International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 8; Issue: 12; December -2019

Malicious Node Detection by Identification of Gray and Black Hole Attacks using Control Packets in MANETs

Divyashree Nayak , Dharamvir
[1,2] Assistant Professor
[1,2] Department of Master Of Computer Applications
[1,2]The Oxford College of engineering Bangalore

Abstract: *A Mobile Ad hoc Network (MANET) is a group of mobile nodes which cooperate in forwarding packets in a multi-hop fashion without any centralized administration. One of its key challenges is finding the malicious node in MANETs. In this paper we have proposed a scheme in which we are sending a control sequence to the neighbour nodes and we are expecting the nodes response. Based on the node response we can identify the malicious node. Attack prevention can be done by providing secure path to the neighbour nodes.The MANETs and UAV networks would soon replace existing Wireless technology due to its ease to deploy and bare minimum infrastructure requirement and dynamic topology.*

Keywords: *MANETs, control packets.*

1. Introduction

Mobile Ad-hoc Networks (MANETs) allow mobilehosts to initiate communications with each other over a network without an established infrastructure or a central network authority. Because of this, MANETs have dynamic topologies because nodes can easily join or leave the network at any time. From a security design perspective, MANETs are vulnerable to various types of malicious attacks. Attacks in MANETs generally purpose and they are first is not to forward the packet or change the parameters of routing messages and to exhaust the battery of nodes by make them traversing the wrong packet in wrong direction and they also change the parameters of the packets such as sequence numbers and by using mechanism like authentication or cryptography as a preventive approach and can be used against attackers. Ad-hoc networks are characterized by dynamic topology, self-configuration, self-organization, restricted power, temporary duration and lack of infrastructure. Each node in the MANET uses wireless interface to communicate with the other nodes. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure such as access points or base stations.

Each node in the MANET uses wireless interface to communicate with the other nodes. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure such as access points or base stations. Ad-hoc On-demand Distance Vector (AODV) is a standard protocol for MANETs that has been designed without consideration for security mechanisms. Malicious nodes can fool the network in order to disrupt or destroy the transmission of packets. One of these attacks is referred to as a black hole attack. A black hole node advertises as having a high destination sequence number and the shortest path to a specific node in order to absorb packets and drop them.

This paper proposes a secure route discovery mechanism that is designed to prevent black hole attacks on AODV-based Mobile Ad-hoc Networks (MANETs). In the proposed mechanism, the source node acts as an important node for judging multiple Route Reply (RREP) packets from intermediate nodes or destination node by using our mechanism to verify the destination sequence number. Moreover, the destination node is also required to verify the sequence number in the Route Request (RREQ) message before generating an RREP message.

2. Related Works

Research related to MANETs covers many topics such as routing, security and defence strategies against threats like black hole attacks. This section gives brief discussion of some of the research that is closely related to the topic of this paper.

Marti et.al presented a method that uses Watchdog and Pathrater to detect black hole attacks. The Watchdog enables neighbour nodes to overhear and detect malicious nodes. Watchdog

makes it possible to detect malicious nodes by finding nodes that are deliberately discarding packets. Pathraterassigns a default value to each node and then observes the transmitting behaviour of each node.

The each node value changes while transmitting the data based on its behaviour. After a period of time, if the value for a node is below a certain threshold, the node will be added to the list of black hole nodes. These methods have the same defection to find malicious node, when the neighbour reply wrong observing message. In other words, this method cannot handle collaborative attacks. If the neighbour nodes collude with each other, they may be able to avoid detection.

Lu et al. proposed the SAODV black hole detection scheme for MANETs that is designed to address some of thesecurity weaknesses of AODV and withstand black hole attacks. Deswal and Singh created an enhanced version ofthe SAODV protocol that includes password security for each of the routing nodes and routing tables that are updated based on timeliness.

Ramaswamy proposed a method for identifying multiple black hole nodes. They were the first to propose a solution for cooperative black hole attacks. They modified theAODV protocol slightly by introducing a Data RoutingInformation (DRI) table and a cross checking mechanism. Each entry of the node is maintained by the table. This method uses the reliable nodes to transfer the packets.

Hongmei Deng proposed a methodology that asks every intermediate node to return next hop information along with the RREPs once a route to a destination has been determined. The source node does not transmit data packets to an intermediate node immediately. Instead, the source node waits for the RREPs and the next hop information and then sends FurtherRequest to the next hop in order to determine if there is a route between it and the intermediate node and also to determine if there is a route to the destination.

