A Review on some aspects of Black Hole Attack in MANET

Ashis Bhattercharjee[#1], Subrata Paul[*2]

[#]*M.Tech Scholar, MIPS, Sriram Vihar, Rayagada, Odisha, INDIA*
**St. Xaviers High School, Bankura, West Bengal, INDIA*

***Abstract*— A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack. The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. In this paper we presented a review on few aspects of Black hole attack in MANET's. We have tried to discuss about the reasons why such attacks are seen in mobile ad- hoc networks and performed an analysis on its performance and result on a few of its simulation parameters.**

Keywords— **Mobile Ad-Hoc networks, Black Hole Attack, AODV Protocol, Security.**

I. INTRODUCTION

A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways and interface with a fixed network. Its nodes are equipped with wireless transmitters/receivers using Antennas which may be omni directional (broadcast), highly-directional (point-to-point), or some combination thereof. At a given time, the system can be viewed as a random graph due to the movement of the nodes, their transmitter/receiver coverage patterns, the transmission power levels, and the co -channel interference levels. In this paper, we are focusing on the concept of black hole attack in ad-hoc network & impact of black hole attack in MANET.

A Black hole is a malicious node that falsely advertises shortest path to the destination node and absorbs all data packets in it. In this way, all packets in the network are dropped. Black hole attacks disturb route discovery process and degrade network's performance [1].

In this paper, performance of AODV is evaluated in presence of black hole(Malicious node) attack and do comparison with the network without black hole attack using various performance metrics such as number of generated packets, number of packet drops, avg. end2end delay, avg. simulation processing time under different scalable network mobility. Simulation & performance analysis will be carried out by using network simulator tool so as to address the relative performances under black hole attack in mobile ad-hoc network [1,2].

II. AN OVERVIEW OF AODV ROUTING PROTOCOL

Ad Hoc On-Demand Vector Routing (AODV) protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only between nodes which need to communicate. The AODV routing protocol builds on the DSDV algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information. That means, the routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is (in relation to another), which is used to grant loop freedom [20].

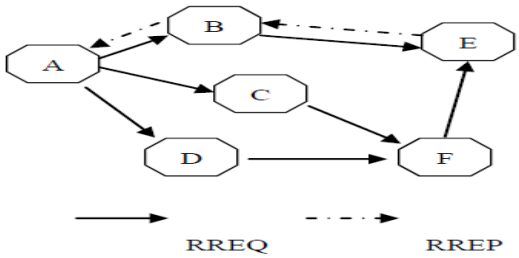

Fig 1: RREQ & RREP message exchange between A & E

Whenever a node needs to send a packet to a destination for which it has no „fresh enough" route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ - 3 - (unless it has a „fresher" one).When the intended destination (or an intermediate node that has a „fresh enough" route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonically increased at each hop). The RREP travels back to the originator of the RREQ (this time as a unicast). At each intermediate node, a route to the

destination is set (again, unless the node has a „fresher" route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bi-directionally. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route „as fresh" as the received one, the shortest one will be up dated. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP. The AODV protocol is vulnerable to the well-known black hole attack. This is illustrated in figure 1 [3,7,20].

III. Black Hole Problem in AODV

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack and a kind of Denial Of Service (DoS) in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the *Route Discovery process*, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

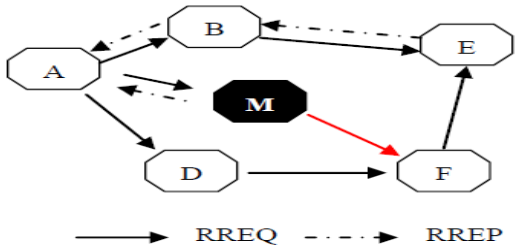

Fig 2: Black hole Attack in AODV

In the above figure , imagine a malicious node M. When node A broadcasts a RREQ packet, nodes B , D and M receive it. Node M, being a malicious node, does not check up with its routing table for the requested route to node E. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node A receives the RREP from M ahead of the RREP from B and D. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, it absorbs all the data and thus behaves like a Black hole [4,5,6].

In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number. Upon receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination [7].

A. Single Black Hole Attack

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks. An example is shown as Figure 1, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs [8,10].

