A Survey on Mitigation of Blackhole Attacks on AODV in MANET

Mohanapriya R [#1], Saranya K[*2], Rajesh Babu M[#3]

[#] *Computer Science and Engineering Department, Anna University*
PPG Institute of Technology, Coimbatore, India
[1] priaraam@gmail.com
[3]drmrajeshbabu@gmail.com

[*] *PPG Institute of Technology*
Coimbatore, India
[2]kksaranmathu@gmail.com

Abstract— **MANET is an infrastructure less network that consists of mobile nodes that communicate with each other over wireless links. The mobile nodes also act routers. Ad hoc on-demand distance vector routing (AODV) is a very popular routing algorithm on MANET. However, AODV is vulnerable to the black hole attack and its versions. The intermediate node may suddenly behave maliciously and drop packets which go through it, thus preventing it from reaching the right destination. The severity of this attack is even more when the black hole nodes work in cooperation with each other. This paper presents a survey on various solutions proposed to avoid the black hole attack and a comparison study of the solutions**.

***Index Terms*— AODV, Black hole Attack, Cooperative Blackhole Attack, MANET.**

I. INTRODUCTION

A wireless sensor network is a collection of autonomous nodes distributed spatially over a network, where each node is connected to one or more sensors [1]. The key functions of WSN are broadcast and multicast, routing, forwarding and route maintenance. Each such sensor network node has several hardware components like a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, a power source, usually a battery, etc. The topology of the WSN can vary from a simple star network to a complex wireless mesh network. Applications of WSN are wider, like immense use in military applications such as ocean surveillance systems, battle field surveillance, attaching micro sensors to weapons for stockpile surveillance, etc [3]. Other applications are Environmental Monitoring, Health Monitoring, Traffic Control, Industrial Sensing, Infrastructure Security etc [3].

Wireless networks can be either infrastructure based networks or infrastructure less networks. In infrastructure based networks, the communicating mobile devices are controlled and coordinated by base stations. Whereas in infrastructure less networks, no centralized control point is present. Ad hoc Networks fall under the category of infrastructure less networks. Security and privacy are the main issues in wireless networks [2]. If attackers exist, they can carry on a wide variety of attacks on the routing algorithm including selective forwarding, black hole, rushing, resource depletion, wormhole, denial of service attacks etc.

Unfortunately, almost all Wireless network routing algorithms are vulnerable to these attacks [2]. In Ad hoc networks, the nodes work in cooperation with each other in managing the network. In addition to acting as hosts, the nodes should also act as routers during the transmission. A Mobile Ad hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. The idea of MANET is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. It is formed instantaneously, and uses multihop routing to transmit information. MANET technology can provide an extremely flexible method of establishing communications in situations where geographical or terrestrial constraints demand a totally distributed network system without any fixed base station, such as battlefields, military applications, and other emergency and disaster situations. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner. Routing Protocols: Many different routing protocols have been developed for MANETs. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology [5].

II. RELATED WORK

A. Routing protocols

Table-driven (*proactive*) protocols: These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. e.g., Destination Sequenced Distance Vector (DSDV)

On demand (re-active) protocols: Source-initiated on-demand routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. e.g., Ad hoc on-demand distance vector protocol (AODV) and Dynamic Source Routing protocol (DSR).

Hybrid protocols: Make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP). In [7], it is shown that proactive protocols consume more energy than re active protocols. In addition, regarding AODV and DSR, AODV is more efficient and effective in comparison with DSR in MANET environment [7].

B. AODV Operation

AODV is an on-demand routing protocol. It creates routes only when needed by the source node. When a node needs to create a route to a destination, it initiates a *route discovery* process within the network. It broadcasts a route request (RREQ) packet to its neighbors, which in turn forward the RREQ to their neighbors, and so on, until the destination. In this process the intermediate node can reply to the RREQ packet only if it has a fresh route to the destination. The destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. After the route establishing, it is maintained by a *route maintenance* procedure until either the destination is unreachable or the route is no longer desired **[5].** Fig. 2. and Fig. 3. depicts the packet format of RREQ and RREP Packet format. The working of AODV is depicted in Fig. 1. Source A broadcasts the RREQ packet towards the Destination E. The node E unicast the RREP packet until it reaches the node A. While the AODV has advantages on less overhead, it is vulnerable to various attacks. When a source host broadcasts RREQ in the network, the malicious host may immediately form a false route reply and execute the attack. It is pretty difficult to detect an on-going attack on AODV before it causes performance degradation.

