ISSN:0975-9646

A Comparative Analysis of DSR and AODV Protocols under Blackhole and Grayhole Attacks in MANET

Monika Verma[#1], Dr. N. C. Barwar[*2]

[#] *M.E. Scholar, Department of Computer Science & Engg., M.B.M. Engineering College,*
J.N.V. University, Jodhpur, India

[*] *Assoc. Prof., Department of Computer Science & Engg., M.B.M. Engineering College,*
J.N.V. University, Jodhpur, India

***Abstract*— Over the past decade, there has been a lot of research in the area of Mobile Ad-hoc NETwork(MANET). MANETs are autonomous, self-organized, infrastructure-less and decentralized wireless systems in which mobile nodes behave as a router as well as host. MANETs are mainly useful in military and other tactical applications such as emergency rescues. Security is the main challenge in these networks due to its nature as mobile and open media. There are various attacks among them blackhole and grayhole are most affecting the network working by dropping packets. In this paper the performance of MANET routing protocols, AODV and DSR, with blackhole and grayhole attack have been analysed under different scenarios using CBR traffic using NS2 taking various parameters such packet delivery ratio, average end to end delay and average throughput to compare and evaluate their performance.**

***Keywords*—MANET, AODV, DSR, Blackhole, Grayhole.**

I. INTRODUCTION

Mobile ad hoc Network (MANET) is a self-configuring network in which mobile nodes are free to move in random fashion and work in cooperatively in ad hoc manner [1]. Nodes can act as host/router or both at the same time. In a MANET, nodes within each other radio ranges can communicate directly, however, nodes outside each other's range have to rely on some other nodes' to relay messages, means success of communication highly depends on other nodes cooperation, this is called multi-hop communication. Routing in a MANET is a challenging task compared to a conventional network because of unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power. There are many routing protocols available for MANET which is broadly classified into three types: proactive (or table-driven), reactive (or on-demand) and hybrid.

MANET often suffers from security attacks because of its features [2], many of them targets the routing protocols. The attacks on routing protocols can generally be classified as passive and active attacks. A passive attack does not disrupt the operation of the protocol, but attempts to figure out valuable information by listening to traffic. Instead an active attack disrupts the operation of the protocol in order to gain unauthorized access, circumscribe availability or degrade the network performance. Some of them are wormhole attack, blackhole attack, grayhole attack, byzantine attack, rushing attack etc.

II. MANET ROUTING PROTOCOLS

A. *Dynamic Source Routing (DSR)*

DSR is a reactive MANET routing protocol means it discovers a route to destination only when it is required [3]. It uses source routing in which source is responsible for providing information of whole path. There is no need of any beacon in DSR. Basically DSR maintains two phases: Route Discovery and Route Maintenance as shown in Fig. 1 and 2. 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.

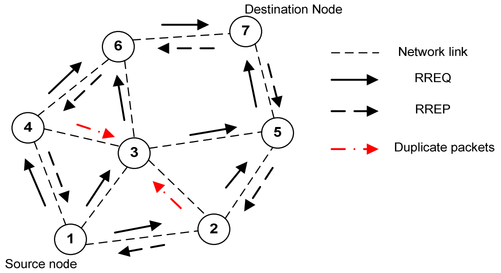

Fig. 1 Route Discovery in DSR

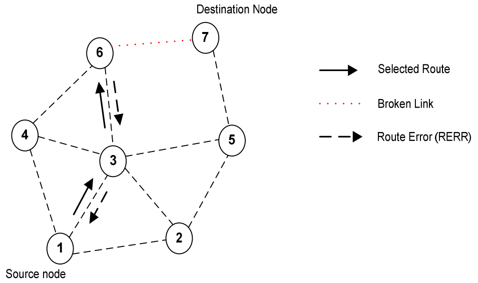

Fig.2 Route Maintenance in DSR

B. *Ad-Hoc On-Demand Distance Vector(AODV)*

Ad hoc On-Demand Distance Vector (AODV) is also an on-demand MANET routing protocol [4]. Basically AODV maintains two phases: Route Discovery and Route Maintenance as shown in Fig. 3 and 4. AODV finds routes using the route discovery process similar to DSR and uses destination sequence numbers to compute fresh routes. In route discovery phase, source node broadcast RREQ packet like DSR. This packet contains the source identifier (SId), the destination identifier (DId), the source sequence number (SSeq), the destination sequence numbers (DSeq), the broadcast identifier (BId) and TTL fields. When an intermediate node receives a RREQ packet, it either forwards it or sends RREP packet to source, if it has a valid route to the destination in its cache. The pair of SId and BId is used to detect if the node has received an earlier copy of the RREQ. Before forwarding RREQ, every intermediate node store the previous node’s address and it’s BId. Intermediate node also maintains a timer with every entry to delete RREQ if reply is not received before it expires. Whenever a RREP is received by a node, it stores the information of the previous node, thus each node maintains only the next hop information. In route maintenance, whenever a link break, the RERR packet propagates to the source, which again initiates a new route discovery process.

