

Detection and Prevention of Black hole Attack in MANET: A Review

Chander Diwaker¹, Chanchal Aghi², Kulvinder Singh¹

¹Assistant Professor, U.I.E.T. Kurukshetra University, Kurukshetra, Haryana, INDIA

²Research Scholar, U.I.E.T, Kurukshetra University Kurukshetra, Haryana, INDIA

Abstract: mobile ad hoc network (MANET) consists of wireless mobile nodes without any pre existing infrastructure or centralized access point such as base station. MANET has dynamic topology which allows nodes to join and leave the network at any point of time. MANET is more vulnerable due to its characteristics such as dynamic topology, distributed cooperation and open medium. Security issues are the most important in MANETs as mobile nodes are more susceptible to vulnerabilities. The black hole attack at network layer is the most attention seeking attack in ad hoc networks. This paper presents a review of various techniques used to detect and prevent the black hole attack.

Keywords: MANET, security, black hole attack, detection and prevention techniques

I. INTRODUCTION

MANETs is a decentralised autonomous system in which different mobile nodes are connected to each other by wireless links. MANET has a routable networking environment on top of a Link Layer ad hoc network. In the network, nodes can be either fixed or mobile. MANET is a dynamic network in which node can join or leave the network at any moment; each device in ad hoc network is free to move independently in any direction so change its links to other devices frequently. In MANET, communication occurs between nodes directly or through intermediate nodes which act as routers [1]. MANETs has some nontrivial challenges, these challenges are open network architecture, shared wireless medium, mobility induced packet loss, frequent network partition and highly dynamic network topology, so in MANET, Security has become a most important concern to provide protected communication between nodes [2]. The black hole attack is one of the most severe security attacks which can significantly disrupt the communications across the network. This paper presents various methods to detect and prevent Black hole attack.

II. BLACK HOLE ATTACK IN MANET

In a black hole attack, Selfish node advertises a shortest route to the sink node to attract traffic to the malicious (selfish) node and then drops those Packets [3]. The Black hole attack at network layer is the most attention seeking attack in ad hoc networks. In Black hole attack the situation can become worse if the black hole node declares itself as having shorter path to almost all nodes. Black hole attack may be either single or corporative. The black hole attack has two properties. First property is, the node exploits the MANET protocol, such as AODV (Ad hoc On-demand Distance Vector) to advertise itself as having a valid path to a destination node, even though the path is invalid, with the intention of intercepting packets. Second property is, the attacker consumes the intercepted packets without forwarding to any other node [4]. Following Fig shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process to find out the valid route. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives Route Request packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost [5].

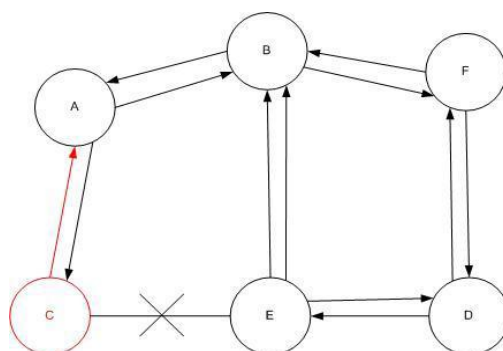


Figure 1. Black hole Attack

III. DETECTION AND PREVENTION TECHNIQUES OF BLACK HOLE ATTACK

A. Detection techniques for single black hole attack

(i) Time-based Threshold Detection Scheme [6]

In this technique a timer is set in the Rimer Expired Table. Timer is use for collecting the other request from other nodes after receiving the first request. This table will store the sequence number of packets and the received time in a Collect Route Reply Table (CRRT), counting the timeout value based on the arriving time of the first route request, analyse the route belong to valid or not based on the above threshold value.

(ii) Resource-Efficient Accountability (REAct) Scheme based on Random Audits

This detection scheme called REAct scheme [7]. When the performance is degrading between source and destination node, the REAct is triggered automatically. REAct constitutes of three phases: (1) the audit phase (2) the search phase and (3) the identification phase. To simply describe the REAct scheme, the target node sends a feedback to the sender when a biggish packet drop ratio is recognized. Then the source node chooses an audit node. Finally, the segment location of malicious node can be distinguished from comparing the source node's behavioural proof. Furthermore, there are some limitations in REAct. First, the REAct is designed for non-cooperative black hole attack only. It's unsuccessful in the collaborative black hole because other malicious node is able to manipulate a fake proof and send to the audit node. Second, the behavioural proof only records the information of transmission packets rather than the nodes. It fails to verify who the producer of the behavioural proofs. Now the attacker is able to cheat source node by changing its behaviour dynamically.