C. Security in MANET

Security always implies the identification of potential attacks, threats and vulnerabilities of a certain system. Attacks can be classified into *passive* and *active attacks*. A passive attack does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to routing traffic, which makes it very difficult to detect.

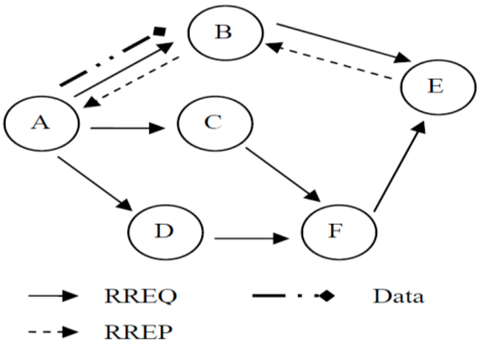

Fig. 1. RREQ Broadcast and RREP Unicast

Type count	R	A	Reserved	Hop
Destination IP Address				
Destination sequence number				
Originator IP address				
Life time				

.Fig. 2. RREQ Packet format

Type	J	R	G	D	U	Reserved	Hop
RREQ ID							
Destination IP address							
Destination sequence number							
Originator IP Address							
Originator sequence Number							

Fig. 3. RREP Packet format

An active attack is an attempt to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network. Active attack can be further divided into external attacks and internal attacks. An *external attack* is one caused by nodes that do not belong to the network [5]. An *internal attack* is one from compromised or hijacked nodes that belong to the network. Internal attacks are typically more severe, since malicious nodes already belong to the network as authorized parties. Therefore, such nodes are protected with the network security mechanisms and underlying services [6]. In the following section, some types of active attacks easily performed against a MANET in the network layer are described.

D. Blackhole Attack

A Blackhole attack is a type of DoS attack, in which malicious node sends a forge reply to the source node pretending that it has the shortest route to the destination. The source will establish a connection by forwarding packets to the malicious node. The node in turn will discard those packets without forwarding them to the destination. There are two types of black hole attack which is described as follows.

In-Network Black hole attack: In **t**his type of black hole attack, there is a malicious node within the network, that takes its position somewhere in the routes of the source and destination. On getting a favorable opportunity this malicious node would try make itself an active participant in the routing. Now the adversary can launch the attack at any point. This type of attack seems to be difficult to detect since the attacker is within the transmission route.

Out-of-Network Black hole attack: This type of attack is done externally, where the attackers are present physically out of the network. These attacking nodes try to accomplish access denial, create network congestion, network disruption, etc. The out-of-network attack can turn into an in-house attack, when it is able to control a node within the network. The working of the out-of-network attack can be described as below.

Step 1. The active route from source to the destination and their corresponding addresses are noted by the attacking node.

Step 2. The attacker sends a RREQ with the above noted destination address field spoofed with an unknown destination address. On setting the hop count value to the lowest number, it also sets the highest sequence number, in order to prove its shortest path.

Step 3. The attacker sends a RREP packet to the node which is nearer in position and also present in the current active path or the packet can be sent directly to the source node if possible.

Step 4. The data that was now received through the RREP packet will be updated in the source routing table.

Step 5. Now the source node selects a new route for data transmission.

Step 6. Once receiving the transmitted data, the attacking node drops all the data that passed through it.

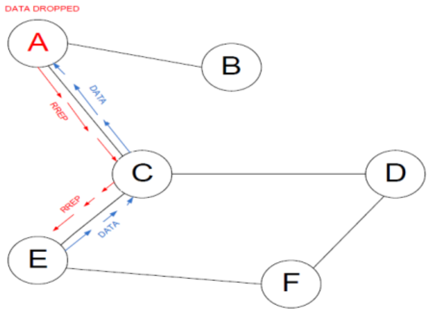

Fig. 4. Black Hole Attack

Fig. 4 depicts the above discussed details. For instance, consider “A” to be a malicious node. Let “E” be the source node and “D” the destination. Now node “A” out the route between the node “E” and the node “D”. The node “A” on receiving a RREQ sends the RREP with the spoofed destination address, lesser hop count and larger sequence number. These details are forwarded to the source node by the intermediate node “C”. Source node now uses this route for further data transmission. Thus node “A” receives all the packets which in turn are dropped by “A”. Thus the packets do not reach the destination. This is called the Black hole attack.

