A Literature Survey on Black Hole Attacks on AODV Protocol in MANET

Ravi Kant
M.tech Scholar
ABES EC, Ghaziabad

Sunil Gupta
HOD(IT/CSE)
DTC, Greater Noida

Harsh Khatter
Assistant Professor
ABES Engineering College
Ghaziabad, India

ABSTRACT
A Mobile ad-hoc network (MANET) is a latest and emerging Research topic among researchers. The reason behind the popularity of MANET is flexibility and independence of network infrastructure. MANET have some unique characteristic like dynamic network topology, limited power and limited bandwidth for communication. MANET has more challenge compare to any other conventional network. The most common routing protocols used in ad-hoc network are AODV (ad-hoc on demand distance vector) protocol. AODV protocol is threatened by "Black Hole" attack. In black hole attack a malicious node advertise itself as having the4 shortest path to the destination node. To combat with black hole attack so many solutions provided by researchers. In this article we study the routing security issue of MANET and analyze in detail one type of attack the "Black hole" attack. We also provide a detailed list of solutions which protect the black hole in MANET's.

KEYWORDS
MANET, Security, Black hole attack, AODV and Packet dropping.

1. INTRODUCTION
A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. Nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages [1]. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the destination host.

In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on, unlike the conventional network. A MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [2]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network. Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task.

Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power. There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV [3] [4]. More sophisticated and subtle routing attacks have been identified in recent published papers, such as the black hole (or sinkhole) [5], Byzantine [6], and wormhole [7] [8] attacks. Currently routing security is one of the hottest research areas in MANET.

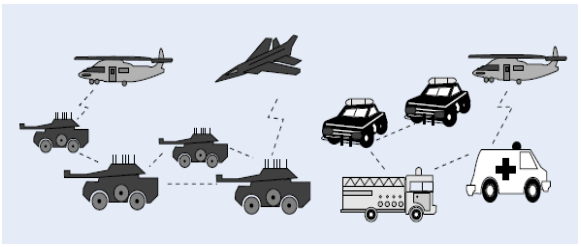

Figure 1 Example Application of MANETs

2. OVER VIEW OF AODV ROUTING PROTOCOL
AODV [9] is a reactive routing protocol designed for a mobile ad hoc network. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

3. BLACK HOLE ATTACK ON AODV PROTOCOL

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

Figure 2 shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

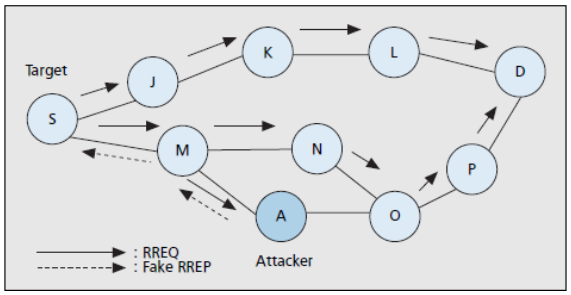

Figure 2 Example of black hole attack on AODV

4. SOLUTIONS TO BLACK HOLE ATTACK IN MANET

In this section, we will review the several solutions to black hole attacks**.**

Hongmie Deng et.al.[10] proposed One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense they avoid the black hole problem and implement a secured AODV protocol. But there are two associated disadvantages. First, the routing delay is greatly increased, especially for a large network. Second, a malicious node can take further action such as fabricate a reply message on behalf of the destination node. The source node cannot identify if the reply message is really from the destination node or fabricated by the malicious node. In this case, the method may not be adequate.

To avoid the situation of the intermediate node taking further action such as fabricating the reply message on behalf of the next hop node. When the source node receives the Further Reply from the next hop, it extracts the check result from the reply packets. If the result is yes, they establish a route to the destination and begin to send out data packets. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, they discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to the whole network to isolate the malicious node. If the next hop has no route to the requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node. Using this method, they avoid the black hole problem, and also prevent the network from further malicious behavior. They don't disable the ability of a replying message from intermediate nodes, but the routing overhead is greatly increased if they do the check process to every intermediate node that sends a reply message. Moreover, they do not need this mechanism in a normal network environment. They propose to use this method whenever they find any suspected node in the network. To find the suspected node, any intrusion detection methods can be used. They use the IADM for the prior work to find the suspected node. Whenever they are suspicious, they trigger they method to detect if the suspected node is really malicious or not.

Al-Shurman et.al. [11] Proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

Satoshi Kurosawa et. al. [12] uses an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is performed

Latha Tamilselvan et. al. [13] proposed a better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source; thereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented. The main drawback of this solution is processing delay in the network.

