Performance Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)

Abhishek Kumar[1] Shweta Kumari[2]
[1,2]M.Tech
[1,2]Department of Computer Science & Engineering
[1,2]Galgotias University, Greater Noida

Abstract— An ad hoc network is a collection of mobile nodes that dynamically form a provisional network. It operates without the use of existing infrastructure. Two on-demand routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol and DSR (Dynamic Source Routing) protocol. The security of the AODV protocol is compromised by a particular of attack called "Black Hole" attack. In this attack, a malicious node advertises itself as having the shortest path with highest sequence number to the node whose packets it wants to intercept. To reduce the probability, it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. AODV protocol provides better performance than the DSR in the presence of Black holes with minimal additional delay and Overhead. Computer simulation using NS2 simulator on Linux operating system shows the behavior of malicious node. In this paper, we simulate and analyzed which routing method is best or suitable in different malicious behaviors

Keywords*:* AODV, DSR, NS2

I. INTRODUCTION

Wireless ad-hoc networks are collected of autonomous nodes that are self- managed without any infrastructure [1]. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks [2][3]. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV [4]. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes [5]. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets.

II. SECURITY

Security [2] in mobile ad hoc networks is particularly difficult to achieve notably because of the vulnerability of the links, the limited physical protection of each of the nodes, the intermittent nature of connectivity, the dynamically changing topology, the absence of a certification authority and the lack of a centralized monitoring or management point.

A. *Malicious Node*

Ad hoc wireless networks rely on the no cooperation of all the participant nodes (malicious node) [3]. There are two attacks, passive and active. Passive attack don't, usually affect the operation of the protocol, however tries to discover valuable information by eavesdropping the traffic. On the other hand, the active attack taps into channel and affect the communication actively by injecting bit into the traffic pattern to limit availability, gain authentication, or play the man in the middle (MITM) role.

B. *Black hole attack*

A Black Hole attack [7][10] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. In the figure-1 shows the scenario.

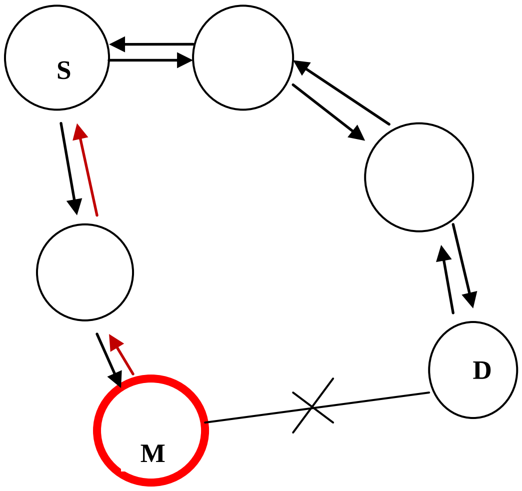


Fig. 1: Black hole Attack

III. Power Management

Power management [2] is an important part of ad hoc wireless network because wireless terminals are mobile, they run on battery power. proper power management is the challenging issue in ad hoc wireless network, which controls two things first one is coverage area and channel interference, second the enhancement of battery power.

IV. Routing

Routing [1][2] is the act of moving information from a source to a destination in an Ad hoc network. During this process, at least one intermediate node within the Ad-hoc network is encountered. The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups through an Ad hoc network. Routing protocols of MANETs can be classified into two categories

A. Table-Driven Routing Protocols

In Table Driven Routing Protocols [1], each node has to keep up to- date routing tables. To maintain reliable routing tables, every node propagates the update messages to the network when the network topology changes.

B. On-Demand Routing Protocols

On-Demand Routing Protocols [1] are not maintained periodically, route tables are created when required.

C. Dynamic Source Routing

The key distinguishing feature of DSR [1] [6] is the use of source routing. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache. Also, any forwarding node caches the source route in a packet it forwards for possible future use. Several additional optimizations have been proposed and have been evaluated to be very effective by the authors of the protocol [1], as described in the following. (i)Salvaging,(ii)Gratuitous route repair,(iii) Promiscuous listening.