Cooperative Blackhole attack is an attack where multiple black hole nodes perform in coordination with each other. In Fig. 5, Let S be the source node and D be the destination node. The other nodes act as the intermediate nodes. Node B1 and node B2 are the Cooperative Black holes. These malicious nodes receive the RREQ along with the other nodes, when the source node transmits it. The Black hole nodes at once send back the RREP. The RREP from B1 reaches the source node sooner than all other RREPs. The source node transmits the packets to B1. On receiving the data packets, B1 either drops all the packets or forwards them to B2, which in turn prevents the data packets from reaching the destination.

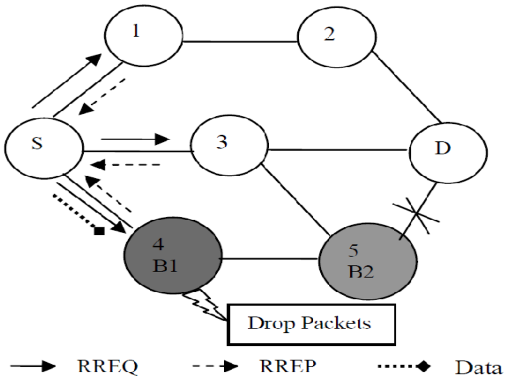

Fig. 5. Cooperative Blackhole Attack

III. LITERATURE SURVEY

In the paper [5] a solution to encounter black hole attack is proposed. Here the AODV is modified. In order to check whether the route advertised exists and free of malicious nodes, the intermediate nodes should add the address of the next hop node in RREP packets. Once the source node receives the RREP packet, it finds the details of the next hop node and sends a Further request to the next hop node in order to verify the existence of the next hop node. The next hop node sends the Further reply packet to the source node to confirm the route information. If the source does not receive the Further reply, the route contains the malicious nodes and the route is removed from the routing table. However, this solution doesn’t address the cooperative black hole attack.

In [8] two solutions are proposed to encounter black hole attacks on AODV protocol. The first proposed solution is to find more than one route to the destination. The source node would unicast a ping packet to the destination node. On receiving the acknowledgement pinged back through different routes the source node will find the safe routes. On the other hand, in order to find the malicious node, each node will maintain two tables to store sequence numbers of last packet sent and received to and from every node respectively. This number is compared with the last sequence number in RREP at source node. If both the numbers match, the data will be forwarded to that route otherwise an alarm message is broadcast to isolate the malicious node in the network. However, in both the solutions time delay is the major drawback.

According to proposed solution in [9] by Tamilselvan et.al, the source node waits for other replies with next hop information. Once it receives the first RREP it sets the timer in the "TimerExpiredTable". Further RREP's from different nodes are stored in "Collect Route Reply Table" (CRRT). The sequence number and the time at which the packet arrived are also stored. The "timeout" value is calculated using the arrival time of the first RREP. It first checks the CRRT for repeated next hop node. If any repeated next hop node is present, it assumes the paths are correct or the chance of malicious paths is limited In this solution the time delay is more. Also cooperative black hole attack cannot be detected.

In [10] a new mechanism called dynamic training method is introduced to detect black hole attack in which the training data is updated at regular time intervals. The average of the difference between the Dst_Seq in RREQ packet and the one held in the list are calculated and this operation is executed for every received RREP packet. The average of this difference is finally calculated for each timeslot which is used in the future. Thus it consumes large amount time to compute for every RREP packet.

In [11] a solution is proposed by modifying the AODV protocol to avoid multiple black holes in the group. It maintains a Fidelity table. Every participating node is given a fidelity level that tells the reliability of that node. Any node having value as 0 is considered as malicious node and is eliminated from the network. The fidelity levels of the nodes along a route is increased on every successful transmission of the data, otherwise the fidelity level of the nodes is decreased. The processing delay in the network is high.

