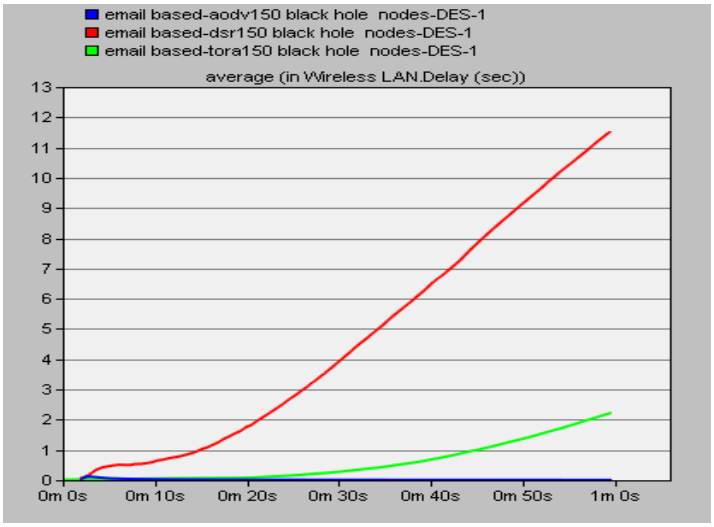
Average delay for each routing protocol as shown in Fig. 3, the average delay for AODV is less than DSR and TORA in each scenario. This is due to fact that the source routing protocols have a longer delay because their route discovery takes more time as every intermediate node tries to extract information before forwarding the reply. TORA route construction may not occur quickly. This leads to potential lengthy delay while waiting for new route to be determined [14]. DSR shows a better delay performance at higher mobility rate. In case of congestion (high traffic) AODV performs better than DSR. Beside the high mobility of nodes during simulation, the high traffic is also considered in our research work. So that AODV has less average delay.



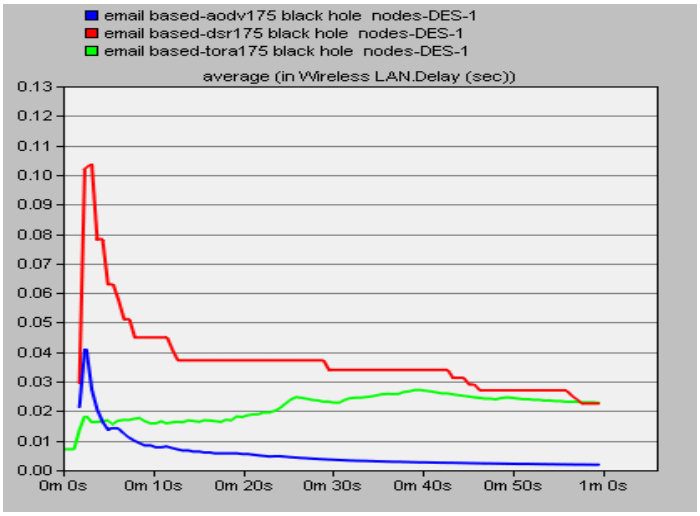
(a)



(b)



(c)

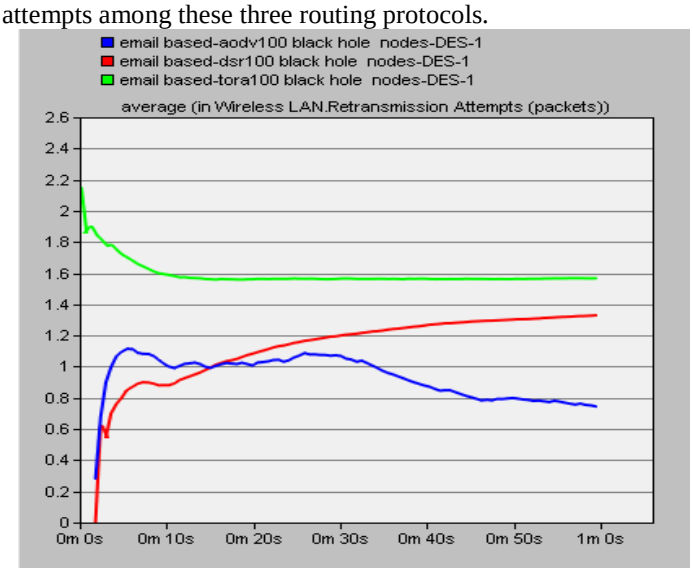


(d)