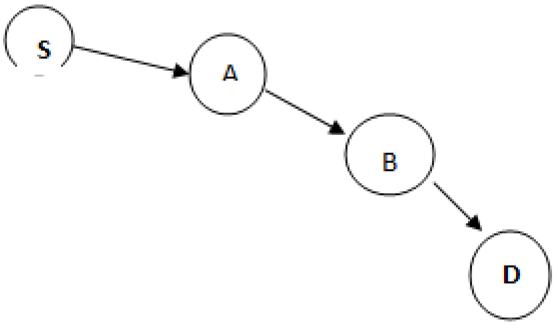


Fig. 2 (a): Route discovery and route maintenance

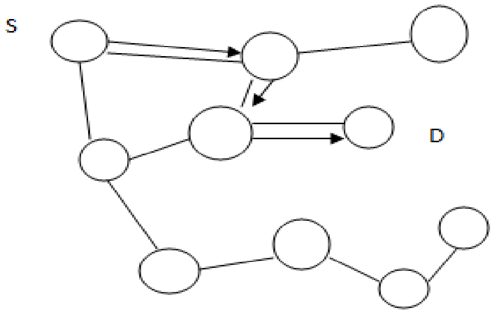


Fig. 2 (b): Packet forwarding in DSR

D. Ad-hoc On Demand Distance Vector

AODV [1] [7] shares DSR's on-demand characteristics in that, it also discovers routes on an "as needed" basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is a departure from DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate a RREP back to the source and, subsequently, to route data packets to the destination.

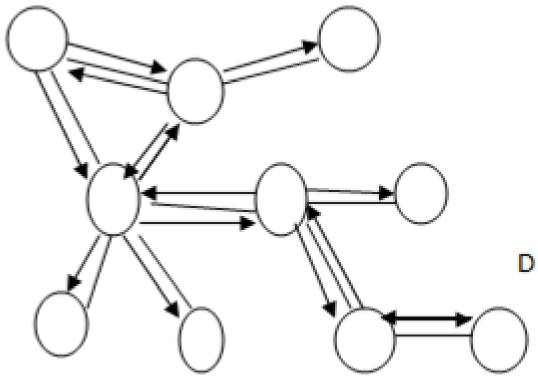


Fig. 3(a): Propagation of RREQ

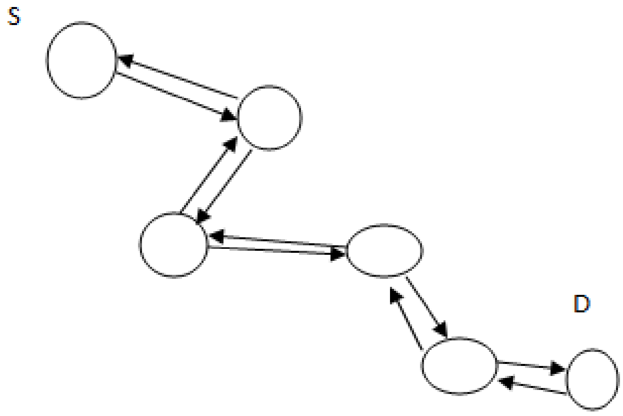


Fig. 3 (b): Propagation of RREP

E. Analysis of DSR and AODV

Analysis of DSR and AODV [4] [5], the two on-demand protocols share certain salient characteristics. However, there are several important differences in the dynamics of these two protocols, which may give rise to significant performance differentials. *First*, by feature of source routing, DSR has access to a significantly greater amount of routing information than AODV. *Second*, to make use of route caching aggressively, DSR replies to all requests reaching a destination from a single request cycle. Having access to many alternate routes saves route discovery floods, which is often a performance bottleneck. In AODV, on the other hand, the destination replies only once to the request arriving first and ignores the rest. The routing table maintains at most one entry per destination. *Third*, the current specification of DSR does not contain any explicit mechanism to expire musty routes in the cache, or prefer "fresher" routes when faced with multiple choices..In contrast, AODV has a much more conservative approach than DSR..*Fourth*, the route deletion activity using RERR is also conservative in AODV. In DSR, however a route error simply backtracks the data packet that meets a failed link. Packets and is maintained as a priority queue with two priorities each served in FIFO order. Routing packets get higher priority than data packets.

