IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Performance Evaluation of Enhanced DSR Protocol under Influence of Black Attacks

Isha Sharma[1], Rajesh Kochher[2]

DAV Institute of Engineering and Technology, Jalandhar[1, 2]

Abstract: Mobile Adhoc Network is a type of pre-existing network framework having collection of mobile nodes, each acting as host as well as router, equipped with wireless communication and networking capability to communicate with one another. MANET goal is to provide communication to the area where limited communication organization exists. For communication between various nodes routing protocols forms important component. DSR computes the routes when necessary and then maintains the same during the entire communication network. But it also suffers from various types of attacks such as Black Hole attack and Gray Hole attack. So this paper is effort to evaluate the performance of DSR and enhances its performance in MANET network by calculating matrices such as voice end-to-end delay, network load, throughput, number of hops per route, retransmission attempts, packet delivery ratio, using OPNET Modeler 14.5.

Keywords: MANET, DSR, Black Hole Attack.

1. INTRODUCTION

Mobile Adhoc Network is a type of pre-existing network framework having collection of mobile nodes, each acting as host as well as router, equipped with wireless communication and networking capability to communicate with one another. MANET goal is to provide communication to the area where limited communication organization exists. The nodes can move randomly and do not necessitate pre-determined association of links to communicate [3]. Mobile nodes which are within the radio range to each other and can communicate directly to each other through wireless links, whereas the nodes which are far away depend on other nodes for communicating messages to nodes at distant locations. So each node in MANET can act as a host or as a router for communication. Due to these characteristics, MANETs is used in number of applications like in military where nodes are scattered on battle field for surveillance mission, in emergency and disaster struck areas where an infrastructure is unavailable or unfeasible to install and for ubiquitous computing for smart homes. To establish communication within the network a routing protocol is needed to discover routes between nodes. Routing in MANET is broadly categorized in to Proactive Routing Protocols and Reactive Routing Protocols [4].

Proactive protocols are Table-driven algorithms, which stumble on the path to every other individual node in the network, if there is a packet sending request or not, and attempt to maintain consistent and efficient up-to-date routing information from each node of network to every other node within the network. The reactive protocols maintain routing information at the network nodes only when there is communication otherwise not and if a node wants to send a packet to another node then reactive protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet within the network[5][6].This research empathizes on Reactive routing protocol's DSR (Dynamic Source Routing) algorithm, due to its above discussed properties.**DSR** computes the routes for data transfer when needed and then maintains the same during the entire communication process. 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.

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 as having two route replies. In addition to the address of the original initiator of the request and the target of the request, each route request packet contains a route record, in which is accumulated a record of the sequence of hops taken by the route request packet as it is propagated through the network during this route discovery.

In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad-hoc network is very challenging.The attacks can be categorized on the basis of behavior of the attack i.e. Passive or Active attack.A passive attack does not alter the data transmitted within the network. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Active attacks are very severe attacks on the network that prevent message flow between the nodes.However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

packets, DOS, congestion etc. [12][13]. The most common attacks are **Black hole or Black Hole Attack** is a type of internal attack, where internal malicious nodes get fit in between the routes of source and destination in the network and capable of conducting the attack during data transmission. Internal attacks are more vulnerable to protect against this misbehaving because it is very difficult to detect them [14]. Black Hole Attack is known as routing misbehavior attack which leads to dropping of messages. Black Hole attack works in two phases. In the first phase the node advertises itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability [15]. This research empathizes on Black Hole attack, it's effects over MANET Network under DSR protocol algorithm, and optimization of DSR algorithm to reduce or eliminate the black hole attack effect over DSR Route Information based IEEE 802.11g MANET.