As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely. In the following, different detection schemes for single black hole attack are presented in a chronological order. The comparisons of different schemes are shown in Table 1.

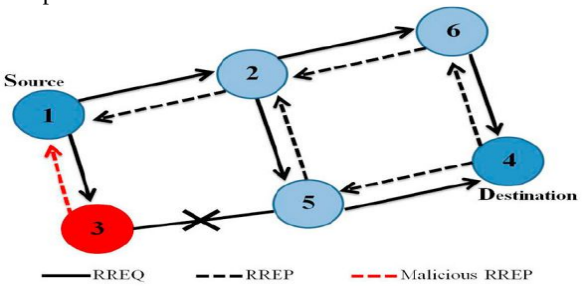

Figure 3 The single black hole problem.

TABLE I
COMPARISON OF SINGLE BLACK HOLE ATTACK DETECTION SCHEMES [8,9,10,11]

Schemes	Routing Protocol	Simulator	Detection Type	Results	Defects
Neighborhood based and Routing Recovery	AODV	NS-2	Single Detection	The probability of one attacker can be detected is 93%	Failed when attackers cooperate to forge the fake reply packets
Redundant Route and Unique Sequence Number Scheme	AODV	NS-2	Single Detection	Verify 75% to 98% of the routes	Attackers can listen to the channel and update the tables for last sequence Number
Time-basedThreshold Detection Scheme [28]	Secure AODV (SAODV)	GloMoSim	Single detection	The PDR of SAODV is around 90 to 100% when AODV is around 80%	The end-to-end delay increases when the malicious node is away from source Node
Random Two hop ACK and Bayesian Detection Scheme	DSR	GloMoSim based	Cooperative Detection	The true positive rate can achieve 100% when existing 2 witness	The proposed scheme is not efficient when k equals to 3, reducing the true Positives
REAct	DSR		Single Detection	Reduces the communication overhead but enlarges the identification delay	The binary search method is easily expose audit node's information
DPRAODV	AODV	NS-2	Single Detection	The PDR is improved by 80-85% than AODV when under black hole attack	A little bit higher routing overhead and end-to-end delay than AODV
Next Hop Information Scheme	AODV	NS-2	Single Detection	The PDR is improved by 40- 50% and the number of packets dropped is decreased by 75- 80% than AODV	Few additional Delay
Nital Mistry et al.'s Method	AODV	NS-2	Single Detection	The PDR is improved by 81.811% when network size varying, and rise 70.877% when mobility varying	Rise in end-to-end delay is 13.28% when network size varying, and rise 6.28% when mobility varying
IDS based on ABM	MAODV	NS-2	Single Detection	The packet loss rate can be decreased to 11.28% and 14.76%	Cooperative isolation the malicious node, but failed at collaborative black hole attacks

B. Collaborative Black Hole Attack

There are various mechanisms have been proposed for solving single black hole attack in recent years. However, many detection schemes are failed in discussing the cooperative black hole problems. Some malicious nodes collaborate together in order to beguile the normal into their fabricated routing information, moreover, hide from the existing detection scheme. As a result, several cooperative detection schemes are proposed preventing the collaborative black hole attacks [12,14].

In the following, different detection schemes for the cooperative black hole attack are presented in a chronological order. The comparison of different schemes is shown in the Table 2.

TABLE III
COMPARISON OF COLLABORATIVE BLACK HOLE ATTACK DETECTION SCHEMES [112,13,14]

Schemes	Routing Protocol	Simulator	Results	Defects
DRI and cross Checking	AODV	No Simulator	No simulation results	-
DRI table and cross checking using FREQ and FREP	AODV	-	A higher throughput performance almost 50% than AODV	5-8% more communication overhead of route Request

DCM	AODV	NS-2	The PDR is improved from 64.14 to 92.93%, and the detection rate is higher than 98%	A higher control overhead than AODV
Hash based Hashed-based	DSR	-	No simulation results	-
MAC and Hash based PRF Scheme	AODV	NS-2	The PDR is higher than 90% when AODV is inaccessible 50%	The malicious node is able to forge a fake reply to dodge the detection Scheme
BBN and RIP	AODV	-	No simulation results	-
BDSR	DSR	Qual NET	The PDR of BDSR is always higher than 90%	The overhead is minimal higher than DSR, but lower than WD approach

IV. Performance Analysis of Black Hole Attacks

This part of the paper explains the various performance metrics required for evaluation of protocols. To reiterate the black hole attack, we begin with the overview of performance metrics that includes End-to-end delay, Throughput and Network load. These matrices are important because of it performance analysis of network. Furthermore, implementation of the simulation setup, tools and its design are explained.

