*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 108-112*
*www.iosrjournals.org*

# Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks: A Survey

Kashmeera N. Khachar, Mrs Jayna B.Shah
*Dept of computer engineering Sardar Vallabhbhai Patel Institute of Technology, India*

***Abstract:*** *A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes. There is no centralized management. Both legitimate and malicious nodes can access the network, so there are many possible attacks in MANET. In a black hole attack, a malicious node attracts traffic towards it and drops all packets without forwarding to the destination. The security of the AODV protocol is compromised by a particular type of attack called black hole attack.*

***Keywords:*** *mobile ad hoc network, legitimate node, malicious node, black hole attack.*

## I. Introduction

A MANET (Mobile Adhoc Network) is a collection of two or more devices equipped with wireless communications and networking capability and can communicate with another node that is immediately within their radio range or one that is outside their radio range (using intermediate node). The applications of MANET include the mission critical applications such as- emergency relief, military operations, and terrorism response where no pre-deployed infrastructure exits for communication. Ad-hoc networks are so flexible that nodes can join and leave a network easily. But this flexibility of mobile nodes results in a dynamic topology that makes it very difficult in developing secure ad-hoc routing protocols. Wireless communication is always unreliable. The use of wireless links renders a mobile ad-hoc network to be vulnerable to attacks of various types. Black hole attack is one of the dangerous among them [1]. In black hole attack a malicious node (called black hole) replies to every route request by falsely claiming that it has a fresh enough route to the destination. In this way all the traffic of the network are redirected to that malicious node which then dumps them all.

Unlike wired networks where an adversary must gain a physical access to network wires or pass through several lines of defense at firewalls and gateways, attacks on mobile ad-hoc network can come from all directions and target at any node. Compared to traditional wired networks (a network in which network traffic could be monitored at central devices such as switches and routers), mobile ad-hoc networks have no network concentration points to filter traffic.

Black hole attack is one of the most common attacks made against the reactive routing protocol in MANETs. The black hole attack involves malicious node(s) fabricating the sequence number, hence pretending to have the shortest and freshest route to the destination. Numerous studies have attempted to devise effective detection methods for this attack. The aim of this paper is to investigate nine black hole detection methods within the scope of ad hoc on demand distance vector (AODV) routing protocol. AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network. The paper is organized as follows. Section 2 provides an overview of the route discovery process of AODV protocol and a description of the characteristics of a black hole attack. Section 3 describes six different attack detection methods. We conclude the paper in Section 4.

### 1.1 Route Discovery in AODV Routing Protocol

To understand the working of AODV, we take an example of five mobile nodes as shown in Figure 2.1. The circles indicate the range of communication for the nodes. As each node has a limited communication range, it can communicate with its neighbor nodes only. At an instant, Node 4 wants to communicate with Node 3, but it is uncertain of the route. Node 4 broadcasts RREQ that is received by its neighbors Node 1 and Node 5. Node 5 doesn’t have any route to Node 3 and therefore it rebroadcasts RREQ that is received back by Node 4. Node 4 drops it. On the other side, if Node 1 has a greater sequence number than RREQ, it discards RREQ and replies with RREP. If not, it updates the sequence number in its routing table and forwards RREQ to Node 2. As Node 2 has a route to Node 3, it replies to Node 1 by sending an RREP. Node 1 sends RREP to Node 4 and route Node 4-Node 1-Node 2-Node 3 is confirmed to send data packets. Node 4 can now send data packets to Node 3 through the specified route.

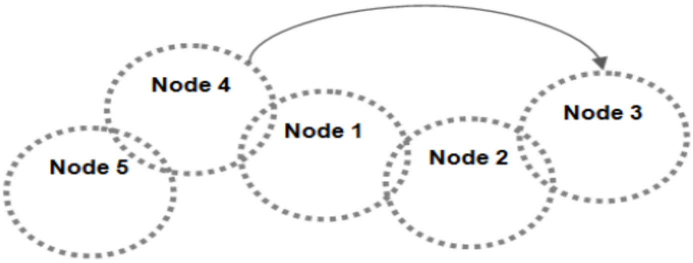

Fig. 2.1 Communication between nodes in Mobile Ad-hoc Network

### 1.2 Black hole Attack

It is a denial of service type attack. In this attack, malicious node attracts traffic towards it and then drops all packets without forwarding them to the destination. Here malicious node attracts traffic by claiming that it has a shorter route towards the destination.

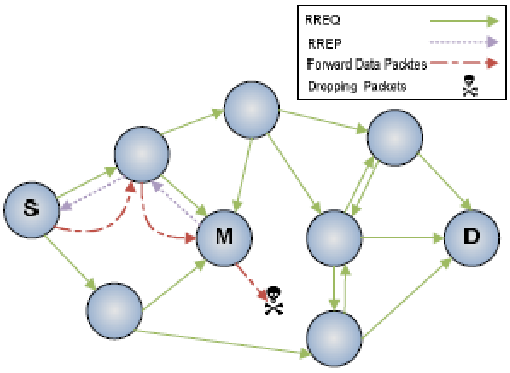

Fig. 2.2 Black hole Attack

As shown in figure 2.2 the adversary node in the network responds any received RREQ by false RREP which it claims having the freshest and shortest path to the destination. When data packets are received, it simply drops them.