2. SIMUATION SETUP

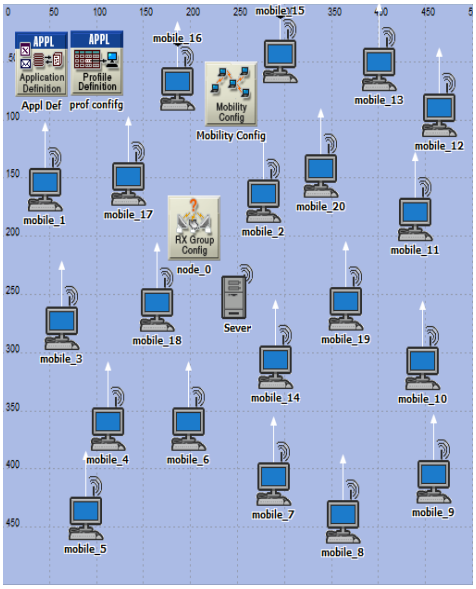

Figure 4: 20 node network scenario

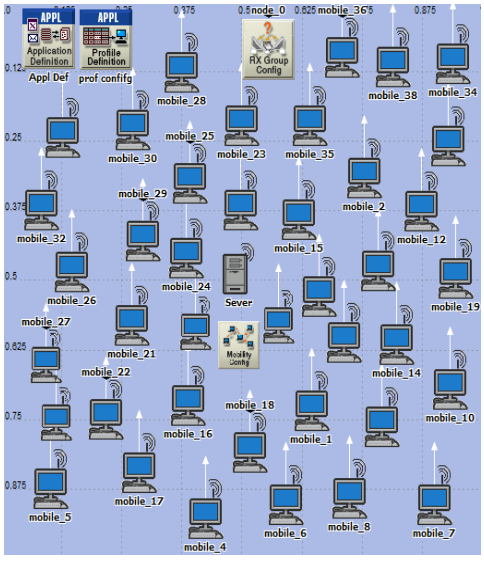

Figure 5: 40 node scenario

The DSR protocol is enhanced by optimizing its maintance hand-off time and Non- propagation route requests. The proposed algorithm is designed using OPNET Modeler 14.5 and investigated different MANET networks with varying network areas of [100*100 m^2, , 200*200 m^2, , 300*300 $m^2$and 400*400 m^2] with mobile nodes with mobility of uniform[0.8-1.2] m/s having densities [20, 40, 60, 80] respectively.

