International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016
ISSN 2091-2730

Performance Analysis of DSR Routing Protocol With and Without the Presence of Various Attacks in MANET

Aaditya Jain

M.Tech Scholar, Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, India

Email: aadityajain58@gmail.com

Abstract— In the present age mobility has become so pervasive that it influences all networking. New communication technologies are evaluated by accessing their potential role in the Internet. Mobile Ad-Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. It enables users to communicate without any physical infrastructure regardless of their geographical location, because of this feature, this is called infrastructure-less network. MANETS are more vulnerable to various types of attacks like blackhole, grayhole, flooding etc than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. The security issues in MANET are mostly concentrated in two parts establishing secure route and securely data transmission. This paper is a simulation based study of DSR on demand MANET routing protocol by using Network Simulator tool NS 2 in the presence of various routing attacks as mentioned above. Basically we emphasis on three performance matrices i.e. packet delivery ratio, average end to end delay and average throughput and based on this we analyze the performance of the DSR routing protocol.

Keywords— MANET, Routing Protocol, DSR, NS2, Routing Attacks, Blackhole, Grayhole, Rushing attack.

I. INTRODUCTION

A mobile ad hoc network (MANET), sometimes called a wireless ad hoc network or a wireless mesh network of mobile nodes, comprises of mobile computing devices (nodes) that uses wireless transmission for communication, without the presence of any established infrastructure or administration such as an access point in wireless local area network or a base station in cellular network [1]. The nodes are free to move randomly and organize arbitrarily thus, the topology of the wireless network may change rapidly and unpredictably. Unlike traditional mobile wireless networks, MANETs do not rely on any central coordinator. Mobile nodes can communicates to each other directly via wireless links if nodes are within each other radio range, while nodes are far apart, should rely on other nodes to relay messages as routers. In mobile ad hoc network each node acts both as a host (capable of sending and receiving) and a router (forwards the data intended for some other node). Hence such networks sometime call as multi-hop wireless ad hoc networks.

To manage multi-hop behavior of MANET there is a need of routing protocol. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. But one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Here we analyze DSR routing protocol performance.

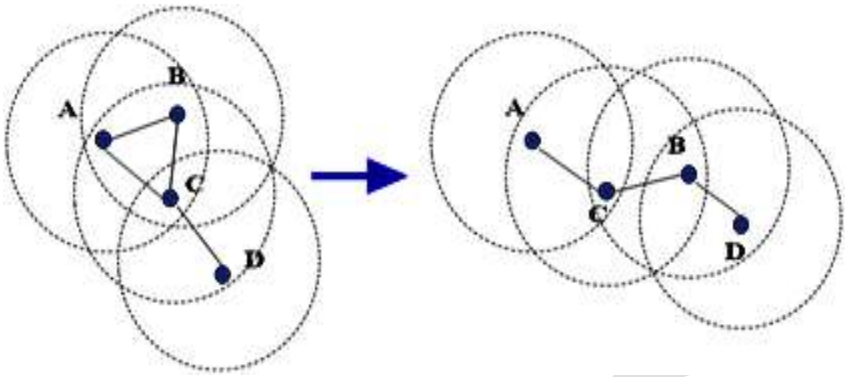

Fig. 1 MANET Dynamic Topology

II. ROUTING ATTACKS IN MANET

Mobile ad hoc network is not free from different active and passive attacks [2]. A passive attack does not disrupt the normal operation of the network, gathering information is the primary aim. On the other hand active attacks disrupt the normal functioning of the network by altering or destroying data. In this paper we emphasis on three types of attacks blackhole, grayhole, and rushing attack.

BLACKHOLE ATTACK

The goal of the malicious node in this attack is to drop all packets that are directed to it instead of forwarding them as intended. It uses its routing protocol in order to advertise itself as having the shortest route to the target node or to any packet that it wants to intercept. The malicious node advertises its availability of new routes without checking its routing table [3, 8]. In this way the malicious node will always have availability of routes while replying to the route request and hence intercept the data packet. As a result of the dropped packets, the amount of retransmission consequently increases leading to congestion.