(iii) Detection, Prevention and Reactive AODV (DPRAODV) Scheme

A new control packet called ALARM is used in DPRAODV [8], while other main concepts are the dynamic threshold value. Unlike normal AODV, the Route Reply sequence no is extra checked whether higher than the threshold value or not. If the value of Route Reply sequence no is higher than the threshold value, the sender is known as an attacker and updated it to the black list. The ALARM is sent to its neighbour nodes that includes the black list, thus the Route Reply from the malicious node is blocked but is not processed. On the other hand, the dynamic threshold value is changed by calculating the average of destination sequence number between the sequence number and Route Reply packet in each time slot. The benefit of this technique is that technique this method is simple as compare to other methods, no energy is consumed for monitoring. But the drawback is, DPRAODV simply detects multiple black holes rather than cooperative black hole attack.

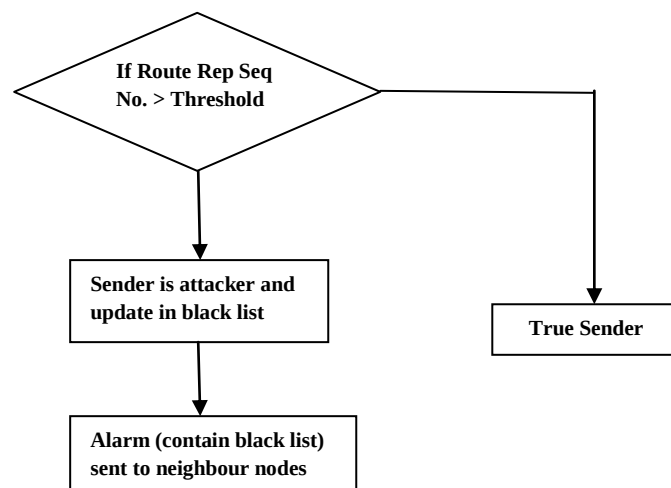


Figure 2 DPRAODV Scheme

(iv) Redundant Route Method and Unique Sequence Number Scheme

There are two techniques to prevent the black hole attack in MANETs. The first technique is to true path to the destination. Based on the neighbour set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response [8]. In detection procedure, two major steps are: 1- Collect neighbour set information. 2-Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively and efficiently detects black hole attack without introducing much routing control overhead to the network. The

working of this scheme is as follow. Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are it represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last packet sequence numbers which are used to identify the last packet sent to every node and the second value is use for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not.. Second technique is considered to be good as compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol. The drawback for this technique is these both techniques fail to detect cooperative black hole attacks.

B. Detection techniques for Collaborative black hole attack

(i) DRI Table and Cross Checking Scheme

Data routing information (DRI) table and cross checking method is use to identify the cooperative black hole nodes. In this technique the AODV routing protocol is modified by adding an additional table i.e. Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) [9]. Every node needs to maintain an extra DRI table, 1 represents for true and 0 for false. The entry is composed of two bits, "From" and "Through" which stands for information on routing data packet from the node and through the node respectively. As shown in Table 1, the entry 1 1 implies that node 1 has successfully routed data packets from or through node 5, and the entry of 0 0 means that node 1 has not routed any data packets from or through node 3. The procedure of proposed solution is simply described as below. The source node (SN) sends (Route Request) RREQ to each node, and sends packets to the node which replies the (Route Reply) RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the IN's honesty. After that, SN sends the further request to IN's NHN for asking its routing information, including the current NHN, the NHN's DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path. The benefits of this technique is it can identify multiple collaborative black hole nodes in a MANET and discovery of secure paths from source to destination that avoid collaborative black hole nodes acting in cooperation. But the main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table.

Node ID	Data routing information From	Data routing information Through
3	0(packet not routed successfully)	0(packet not routed successfully)
5	1(packet successfully routed)	1(packet successfully routed)

Table 1. Data Routing Information

(ii) Distributed Cooperative Mechanism (DCM)

Distributed and cooperative mechanism DCM is used to solve the collaborative black hole attacks. Because the nodes work cooperatively, they can analyze, detect, mitigate multiple black hole attacks [6]. The DCM is composed of four sub-modules which shown in following figure. In the local data collection phase, an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node initiates the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If the inspection value is positive, the questionable node is regarded as a normal node. Otherwise the initial detection node starts the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbours to participate in the decision making. Because the notify mode utilizes broadcasting method, the network traffic is increased. A constrained broadcasting algorithm is used to restrict the notification range within a fixed hop count. Finally, the global reaction phase is executed to set up a notification system, and sends warning messages to the whole network. There are reaction modes in global reaction phase. Though the first reaction mode notifies all nodes in the network, but might waste lots of communication overhead. Each node only concerns its own black hole list and arranges its transmission route in other mode, however it might be exploited by malicious nodes and needs

more operation time. Advantage of this technique is that, DCM has a higher data delivery ratio and detection rate even if there are various black hole nodes.