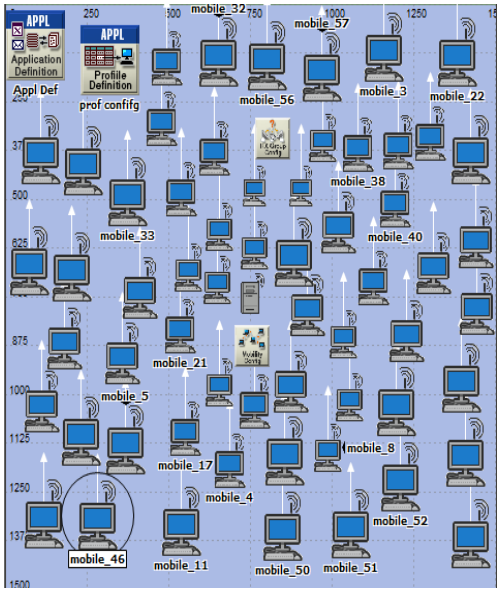

Figure 6: 60 Node Network Scenario

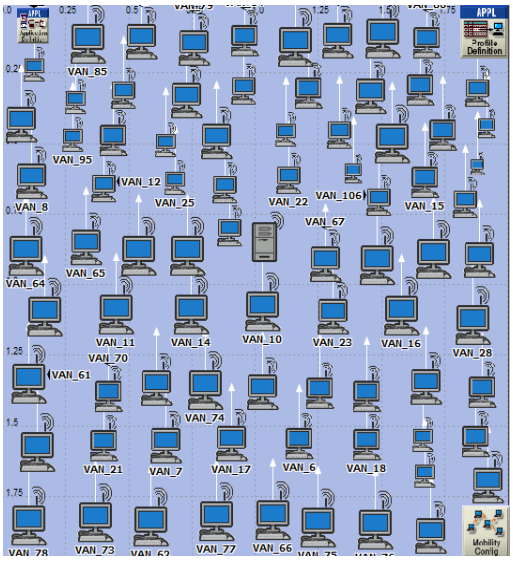

Figure 7: 80 node network scenarios

3. RESULTS AND DISCUSSION

To evaluate the overall performance of various reactive ad-hoc routing protocols, we have determined the various QoSparameters such as Throughput, End-to-End Delay, Route Discovery time, number of hops per route, Network Load for MANET network.

i) To analyze the performance of DSR for End-to-End Delay parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of End-to-

DOI 10.17148/IJARCCE.2015.41272

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

End Delay parameter is minimum for 20 nodes at 0.25 maintenance timeas shown in figure 8 and maximum at 0.15 for 80 nodes.

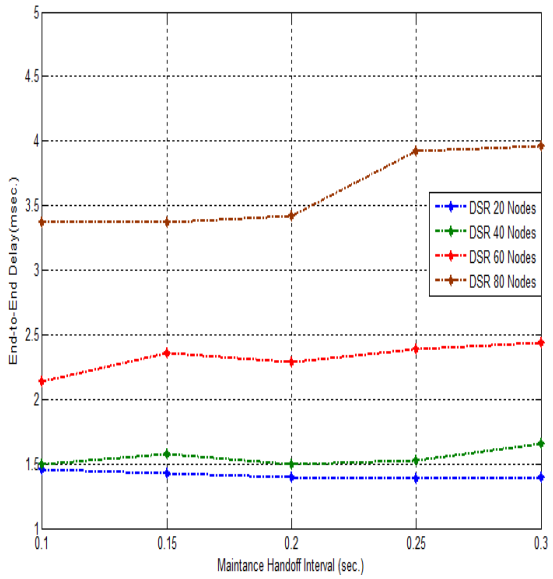

Figure 8: End-to-End Delay of traffic stations in IEEE 802.11g MANET at varying MHI

ii) To analyze the performance of DSR for Retransmission attempts parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of Retransmission attempts parameter is minimum for 20 nodes at 0.25 maintenance time as shown in figure 9and maximum at 0.3 for 80 nodes.

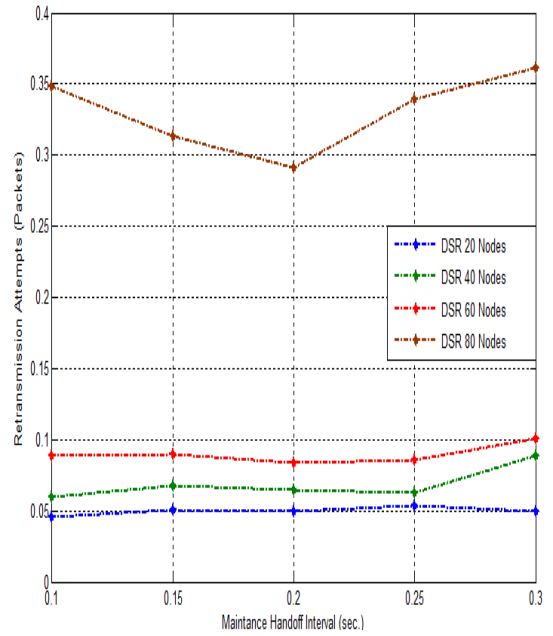

Figure 9: Retransmission Attempts of IEEE 802.11g MANET at varying MHI

iii) To analyze the performance of DSR for MANET throughput parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of MANET throughput parameter is maximum at 0.2 for 80 nodes as shown in figure 10.