GRAYHOLE ATTACK

Grayhole attack is an extension of blackhole attack in which a malicious node's behavior is exceptionally unpredictable. There are three behaviors of Grayhole attacks [4]. In first, the malicious node may drop packets from certain nodes while forwards all other packets. In second type, a node may behave maliciously for a certain time, but later on it behaves just like other ordinary nodes. Third type of attack is the combination of both attacks i.e. the malicious node may drop packets from specific nodes for certain time only, later it behaves as a normal node. Due to these characteristics, detection of grayhole attacks is not an easy task.

RUSHING ATTACK

The working principal of this attack is same as an effective denial-of-service attack. In this attack, the route request (RREQ) packet sent by the source node to the malicious node is flooded throughout the network by this malicious node quickly enough to prevent other nodes from reacting to the same RREQ[3,4]. The other nodes that receive the duplicate RREQ from the attacker simply ignore them. Hence, any route discovered by the source node will have the malicious node as an intermediate point in the route. Most of the current on-demand ad hoc routing protocols are vulnerable to this attack due to the fact that most of them use duplicate suppression during the route discovery process.

III. MANET ROUTING PROTOCOL

Routing protocols in MANET specifies how nodes communicate with each other, routing information that enables them to select routes between any two nodes on a network. So the communication in the network depends on the efficiency and optimality of the routing algorithm. According to root finding methodology two types of strategies we preferred Proactive Routing and Reactive Routing [5].

In proactive routing all routes to each destination are maintained in up to date table like in "Destination Sequenced Distance Vector" routing protocol where as in reactive routing protocol route is only found when it is asked by the source node and route is maintained unless it is asked to terminate by the source node or after time exceed like in Dynamic Source Routing protocol.

DYNAMIC SOURCE ROUTING PROTOCOL

The Dynamic Source Routing (DSR) is an on demand routing protocol that is based on the concept of source routing in which source is responsible for providing information of whole path [6]. It is designed especially for use in multihop ad hoc networks of mobile nodes. DSR is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the network. DSR has a unique advantage by virtue of source routing [9].

In Route Discovery phase source finds path to destination by broadcasting RREQ packet. Each node retransmits the RREQ packet if it has not forwarded a copy of it, provided that the Time-To-Live has not been exceeded. Each RREQ carries a sequence number generated by the source node and the path it has traversed. In this protocol intermediate node uses cache that stores all possible information extracted from the source route contained in a data packet. When destination receives the RREQ packet, it sends a RREP packet to source node, listing the route taken by request packet. Source node selects route with lowest latency. In route maintenance, whenever a link break, the RERR packet propagates to the original source, which in turn initiates a new route discovery process. DSR also allows piggy-backing [10].