The source node receives FurtherReply from the next hop. If the answers are yes for both questions, then the route is built. If the answer to either of the questions is no, then the source node will send an alarm packet to alert other nodes on the network. This methodology has an obvious drawback though. It only can address a single black hole. It cannot prevent cooperative black hole attacks if the next hop colludes with the former. In a situation like this, the source gets the wrong message.

Most of the research papers above discussed methods for avoiding black hole attacks against MANETs that are based on the AODV protocol and other protocols. However, our proposed mechanism is a new solution that provides high performance and prevents black hole attacks on the AODV protocol.

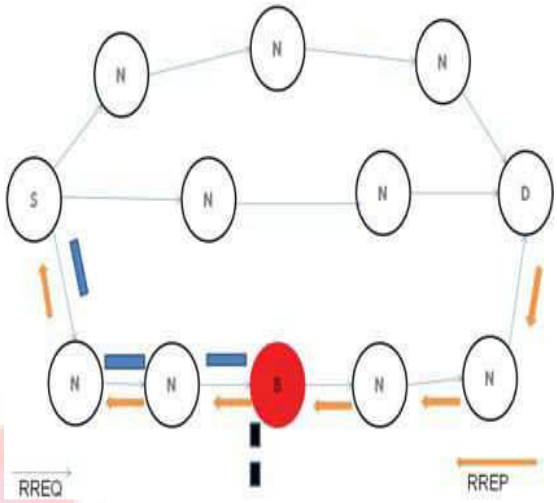

Figure1: Security Attacks in MANETs

3. Problem Statement

The typicalnetwork scenarios, data is collected by sensor nodes throughout some area, and needs to be made available at some central node(s), where it is processed, analysed and used by applications. In many cases, data generated by different sensors can be jointly processed while being forwarded towards the BS or sink node, e.g., by fusing together sensor readings related to the same event or physical quantity, or by locally processing raw data before it transmitted.

In this system, the malicious node advertise itself to have the shortest route for the communication and transferring of packets, and thus drops the packets without forwarding them to the neighbouring nodes. As soon as node receives the RREQ message from source node, it immediately sends back a fake packet to it. When source node starts sending packets to the destination by using this route, the malicious node drops all packets instead of forwarding it.

4. Proposed Approach

In the existing AODV Routing protocol we have been introducing two packets which are Response sequence (Rseq) packet and Code Sequence Packet (Cseq). These packets are transmitted in the AODV-MAC layer when a node wants to access the channel. Each intermediate

node sends the Cseq to all its neighbours then neighbours intern send their Rseq to the intermediate node. If the Cseq and Rseq matches from the neighbour then the Intermediate node allow the connection to the network layer, Otherwise, it discard the node and send the information to all other nodes that particular node as malicious one.

It checks the fix value of sequence packet in the Code sequence table.If seq packet is match with respective Cseq packet then Rseq packet is accepted, otherwise it discarded. Figure 2 shows the route discovery process inAODV in the presence of a malicious node D. Source node A broadcasts Code sequence packet (Cseq) within its communication range, B,C,E,F and G receive the Cseq packet and re-broadcasts Cseq to their neighbours until a node.

Each node sends Rseq packet to the source node on the reverse path of Cseq. The malicious node D sends Rseq to the source but source node check it with the Cseq packet then the result comes different. The Proposed method is used to prevent the malicious node and find the secured routes in the MANETs.

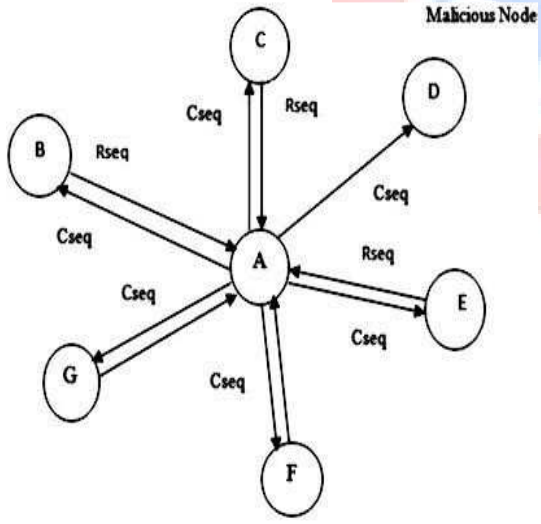

Figure2: route Discovery Process with Proposed Approach.