In [12] CBDAODV mechanism is proposed. A source node will accept at least two RREP packets from different replying nodes. Thus by utilizing another routing path, the source node itself can evaluate the reliability of the currently selected route and make a rerouting decision once it suspects the reliability of currently selected route. Through another route, a confirmation control packet which consists of the name of the second malicious node to which the first malicious node sends the data packets is sent. On receiving the packet, the destination node will reply it to indicate the existence of the route between the destination and the malicious node. If the reply packet indicates that no path exits, the source node now switches its routing path to the alternate route and retransmits its data packets. Also the malicious nodes are put to observation to identify whether the nodes regularly work in cooperation with each other.

In [13] a mechanism is proposed to defend cooperative black hole attack. Each node observes the data forwarding nature of its neighboring node. This information is recorded in a DRI (Data Routing Information) table. Each node maintains an additional DRI table. In the DRI table, 1 stands for 'true' and 0 for 'false'. The first bit stands for information on routing data packet *from* the node, while the second bit stands for information on routing data packet *through* the node . If the entry is 0 0 for a node N implies that, a node has NOT routed any data packets from or through N. An Additional cross checking method is also done. The source node broadcasts a RREQ message to discover a secure route to the destination node. The Intermediate Node (IN) generating the RREP has to provide its Next Hop Node (NHN) and its DRI entry for the NHN. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node or not.

In [14] DPRAODV mechanism is proposed. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in routing table.does an addition check to find whether the RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated as in [4] in every time interval. As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. So, in this way, the malicious node is isolated from the network by the ALARM packet. The threshold value is the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet.

The paper [15] proposes an authentication mechanism for identifying black hole nodes in MANETs. An authentication mechanism is constructed based on the concept of the hash function, MAC in order to ensure authentication for every the RREPs at source node. However it is necessary to discuss how to prevent a forge reply if the hash key of any node is disclosed to all the other nodes.

In [16] MOSAODV mechanism is presented. In that a timer is set in the source node to collect all the RREP packets and those packets with exponentially high destination sequence number are discarded. In [16], all the RREPs are stored in the newly created table until the modified wait timer. The modified wait timer is initialized to be half the value of RREP wait time – the time for which source node waits for RREP control messages before regenerating RREQ. The source node after receiving first RREP control message waits for modified wait time. For this time, the source node will save all the coming RREP control messages in the new table. Subsequently, the source node analyses all the stored RREPs from the new table, and discard the RREP having very high destination sequence number. The node that sent this RREP is suspected to be the malicious node. Once, such malicious node is identified, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table for that node is not maintained.

In [17], ABM (Anti-Black hole Mechanism) is discussed. The suspicious value of a node is estimated according to the amount of abnormality in RREQ and RREP packets being transmitted from the node. When the suspicious value exceeds a threshold level, the nearby IDS will blacklist the identified black hole and the time of identification and broadcast the message in order to isolate the malicious node in the network cooperatively. Thus the cooperative black hole nodes can be identified. The drawback is that in addition to the routing table maintenance, the mobile nodes have to maintain training data and regular updates.

The Table 1 depicts the comparison of the above discussed literature works on solution to the blackhole attack and its versions. The comparison is based on the factors like techniques proposed, modification of the AODV and type of the blackhole attack.

IV. CONCLUSION

This paper presents a study on WSN and MANET. The routing protocols on which the MANET environment functions are discussed. The importance of AODV and its operations are discussed. Security challenges of MANET are analyzed, and the severity of black hole attack is studied. This paper portrays the various works related to black hole attack detection mechanism in AODV-based MANETs. The solutions are compared based on certain factors. It is observed that these mechanisms possess certain disadvantages besides detecting blackhole attacks.