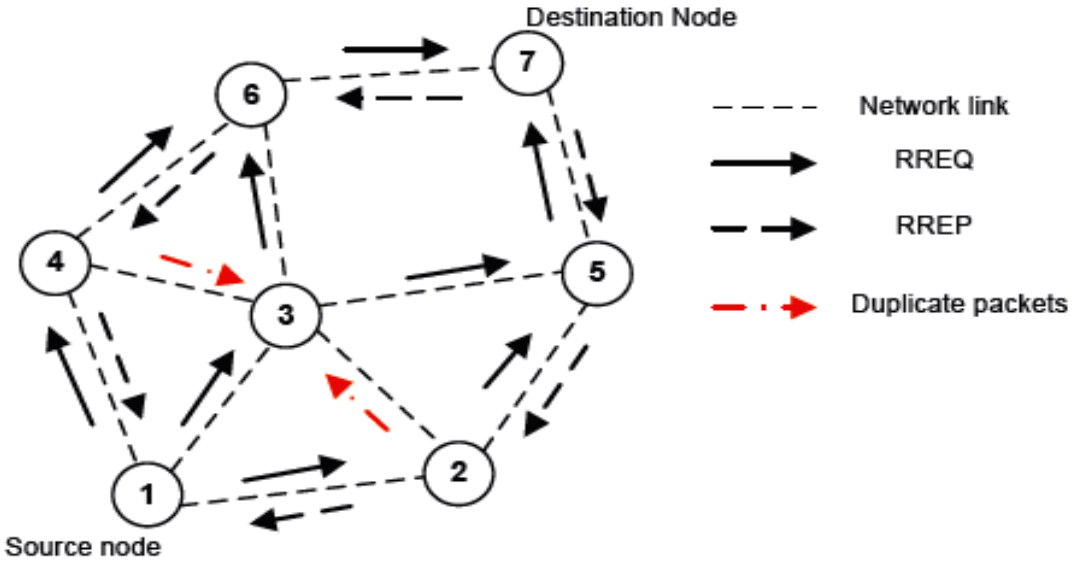

Fig. 2 Route Discovery in DSR

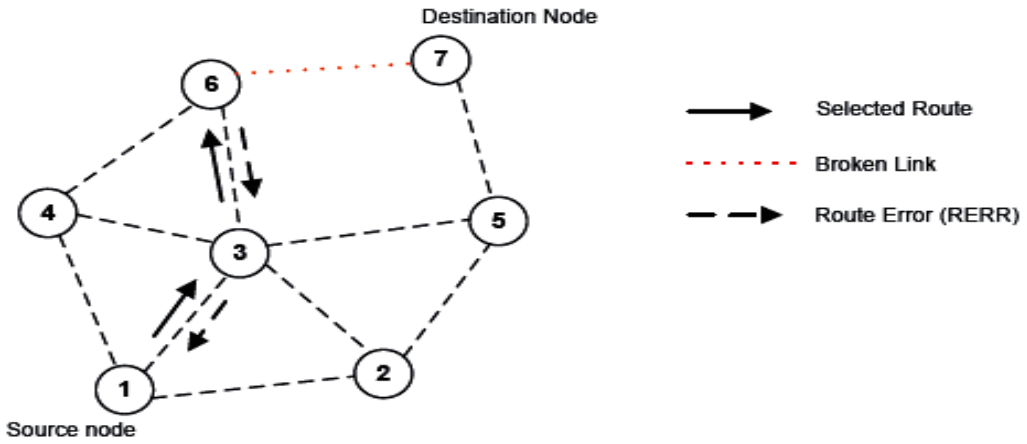

Fig. 3 Route Maintenance in DSR

IV. SIMULATION MODEL

Network Simulator is event driven object oriented simulator [7]. It uses Object Oriented Tool Command Language (OTcl) to interpret user simulation scripts and Tcl language is fully compatible with the C++.The overall goal of simulation study in this paper is to analyze the performance of DSR on demand based routing protocol with and without the presence of various attacks like blackhole, grayhole and rushing attack. The simulations were performed using Network Simulator 2 (NS2). The source-destination pairs are spread randomly over the network. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. Different network scenario for different number of nodes and pause times are generated.

PERFORMANCE METRICS

- Packet Delivery Ratio-The ratio of the data packets delivered to the destination to those generated by the source.
- Average End to End Delay-This metrics represents average end-to-end delay that indicates how long it took for a packet to travel from the source to the application layer of the destination.
- Average Throughput-This metrics represents the average number of bits arrived per second at destination and measured in bps.

SIMULATION PARAMETERS

Table 1shows mobility scenarios that are generated by using a random way point model by varying 25 to 150 nodes moving in simulation area of 1000m x 1000m. This simulation used the following parameters.

Table1 Simulation Parameters

Simulator	NS-2 (Version 2.35)
Simulator Time	500 (s)
Number of Nodes	25, 50, 75, 100, 125, 150

Simulation Area	1000 x 1000m
Routing Protocol	DSR
Traffic	CBR (Constant Bit Rate)
Pause Time	10 (ms)
Packet Size	512 bytes
Movement Model	Random Way Point
Movement Model	Random Way Point

PERFORMANCE ANALYSIS UNDER BLACKHOLE ATTACK

Fig 4 shows that packet delivery ratio of DSR with blackhole attack and without blackhole attack. It is observed from the graph that the performance of packet delivery ratio in DSR is better as compare to blackhole attack. Due to this attack packets got dropped and it causes decrease in delivery ratio of packets.