A. Performance Metrics

The performance metrics chosen for the evaluation of black hole attack are packet end-to-end delay, network throughput and network load.

The packet end-to-end delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. This includes the overall delay of networks including buffer queues, transmission time and induced delay due to routing activities. Different application needs different packet delay level. Voice and video transmission require lesser delay and show little tolerance to the delay level.

The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds. In MANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter [16].

The third parameter is network load, it is the total traffic received by the entire network from higher layer of MAC which is accepted and queued for transmission. It indicates the quantity of traffic in entire network. It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission. It does not include any higher layer data traffic rejected without queuing due to large data packet size [19].

B. Simulation Tool

The tool used for the simulation study is OPNET 14.5 modeler. OPNET is a network and application based software used for network management and analysis [15]. OPNET models communication devices, various protocols, architecture of different networks and technologies and provide simulation of their performances in virtual environment. OPNET provides various research and development solution which helps in research of analysis and improvement of wireless technologies like WIMAX, Wi Fi, UMTS, analysis and designing of MANET protocols, improving core network technology, providing power management solutions in wireless sensor networks. In our case we used OPNET for modeling of network nodes, selecting its statistics and then running its simulation to get the result for analysis.

C. Modeling of Network

At first network is created with a blank scenario using startup wizard. Initial topology is selected by creating the empty scenario and network scale is chosen by selecting the network scale. In our case we have selected campus as our network scale. Size of the network scale is specified by selecting the X span and Y span in given units. We have selected 1000 * 1000 meters as our network size. Further technologies are specified which are used in the simulation. We have selected MANET model in the technologies. After this manual configuration various topologies can be generated by dragging objects from the palette of the project editor workspace. After the design of network, nodes are properly configured manually [17].

D. Collection of Results and Statistics

Two types of statistics are involved in OPNET simulation. Global and object statistics, global statistics is for entire network's collection of data. Whereas object statistics involves individual nodes statistics. After the selection of statistics and running the simulation, results are taken and analyzed. In our case we have used global discrete event statistics (DES) [18].

E. Simulation Setup

Figure 4 employs the simulation setup of a single scenerio comprising of 30 mobile nodes moving at a constant speed of 10 meter per seconds. Total of 12 scenarios have been developed, all of them with mobility of 10 m/s. Number of nodes were varied and simulation time was taken 1000 seconds. Simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024).

The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.005 watts. Random way point mobility is selected with constant speed of 10 meter/seconds and with pause time of contant 100 seconds. This pause time is taken after data reaches the destination only.

Our goal was to determine the protocol which shows less vulnerability in case of black hole attack. We choose AODV and OLSR routing protocol which are reactive and proactive protocols respectively. In both case AODV and OLSR, malicious node buffer size is lowered to a level which increase packet drop. Furthermore the simulation parameters are given in Table 3 [16,18].

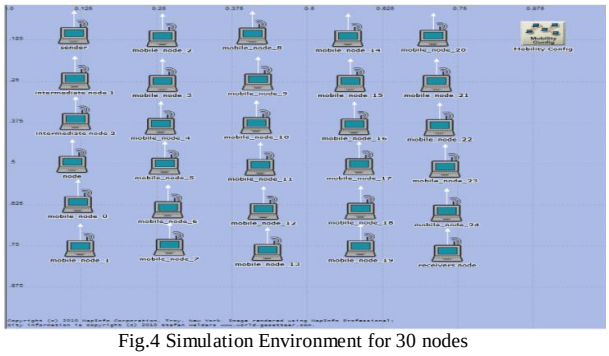

Fig.4 Simulation Environment for 30 nodes

TABLE IIIII
SIMULATION PARAMETERS.

