International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

Black Hole Attack Prevention Techniques In An Ad-Hoc Network

Bessy Bijo Abraham
Assistant Professor, Department of IT, Malla Reddy Engineering College For Women, Telangana, India
bessybijo@gmail.com

ABSTRACT

An ad-hoc network is a group of wireless and mobile nodes that function without any open infrastructure and has the capability to form a temporary network dynamically. Ad-hoc On-demand Distance Vector (AODV) is one of the commonly used routing protocols in an ad-hoc typed network. This protocol experiences a particular type of attack which is called the ‘Black Hole attack’. It comprisesa malicious node advertising itself as it is having the shortest route to the destination which is the node that it wants to attack. This allows the malicious node to deprive the traffic from the source node and to prevent this attack from occurring, it is very important to detect the abnormal actions occurring during the attack. This paper makes a survey of the various mechanisms where the nodes responsible for causing the black hole attack can be removed from the network there by allowing a secure transmission of information across the network.

General Terms

Route Request, Route Replies, Intrusion Detection Systems, Confirmation Request, Anomaly Detection

Keywords

MANET, AODV, Black Hole Attack, malicious node, Security

1. INTRODUCTION

Mobile ad-hoc network (MANET) is a collection of mobile hosts that requires no intervention of existing infrastructure or centralized access point such as a base station. Various applications of MANETs include emergency operations like disaster recovery, military applications, etc due to their easy deployment. Due to the inherent characteristics like dynamic topology and lack of a centralized management security, MANETs are vulnerable to several kinds of attacks. Black Hole attack is one among them. In this type of attack, a malicious node sends an advertisement about a shortest path, pretending to be the destination node, to the source node. In an ad-hoc network running the AODV protocol, a source node that receives multiple Route Replies(RREP) compares the destination sequence numbers in the RREP packets. The one with the greatest destination sequence number will be considered the latest routing information and will be selected as the valid route. In case, the sequence numbers are equal, the route with the smallest hop count will be selected. If an attacker steals the identity to be the destination node and sends RREP packets with a destination sequence number that is higher than that of the original destination node to the source node, then the attacker would be able to receive the traffic, which makes the source and destination unable to communicate with each other. This is how the black hole attack affects the ad-hoc network.

The main objective is to survey all available solutions to avoid black hole attacks in mobile ad-hoc networks and to provide secure transmission of data across the network.

2. AODV

The AODV Routing protocol uses an on-demand source initiated approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It uses destination sequence numbers to identify the most recent and appropriate path. The most important difference between AODV and Dynamic Source Routing (DSR) is that DSR uses source routing technique in which a data packet holds information about the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission in their routing tables. Every mobile node in the ad-hoc network has a routing table that holds information about the next hop node for a route to the destination node. When a source node wants to route a packet to a destination node, it uses the route specified in its routing table, if a fresh enough route to the destination node is available. Otherwise, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further forwarded till it reaches an intermediate node that has a new route to the destination node specified in the RREQ packet, or directly to the destination node itself. A single RouteRequest message can be used to obtainmultiple routes to different destinations. Each intermediate node receiving the RREQ message makes an entry for the node which forwarded the RREQ message and the source node in its routing table. The destination node or the intermediate node that has a fresh route to the destination node, unicasts the Route Response (RREP) message to the neighbor node from which it received the RREQ. An intermediate node makes an entry for the neighbor node from which it received the RREQ message in its routing table, and then forwards the RREP message in the reverse direction. On receiving the RREP message, the source node updates its routing table with an entry for the destination node as well as the node from which it received the Route reply message. The source node starts forwarding the data packets to the destination through the neighbor node that first replied with an RREP message.

The main difference between AODV and other on-demand routing protocols is that AODV uses a destination sequence number (DestSeqNum) to determine an up-to-date route to the destination. A node updates its path information in the routing table only if the DestSeqNum of the received packet is greater than or equal to the DestSeqNum of the last packet stored at the node with a smaller hop count.

