A SURVEY ON DETECTING CO-OPERATIVE BLACK HOLE ATTACK ON MULTICAST IN MOBILE AD-HOC NETWORK

Lalbihari Barik
Department of Information Systems, Faculty of Computing & Information Technology in Rabigh, King Abdulaziz University, Kingdom of Saudi Arabia.

Abstract

Mobile Ad-hoc Network (MANET) is a self-directed decentralized wireless network where mobile nodes are move freely in the network with dynamic topology. Therefore, the main issue in MANET is security. The route search process in MANET performed by one of the responsive, active or hybrid route protocols. MANETs are vulnerable to any security attack, where one of these attacks is the black hole attack. In a black hole attack, where the malicious node advertises itself that it has the shortest route to the destination and tries to fool the source node. After the response received from the malicious node, the source node leaves all other paths and transferring data to the malicious node. Instead of forwarding to the next node, a malicious node leaves all data packets after data packet received from the source node. Common two classification of black hole attacks listed as: (i) Single Black Hole (SBH), and (ii) Cooperative Black Hole (CBH). In SBH attack, only one malicious node is present and whereas in CBH attack, there is two or more malicious node attack in cooperation with each other. Many techniques in literature available for the identification and prevention of black hole attack. In this research, the researcher discussed some techniques for detecting cooperative black hole attack in MANET using the Ad-hoc On-demand Distance Vector (AODV).

Index Terms: MANET, RREQ, RREP, Black hole attack.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a self-directed decentralized wireless network where no access point required [13,15-17]. It is a wireless network that has no fixed infrastructure. With dynamic topology, there is no central infrastructure for controlling the network, nodes forwarded by forwarding the packet over the network, and at any time leave or join the network. Some routing protocols used by nodes to connect are Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector (AODV), and Destination Sequenced Distance Vector (DSDV) [13-18].

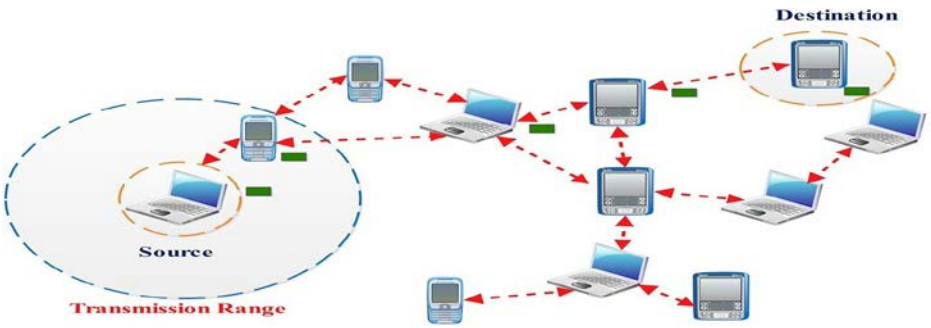

Fig. 1 Mobile Ad-hoc Network

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-5, ISSUE-11, 2018
DOI:10.21276/ijcesr.2018.5.11.1

The lack of infrastructure and its topology security are fundamental issues in MANET. As MANET works without any central infrastructure, it suffers from many attacks like a black hole, worm hole, sink hole, Sybil, flooding, attack, Denial of Service (DoS) attack, etc. [11-14]. In a black hole attack, a malicious node advertises itself that it has the shortest route to the destination and tries to fool the source node.

After receiving the data packet, the malicious node drops all the packets that it has to move forward to its neighbor node. Further, this malicious node that drops all data packets uses the path of the protocol to find out the vulnerabilities of the search process, such as AODV [13].

II. OVERVIEW OF AODV

The AODV protocol is a fast adaption to dynamic route in which a route to the destination created only when required. The AODV protocol uses the following three types of messages: *(i)* Route Request (RREQ), *(ii)* Route Reply (RREP), and *(iii)* Route Error (RERR). The packet format of RREQ and RREP message show in the following tables [10].