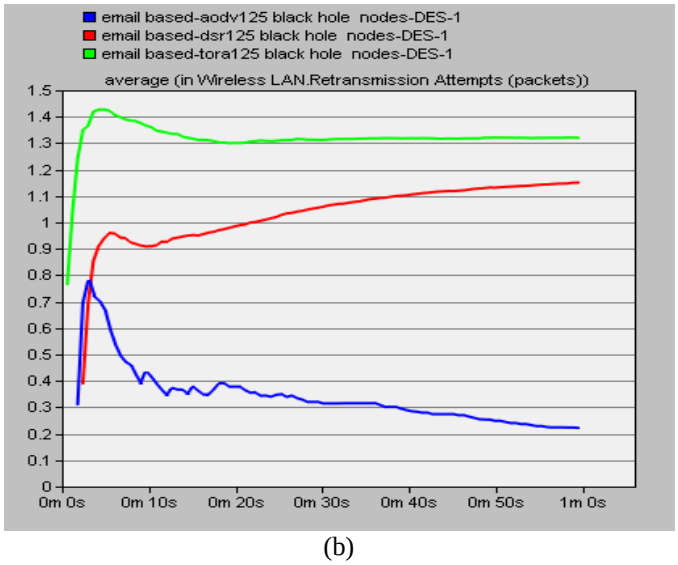
Fig. 3 Average delay for different black hole nodes of (a) 100 nodes, (b) 125 nodes, (c) 150 nodes, (d) 175 black hole nodes

B. Retransmission Attempts

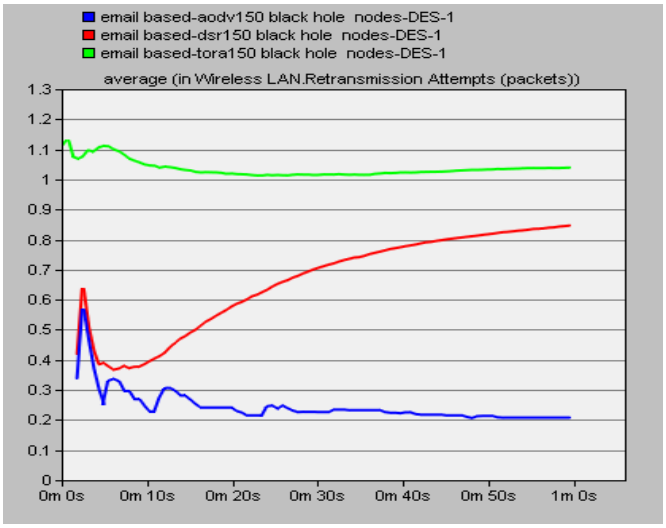
The comparison between the routing protocols on the basis of retransmission attempts as depicted in Fig. 4 (a-d). While increasing the number of black hole nodes in the MANET, retransmission attempts decreases for AODV, DSR and TORA routing protocols. This is due to effect of black hole attack on these routing protocols. AODV has minimum numbers of Retransmission attempts among these three routing protocols.



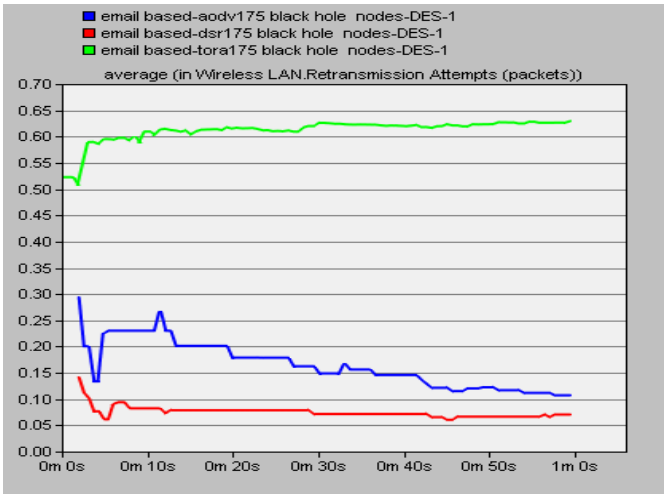
(a)



(b)



(c)