Fig 5 shows the average end to end delay of DSR routing protocol. The graph shows that delay with blackhole attack is much higher than without blackhole because the packets are dropped by malicious node and DSR adjust its changes in it during node restart and node pausing thus increases the delay.

Fig 6 shows the average throughput of DSR routing protocol in the presence and absence of blackhole attack. It is observed that average throughput of DSR under blackhole is less than normal DSR. When the numbers of nodes are increased, the performance of protocol is reduced but then it maintained constant up to the number of nodes 125 then it slightly increase due to effect of blackhole.

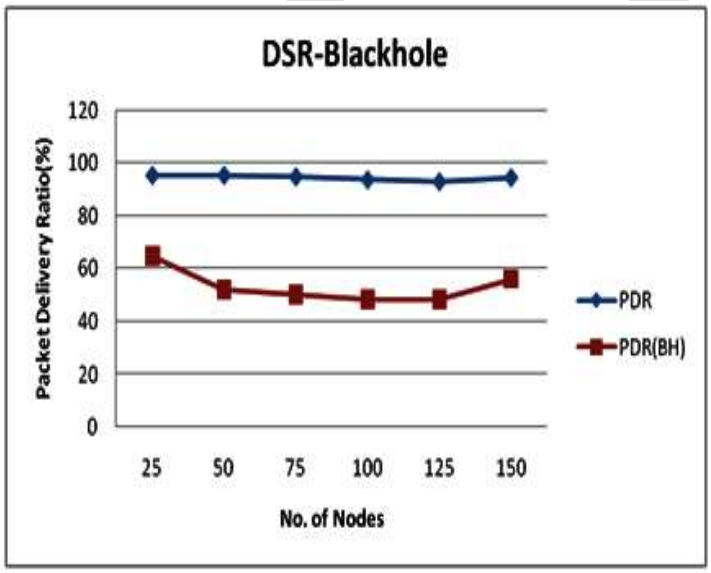

Fig. 4 Packet delivery ratio in DSR with and without blackhole attack

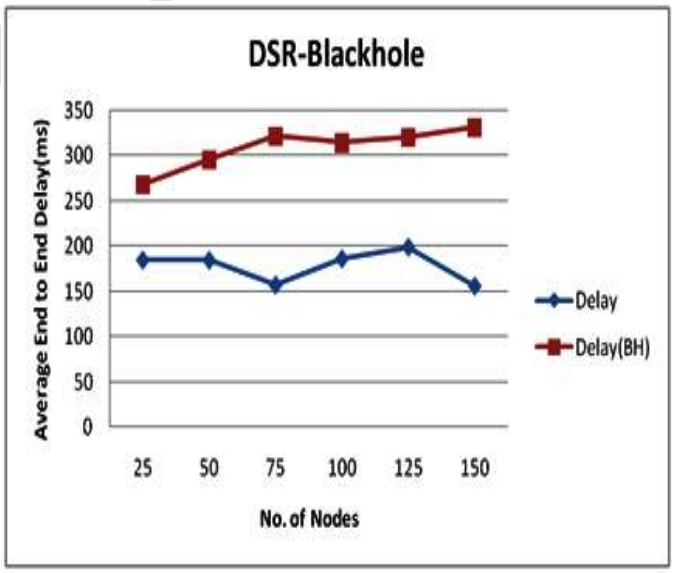

Fig. 6 Average throughput of DSR with and without blackhole attack