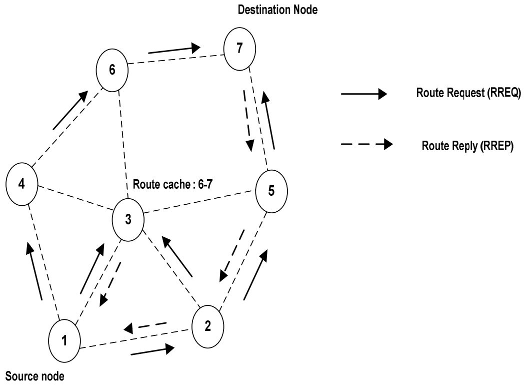

Fig. 3 Route discovery in AODV

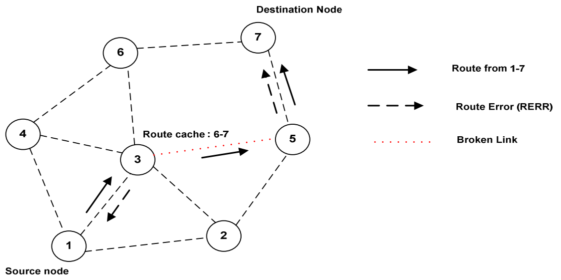

Fig. 4 Route Maintenance in AODV

III. Routing Attacks In Manet

A. *Blackhole Attack*

Blackhole attack is a kind of active attack [5]. In this attack, Blackhole immediately sends a false route reply messages when it receives an RREQ message, without checking its routing table. These false route reply messages are to inform other nodes in the network that the destination is on the next hop from this attacker node and the attacker node has the best route to that destination. All neighbouring nodes update their routing tables and make the attacker node their next hop for the destination. Now when this attacker node receives the data packets, it drops all the packets and the packets do not reach the destination [9].

B. *Grayhole Attack*

Grayhole attack is extension of blackhole attack [5]. In this attack grayhole node attracts traffic like blackhole attack but does not drop all packets. It may simply drops packets coming from (or destined to) certain specific node(s). Another type of grayhole node may drops packets for some time duration and then switch to normal behaviour. A grayhole may also use combination of both types which make it difficult to detect [9].

IV. NS2 Simulation

Network Simulator is event driven object oriented simulator [13]. It uses OTcl (Object oriented Tool Command Language) programming language to interpret user simulation scripts and Tcl language is fully compatible with the C++. NS is an interpreter of Tcl scripts of the users; they work together with C++ codes.

A. *Performance Metrics*

The following performance metrics are considered for evaluation of MANET routing protocols:

1) *Packet Delivery Ratio*: The ratio of the data packets delivered to the destination to those generated by the source.

2) *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.

3) *Average Throughput:* This metrics represents the average number of bits arrived per second at destination and measured in bps.

In this work NS simulator is used for the simulation. 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. Table I show the parameters used in simulation.

TABLE I
Simulation Parameters

Simulator	**NS-2 (version 2.35)**
Simulation Time	500 (s)
Number of Nodes	25,50,75,100,125,150
Simulation Area	1000 x 1000m
Routing Protocols	AODV and DSR
Traffic	CBR(Constant Bit Rate)
Pause Time	10 (ms)
Packet Size	512 bytes
Movement Model	Random Way Point

B. Simulation Results and Performance Analysis

Fig. 5 shows the packet delivery ratio of AODV and DSR routing protocols under blackhole attack. The graph shows that when the numbers of nodes are less, then DSR outperforms as compare to AODV but when number of nodes increased then packet delivery ratio of DSR is less as compare to AODV because AODV inherits the properties of both DSDV and DSR.