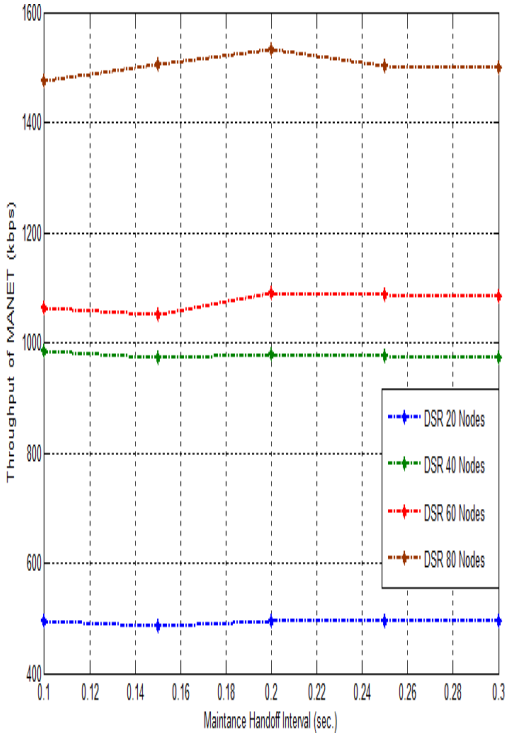

Figure 10: Throughput IEEE 802.11 g MANET at varying MHI

iv) To analyze the performance of DSR for Network Load parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of Network Load parameter is minimum at 0.1 for 20 nodes and maximum at maintenance hold off value of 0.25 for 80 nodes as shown in figure 11.

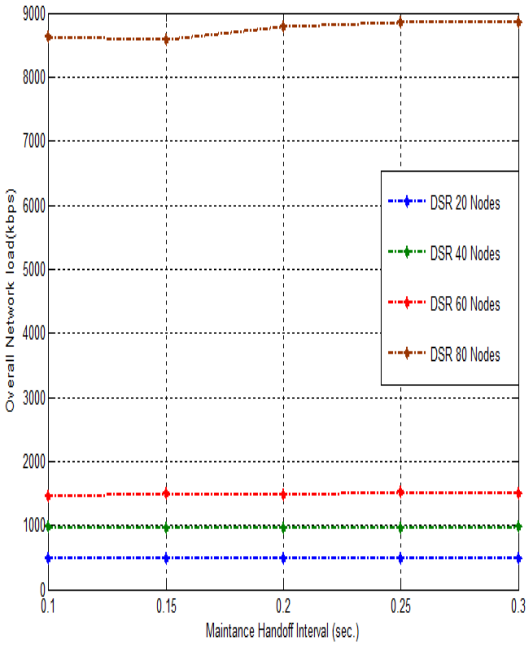

Figure 11: Network Load of IEEE 802.11g MANET at varying MHI

v) To analyze the performance of DSR for Packet Delivery Ratio parameter, it is plotted at Y axis along with

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

maintenance hold off time at X axis. The value of Packet Delivery Ratio parameter is maximum at 0.1 for 20 nodes and minimum at maintenance hold off value of 0.25 for 80 nodes as shown in figure 12.

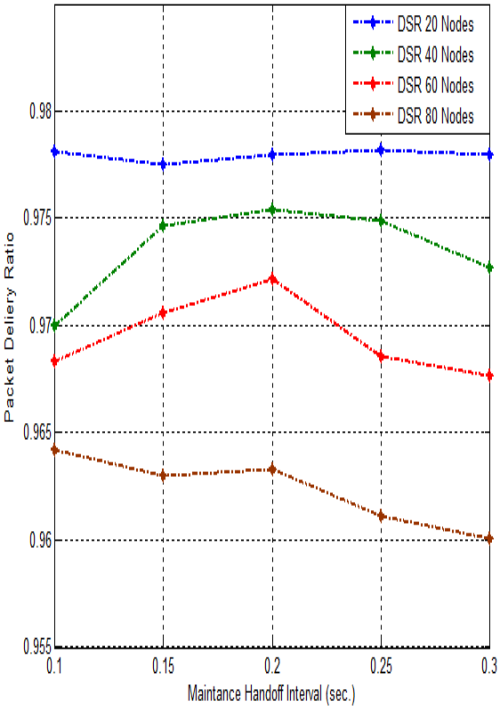

Figure 12: Packet Delivery Ratio of IEEE 802.11g MANET

vi) To analyze the performance of DSR for Normalized routing Load parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of Normalized routing Load parameter is minimum at 2.0 for 40 nodes and maximum at maintenance hold off value of 1 for 80 nodes as shown in figure 13.