Table 1: Format of RREQ packet

Route Request (RREQ) Packet					
Source IP address	Source Sequence number #	Broadcast ID	Destination IP address	Destination sequence number #	Hop count

Table 2: Format of RREP packet

Route Reply (RREP) Packet				
Source IP address	Destination IP address	Destination sequence number #	Hop count	Lifetime

A. The route discovery process in AODV

When a source node data packets transmitted, it checks in the routing table. If there is no route found, then it starts the route discovery process by sending the RRQ message. The source node broadcasts RREQ message to a neighboring node or intermediate destination route or destination node which further generates the RREP packet. After that this packet send it back to the source node. If no destination path is detected, then the nodes will need to reorder their neighboring node to the RRQ. If the answer did not receive before the expiration date, then RREQ is a timer connected to each node to destroy the packet.

III. BLACKHOLE ATTACK

Researcher discussed in black hole attack, malicious node advertises itself that it has the shortest route to the destination and tries to fool the source node. The source node ignores all other paths towards malicious nodes and transfers data after receiving the response from the malicious node. After obtaining a data packet from the source node, instead of forwarding a malicious node to them on the next node, all data packets are dropped. There are different types of black holes listed in the following Fig. 2.

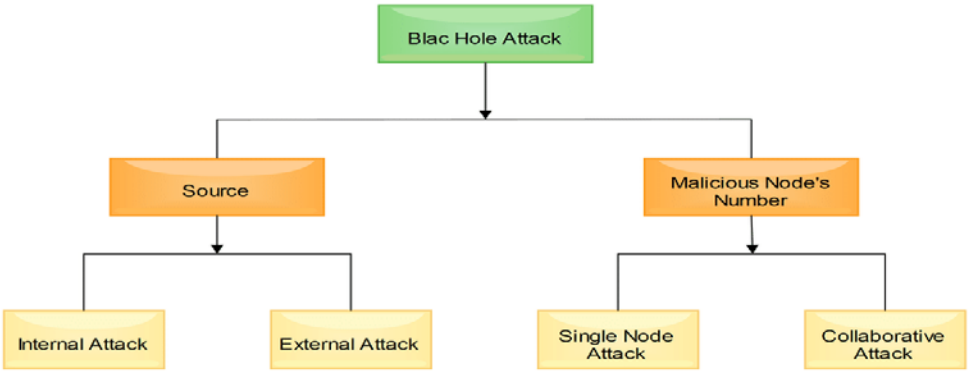

Fig. 2 Types of black hole attack

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-5, ISSUE-11, 2018
DOI:10.21276/ijcesr.2018.5.11.1

Black hole attacks categorized into the following two types:

A. Single Black Hole (SBH) attack
B. Cooperative Black Hole (CBH) attack

A. Single Black Hole (SBH) attack

This type of attack is also termed as Simple Black Hole attack. In SBH attack, only one malicious node exists in the network, which claims the shortest route to the destination. In lieu of forwarding them they attracts the data packets and drops them. Occasionally these malicious nodes work in coordination, which further results in collaborative black hole attacks [1, 9].

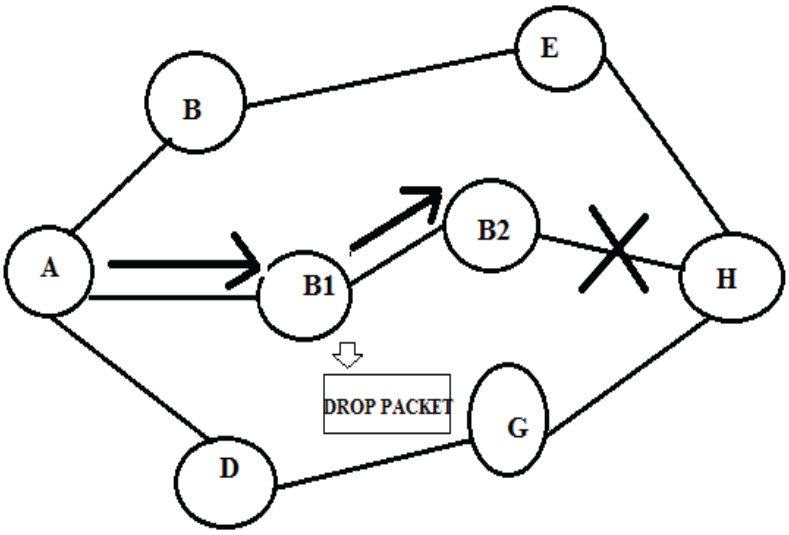

Fig. 3 Single Black Hole (SBH)attack

B. Cooperative Black Hole (CBH) attack

In CBH attack, two or more node act maliciously in cooperation with each other in the network. Following Fig. 4 shows the CBH attack. Here, node B1 and node B2 are malicious nodes working in collaboration. Hence, node B2 can either drop the data packets or forward them to node B1. Similarly node B1 can either drop the packets or sent them to the adjacent malefic node in alliance.