A RouteRequest message carries the source identifier (SID), the destination identifier (DID), the source sequence number (SrcSeqNum), the destination sequence number (DestSeqNum), the broadcast identifier (BID), and a time to live (TTL) field. DestSeqNum indicates the freshness of the route that the source had accepted. When an intermediate node receives a RouteRequest message, it either forwards the RREQ message or prepares a RREP message if it has a valid route to the destination. A route validity can be determined at the intermediate node by comparing the sequence number at the intermediate node with the destination sequence number in the RREQ packet. If an RREQ message is received multiple times, which is indicated by the BID-SID pair, the duplicated copies are discarded. Only the intermediate nodes having valid routes to the destination and the destination node itself are allowed to send RREP packets to the source. Every intermediate node, while forwarding a RREQ, enters the address of the previous node and its BID in its routing table. A timer is used to delete this entry in case a RREP message is not received before it expires. This helps in storing an available path at the intermediate node, as AODV protocol does not employ source nodes to route data packets. When a node receives an RREP packet, information about the node from which the packet was received is also stored in the routing table in order to forward the data packet to it as the next hop towards the destination. The AODV protocol is vulnerable to the well-known black hole attack.

2.1 Black Hole Attack

A Black Hole attack otherwise called the packet drop attack is a type of DoS attack where a malicious node attracts all packets by falsely claiming that a fresh route to the destination and then absorbs them without forwarding the packets to the destination, thereby attaining all benefits of capturing all the message packets on behalf of the destination node. A black hole attack is referred to as a node dropping all packets and sending forged routing packets, to route packets from the source to itself. In this type of attack, a malicious node spuriously announces a short and a fresh route to the sink node (i.e., the destination) to attract additional traffic to the malicious node and then drops them. A source node that wants to send data packets to the destination node initiates the routing discovery process in an AODV protocol. Imagine a malicious node M. When a node P broadcasts an RREQ packet, all the nodes including Q, R and the malicious node M receive it. Node M, being a malicious node, does not check up with its routing table for the requested route to node T which is the destination. Hence, it immediately sends back an RREP packet, claiming that it has a route to the destination. Node P receives the RREP from M even before Q and R could send one. Node P misunderstands that the route through M is the shortest route and sends any packet to the destination through it. When the node P sends data to M, it attracts and captures all the data without forwarding them to the destination and thus acts like a 'Black hole'. In this way a malicious node M can completely modify the packet and generate false information which causes the network traffic to be diverted or dropped.

The black hole attack has two characteristics. Firstly, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to the desired destination node, even though the route is an invalid and a spurious one, with the intention of capturing packets. Secondly, the attacker uses the captured packets for its own benefit without forwarding it. However, the attacker faces the possibility of a danger that the neighbor nodes will monitor and expose the ongoing attacks to all concerned nodes. There is a more delicate form of these attacks where an attacker can selectively forward packets, i.e., an attacker can suppress or modify packets originating from some nodes, while unaffecting the data from the other nodes, which confines the doubt of its attack.

The following sections deal with some of the various existing techniques that help in the prevention of black hole attacks in an ad hoc network.

3. EXISTING APPROACHES

3.1 Intrusion Detection Systems

Intrusion Detection Systems (IDS) [2] are one of the basic techniques in use to prevent any attacks against security threats. Intrusion detection can be categorized as network based IDS and host based IDS. Network based IDS (NIDS) can be set up on data concentration points of a network such as switches and routers. It monitors traffic at chosen points on a network (like the switches, routers, etc…) or the interconnected set of networks. The NIDS scans the traffic packet by packet, in order to try to identify the intrusion patterns. The NIDS also scrutinizes network-level, transport-level or application-level protocol action in contrast to a host-based IDS; a NIDS inspects packet traffic that is heading toward potentially susceptible computer systems on a network.

3.2 Route Confirmation Approach (RCA)

In [3], the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) technique to avoid the black hole attack in the network. In this approach, the intermediate node not only sends RREP messages to the source node but also sends CREQ messages to its next-hop node toward the destination node.This is to enquire about the route to the destination node. After receiving a CREQ message, the next-hop node searches its cache for a route to the destination. If it has the route, it sends the CREP to the source. On receiving the CREP message, the source node confirms the validity of the route by comparing the route in RREP message and the one in CREP. If both are the same, the source node confirms that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in agreement with each other, that is, when the next-hop node is an attacker working together with the malicious node sending CREPs that support the incorrect path.