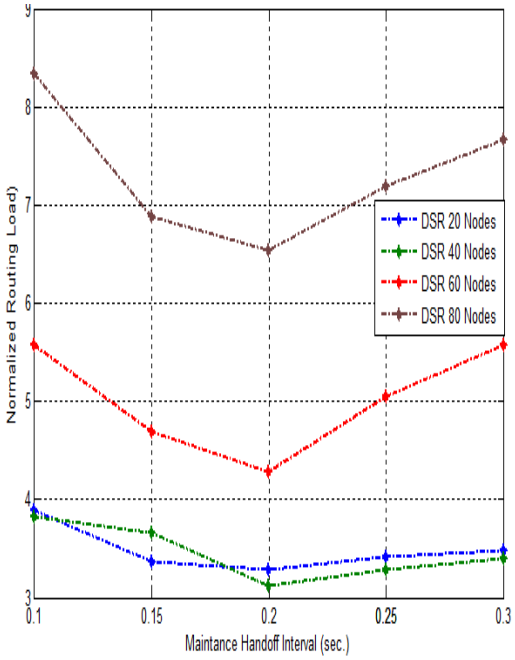

Figure 13: Normalized Routing Load of MANET Network

vii) To compare the performance of DSR and EDSR for End to End Delay parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of End to End Delay parameter for EDSR is reduced as compared to DSR as shown in figure 14.

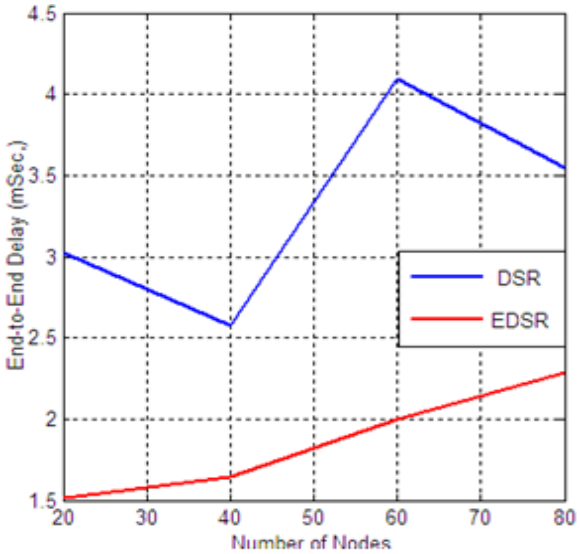

Figure 14: End-to-End Comparison b/w DSR & EDSR in IEEE 802.11g MANET w.r.t Node Density under Black Hole Attack

viii) To compare the performance of DSR and EDSR for Retransmission Attempts parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of Retransmission Attempts parameter for EDSR is reduced as compared to DSR as shown in figure 15.

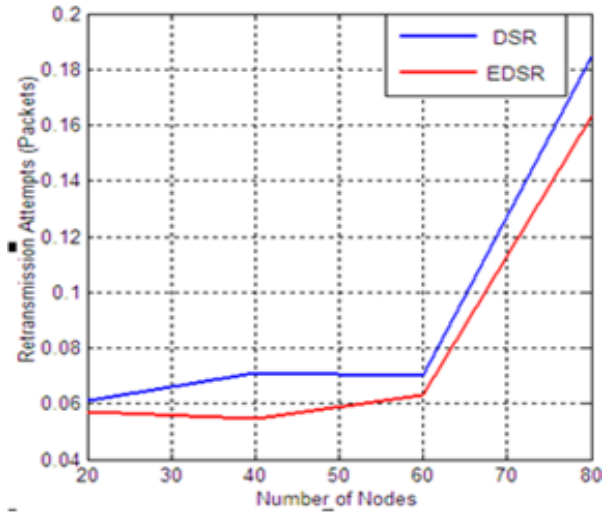

Figure 15: Retransmission Attempts Comparison b/w DSR & in IEEE 802.11g MANET w.r.t Node Density under Black Hole Attack