V. Behavior Of Black Hole In DSR Routing

In the DSR Black hole attack [6][10] tries to sabotage other nodes the main malfunctions are disable packet forwarding function &disable routing function. The simulation result shows the Packet Delivery Fraction falls to55% when only one malicious node performs the black hole attack. Nodes Mobility and CBR connection don't affect the metric packet delivery fraction. RREQ dropping do not affect the packet delivery fraction. However, it can really affect the average End to End Delay and lead to congestion in a low density network.

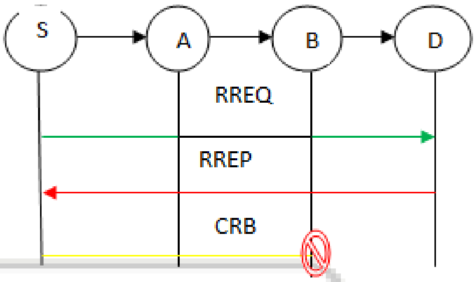


Fig. 4 (a): Black hole in DSR Routing

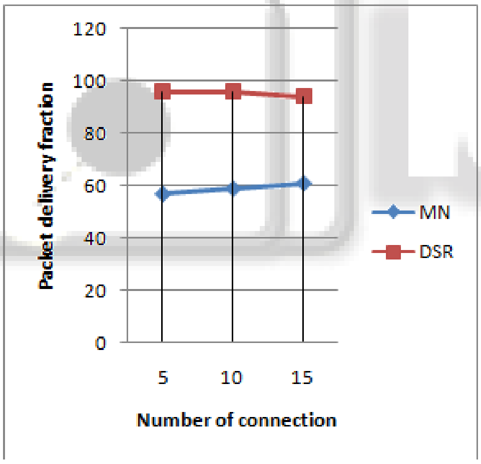


Fig. 4(b): Simulation results of malicious behavior

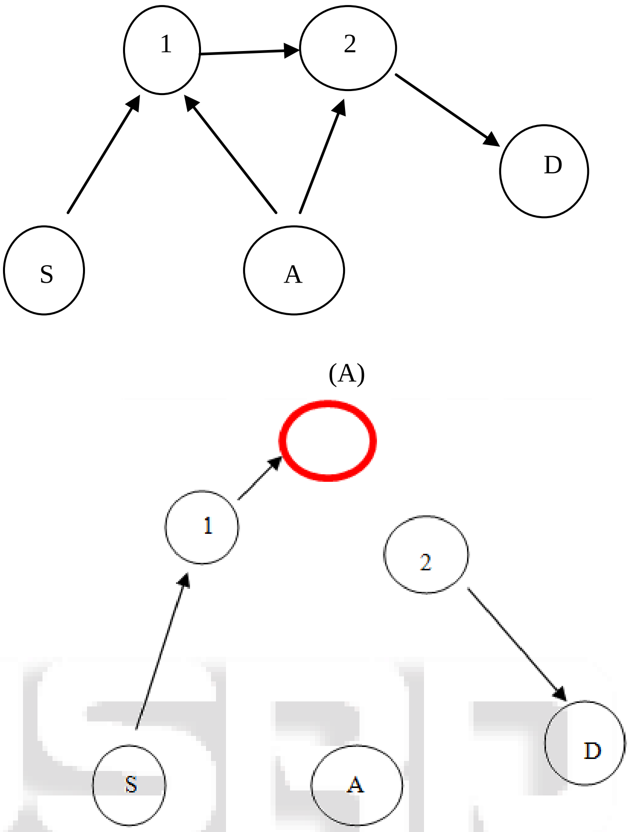
VI. Behavior Of Black Hole In AODV Routing

A black hole [2] [7] has two properties. First, the node exploits the ad hoc routing protocol (here AODV) to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets.

Black hole attacks in AODV protocol routing level can be classified into two categories Route Request (RREQ) Black hole attack and Route Reply (RREP) Black hole attack.

A. *Black hole attack caused by RREQ*

An attacker can send fake RREQ messages to form black hole attack. In RREQ Black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will bebroken down as shown in Fig.-5.