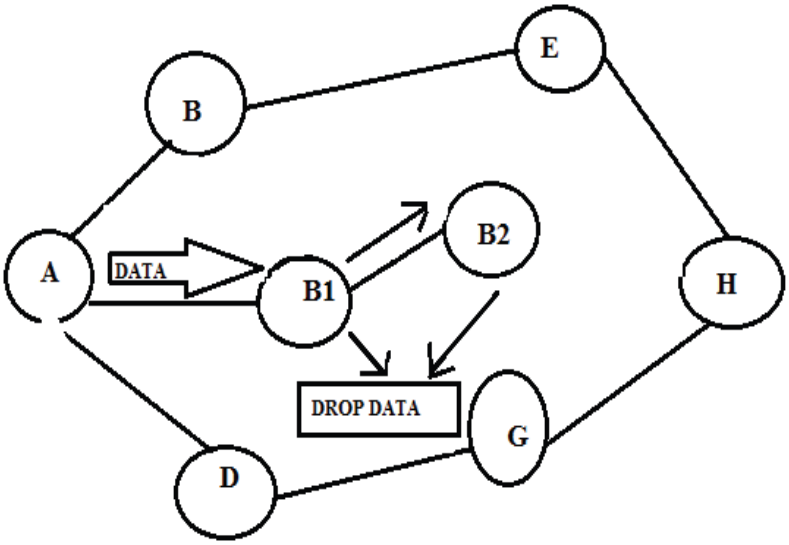

Fig. 4 Cooperative Black Hole (CBH) attack[9]

IV. LITERATURE SURVEY

In the literature survey, researcher reviewed on Expiry Timer Expired Table (ETET) and Collect Route Reply Table (CRRT) Mechanism, Fidelity level based black hole attack prevention scheme, Dynamic learning system against black hole attack in AODV, Data Routing Information (DRI) table and Cross-checking scheme, and Extended Data Routing Information (EDRI) table based scheme. The detailed explanation is

available in this section.

A. Timer Expired Table (ETET) and Collect Route Reply Table (CRRT) Mechanism

Tamilselvan, & Sankaranarayanan proposed a method which is an improvement of essential AODV routing protocol which can secure against black hole attack [2-3]. In this mechanism, without sending the data packet to the RREP initiator at one time, it has to wait until another neighbor node gives information about their next hop. Once the first request received, the timer sets to Expiry Timer Expired Tables (ETET) to collect requests from different nodes. In the Collect Route Reply Table (CRRT), it will store the sequence number and arrival time of the packet. It calculates the value based on the time that the route requested first.

B. Fidelity level based black hole attack prevention scheme

Tamilselvan, & Sankaranarayanan proposed a method which is an improvement of essential AODV routing protocol [3]. This technique identifies multiple black hole nodes which are participating with each other, and a safe route discovered. In this method, it assumes that nodes are already certified and therefore participate in the communication. In order to combat the attack of black hole, their approach is to use a 'fidelity table' in which each participant node will be assigned a Fidelity level that acts as a measure of the reliability of that node. If any node in the fidelity level falls to '0', then this node is identified as a black hole node, and it removed from the network. An acknowledgment is sent back to the source node by the destination node after receiving a data packet.

The source node can increment the fidelity level of the intermediate node after receiving this acknowledgment. Within a time out period, source node did not receive any response; then it will decrement the fidelity level of intermediate node which replied. It also decrements the fidelity level of the node, which gave as a next hop node of that intermediate node to detect cooperative black hole nodes [7].