ix) To compare the performance of DSR and EDSR for Normalized Routing load parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of Normalized Routing load parameter for EDSR is reduced as compared to DSR as shown in figure 16.

DOI 10.17148/IJARCCE.2015.41272

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

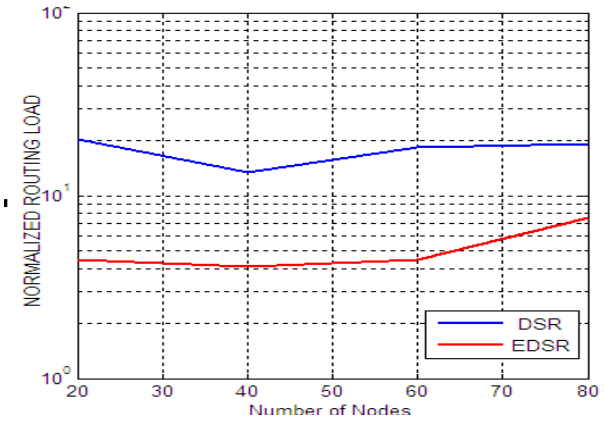

Figure 16: Normalized Routing Load Comparison b/w DSR & EDSR in IEEE 802.11g MANET w.r.t Node Density under Black Hole Attack

x) To compare the performance of DSR and EDSR for Number of Hops parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of Number of Hops parameter for EDSR is reduced as compared to DSR as shown in figure 17.

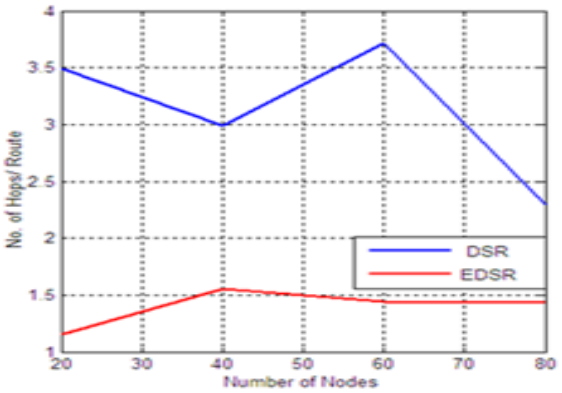

Figure 17: No. of Hops/ Route b/w DSR & in IEEE 802.11g MANET w.r.t Node Density under Black Hole Attack

xi) To compare the performance of DSR and EDSR for Packet Delivery Ratio parameter, it is plotted at Y axis along with maintenance hold off time at X axis. The value of Packet Delivery Ratio parameter for EDSR is enhanced as compared to DSR as shown in figure 18.

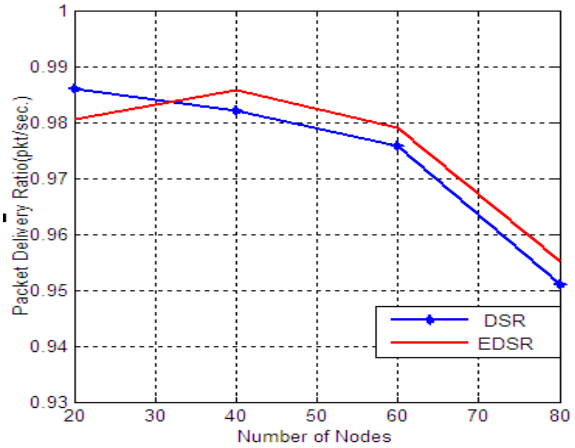

Figure 18: Packet Delivery Ratio Comparison b/w DSR & EDSR in IEEE 802.11g MANETw.r.t Node Density under Black Hole Attack