TABLE I
COMPARISON OF VARIOUS SOLUTIONS TO DETECT BLACKHOLE ATTACK

AUTHORS	MECHANISM ADOPTED	IS AODV/ROUTING TABLE MODIFIED?	TYPE OF BLACKHOLE	REMARKS
Deng H, et al. [5]	Source sends Further request to NextHopNode. Further reply is received.	Yes	Single Blackhole	Cooperative black holes are not detected
Al-Shurman, M , et al.[8]	At the source node , the last seq. no of the RREP is compared with the last seq. no of the packet	No	Single Blackhole	Time delay
Tamilselvan, L ,et al. [9]	Maintains Timer_Expired_Table and Collect_Route_Reply_Table	No	Single Blackhole	-Time delay -Cannot detect Cooperative black holes
Satoshi Kurosawa, et al. [10]	Avg of difference between Dst_Seq of RREQ and the one in the list is calculated	No	Single Blackhole	Time consuming
Latha Tamilselvan, et al. [11]	The node with fidelity value 0 is malicious	Yes	Multiple Blackholes	Processing delay
Nai-Wei Lo, et al. [12]	CBDAODV: Using the second shortest path, the source checks the reliability of the first shortest path	Yes	Cooperative black holes	Do not broadcast the blacklist
Ramaswamy S , et al. [13]	DRI table is maintained. The node with the entry 0 0 is suspected as malicious	No	Cooperative black holes	Do not broadcast the blacklist
Raj PN , et al. [14]	DPRAODV: Threshold value is calculated. If the value of RREP_Seq_no is higher than the threshold, the node is suspected.	Yes	Multiple Blackholes	Cooperative black holes are not detected
Zhao Min, et al. [15]	Authentication Mechanism based on Hash function, MAC for every RREPs.	No	Multiple Blackholes	No mechanism to prevent a forge reply if the hash key of any node is disclosed
Mistry NH, et al. [16]	MOSAODV: Source discards the RREP with high destination seq. no and isolates the node	Yes	Multiple Blackholes	Cooperative black holes are not detected
Ming-Yang Su , et al. [17]	ABM: The node is suspected if the value of a node exceeds the threshold value	No	Cooperative black holes	Additional training data is to be maintained

REFERENCES

[1] Bellavista, P. ; Cardone, G. ; Corradi, A. ; Foschini, L., "Convergence of MANET and WSN in IoT Urban Scenarios", IEEE Sensors Journal, Vol. 13, Iss. 10, pp. 3558 - 3567, Oct. 2013.

[2] Royer E and Toh C, “A review of current routing protocols for ad-hoc mobile wireless networks. Mobile Wireless Networks”, IEEE Personal Communications, pp. 46–55, Apr 1999.

[3] Udhayan J, and Rajesh Babu M, "Lightweight vigilant procedure to implement security measures in highly roving military operations",Journal of Computer Science,Vol. 9, Iss. 10,2013.

[4] Perkins CE, Belding-Royer E, Das S “Ad hoc on-demand distance vector(AODV) routing”, The Internet Engineering Task Force(IETF), RFC 3561, 2003

[5] Deng H, Li W, Agrawal DP, “Routing security in wireless ad hoc networks”, IEEE Commun Mag, Vol 40, Iss 10, pp. 70-75, 2002.

[6] Ning P and Sun K, How to Misuse AODV: A Case Study of Inside Attacks against Mobile Ad-Hoc Routing Protocols, Proc. IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, 2003.

[7] Khatri P, Rajput M, Shastri A, Solanki K, Performance study of ad-hoc reactive routing protocols. J Computer Science, Vol. 6, Iss.10, pp.1159– 1163, 2010.

[8] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[9] Tamilselvan, L.; Sankaranarayanan, V., "Prevention of Blackhole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007.

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, “Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method” International Journal of Network Security, Vo l.5, No .3, P P.338–346, Nov. 2007.

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

[12] Nai-Wei Lo, Fang-Ling Liu,“ A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET”, Intelligent Technologies and Engineering Systems, pp 59-65, 2013.

[13] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, “Prevention of cooperative black hole attack in wireless ad hoc networks”, International conference on wireless networks, CSREA Press, Las Vegas, pp .570–575, 2003.

[14] Raj PN, Swadas PB, “DPRAODV: a dynamic learning system against blackhole attack in AODV based MANET”, IJCSI Int J Comput Sci, Iss. 2, pp.54–59, 2009.

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

[16] Mistry NH, Jinwala DC, Zaveri MA, “MOSAODV: solution to secure AODV against blackhole attack, Int J Computer Network Security Vol.1, Iss.3,pp.42–45, 2009.

[17] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010..