C. Dynamic learning system against Black hole attack in AODV

In the basic AODV, the node obtaining the RREP packet first ensures the value of the sequence number in its routing table and if the packet is more than one RREP_seq_no in the routing table, then accept the packet. In their research, Raj & Swadas proposed a mechanism, which makes an additional investigation to determine whether the value of RREP_seq_no is higher than the threshold value [4]. The threshold value calculated as the average of the difference between the RREP packet and the sequence number in the routing table. On the possibility of RREP_seq_no higher than the threshold value, the node is identified as a black hole node and adds the node to the exclusion. A new control packet called ALAMR, which has a black list node in the form of a parameter; sent to its neighbor node with the goal that the neighboring node detects that the RREP packet is to drop from the node.

D. Data Routing Information (DRI) table and Cross-checking scheme

Sen & et al. proposed a technique for securing against CBH attack. They alter the AODV protocol by presenting two ideas: (i) Data Routing Information (DRI) table, and (ii) Cross-checking [5].

(i) Data Routing Information (DRI) table

In this technique, at the time of the route discovery process, a node sends two bits of additional information that responds to the RREQ message sent by the source node. An extra DRI table is kept up by every node. In this DRI table, piece '0' remains for 'false' and bit '1' remain for 'true'. The first bit ‘From’ remains for information on how to route the data packet from the node and the second bit 'Through’ node keeps information to route the data packet.

(ii) Cross checking

In this paper, the proposed method relies on a reliable node to send data packets. In enhanced AODV, the intermediate node (IN), which produces the RREP in response to the RREQ message from the source node (SN), must report the Next Hop Node (NHN) and the DRI route for that NHN. After accepting the source node RREP from the intermediate node, it will check its own special DRI table to see if the IN is reliable. If IN is reliable, SN starts transmitting data packets; then SN sends Further Request (FRq) message to NHN. In the wake of accepting FRp message, source node checks whether SN has directed data packet through NHN to ensure NHN is reliable or not. If the NHN is reliable, then the SN will check whether

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-5, ISSUE-11, 2018
DOI:10.21276/ijcesr.2018.5.11.1

the IN is BH or not. IN is a BH, If through entry of DRI table of IN is '1' and from the entry is '0'. The route is secure if IN is not BH and NHN is reliable.

E. Real-time monitoring scheme

Kshirsagar & Patil has utilized the technique which initially finds for the RREP initiator's neighbor node, i.e., the suspicious node sends suspected node and advises that neighbor node to screen all the packets [8]. Neighboring node put itself in a screening packet sent by malicious nodes.

The neighbor node keeps two counters: (i) fcount: The number of packets sent for counting purpose, and (ii) rcount: utilized for checking the number of the received packet. When it delivers a packet in the suspicious node, the neighboring node increases the fcount. Advance on the off chance that the suspect node that will be screened by the neighboring node, and it increases the rcount. A neighboring node forwards the packet to the suspicious node until the fcount does not receive a limit; From that point, if the rcount is '0', the RREP initiator node is identified as a malicious node.

F. Extended Data Routing Information (EDRI) table based scheme

Bindra et al., Kshirsagar & Patil proposed a system which handles the BH and gray hole attacks by keeping an Extended Data Routing Information (EDRI) table on every node in addition to the Routing Table of the AODV [6, 8].

The EDRI also obliges the gray behavior of the table nodes. Although it gives resultant opportunities to reputed nodes in the form of BH, additionally it records the previous malicious instances of that node. Therefore results in a goal that a better understanding of the node can make, and the node is given its next shot in like manner. A counter monitor shows how many times a node has obtained, and this counter estimate is proportional to the time that another opportunity should give before that node. A node that is found to be acting maliciously, does not end up once again.

V. COMPARISON OF EXISTING TECHNIQUES

In this section comparison of existing technique based on parameters like the type of black hole, packet delivery ratio, average end-to-end delay, and network overhead is carried out.