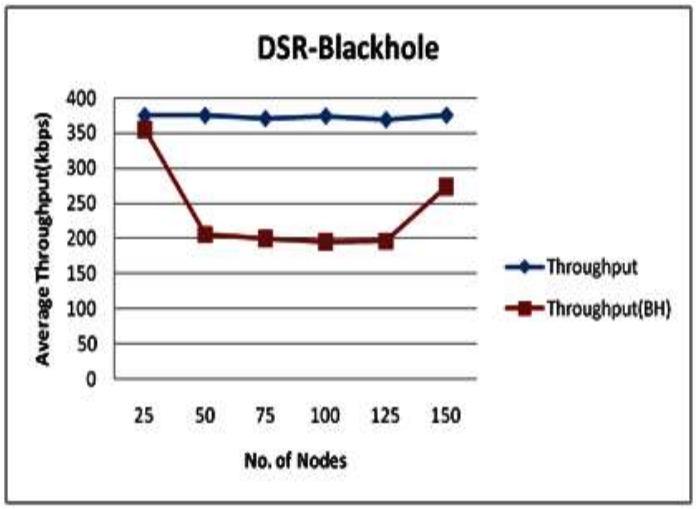

Fig. 5 Average end to end delay in DSR with and without blackhole attack

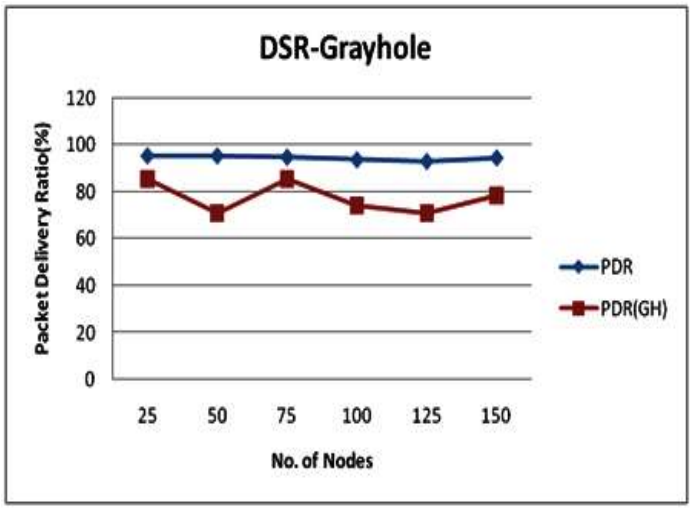

Fig.7 Packet delivery ratio of DSR with and without grayhole attack

PERFORMANCE ANALYSIS UNDER GRAYHOLE ATTACK

Fig. 7 shows the DSR with and without grayhole attack. It is observed that packet delivery ratio of DSR under grayhole attack decreases because grayhole attack drops the packets arbitrary so many packets do not reach to destination.

Fig. 8 shows the effect of grayhole on average end to end delay of DSR. Delay of DSR with grayhole is higher than without grayhole because it adds additional delay in route discovery phase.

Fig. 9 shows that with increasing density of nodes in network, difference between average throughput of DSR with and without grayhole attack is high and throughput under grayhole is less because attacker node discards many packets attracted by it.

