A Review On Detection And Mitigation Of Black And Gray Hole Attacks In Manet

Bhawana Dewangan¹ Minu Choudhary²

¹ Department Of Computer Science Engineering, Rungta College Of Engineering And Technology Bhilai, Chhattisgarh 490024, India
² Department Of Computer Science Engineering, Rungta College Of Engineering And Technology Bhilai, Chhattisgarh 490024, India

Abstract
In wireless ad hoc networks, the absence of any control on packets forwarding, make these networks vulnerable by various deny of service attacks (DoS). A node, in wireless ad hoc network, counts always on intermediate nodes to send these packets to a given destination node. An intermediate node, which takes part in packets forwarding, may behave maliciously and drop packets which goes through it, instead of forwarding them to the following node. Such behavior is called black hole attack. In this paper, after having specified the black hole attack, a secure mechanism, which consists in checking the good forwarding of packets by an intermediate node, is required. In this paper a survey is taken from previous works.

Keywords: MANETs, Black Hole Attack, Gray Hole Attack, AODV, NS-2.

1. Introduction
A Mobile Ad Hoc Network (MANET) is a group of mobile nodes that cooperate and forward packets for each other. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, and thus they are ideally suited for scenarios in which pre-deployed infrastructure support is not available. MANETs have some special characteristic features such as unreliable wireless links used for communication between hosts, constantly changing network topologies, limited bandwidth, battery power, low computation power etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are either absent or less severe in wired networks. MANETs are vulnerable to various types of attacks including passive eavesdropping, active interfering, impersonation, and denial-of-service. Intrusion prevention measures such as strong authentication and redundant transmission should be complemented by detection techniques to monitor security status of these networks and identify malicious behavior of any participating node(s). One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. In this paper, we discuss one such attack known as Gray Hole Attack on the widely used AODV (Ad hoc On-demand Distance Vector) routing protocol in MANETs. A mechanism is presented to detect and defend the network against such an attack which may be launched cooperatively by a set of malicious nodes.

2. Related Work
Researcher has proposed various methods to detect and mitigate the effect of Black Hole and Gray Hole attacks in Manets. Network simulator 2 is used to evaluate the performance of above method. In this method the route discovery processes of R-AODV and MR-AODV is compared and an algorithm is designed further this design is analyzed and simulated. R-AODV improves route discovery process of AODV by bringing in security into AODV protocol and prevents Black hole and Gray hole nodes from taking part in data transmission phase.

2.1 R.H. Jhaveri et. al. proposed a modified version of R-AODV to detect and isolate multiple black hole and gray hole nodes during route discovery process. Network simulator 2 is used to evaluate the performance of above method. In this method the route discovery processes of R-
AODV and MR-AODV is compared and an algorithm is designed further this design is analyzed and simulated. R-AODV improves route discovery process of AODV by bringing in security into AODV protocol and prevents Black hole and Gray hole nodes from taking part in data transmission phase. It uses number of sent out RREQs, number of received RREPs and routing table sequence number to dynamically calculate a PEAK value after every received RREPs; the PEAK value is calculated by adding these three parameters to the previous PEAK value. N.Mistry et. al has done some modifications to the AODV routing protocol and justified the solution by using Network Simulator 2.33 to ensure the security against the black hole attacks. In this process the default intermediate node and the destination node is remains unaltered. The modifications are done in the source node itself using an additional function called Pre Receive Reply (Packet P). All these process are illustrated by pseudo code followed by analysis of the process and simulation. AODV is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on-demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated. AODV uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase.

A. Mishra et. al. had included an advanced DRI table with additional check bit. The simulation on Network Simulator is carried out and the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection and elimination of the attack and maximizing network performance by reducing the packet dropping ratio in network.

H. Weerasinghe et. al. had considered some solutions regarding cooperative black hole attack in mobile Ad-Hoc networks and done experiments on it followed by evaluation techniques using packet loss percentage, average end-to-end delay and route request overhead. The experiments show that the AODV greatly suffers from cooperative black holes in terms of throughout and packet losses and also the proposed solution presents good performance in terms of better throughout rate and minimum packet loss percentage over other solutions, and also this solution proposed can accurately prevent the cooperative black hole attacks. Each node maintains a data routing information (DRI) table. This table keeps track of whether or not the node did data transfers with its neighbors.

P. Agrawal et. al. proposed a complete protocol to detect a chain of cooperating malicious nodes in an Ad-Hoc network that disrupts transmission of data by feeding wrong routing information technique is based on sending data in equal but small sized blocks instead of sending whole of data in one continuous stream. The flow of traffic is monitored independently at the neighborhoods of both source and destination. The results of monitoring are gathered by a backbone network of trusted nodes. With assumption that a neighborhood of any node in the ad hoc network has more trusted nodes than malicious nodes, our protocol can not only detect but also remove a mediate node and the destination node is remains unaltered. The modifications are done in the source node itself using an additional function called Pre Receive Reply (Packet P). All these process are illustrated by pseudo code followed by analysis of the process and simulation. AODV is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on-demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated. AODV uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in. In general, the nodes participating in the communication.

3. Adhoc On Demand Distance Vector Routing

- The Ad Hoc On-demand Distance Vector Routing (AODV) protocol is a reactive unicast routing protocol for mobile adhoc networks. It operates in two phases namely route discovery and route maintenance AODV uses route discovery by broadcasting RREQ to all its neighboring nodes, Sequence numbers help in avoiding the possibility of forwarding the same packet more than once. When a source node requires a route to a destination, it broadcasts a route request (RREQ) packet across the network. These broadcasted RREQ packet is received by each node present in the network during its travel each node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node simply rejects the newly received RREQs If the RREQ’s sequence number for the destination is greater than that recorded by the intermediate
node, then intermediate node must not use its recorded route to respond to the RREQ. Route maintenance module: AODV uses Hello messages to maintain the connectivity between nodes. Each node periodically sends a Hello message to these neighbors and awaits Hello messages on behalf of these neighbors. If Hello messages are exchanged in the two directions, a symmetrical link between nodes is always maintained if no link interrupt occurs. The broken link can be repaired locally by the node upstream, else a route error message is sent to the source $S$. This last can launch again, if necessary, the route discovery procedure. It should be noted that the link interrupt is the consequence of the mobility or the breakdown of nodes.

A node uses the service discovery protocol so that it discover the service of its nearby node.

v) In the manet any node can node can participate in forwarding the data packets.

5. Conclusions

A Black Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem.

Acknowledgments

I sincerely thank all those people who helped me in completing this review paper.

References

[3] Piyush Agrawal (IIT KANPUR), R.K Ghosh (IIT KANPUR) and Sajal K. Das- “Cooperative Black And Gray Hole Attack In MANET.”

FIG 1 Shows RREQ and RREP under Black Hole Attac

4. Characteristics

i) Manet require limited security.

ii) Manet can be set up anywhere.

iii) There is no need of centralised controller.

iv) In the Manet the nodes communicate by sending request and response message.