4. CONCLUSION

The simulation model of MANET network using DSR protocol is developed using OPNET 14.5 simulator and analyzed for different parameters. DSR value is evaluated at different densities like 20,40,60,80 nodes and also its value is enhanced for different parameters like end to end delay parameters, no of hops per route, retransmission attempts etc it's showed how the EDSR (Enhanced DSR) value is enhanced at different parameters.

REFERENCES

[1]. Kim, Y., Jeong, B.J., Chung, J., Hwang, C.S., Ryu J.S., Kim, K.H. and Kim, Y. K., "Beyond 3G: Vision, Requirements, and Enabling Technologies," IEEE Communications Magazine, pp. 120- 124, 2003.

[2]. IEEE Computer Society, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std. 802.11, 2007.

[3]. IETF MANET Working Group, "Mobile Ad Hoc Networks (MANET)," Working Group charter available: http://www.ietf.org/html.charters/manet-charter.html.

[4]. Taneja, S., Kush, A. (2010), "A Survey of Routing Protocols in Mobile Ad-hoc Networks", International Journal of Innovation, Management and Technology, vol. 1, No. 3, pp. 279-285.

[5]. Abolhasan, M., Wysocki, T., Dutkiewic, E. (2004), "A Review of Routing Protocols for Mobile Ad -Hoc Networks," ELSEVIER, Ad-hoc Networks (2004), vol. 2, pp. 1-24.

[6]. Elizabeth, M., Toh, C. (2007), "A Review of Current Routing Protocols for Ad-hoc Mobile Wireless Networks," Ad-hoc Networks 2, pp. 1-22.

[7]. Vishal Sharma, Vijay Banga, MandipKaur, "A Survey on Reactive Adhoc Routing Protocols in MANET Networks," CiiT-International Journal of Wireless Networking,DOI: WC042012001, ISSN: 0974-9640, 2012.

[8]. Johnson B., Maltz A., Hu C., "The Dynamic Source Routing Protocol for Mobile Adhoc Networks (DSR)," IETF Draft, work in progress, 2003, available at http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt.

[9]. Johnson, B., Maltz, A., Hu, C. (2004), "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks (DSR)," IETF Draft, work in progress, available at http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt.

[10]. Vishal Sharma, Vijay Banga, MandipKaur, "DSR Route Information based IEEE 802.11g MANET under the Influence of Node-Mobility," International Journal of Computer Applications, vol. 49, no.10, pp. 8-14, July 2012.

[11]. Vishal Sharma, Vijay Banga, MandipKaur, "Performance Evaluation of Reactive Routing Protocols in MANET Networks using GSM based Voice Traffic Applications," Accepted, Optik, Elsevier, Ref. No. 12-141, Date of Acceptance June 14, 2012.

[12]. D. Manikantanshila, Yu Cheng , TrichaAnjali, "Mitigating selective forwarding attacks with a Channel aware detection Approach in WMNS" IEEE Transactions on Wireless communications Vol.9, No.5, 2010.

[13]. G.S Mamatha, S.C. Sharma, "Network layer attacks and defense mechanism in MANETS- A Survey," International Journal of Computer Applications, 2010.

[14]. M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional conference, 2004.

[15]. Arya M., Jain Y., "Gary hole attack and prevention in Mobile Adhoc Network," International Journal of Computer Applications, Vol.27, No.10. Aug 2011.