Zhao Min et.al [14] have discussed an authentication mechanism for identifying black hole nodes in MANETs. An authentication mechanism is constructed based on the concept of the hash function, MAC, and PRF, which is used for checking the RREPs at source node to send the data packets. The proposed mechanism eliminates the need for a PKI or other forms of authentication infrastructure, however it needs to be discuses, how to handle unlimited message authentication by switching one-way-hash chains and how to prevent a malicious node cannot forge a reply if the hash key of any node is to be disclosed to all nodes.

Table1: Comparison of available solutions to black hole attacks on AODV.

S.No	Technique proposed by	Techniques / Solutions	Introduced new packets(yes/No)	Modifies AODV/ Routing tables(yes/no)	Type of black hole attack	Drawbacks
1	Hongmei Deng Deng, Wei Li, and Dharma P. Agrawal, 2002	Further route request and reply to next hop node	yes	no	Single black hole	Routing overhead, Cannot Prevent Cooperative Black holes.
2	Mohammad Al-Shurman and Seong-Moo Yoo 2004	Checks the shared hops from RREP"s and maintains last packet sequence numbers that are sent and received	yes	no	Single black hole	Time delay
3	Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto 2007	A new detection method based on dynamically updated training data.	no	no	Single black hole	Network delay
4	Latha Tamilselvan, Dr.V. Sankaranarayanan 2008	Fidelity table based on the acknowledgements received by the source node.	yes	yes	cooperative black hole	Time delay
5	Zhao Min Zhou Jiliu 2009	Authentication mechanisms bas ed on the hash function, MAC and the PRF	no	no	Co operative black hole	Low message authentication, may forge RREP with hash key of node
6	XiaoYang Zhang , Yuji Sekiya and Yasushi Wakahara 2009	IN node generates SREQ to the desti-nation for fresh SN.	yes	no	Single black hole	Time delay, multiple black holes.
7	Payal N. Raj, Prashant B. Swadas 2009	Compares the RREP sequence numbers with threshold value using dynamic learning method	yes	no	Single black hole	Time delay, co-operative black hole nodes
8	Yibeltal Fantahun Alem Zhao Cheng Xuan 2010	Intrusion detec tion using anomaly detection (IDAD)	yes	no	Single black hole	Neighbor nodes may give false information
9	Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, Sept. 2010	An Anti-Black hole Mechanism (ABM) using IDS	yes	yes	Multiple black holes	Time delay
10	Lalit Himral, Vishal Vig & Nagesh Chand 2011	Checking SN "s of source node and first route reply.	no	yes	Single black hole	Time delay, co-operative black hole nodes
11	Kamarularifin Abd. Jalil1, Zaid Ahmad2, Jamalul-Lail Ab Manan2011	Enhance Route Discovery for AODV(ERDA)	no	yes	Single black hole	Co operative black holes
12	Kitisak Osathan unkul and Ning Z 2011	Secured ETX metric (Expected Transmission Count)	yes	yes	Co-operative black holes	Time delay and overhead due to much calculatio

XiaoYang Zhang et.al. [15] Introduced a new detection method based on checking the sequence number in the Route Reply packets by making use of a new message originated by the destination. In this method, when an .intermediate node unicasts a RREP packet, the node also unicasts a newly defined control message to the destination node to request for the up-to-date SN. Upon receiving, the destination node unicasts a reply message to inform the source node of the up-to-date SN. This reply from the destination node enables the source node to verify if the intermediate node has sent a faked RREP message by checking if the SN in the RREP message is larger than the up-to-date SN. This method has more network overhead and time delay since node in the network generates new packets.

Payal N. Raj et. al. [16] modifies the behavior of AODV to include a mechanism for checking the sequence number of the received RREP. As the source node receives the RREP it compares the sequence number of the received RREP to a threshold value. The replying node is suspected to be a black hole if its sequence number is greater than the threshold value. The source node adds the suspected node to its black list, and propagates a control message called an alarm to publicize the black list for its neighbors. The threshold is the computed average of the difference between the destination sequence number in the routing table and the destination sequence number in the RREP within certain periods of time. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated.

Alem, Y.F et.al. [17] Proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data collected and it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication.

Ming-Yang et. al [18] proposed an intrusion detection system called Anti-Blackhole Mechanism (ABM) in which the suspicious value of a node is estimated according to the amount of abnormal difference between RREQs and RREPs transmitted from the node; all nodes perform ABM. With the requirement that intermediate nodes are prohibited to reply to RREQs, if an intermediate node is not the destination and never broadcasts RREQ for a specific route, but forward a RREP for the route, then its suspicious value will be increased in the nearby node's suspicious node table. When the suspicious value of a node goes beyond threshold, a Block message is broadcasted by the node to all other nodes in the network to isolate the suspicious node cooperatively. Though, the solution assumes that an authentication mechanism already exists in MANET.