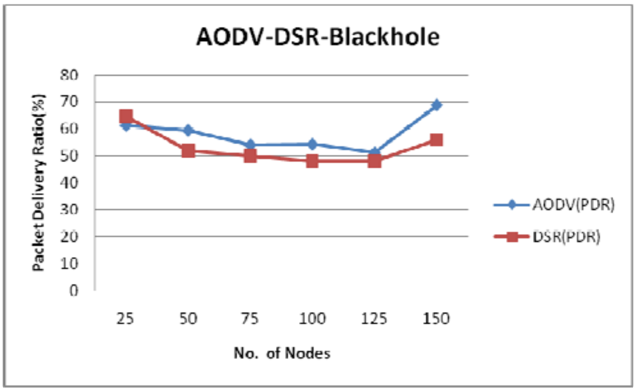

Fig. 5 Packet Delivery Ratio of AODV and DSR with blackhole attack

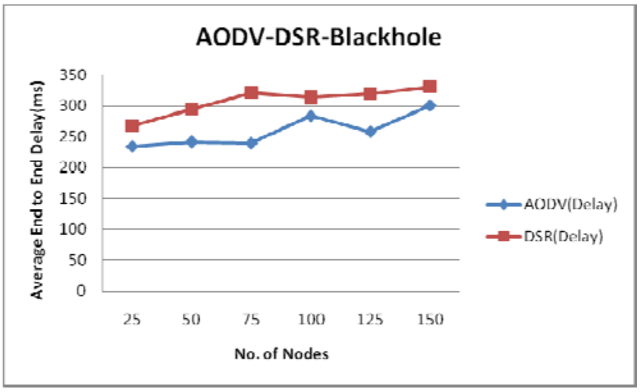

Fig. 6 Average End to End Delay of AODV and DSR with blackhole attack

Fig. 6 illustrates average end to end delay of AODV and DSR routing protocols with blackhole attack. It is clearly seen from the graph that end to end delay of DSR is higher than AODV due to caching overhead of DSR.

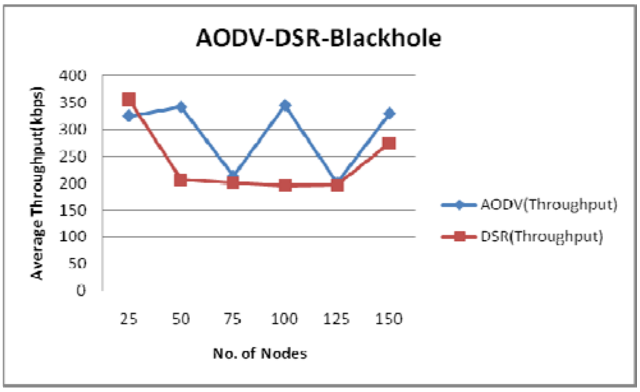

Fig. 7 Average Throughput of AODV and DSR with blackhole attack

Fig. 7 depicts the effect of varying amount of nodes on the average throughput. It is seen from the graph that throughput of DSR is less than AODV in the presence of blackhole attack.

From the overall observation of AODV and DSR routing protocols under blackhole attack it observed that DSR is more affected by blackhole than AODV in high node density network because of additional routing overhead of DSR.

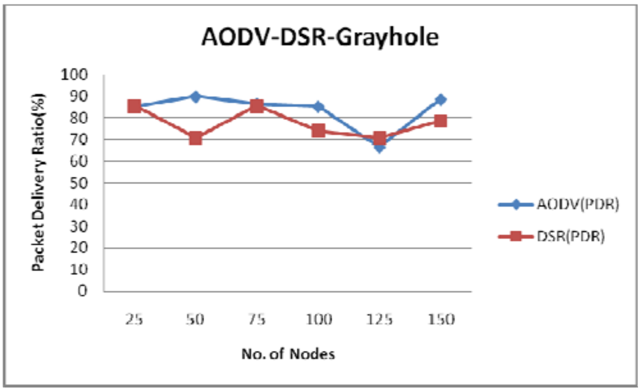

Fig. 8 Packet Delivery Ratio of AODV and DSR with grayhole attack

Fig. 8 shows the packet delivery ratio of AODV and DSR routing protocols under grayhole attack. The graph shows that packet delivery ratio of DSR is less than AODV because AODV inherits the properties of both DSDV and DSR.