If there is large difference between the Cseq of source node and Rseq of neighbour or intermediate node, then it concludes as network affected by some malicious node. In computer networking, black hole attack is type of denial-of service attack in which a router that is supposed to relay packets instead discard them and route reply will be from the malicious node with high destination sequence number where gray hole attack is subsequent threat of wormhole attack on network and transport layer, where malicious node misguides the source node by using shortest path attraction. Attack detection can be done by introducing control packets called Code sequence and Rseq packets. As the malicious node detected network takes alternative route called secure route and previous route will be ignored.

5. Control Packets Mechanisms:

a) Coordination betweenCseq and Rseq packets.

i. Collecting Response

The incoming responses Rseq packets are collected in a table, called code sequence table. The entries will have fields like, source address, destination address, hop count, next hop, lifetime, destination sequence number, source and destination' s header address. The responses will be collected till a timer expiry event.

ii. Choosing a Response

A valid route is selected from among the received response based on the code sequence table. This table will maintained and hold the values of the each participating nodes in the network. The basic idea is to select the node which having shortest path.

iii. Updating the Shortest Path

Every destination node sends back an acknowledgement to source node,upon reception of the data packets. The receipt of the acknowledgement enables the source node to update the routing tale as well as code sequence table.

iv. Eliminating the Black and Gray holes

When intermediate nodes drops to 0, it implies it has not forwarded the data or it misguides the particular data packet, and that node acts as a malicious in the network. Based on particular packets dropping and forwarding, attacks can be detected whether it is a black hole or gray hole. Prevention can be provided by ignoring the malicious node and enables the secure path which is shortest path and it is depends on the code sequence table.