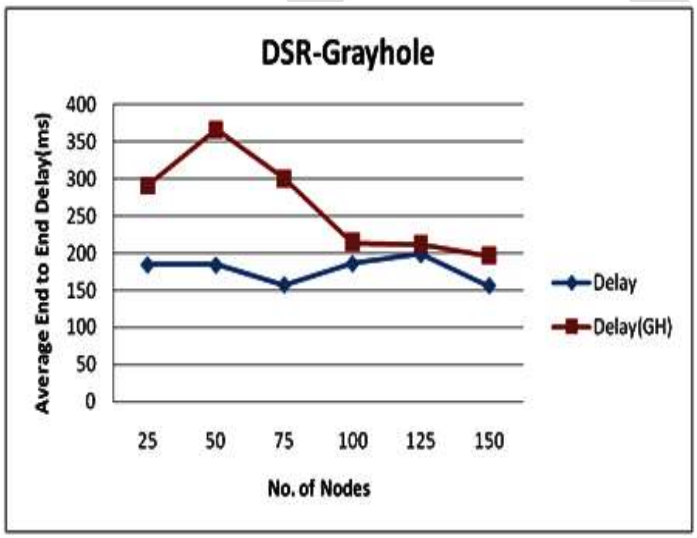

Fig. 8 Average end to end delay of DSR with and without grayhole

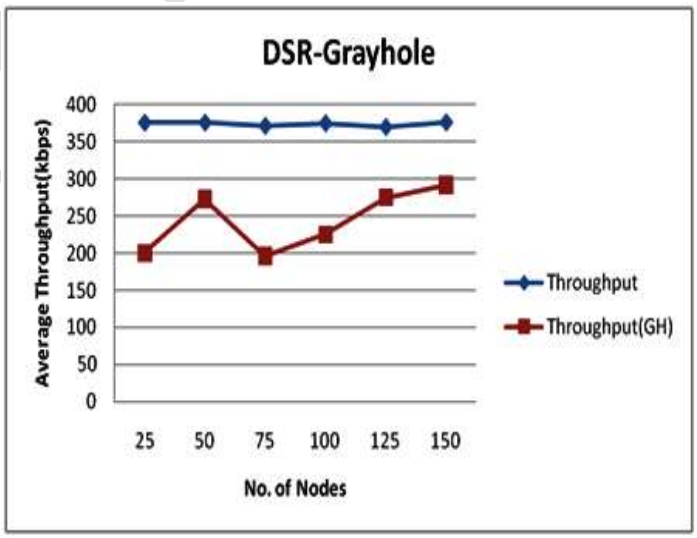

Fig. 9 Average throughput of DSR with and without grayhole attack

Performance analysis under rushing attack

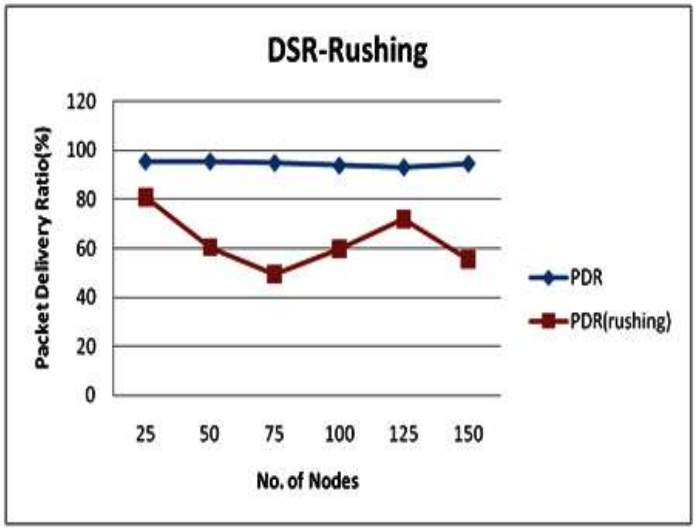

Fig. 10 Packet delivery ratio of AODV with and without rushing attack

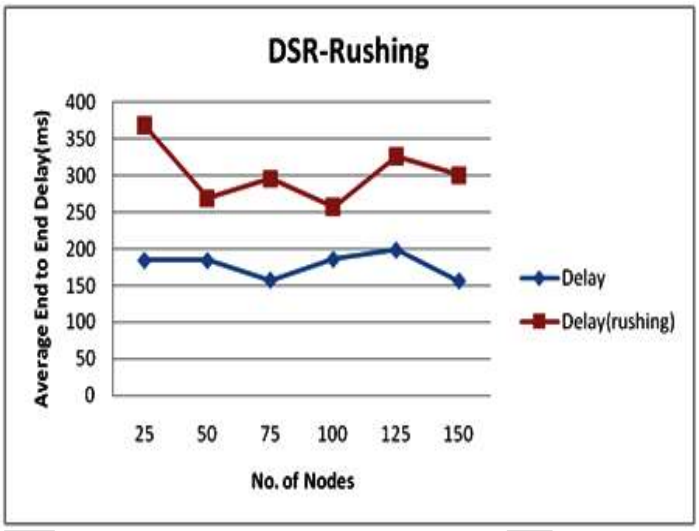

Fig. 11 Average end to end delay of AODV with and without rushing attack

Fig 10 shows the packet delivery ratio of AODV with and without rushing attack. Graph shows that packet delivery ratio of AODV with rushing is less than normal AODV because some packets are dropped by byzantine attack.

Fig 11 shows the impact of rushing attack on average end to end delay of AODV routing protocol. Graph shows that end to end delay of AODV with rushing attack is higher than AODV without attack because it is also used Jellyfish attack which produces delay before the transmission and reception of data packets in the network.

Fig 12 shows the average throughput of AODV with and without rushing attack. It shows that throughput of AODV is higher than throughput of AODV with rushing attack due to property of byzantine attack in which attacker drop packets so received packets are less than original AODV.