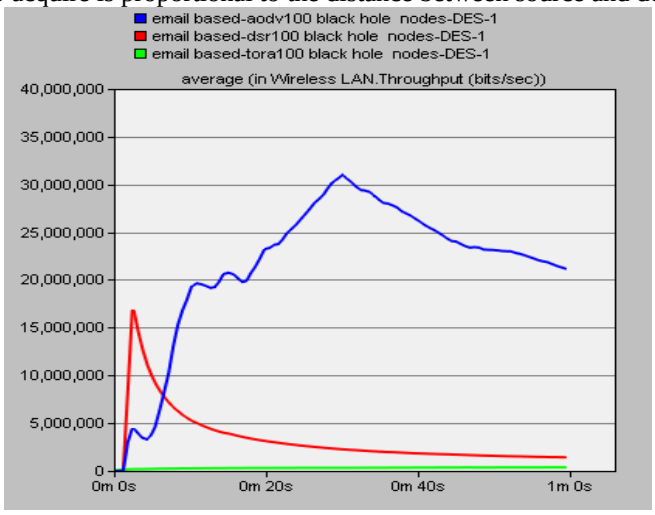


(d)

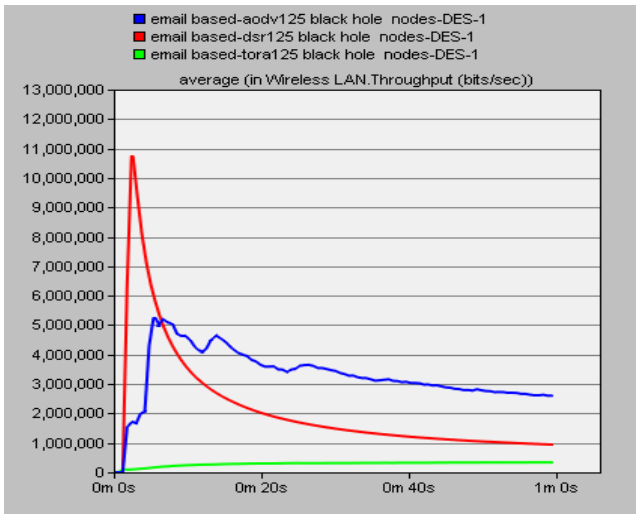
Fig. 4 Retransmission attempts for different black hole nodes of (a) 100 nodes, (b) 125 nodes, (c) 150 nodes, (d) 175 black hole nodes

C. Throughput

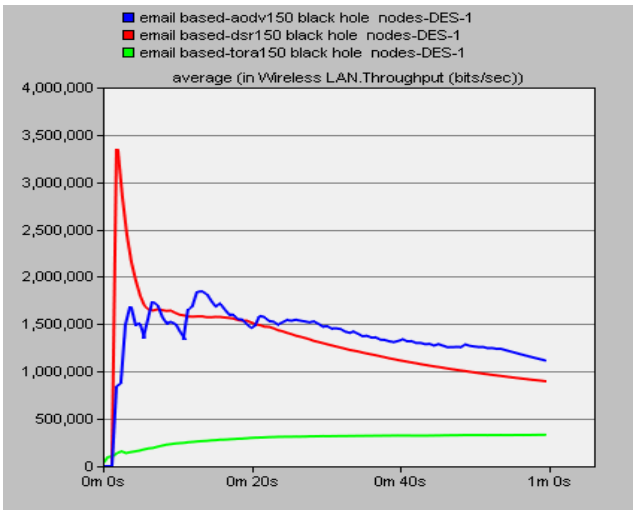
From Fig. 6, it is clear that throughput value of DSR increases initially and reduces with respect to time. Throughput value of AODV slowly increases initially and maintains its value with respect to time. Throughput value of TORA remains constant. With the increase in the number of black hole nodes in the network i.e. from 100 to 125, then 125 to 150, then 150 to 175 nodes, the performance of AODV is better with respect to throughput under black hole attack. This is due to reason that AODV and DSR routing protocols drop a considerable numbers of packets during route discovery process, time taken by route to acquire is proportional to the distance between source and destination node.