Lalit Himral et.al [19] have proposed method to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely it is from the malicious node, immediately remove that entry from the RR-Table. The proposed method cannot find multiple black hole nodes.

Kamarulari fin Abd et.al.[20] have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When RREQ packet is sent out by the source node S to find a fresh route to the destination node D. RREP packet received by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M Since the value of parameter rt_upd is „true, node S accepts the next RREP packet from other node to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table. The current route entry in routing table will be overwritten by the later RREP coming from other node. ERDA method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP. However, it cannot detect cooperative black hole attack.

Kitisak Osathanunkul et. al. [21] aimed of SETX protocol is to provide a method to prevent black hole nodes from advertising a fabricated forwarding delivery ratio (df) of a wireless link between itself and one of its neighbors'. Non-cooperative black hole attacks mean that malicious nodes perform the attacks individually. They do not collaborate in launch an attack. There is another type of black hole attacks, by which malicious nodes share routing information with each other and launch black hole attacks in collaboration. This latter attack type is called cooperative black hole attacks . Our SETX protocol cannot thwart cooperative black hole attacks, as it is possible for several cooperative black hole nodes to help each others to obtain the necessary probes. For example, if a black hole node, A, has missed out some probes, but if black hole node B or C are able to receive the probes that A badly needs. Then B or C can tunnel these probes to A. So A can use these probes to convince the initiator that he has a better df value, thus a better route to the intended destination.
A trust management scheme can be used to deal with cooperative black hole attacks. Trust management schemes are a method that allows nodes to monitor the behavior of their neighbors'. If their neighbors' intentionally drop a packet, the trust level will be affected. If the trust level of a neighboring node drops below a given threshold level, this neighboring node will be considered as a malicious node. This trust based approach to countering cooperative black hole attacks means that black hole nodes may be able to attack the network (i.e. drop the packets) for a while before they are detected. Once they have been detected, an alarm can be sent out to other nodes. In addition, adopting a trust based scheme can be more complicated. This often means that the nodes in the network would have to passively listen to the neighbors' packet transmissions and exchange trust related values among them. This will consume network bandwidth and impose additional overheads to the network, but it can be a solution against cooperative black hole attacks.

5. CONCLUSION

As we already know why MANET is so popular in present scenario? It has some extra ordinary features due to which it is acceptable globally. MANET have so many features and as well as it have some security issues. In this paper we have just provide a list of solutions in MANET on a specific attack that is black hole attack. There are so many solutions which provide better security in case of single malicious node but these solutions are not effective in case of multiple malicious node. Some solutions may require some special hardware like GPS. In this paper a brief introduction is provide for each solution with their improvements and drawbacks. Fir future research work researchers have to focus on improving the effectiveness of the security scheme as well as minimize the cost to make them suitable for a MANET environment.

6. REFERENCES

[1] C. Perkins, Ad Hoc Networks, Addison-Wesley, 2001.

[2] S. Ci et al., "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,"IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.

[3] M. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

[4] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta, 2002.

[5] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing. IEE Security & Privacy, pp. 28-39, 2004.

[6] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[7] Y. Hu, A Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks. Proc. of IEEE INFORCOM, 2002.

[8] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002

[9] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc Ondemand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[10] Deng H., Li W. and Agrawal, D.P., "Routing securi ty in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[11] Mohammad Al-Shurman et. Al" Black Hole Attack in Mobile Ad-Hoc Network" ACMSE'04, Apri l 2-3, 2004, Huntsville, AL, USA .

[12] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipthey, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Jtheynal of Network Securi ty, Vol.5, Issue 3, pp: 338–346, 2007

[13] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008

[14] Zhao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineeri ng and Electronic Commerce, 2009. IEEC '09.International Symposium on, vol., no., pp.26-30, 16-17 May 2009.

[15] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009.

[16] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Jtheynal of Computer Science Issues, Vol. 2, 2009.

[17] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd

[18] Ming-Yang Su, "Prevention of Selective Black hole Attacks on Mobile Ad hoc Network through Intrusion Detection Systems", Computer Communications, 2010. Communications, 2007, pp. 21-26.

[19] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Jtheynal of Engineeri ng Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[20] Kamarulari fin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Mitigation of Black Hole Attacks for AODV Routing Protocol", Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.

[21] Kitisak Osathanunkul and Ning Zhang" A Countermeasure to Black Hole Attacks in Mobile Ad hoc Networks" 978-1-4244-9573-3/11/$26.00 ©2011 IEEE.