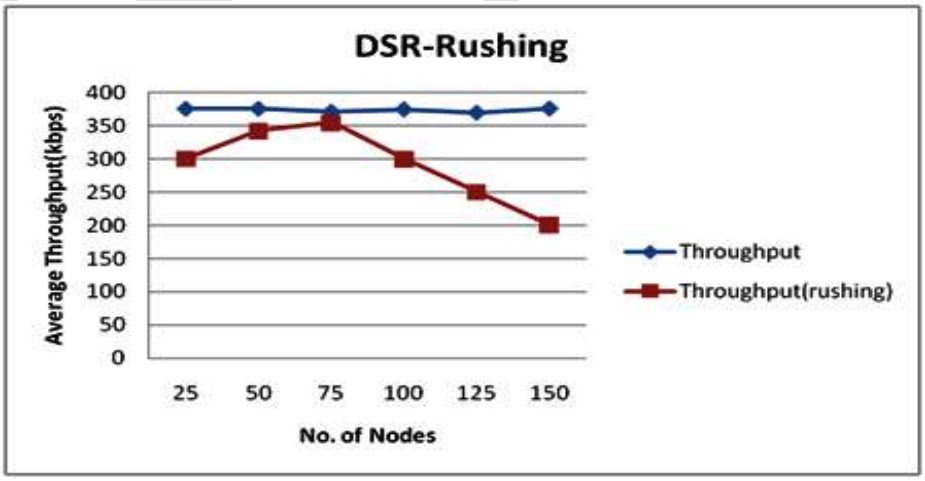

Fig. 12 Average throughput of AODV with and without rushing attack

V. ACKNOWLEDGMENT

I would like to express my deep sense of respect and gratitude towards “Dr. Bala Buksh”, Professor Department of Computer Science

& Engg., who has been the guiding force behind this work. Without his unconditional support it wouldn't have been possible.

VI. CONCLUSION

MANET can be deployed easily in a situation where a traditional network is not possible due to its special characteristics such as flexibility and dynamic nature. The aim behind this research paper is to analyze the effect of many attacks under CBR traffic in different scenarios for DSR MANET routing protocol. Based on investigations and data analysis of simulation results, it is concluded that without the presence of any routing attack DSR perform well in lightly loaded networks. But the presence of blackhole, grayhole, and rushing attack at the time of routing effects on overall performance of DSR protocol by decreasing packet delivery ratio and average throughput but by increasing average end to end delay.

REFERENCES:

[1] S. Basagni, M.Conti, S. Giordano and I. Stojmenovic, "Mobile Ad Hoc Networking", A John Wiley & Sons, Inc., Publication, 2004, ISBN 0-471-37313-3.

[2] Djamel Djenouri, L Khelladi, and N Badache. A survey of security issues in mobile ad hoc networks. IEEE communications surveys, 7(4), 2005.

[3] A. Pegueno and J. R. Rivera, Extension to MAC 802.11 for performance Improvement in MANET, Masters Thesis at Karlstads University, Sweden, December 2006.

[4] Amara korba, Abdelaziz, Mehdi Nafaa and Ghanemi Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", IEEE 15th International Conference on Computer Modelling and Simulation, 2013.

[5] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. A secure routing protocol for ad hoc networks. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, pages 78-87, 2002.

[6] D B. Johnson, D A. Maltz, and Y. Hu, "The Dynamic Source Routing Protocol For Mobile Ad Hoc Network", *Internet-Draft*, July 2004.

[7] NS-2 Network Simulator http://www.isi.edu/nsnam/ns.

[8] Sun, Y. Guan, J. Chen and U.W. Pooch, "Detecting black-hole attack in mobile ad hoc networks", Proc. 5th European Personal Mobile Communications Conference, Apr. 2003, pp. 490-495.

[9] Robinpreet Kaur & Mritunjay Kumar Rai "A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012.

[10] M. Krishnamoorthi, Dr. K. Gokulraj, "A Study on AODV and DSR MANET Routing Protocol", International Journal of Computer Networks & Wireless Communications, Vol. 5, No 4, 2015.