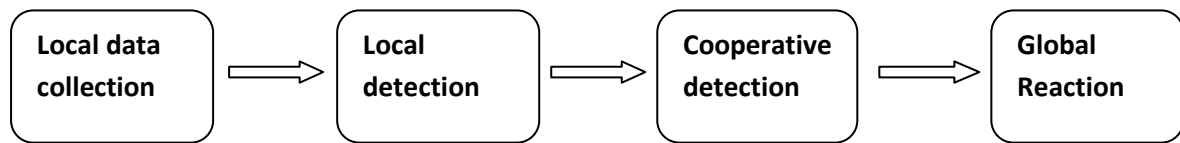


Figure 3 Sub-modules of Distributed Cooperative Mechanism (DCM).

(iii) Hash based Scheme [10]

A hash based defending method is used to generate node behavioural Proofs which involve the data traffic information within the routing path. The developing mechanism is based on auditing technique for preventing collaborative packet drop attacks, such as collaborative black hole problems. The proposed solution is originated from an audit-based detection method. The vulnerability of REAct system is that cooperative adversaries can specialize in attacker identification phase by sharing Bloom filters of packets between them. The major difference between these two schemes is discussed as follows. A hash based node behavioural proofs is proposed to defend the collaborative attacks. The audited node n is needed and settled by the source node S , and then S sends the sequence numbers of selected packets to auditing node. After source node sends out these packets, an additional random number t_0 is attached to the tail of every packet. The intermediate node n_1 combines the received packet and its own random number r_1 to calculate its value t_1 , and this operation is continued within every intermediate node until n receives the packet. The benefit of this technique is that this approach will allow the system to successfully locate the routing segment in which packet drop attacks are conducted.

IV. CONCLUSION

In the mobile ad hoc network (MANET), an attack always degrades the overall performance of the present network system. Black hole attacks are severe attacks that can easily be launched in networks with confidentiality and affects the performance of routing protocols. In this paper, we introduced the black hole attack along with its classification that can have serious consequences on many proposed ad hoc network routing protocols. Various methods and techniques used for the detection and prevention of Black hole attacks such as DRI Table and Cross Checking Scheme, Hash based Scheme, Distributed cooperative mechanism and Redundant Route Method and Unique Sequence Number Scheme along with their advantages and drawbacks are also discussed.

V. REFERENCES

- [1] Samba Sesay, Zongkai Yang and Jianhua He, "A Survey on Mobile Ad Hoc Wireless Network", Information Technology Journal 3 (2): 168-175, 2004.
- [2] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications. 11 (1), pp. 38-47.
- [3] Jian Yin and Sanjay Kumar Madria, "A Hierarchical Secure Routing Protocol against Black Hole Attacks in Sensor Networks", IEEE in 2006, ISBN 0-7695-2553-9.
- [4] Mohammad Al-Shurman and Seong-Moo Yoo, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE'04, April 2-3, 2004, pp. 96-97.
- [5] Irshad Ullah, Shoaib Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" in Thesis no: MEE 10:62 in June, 2010.
- [6] Tamilselven L and Sankaranarayanan, "Prevention of Black hole Attack in MANET" International Conference on wireless Broadband and Ultra Wideband Communications, 27-30 August 2007.
- [7] Fan-Hsun Tseng, Li-der chou and Han-chieh chao, "A survey of black hole attack in wireless mobile adhoc networks", springer journal 2011.
- [8] Ankita singh Kushwah, Kritika Khator and Atul Singhal, "A Review on Prevention and detection Techniques for Black hole Attack in Manet", ISSN: 2319-6327, Vol. 2, No. 1 (2013), pp. 24-27.
- [9] H.Weerasinghe and H. Fu.Preventing, "Cooperative black hole attacks in mobile adhoc networks:simulation implementation and evaluation", Future generation communication and networking, volume 2,IEEE 2007, pp. 362-367.
- [10] Wang W, Bhargava B and Linderman M, "Defending against Collaborative Packet Drop Attacks on MANETs" ,2nd International Workshop on Dependable Network Computing and Mobile Systems,27 september 2009.