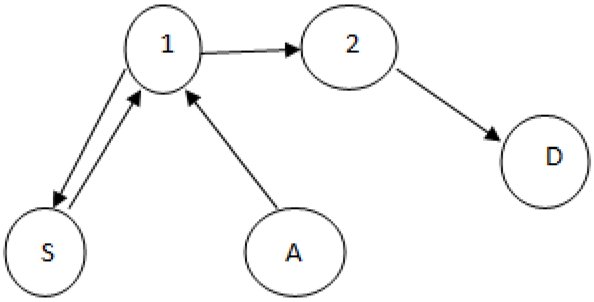
(A)

(B)

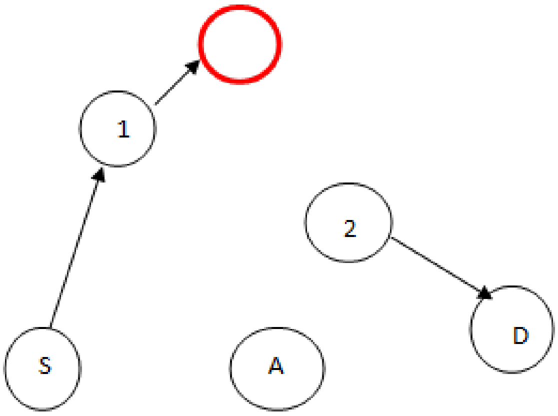
Fig. 5: Black hole is formed by Faked RREQ

B. *Black hole attack caused by RREP*

The attacker unicast the fake RREP message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node. Then RREP Black hole is formed. It is shownas fig.-6.



(A)



(B)

Fig. 6: Black hole is formed by Faked RREP

We use the ns2 [8],[9] for simulation of black hole attack in AODV routing as such *ns2* provides a good platform for MANET simulation. It contains models and modules for the ad-hoc routing protocols. Using the *ns2* environment, some common parameters are listed in Table 1.

VII. SIMULATION

The variable parameter used in simulation is described as follows:

A. Network Density

This aspect is represented by the number of nodes in a fixed area where an MANET is run. Two kinds of densities are considered: high density refers to the usage of 50nodes in an area of 800m x 840m, and low density 20 nodes inthe same area. The denseness of a node in a MANET would influence the performance of the routing protocols used in the network. Thus, it should be expected that an increased density of nodes in the network would decrease the routing protocols performance as a direct effect of less bandwidth and higher congestion but might also reduce the deleterious effect of malicious nodes.

Parameter	Value	Parameter type
Area	800mx 8400m	Fixed
Radio range	600m	Fixed
Link capacity	2Mbps	Fixed
Pause time	5 sec	Fixed
Simulation time	1000 sec buffer	Fixed
Size	10Kbites	Fixed
Application	CRB	Fixed
Packet size	512 bytes	Fixed
Network density	High(50 nodes)/low(20 nodes)	Variable
Network mobility	High(15m/s)/low(2m/s)	Variable
Routing Protocol	AODV/DSR	Variable
Malicious nodes	Black Hole	Fixed

Table 1: Parameters used in simulation

B. Network Mobility

One network mobility scenarios are simulated. Within a high mobility network, all nodes move with a maximum speed of 20m/s while within a low mobility network, all nodes move with a maximum speed of 2 m/s. The performance of routing protocol will be worse under high network mobility.

C. Routing protocol:

Ad hoc routing protocols are used: AODV and DSR. The fig.-7 shows the effect of black hole attack in AODV routing in the form of trace-out file, the graph is generated in MS excel.

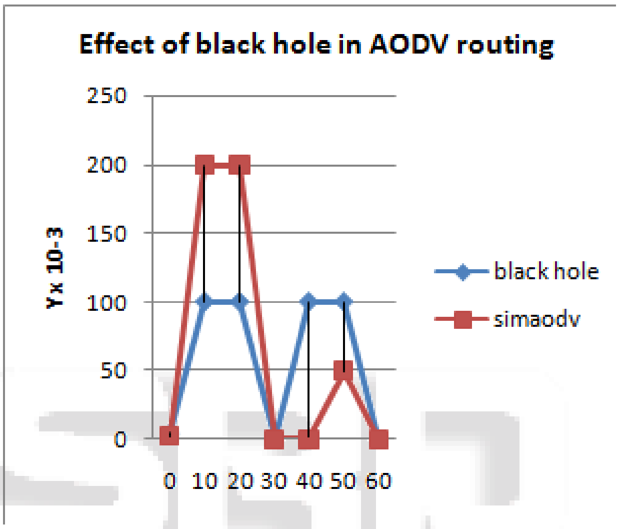


Fig. 7: Effect of Black Hole

VIII. CONCLUSION

In this paper, we analyzed result of the Black Hole attack in an AODV and DSR routing. In our simulation, for analyzing the Performance we consider the throughput as main measure. The study and results shows that DSR data loss is around 45%-55% in the presence of black hole attack, while 35%-40% in the AODV routing. Although, there is trivial difference in the performance but as the number of malicious nodes increases in the network the performance difference may have some significance. Hence, we may conclude that AODV shown the better performance in the presence of such malicious node.