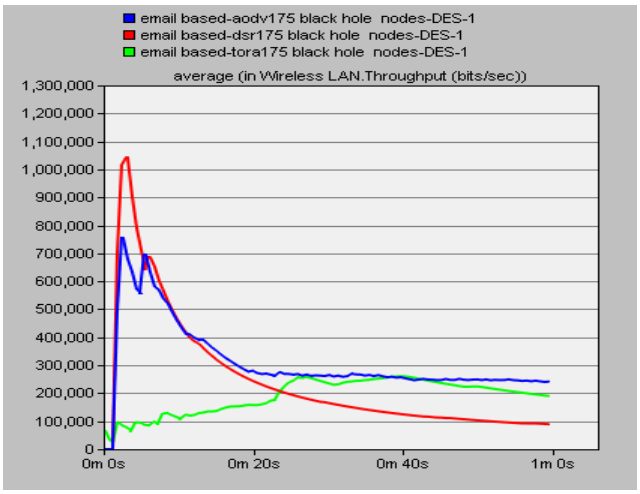
(a)



(b)



(c)



(d)

Fig. 5 Throughput for different black hole nodes of (a) 100 nodes, (b) 125 nodes, (c) 150 nodes, (d) 175 black hole nodes

V. CONCLUSIONS

We have considered the black hole attack in MANET to investigate the performance of different routing protocols for E-mail application using OPNET 14.5. The investigation showed that AODV routing protocol has less average delay followed by TORA and DSR for all scenarios. Also AODV has minimum retransmission attempts. But while increasing malicious nodes in network i.e. 175 the performance of DSR wins over AODV and TORA. Simulation results also showed that throughput of DSR increases initially. But with respect to simulation time it decreases and AODV has maximum average throughput than both DSR and TORA.

REFERENCES

[1] L. Guo, Y. Peng, X. Wang, D. Jiang, and Y. Yu, "Performance evaluation for on-demand routing protocols based on opnet modules in wireless mesh networks," Computers & Electrical Engineering, vol. 37, no. 1, pp. 106–114, 2011.

[2] G. Adam, V. Kapoulas, C. Bouras, G. Kioumourtzis, A. Gkamas, and N. Tavoularis, "Performance evaluation of routing protocols for multimedia transmission over mobile ad hoc networks," in Wireless and Mobile Networking Conference (WMNC), 2011 4th Joint IFIP. IEEE, 2011, pp. 1–6.

[3] S. Tamilarasan and D. R. Sivaram, "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, no. 1, p. 1, 2012.

[4] V. Narsimaha, "The performance comparison of an aodv, dsr, dsdv and olsr routing protocols in mobile ad-hoc networks," Journal of Computer Applications (JCA), vol. 5, no. 2, p. 2012, 2012.

[5] S. Gandhi, N. Chaubey, P. Shah, and M. Sadhwani, "Performance evaluation of dsr, olsr and zrp protocols in manets," in Computer Communication and Informatics (ICCCI), 2012 International Conference on. IEEE, 2012, pp. 1–5.

[6] G. S. Aujla and S. S. Kang, "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), vol. 1, p. 1, 2013.

[7] S. Khurana and A. Grover, "Simulation and analysis the effect of varying no. of nodes on aodv and dsr for different applications." International Journal of Computer Applications, vol. 77, p. 1, 2013.

[8] S. B. Gupta, T. Navneeth, S. Sundar, and C. Vidhyapathi, "Performance evaluation of manet routing protocols under varying node mobility." International Journal of Engineering & Technology (0975-4024), vol. 5, no. 3, p. 1, 2013.

[9] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, no. 1, pp. 107–117, 2011.

[10] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. E. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks." in International Conference on Wireless Networks, vol. 2003.

[11] A. Mohebi, E. Kamal, and S. Scott, "Simulation and analysis of aodv and dsr routing protocol under black hole attack." International Journal of Modern Education & Computer Science, vol. 5, no. 10, p. 1, 2013.

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

[13] Gupta, Anuj K and Sadawarti, Harsh and Verma, Anil K, "Performance analysis of AODV, DSR \& TORA routing protocols," IACSIT international journal of Engineering and Technology, vol. 2, pp. 226-231, 2010.

[14] A. K. Gupta, H. Sadawarti, and A. K. Verma, "Performance analysis of aodv, dsr & tora routing protocols," IACSIT international journal of Engineering and Technology, vol. 2, no. 2, pp. 226–231, 2010.