[16]. Royer, M., Toh, K. (1999), "A Review of Current Routing Protocols for Ad-hoc Mobile Wireless Networks", IEEE Personal Communications, vol. 6, no. 2, pp. 46-55.
[17]. Frodigh, M., Johansson, P., Larsson, P. (2000), "Wireless Ad-hoc Networking- The Art of Networking without a Network," Ericsson Review No. 4, pp. 248-262.
[18]. Perkins, E., Royer, M., Das, R., Marina, K. (2001), "Performance Comparison of two On Demand Routing Protocols for Ad-hoc Networks," proceedings of IEEE Personal Communications, pp. 16-28.
[19]. Das, R., Castaneda, R., Yan, J., Sengupta, R. (2002), "Comparative Performance Evaluation of Routing protocols for Mobile Ad-hoc Networks," proceedings of 7th IEEE International Conference on Computer Communications and Networks- 98, vol. 1, pp. 153 - 161.
[20]. Johnson, B., Maltz, A., Hu, C. (2003), "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks (DSR)," IETF Draft, work in progress, available at http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt.
[21]. Johnson, B., Maltz, A., Hu, C. (2004), "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks (DSR)," IETF Draft, work in progress, available at http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt.
[22]. Kaosar, G., Asif, M., Sheltami, R., Ashraf, M. (2006), "Performance Improvement of Dynamic Source Routing Protocol Considering the Mobility Effect of Nodes in Cache Management," proceedings of IEEE International Conference on Wireless and Optical Communications Networks, IFIP 2006, pp.1-5.
[23]. IEEE Computer Society (2007), "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std. 802.11.
[24]. Shrestha, A., Tekiner, F. (2009), "On MANET Routing Protocols for Mobility and Scalability," IEEE International Conference on Parallel and Distributed Computing, Applications and Technologies, 2009, pp. 451-456.
[25]. Almutairi, A.F., El-Hendawy, T.M. (2011), "Performance investigation using different software of Dynamic Source Routing in ad-hoc networks," proceedings of IEEE GCC Conference and Exhibition, GCC 2011, pp. 307-310.
[26]. Banerjee S., "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks," Proceedings of the World Congress on Engineering and Computer Science, WCECS 2008, San Francisco, USA, 2008,
[27]. Sharma V., Banga V., Kaur M., "Performance Evaluation of Reactive Routing Protocols in MANET Networks using GSM based Voice Traffic Applications," Optik, Elsevier, 2012.
[28]. Sharma V.,Banga V., Kaur M. , "DSR Route Information based IEEE 802.11g MANET under the Influence of Node-Mobility," International Journal of Computer Applications, vol. 49, no.10, pp. 8-14, 2012.
[29]. Nitesh A., Pardhi P. R., "Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, 2013.
[30]. Dr. K. Selvakumar, N.Malarvizhi and V. SenthilMurugan, " Performance Evaluation of AODV Routing Protocol Under Black Hole Attack," Advances in Natural and Applied Sciences, 9(6) Special 2015, Pages: 150-155.
[31]. A.Ranichitra, V.LakshmiPraba," Security Enhancements of AODV Protocol: A Comparative Study," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.
[32]. Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.
[33]. AnuBala, MunishBansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", Proceedings of IEEE, 1st International Conference on Networks & Communications, 2009, pp. 141-145.
[34]. GaoXiaopeng and Chen Wei,"A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", Proceedings of IEEE, IFIP International Conference on Network and Parallel Computing – Workshops, 2007, pp. 209-214.
[35]. H. Jhaveri, J. Patel, C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks," Proceedings of IEEE, Second International Conference on Advanced Computing & Communication Technologies, 2012.
[36]. A.Pirzada, C. McDonald, and A. Datta, "Performance Comparison of Trust-Based Reactive Routing Protocols," IEEE Transactions on Mobile Computing Vol. 5, No.6 ,pp. 695-710, 2006
[37]. M. H. Mamoun, "Important Characteristic of Differences between DSR and AODV Routing Protocol," MCN 2007 Conference, November 7-10, 2007.
[38]. A. Tuteja, R. Gujral, S.Thalia, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET," Proceedings of IEEEE, International Conference on Advances in Computer Engineering, pp. 330-333, 2010.