6. Snapshots

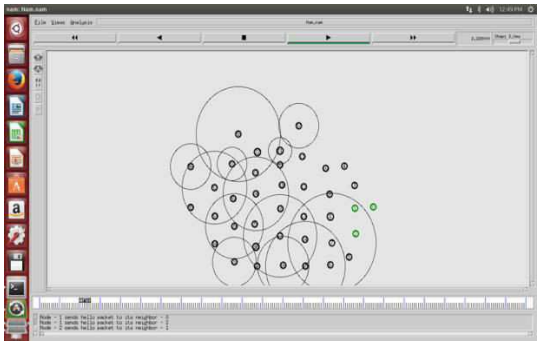

Figure 3: Snapshot for Node Deployment

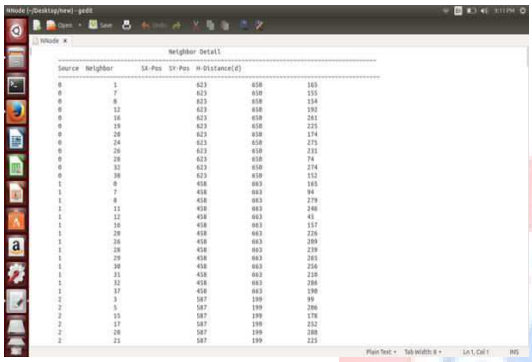

Figure 4: Routing table formation

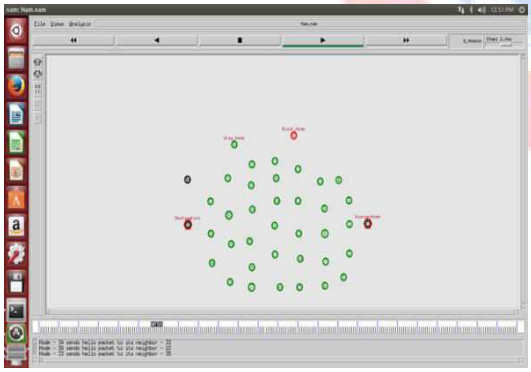

Figure 5: Source and destination node selection

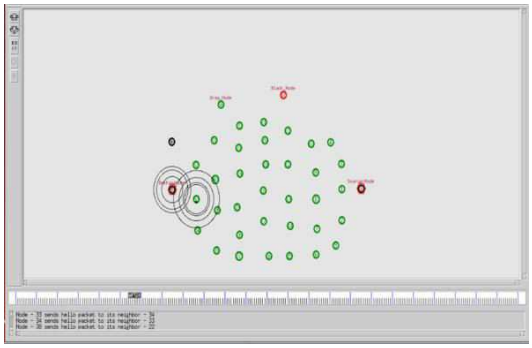

Figure 6: Broadcasting hello packets

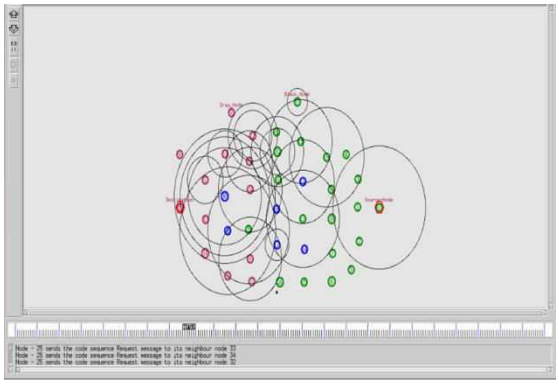

Figure 7: Forwarding code sequence message

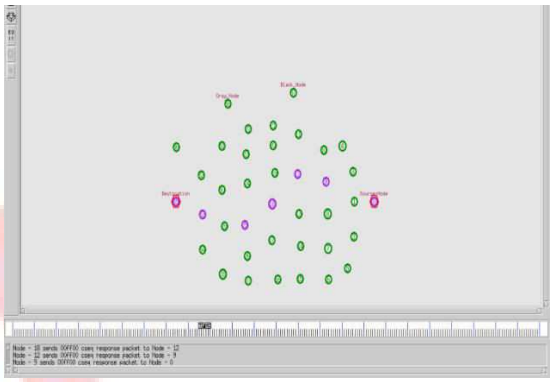

Figure 8: Receiving response packet

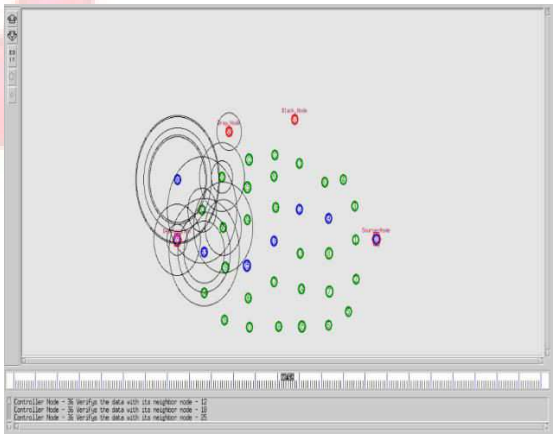

Figure 9: Sending Encrypted Message

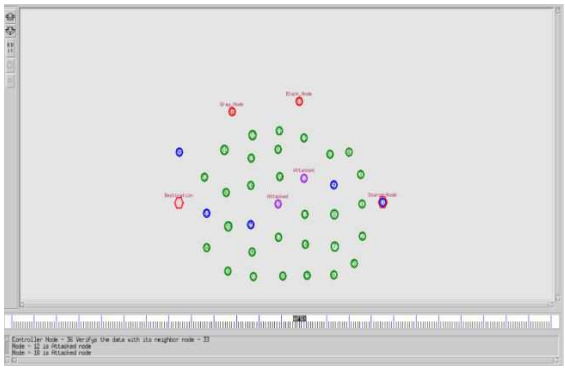

Figure 10: Data verification by the neighbour nodes

7. Conclusion

In this paper the routing security issues of MANETs, are discussed. Two types of attack are considered here, those are black and gray hole which are easily deployed against the MANETs. Through default AODV protocol, it is easier to breach the security of a MANET. AODV is susceptible to many attacks including Grayhole and Black hole attacks. In this work we investigated some of the existing solutions for these attacks and proposed a novel approach to counter these attacks that efficiently finds short and secure route to the destination. The theoretical analysis shows that our approach would greatly increase PDR with negligible difference in routing overhead. The algorithm is equally applicable to other reactive protocols.

7. References

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, Vol.40, no.10, october2009.

[2] Ramaswamy V, "Gray and Black Hole Attack Detection using Control Packets", seminar on Net Work Security, HUT TML 2010.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks". In mobile Computing and Networking(MOBICOM), pages 255-265, 2011

[4] PiyushAgrawal, R. K. Ghosh and Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks, 2nd InternationalConference on Ubiquitous Information Management and Communication, pp. 310–314, (2008).