## II. Black Hole Detection Methods

### 2.1 Detection Based On Path Based Method

The author [2] has proposed a path based scheme to detect black hole attack. In this method, a node does not watch every node in the neighbor, but only observes the next hop in the current route path. The algorithm is divided into three steps: (1) When a packet is forwarded out, its digest is added into the FwdPktBuffer and the detecting node overhears. (2) Once the action that the next hop forwards the packet is overheard, the digest will be released from the FwdPktBuffer. (3) In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold. If the forwarding rate is lower than the threshold, the detecting node will consider the next hop as a black or gray hole.

The proposed algorithm does not send out extra control packets so that Routing Packet Overhead does not increase. It requires no encryption on the control packets to avoid further attacks on detection information sharing. It will greatly increase the false positive probability.

### 2.2 Detection Based On Collaborative Bayesian Watchdogs

The author [3] has proposed a collaborative bayesian watchdog based on a message-passing mechanism in every individual watchdog that allows publishing both self and neighbour reputations. The standard watchdog simply overhears the packets transmitted and received by its neighbours, counting the packets that should be retransmitted, and computing a trust level for every neighbour as the ratio of “packets retransmitted” to “packets that should have been retransmitted”. If a node retransmits all the packets that it should have retransmitted, it has a trust level of 1. If a node has a trust level lower than the configured tolerance threshold, that node is marked as malicious.

Every node running watchdog collects the reputation information to obtain the values of α and β for every neighbor. The idea of the approach is that if a bayesian watchdog works well for detecting black holes, a group of collaborating neighboring bayesian watchdogs would be able to perform faster and more accurate detections. Similarly to the bayesian watchdog, the collaborative bayesian watchdog overhears the network to collect information about the packets that its neighbors send and receive. Additionally, it obtains α and β values for its whole neighborhood. These values are exactly the same than those obtained by the bayesian watchdog with the same observations; called 'first hand information' or 'direct reputations'. Periodically, the watchdog shares these data with its neighbors and it is called 'second hand information' or 'indirect reputation'.

The collaborative watchdog is able to reduce drastically the detection time of black hole nodes while also reducing the impact of false positives and false negatives.

### 2.3 Detection Based On Learning Automata

In [4], author has proposed a method to detect black hole attack using learning automata. Learning automata is a machine which operates in a random environment. It tries to learn adopting itself with the environment, using feedback. Each automaton has a finite set of actions and each action has a certain probability that is updated according to the feedbacks received from environment. Feedbacks are in the terms of reward and punishment. If the automaton performs an action correctly it gets reward, otherwise it will be punished.

According to the received feedbacks from environment, each automaton updates its action probabilities which finally impacts on choosing the future action. The main goal is that automata learn to select the best action out of their finite action list. Therefore, the best action is the one that maximizes probability of getting reward from the environment.

Every node in the network has a list of its immediate neighbors. Each node keeps a value of trust which is assigned to each of its neighbors and implies the reliability degree. The initial value of trust for each neighbors are 1. It is assumed that each node in the network trust all its immediate neighbors. Hence, it is supposed that all nodes have normal behavior in the network. Nodes update the value of trust associated to their neighbors by receiving feedback from the network. For each neighbor's of a node, there is a learning automaton that can calculate the degree of confidence in the neighbor. By considering the degree of confidence in any of the neighbors, the act of sending or not sending the node is selected by the automata. In fact, the probability of selecting each of the automata is arranged according to their degree of confidence .In other words; the probability of selecting action send is proportionate with degree of confidence. Finally, regarding feedback environment, the degree of confidence in any of the neighboring nodes are updated, this process are going to identification adversary nodes. After calculating the confidence of each node, the confidence of path can be considered as minimum degree of confidence in nodes.

### 2.4 Detection Using Fuzzy Logic

The author [5] has proposed a novel method based on fuzzy logic to detect black hole attack. The system isolates the black hole node from the network. The proposed solution is used by every node in the network. So, every node in the network can determine the behavior of its neighbors, if neighbor is malicious, an alarm packet is broadcasted in the network with the IP address of malicious node and that node thereafter is not allowed to participate in packet forwarding operation. The fuzzy model is integrated with AODV routing protocol. It consists of following four components namely Fuzzy Parameter Extraction, Fuzzy Computation, Fuzzy Verification Module and Alarm Packet Generation Module. During fuzzy parameter extraction, the system extracts the parameters required for analysis from network traffic. These parameters are passed to fuzzy computation module, which applies various fuzzy rules and membership functions to calculate fidelity level of the node. This fidelity level is compared with threshold value in fuzzy verification module to check the behavior of node and if, fidelity level is less than threshold level, an alarm packet with the IP address of detected malicious node is broadcasted in the network. The proposed system not only detects the black hole attack in early stage of communication, but isolates it from the network. Thus improving the performance to great level.