3.3 Multiple Route Replies(MRR)

In [4], the authors have discussed the AODV protocol that suffers from the Black hole attack in MANETs and has proposed a realistic solution for the black hole attacks, which can be implemented on the AODV protocol. This mechanism expects a source node to wait until an 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 confirms that the route is safe and can be used. The main drawback of this solution is that it introduces time delay, because it has to wait until multiple RREPs arrive.

3.4 Statistical Anomaly Detection(SAD)

In [5], the authors investigate the effects of black hole attack in MANETs and shows that a malicious node must increase the destination sequence number adequately to persuade the source node that the route provided is amply enough. Based on this investigation, the authors suggest a statistical based anomaly detection approach to detect the black hole attack in the network, based on the difference between the destination sequence numbers of the multiple received RREPs. The advantage of this approach is that it can detect the black hole at low cost without launching extra routing traffic, and it does not require any modification of the existing protocol. However, false positives, where the malicious node raises a false alarm indicating that a given condition has been fulfilled when it actually has not been, are the main drawback of this approach due to the nature of anomaly detection.

3.5 Further Request Approach(FRA)

In [6], according to the authors' solution, when any intermediate node replies for an RREQ message, information regarding the next hop to the destination should be included in the RREP packet. The source node then sends a further request (FREQ) message to the next hop of the node that replied to the RREQ message and asks about the node that replied as well as the route to the destination. By using this method the credibility of the responding node can be identified, only if the next hop is trusted. However, this solution cannot prevent cooperative black hole attacks on MANETs. For instance, if the next hop also obliges with the replied node, the reply for the FREQ will be simply answered "yes" for both the questions. Then the source will believe the next hop and transmit data through the replied node which is a black hole node.

3.6 Prior - Receive Reply Method

The paper [1] proposes an algorithm that identifies the malicious node which is responsible for the black hole attack. In this method we can check whether there is any large difference between the sequence number of the source nodes and intermediate nodes who has sent back RREP messages or not. Naturally, the first route reply in the routing table will be from the malicious node with high destination sequence number. The first destination sequence number can be compared with the source sequence number. If there exists much difference between source and destination sequence number, then the destination node is a malicious node, allowing the elimination of that entry from the routing table immediately. This is done as 5 different processes which include the initialization process, storing process, identification and removal of the malicious node, node selection process and finally the default process.

Table 1.Comparison of the various techniques

Technique	Objective	Scalability	Efficiency
IDS	Monitors data traffic at data concentration points	Restricted to data concentration points	Mainly for potentially susceptible systems
RCA	Prevents fake routing information from entering the network	Can be applied only to avoid one malicious node	Efficient in terms of one black hole node
FRA	To identify the credibility of the responding node	Scalable to any network where each node has trusted neighbors	Not suitable for cooperative attacks
MRR	Detecting and removing black hole nodes in the MANET at the initial stage itself without any delay.	Scalable as it covers the security of more than two nodes	Inefficient in terms of time delay
SAD	High accuracy detection	Adaptive even in a changing network environment	Efficient except for false positives

4. CONCLUSIONS

A survey on the various techniques that are employed in the prevention of black hole attacks in an ad hoc network with the AODV routing protocol as the base protocol has been done. Each technique has advantages and disadvantages of their own, but all of them focus on how to avoid malicious nodes from intercepting the network and throw confusions in an otherwise trustworthy data transmission. Security can be enhanced in an ad hoc network by introducing cryptographic concepts in to the techniques, at the same time by reducing the processing overhead of encryption and decryption.

5. REFERENCES

[1] Dr. S. Tamilarasan, Securing AODV Routing Protocol from Black Hole Attack, International Journal of Computer Science and Tele communications, Volume 3, Issue 7, July 2012.

[2] Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by YibeltalFantahumAlem& Zhao HhengXaun from Tainjin 300222, China 2010, IEEE.Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[3] BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE Wireless Communications • October 2007.PP: 85-90.Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[4] Modified AODV Protocol against Black hole Attacks in MANET by K. Lakshmi1, S.ManjuPriya, A.Jeevarathinam, K.Rama, K.Thilagam, Lecturer, Dept. of Computer Applications, Karpagam University, Coimbatore, International Journal of Engineering and Technology. Vol.2 (6), 2010.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[6] Weerasinghe.H. "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", IEEE Student Member.

[7] Seung Yi, Prasad Naldurg, Robin Kravets, "Security-Aware Ad-Hoc Routing for Wireless Networks".