REFERENCE

[1] Charles E. Perkins, “Ad Hoc Networking”, Addison-Wesley, Pearson edu., Jan. 2001.

[2] J. Schiller, “Mobile Communications”, Addison-Wesley,Pearson education August 2003.

[3] Frank Kargl, Andreas Klenk, Stefan Schlott, MichaelWeber, “Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks”, Proceedings of the 1st European onSecurity in Ad-Hoc and Sensor Networks, ‘ESAS 2004’,2004.

[4] C. E. Perkins, E. M. Royer, S. R. Das, M. K. Marina,“Performance comparison of two on-demand

routing protocols for ad hoc networks", Proc. of IEEE Personal Communications (also IEEE Wireless Communications),vol. 8, no. 1, pp. 16-28, Feb. 2001.

[5] Mon Bo Su, Xiao Hannan, A. Adereti, J. A. Malcolm, B. Christianson, "A Performance Comparison of Wireless Ad-Hoc Network Routing Protocols under Security Attack" ,Proc. of Third International Symposium on Information Assurance and Security, 'IAS 2007', pp. 50-55, Aug. 2007.

[6] A. Babakhouya, Y. Challal, A. Bouabdallah, "Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks", Proc. of Second International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST '08, pp. 592-597, Sept. 2008

[7] L. Tamilselvan, V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET", Proc. of 2nd Internationalb Conference on Wireless Broadband and Ultra WidebandCommunications, AusWireless 2007, pp. 20-21, Aug. 2007.

[8] The*ns* Manual (formerly *ns* Notes and Documentation) http://www.isi.edu/nsnam/ns/ns-documentation

[9] CMU Monarch project, http://www.monarch.cs.edu/

[10] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, J. Tolle, "Detecting Black Hole Attacks in TacticalMANETs using Topology Graphs", Proc. of 32nd IEEEConference

[11] Sajjad Ali , Asad Ali ,"Performance Analysis of AODV, DSR and OLSR in MANET", Department of Electrical Engineering with emphasis on Telecommunication Blekinge Institute of Technology, Master's Degree Thesis, Sweden 2009.

[12] Naga .V. Yedida, Rajesh Reddy Challa, "Performance Comparison of AODV, DSR and OLSR Routing Protocols in Static Scenarios", Center for Advanced Computer Sciences. E-mail: xy4835,rxc2763@louisiana.edu.

[13] S. Gowrishankar, T.G. Basavaraju, M. Singh, Subir Kumar Sarkar, "Scenario based Performance Analysis of AODV and OLSR in Mobile Ad hoc Networks", Proceedings of the 24th South East Asia Regional Computer Conference, November 18-19, 2007, Bangkok, Thailand, Special Issue of the International Journal of the Computer, the Internet and Management, Vol.15 No. SP4, November, 2007.

[14] N Vetrivelan, Dr. A V Reddy ,"Performance Analysis of Three Routing Protocols for Varying MANET Size ",Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol. II IMECS 2008, 19-21 , Hong Kong, March 2008.

[15] Asar Ali, Zeeshan Akbar," Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications", Blekinge Institute of technology, Master's Degree Thesis, October2009.

[16] Singh Annapurna, Mishra Shailendra, "Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.

[17] S. Gowrishankar, T.G. Basavaraju, M. Singh, Subir Kumar Sarkar, "Scenario based Performance Analysis of AODV and OLSR in Mobile Ad hoc Networks", Proceedings of the 24th South East Asia Regional Computer Conference, Bangkok, Thailand, Nov., 18-19, 2007, pp. 8.1 – 8.6.

[18] Hsun Tseng , Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks on MANET " , international conference on black hole attack in MANET , Human-centric Computing and Information Sciences 2011, 1:4Springer 11/2011