Table 3: Comparison of existing techniques

Techniques	Parameters of Comparison			
	Type of Black Hole	**Packet Delivery Ratio**	**Average End-to-End Delay**	**Network Overhead**
Timer Expired Table and Collect Route Reply Table' (CRRT) mechanism [2]	Single black hole	Increase as compared to normal AODV	Increase in average end-to-end delay	More
Fidelity level based black hole attack prevention scheme [3]	Cooperative black hole	Increase as compare to AODV	Increase due to additional waiting before sending the reply	More
Dynamic learning system against black hole attack in AODV [4]	Single black hole	Increase	Less delay	Slightly increased due to ALARM packet
Data Routing Information (DRI) table and Cross-checking scheme [5]	Cooperative black hole	More	Increase	More
Real-time monitoring scheme [6, 8]	Single black hole	Increase with high mobility	Less delay	More

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-5, ISSUE-11, 2018
DOI:10.21276/ijcesr.2018.5.11.1

VI. CONCLUSION

Security has become the major issue in MANET, and because of its dynamic topology and absence of a central entity it is vulnerable to any kinds of attack, and one of this is black hole attack. In black hole attack, a malicious node tries to fool the source node by advertising that it has the shortest path to the destination. After getting the data packet, the malicious node drops all the packets, which it has to forward to its neighbor node. This paper contains a survey of various techniques to detect the black hole attack. Black hole attack affects adversely on the network so there must be a perfect technique to detect black hole.

REFERENCES

[1] Palanisamy, V., Annadurai, P., & Vijayalakshmi, S. (2010, December). Impact of black hole attack on multicast in ad hoc network (IBAMA). In Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on (pp. 1-4). IEEE.

[2] Tamilselvan, L., & Sankaranarayanan, V. (2007, August). Prevention of blackhole attack in MANET. In Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on (pp. 21-21). IEEE.

[3] Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. JNW, 3(5), 13-20.

[4] Raj, P. N., & Swadas, P. B. (2009). Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371.

[5] Sen, J., Koilakonda, S., & Ukil, A. (2011, January). A mechanism for detection of cooperative black hole attack in mobile ad hoc networks. In Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on(pp. 338-343). IEEE.

[6] Bindra, G. S., Kapoor, A., Narang, A., & Agrawal, A. (2012, September). Detection and removal of co-operative blackhole and grayhole attacks in MANETs. In System Engineering and Technology (ICSET), 2012 International Conference on (pp. 1-5). IEEE.

[7] Wahane, G., & Lonare, S. (2013, July). Technique for detection of cooperative black hole attack in MANET. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on (pp. 1-8). IEEE.

[8] Kshirsagar, D., & Patil, A. (2013, July). Blackhole attack detection and prevention by real time monitoring. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on (pp. 1-5). IEEE.

[9] Hiremani, V. A., & Jadhao, M. M. (2013, December). Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET. In Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on (pp. 944-948). IEEE.

[10] Dangore, M. Y., & Sambare, S. S. (2013, November). Detecting and overcoming blackhole attack in aodv protocol. In Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 2013 International Conference on (pp. 77-82). IEEE.

[11] Singh, M., & Kaur, G. (2013). A Surveys of Attacks in MANET. International Journal of Advanced Research in Computer Science and Software Engineering, 3(6).

[12] Wahane, G., Kanthe, A. M., & Simunic, D. (2014, May). Technique for detection of cooperative black hole attack using true-link in Mobile Ad-hoc Networks. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on (pp. 1428-1434). IEEE.

[13] Chaubey, N. K., & Barik, L. B. (2017). Empirical Study of NDTAODV, SAODV and AODV Routing Protocol in the presence of RREQ Flood Attacks in MANETs. IJCSNS, 17(11), 90.

[14] Yasin, A., & Abu Zant, M. (2018). Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing, 2018.

[15] Woungang, I., Dhurandher, S. K., Peddi, R. D., & Obaidat, M. S. (2012, May). Detecting blackhole attacks on DSR-based mobile ad hoc networks. In Computer, Information and Telecommunication Systems (CITS), 2012 International Conference on (pp. 1-5).

IEEE.Raj, P. N., & Swadas, P. B. (2009). Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371.

[16]Dhenakaran, D. S., & Parvathavarthini, A. (2013). An overview of routing protocols in mobile ad-hoc network. International Journal of Advanced Research in Computer Science and Software Engineering, 3(2).

[17]Al-Omari, S. A. K., & Sumari, P. (2010). An overview of mobile ad hoc networks for the existing protocols and applications. arXiv preprint arXiv:1003.3565.

[18]Aggarwal, A., Gandhi, S., & Chaubey, N. (2014). Performance analysis of AODV, DSDV and DSR in MANETS. arXiv preprint arXiv:1402.2217.