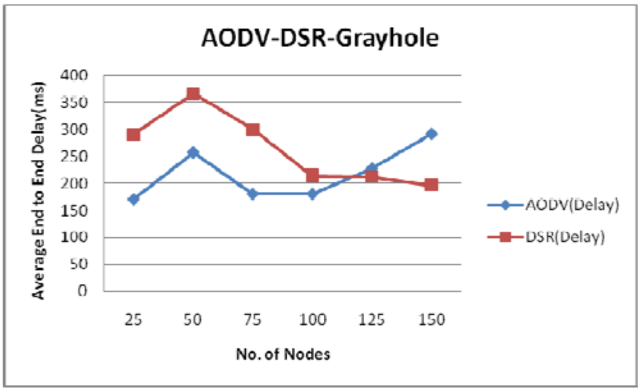

Fig. 9 End to End Delay of AODV and DSR with grayhole attack

Fig. 9 illustrates average end to end delay of AODV and DSR routing protocols with grayhole attack. Delay of DSR is higher than AODV because of higher routing load and multiple route caches for a destination.

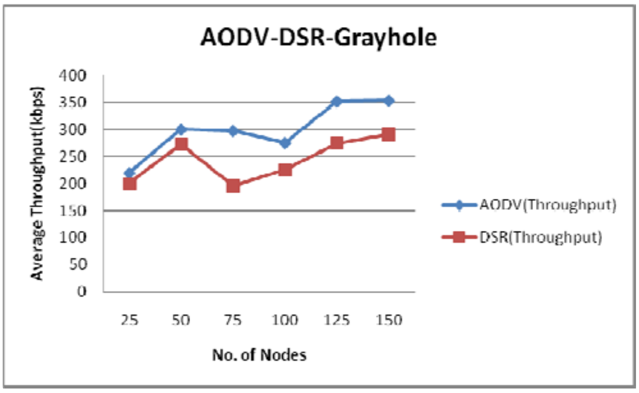

Fig. 10 Average Throughput of AODV and DSR with grayhole attack

In Fig. 10, effect of number of nodes on the average throughput is shown. Graph shows that throughput of DSR is less than AODV in the presence of grayhole attack.

From the overall observation of AODV and DSR routing protocols under grayhole attack, it observed that DSR has lower performance in the presence of garyhole than AODV in high node density network because of additional routing overhead of itself.

V. Conclusions

In this paper, performance analysis of blackhole and grayhole attacks under CBR traffic in different scenarios taking AODV and DSR MANET routing protocols are simulated under NS2. Different performance metrics like Packet Delivery Ratio, Average End-To-End delay and Average Throughput are used for analysis. It is concluded that (i) packet delivery ratio of DSR is less than AODV in blackhole as well as grayhole but the overall performance of both the protocols have slightly improves in grayhole. (ii) Average end to end delay is higher in DSR as compare to AODV in blackhole and grayhole but delay of both the protocols have slightly improves in grayhole as compare to blackhole. (iii) Average throughput of DSR is less than AODV in blackhole as well as grayhole but the overall performance of both the protocols have slightly improves in grayhole.

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] Imrich Chlamtac, Marco Conti and Jennifer J.-N.Liu, "Mobile ad hoc networking: imperatives and challenges", *Ad Hoc Networks*, 2003 Elsevier.

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

[4] C.E. Perkins, E. Royer, and S.R. Das, "Ad Hoc On Demand Distance Vector(AODV) Routing," *Internet Draft*, July 2003.

[5] 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.

[6] H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks", *University of Cincinnati, IEEE Communication Magzine*, Oct, 2002.

[7] F.Tseng, L. Chou and H.Chao, "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks", *Journal on Human-Centric Computing and Information Sciences*, Springer, Vol.1, No.4, pp. 1-16, 2011.

[8] Mohammed Saeed Alkatheiri, Jianwei Liu and Abdur Rashid Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs", 978-1-61284-307-0/11, 2011 IEEE.

[9] Hizbullah Khattak, Nizamuddin, Fahad Khurshid and Noor ul Amin, "Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash", 978-1-4673-5200-0/13, 2013 IEEE.

[10] Neeraj Arora and Dr. N. C. Barwar, "Performance Analysis of DSDV, AODV and ZRP under Blackhole attack", *International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181, Vol. 3 Issue 4, April – 2014.

[11] Neeraj Arora and Dr. N.C. Barwar, "Performance Analysis of Black Hole Attack on different MANET Routing Protocols", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5 (3), 2014.

[12] Neeraj Arora and Dr. N.C. Barwar, "Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Volume 3, Issue 4, April 2014.

[13] [Online]. Available: http://www.isi.edu/nsnam/ns

[14] Bryan Hogan (2010) [Online]. Available: http://www.skynet.ie/~bryan/dsr_faq/

[15] Ketan S. Chavda, Ashish V.Nimavat, Wadhwancity, "Removal of Black Hole Attack in AODV Routing Protocol of MANET", *4th ICCCNT* – 2013, Tiruchengode, India.