### 2.5 Detection Using Anamoly Detection

The proposed techniques in [6] uses host-based IDS scheme. It assumes every activities of a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. To do so an anomaly detection system needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data is collected and is given to the anomaly detection system, the anomaly detection system is able to compare every activity of a host with the audit data on a fly. If any activity of a host resembles the activities listed in the audit data, the anomaly detection system isolates the particular node by forbidding further interaction. It do not trust on peer nodes.

### 2.6 Detection Of Co-operative Black Hole Attack

The author [7] maintains an Extended Data Routing Information (EDRI) Table at each node in addition to the Routing Table of the AODV protocol. The EDRI table accommodates the gray behavior of nodes as well. Although, it gives subsequent chances to the nodes identified as black holes, it also keeps a record of the previous malicious instances of that node so that a better understanding of the node can be made and the node is given its next chance accordingly. A counter keeps track of how many times a node has been caught and the value of this counter is proportional to the time which has to pass before that node is given another chance. A node which is frequently being caught acting malicious is eventually not given a chance again. Refresh packet, BHID Packet, Further request and further reply packets are also used in addition to the existing RREQ and RREP.

### 2.7 MR-AODV To Mitigate Black Hole Attack

The author has proposed modification of the R-AODV called MR-AODV in [8]. When a malicious node is detected by an intermediate node after receiving RREP, R-AODV marks the RREP as DO_NOT_CONSIDER and marks the node sending RREP as MALICIOUS_NODE in the routing table; the RREP is then forwarded on the reverse path to the source which updates routing tables of all the nodes on the reverse path with malicious node entry; a route towards destination is chosen by selecting unmarked RREPs.

On the other hand, in MR-AODV, when a node detects a malicious node, it updates the routing table with malicious node entry and discards the RREP. It is neither forwarded on the reverse path nor requires a DO_NOT_CONSIDER flag; thus, all RREPs reaching to the source node will be sent by genuine nodes only; the RREP indicating shortest fresher path will be chosen for data transmission by the source node. Thus, MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior.

Both R-AODV and MR-AODV are equally capable of isolating multiple malicious nodes and giving equal rise in PDR, but MR-AODV has an edge over R-AODV as it discards RREP sent by malicious nodes instead of forwarding it on the reverse path.

### 2.8 Detection Using Promiscuous Mode

The author[9] proposed a method which uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety. Promiscuous mode means that if a node A is within the range of node B, it can overhear communication to and from B even if those communication do not directly involve A. If a malicious node is found, an alarm message is flood to the network about the malicious node to isolate it. Simulation results show that we are able to secure AODV protocol from black hole attack and achieve increased throughput while keeping the routing overhead minimal.

## III. Conclusion

In this paper we have presented various existing methods related to black hole attack detection in mobile ad hoc networks. We will develop a more complex black hole attack scenario. Our goal is to construct a detection algorithm with high detection ratio and low overhead.

## References

[1] Y. Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks,” Sixth Annual International Conference on Mobile Computing and Networking (MobiCom’2000), Boston, August 6-11, 2000.

[2] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, “An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network” 24th IEEE International Conference on Advanced Information Networking and Applications 2010

[3] Manuel D. Serrat-Olmos, Enrique Hernández-Orallo, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni, “Accurate Detection of Black Holes in MANETs using Collaborative Bayesian Watchdogs” IEEE International Conference 2012

[4] Mohammad Taqi Soleimani and Abdorasoul Ghasemi, “Detecting Black Hole Attack in Wireless Ad Hoc Networks Based On Learning Automata”

[5] Kulbhushan, Jagpreet Singh, “Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET”IJCA Special Isson Network Security and Cryp to graphy NSC 2011.

[6] Yibeltal Fantahun Alem and Zhao Cheng Xuan, “Preventing Black hole Attack in Mobile Ad-hoc Networks using Anomaly Detection” IEEE International Conference-2010

[7] Gundeep Singh Bindra, Ashish Kapoor , Ashish Narang , Arjun Agrawal, “Detection and Removal of Co-operative Black hole and Gray hole Attacks in MANETs” International Conference on System Engineering and Technology September 11-12, 2012, Bandung, Indonesia

[8] Rutvij H. Jhaveri, “MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs” Third International Conference on Advanced Computing & Communication Technologies 2013

[9] Pramod Kumar Singh,Govind Sharma:” An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET” IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications 2012

[10] Prof. Dhaval Thakar ,Prof. Nainesh Prajapati : “A Modified AODV –Algorithm For Prevention Of Black Hole Attack In Mobile Adhoc Network” International Journal of Conceptions on Electrical and Electronics Engineering,vol.1, Issue 1, Oct 2013

[11] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard:” Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” International conference on Wireless Networks,Las Vegas,Nevada,United States,2003

[12] Latha Tamliselven, Dr. V Sankaranarayanan : " Prevention of Blackhole Attack in MANET" IEEE The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications 2007

[13] Nisha P John , Ashly Thomas : "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review" International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012

[14] Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2, and Yoshiaki Nemoto: " Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security ,Vol 5, Nov. 2007