SIMULATION PARAMETERS	
Examined Protocols	AODV and OLSR
Simulation Time	1000 seconds
Simulation Area (m x m)	1000 x 1000
Number of Nodes	16 and 30
Traffic Type	TCP
Performance Parameter	Throughput, Delay, Network load
Pause Time	100 secs
Mobility (m/s)	10 m/s
Packet Arrival-time (s)	Exponential (1)
Packet Size (bits)	Exponential (1024)
Transmit Power (W)	0.005
Data Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

V. CONCLUSION

In this work, we brought out few aspects on the Black hole Attacks observed in MANETS. This paper begins with a general introduction on few topics under discussion. Then we further elaborated on the AODV Protocol and how Black Hole attacks occur in the network. We discussed the types of Black hole attacks and their associated detection schemes. Finally we concluded our discussion by providing a performance analysis on the Black hole attacks in which a simulation setup was made and Simulation parameters were studied.

V. REFERENCES

[1]. Burbank JL, Chimento PF, Haberman BK, Kasch WT *"Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology"*. IEEE Communication Magazine 44(11):39–45,2009.

[2]. Abolhasan, M., Wysocki, T., Dutkiewicz, E: *"A review of routing protocols for mobile ad hoc network"s*. Elsevier, Amsterdam, 2004.

[3] Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, *"Performance analysis of ad-hoc networks under black hole attacks"*. Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 – 153.

[4] A. Shevtekar, K. Anantharam, and N. Ansari, *"Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett.*, vol. 9, no. 4, Apr. 2005, pp. 363–65.

[5] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, *"Black hole Attack in Mobile Ad Hoc Networks"* Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, APRIL 2004, pp. 96-97.

[6] Y-C Hu and A. Perrig, *"A Survey of Secure Wireless Ad Hoc Routing," IEEE Sec. and Privacy*, May–June 2004.

[7] K. Sanzgiri *et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 2002 IEEE Int'l. Conf. Network Protocols*, Nov. 2002.

[8] Sun B, Guan Y, Chen J, Pooch UW *"Detecting Black-hole Attack in Mobile Ad Hoc Network"s*. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003

[9] Al-Shurman M, Yoo S-M, Park S *"Black Hole Attack in Mobile Ad Hoc Network"s*. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004

[10] Tamilselvan L, Sankaranarayanan V *"Prevention of Blackhole Attack in MANET"*. Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007

[11] Djenouri D, Badache N *"Struggling Against Selfishness and Black Hole Attacks in MANETs"*. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6, 2008.

[12] Oliveira R, Bhargava B, Azarmi M, Ferreira EWT, Wang W, Lindermann M *"Developing Attack Defense Ideas for Ad Hoc Wireless Networks"*. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009

[13] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K *"Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks"*. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003

[14] Weerasinghe H, Fu H *"Preventing Cooperative Black Hole Attacks in*

Mobile Ad Hoc Networks: Simulation Implementation and Evaluation". Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007.
[15] Opnet Technologies, Inc. *"Opnet Simulator,"* Internet: www.opnet.com, date last viewed: 2010-05-05
[16] S. Kurosawa et al., *"Detecting Blackhole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic"*
[17] M. Al-Shurman, S-M. Yoo, and S. Park, *"Black Hole Attack in Mobile Ad-Hoc Networks,"* ACM Southeast Regional Conf. 2004.
[18] H. Deng, W. Li, Agrawal, D.P., *"Routing security in wireless Ad-Hoc networks,"* Cincinnati Univ.,OH, USA; IEEE Communications Magazine, , Vol.40, pp.70- 75, ISSN: 0163-6804, Oct. 2002.
[19] Subrata Paul, Anirban Mitra, Ramanuja Nayak, *"On some Security aspect of HPC Environment"*, International Journal Of Engineering And Computer Science, Vol 3 (1), January 2014, Pp .3758 - 3762.
[20] Anirban Mitra, BK Ray, *"A GSM-Free Scheme for Location Management"*, Journal of the Institution of Engineers (IE - India), 88, 2008, pp.9-12.
[21] Anirban Mitra, R Nayak, *"Location Management for Mobile Devices In Ad Hoc Network and Implementing its Security Aspect"*, Proceeding of National Conference in Computational Intelligence and Network Security, CINS, VEC - Chennai, India, March 2010.