International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 4, April 2015

Advance Security in Mobile Ad Hoc Network Using Direct and Indirect Observation

[1]C.Balaraman,[2]Mr.M.Balamurugan
[1]P.G student, Sri SaiRam Engineering College, Chennai.
[2]Assistant Professor, Sri SaiRam Engineering College, Chennai.
[1]elubala@gmail.com,[2]balamurugan.CSE@sairam.edu.in

Abstract : **The dynamic behavior of MANETs may lead to many security vulnerabilities. To avoid the hackers, a globally trust management that enhances security in MANETs is used. The trust management scheme has two methods, trust from direct observation method and trust from indirect observation method. The direct observation method source can monitor one hop neighbor node. On the other hand, with indirect observation, source will send recommendation message to all the neighbor nodes, and each neighbor will send the trust value of its neighbors to source node. Source will validate the message and select the best route without malicious activities. The two trust modal are combined to produce more accurate trust values and it provide more security. Reputation is added in trust evaluation. Modified AODV protocol is used here for solving black hole attack in MANETs.**

Keywords - **Security, Mobile ad hoc networks(MANETs), Trust management, AODV protocol**

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of independent mobile nodes that can transmit information to each other via radio waves. The nodes with in an radio range can directly transmit an information whereas others need the aid of intermediate nodes to route their packets. These networks are It is a fully distributed network and can work at any place without the help of any infrastructure. These networks is highly exile and robust.

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become

a target for malicious adversaries who intend to attack the network or the applications running on it.

Ad hoc networks are self-organizing also self-configuring multihop wireless networks where, their structure changes dynamically. This is because of their mobility nature. The nodes in the network act as a router not only as a host to route the data in the network. A collection of mobile hosts with wireless network interfaces may form a lacking continuity without the help of any established infrastructure or centralized administration. This type of wireless network is known as an *ad hoc network*.

There are many applications to ad hoc networks. Some well known mobile ad hoc network applications are:

collaborative work-for some business environments, the need for collaborative computing might be more important outside office environments than inside. Crisis-management application-at the time of natural disasters the entire infrastructure is in disarray so the restoring of communications quickly is essential. By using ad hoc networks, an infrastructure could be set up in hours instead of days/weeks required for wire-line communication.

The advantages of MANETs are: To provide the easy way of access the information and services inspite of geographic position. It is a dynamic in nature so it can be establish at any place and time. It works without any pre-existing infrastructure.

II. COMMUNICATION MODAL

Initially we are placing nodes in the network and we choose a source and destination. If the source has no route to the destination, then source A initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node. If a closer neighbor node is available, the RREQ packet is forwarded to that node. If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.

When destinations receive the RREQ, it will generate RREP and it will send the same path. Finally we establish the route for data traffic. An example communication model show in fig.1

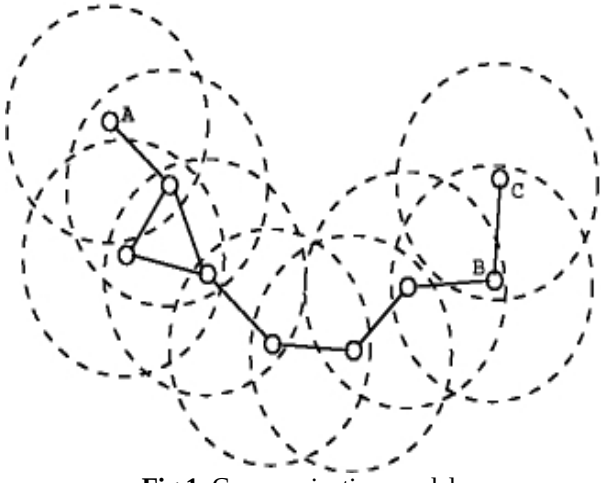


Fig.1. Communication model.

The source node A send route request from all the neighbor nodes. After destination node C reply the acknowledgement message to source node A. finally finding the best route and data will be forward.

III. TRUST MODEL

The definition of trust in MANET is explanation of sociology. Trust value means to identify or observed the particular node of the activity. The trust mechanism has some following properties are: context dependence, function of uncertainty, quantitative value, and asymmetric relationship. There are two types of observation method will be present in the trust model.

A Direct observation

The source can monitor by one hop neighbor node. This trust value is calculated by nodes activities such as node energy level and high sequence number. Hacker node will show always high energy level and high sequence number for data forwarding. Based on these values direct trust will generate.

B Indirect observation

In indirect observation, source will send recommendation message to all the neighbour nodes, and each neighbour will send the trust value of its neighbours to source node. Source will validate the message and select the route without malicious activities. Source node analyzes the trust value of the nodes periodically. Source node uses direct and indirect observation method in order to get the trust value of the node. It won't choose a route which route has hacker node. It will select alternate route for data forwarding. It will check hacker details periodically. Finally source node will eliminate the hacker node.

IV. TRUSTED WITH AODV

AODV Routing Protocol uses an on-demand approach for finding routes is established only it is required by a source node for transmitting data packets. The most recent path is identified by using the destination sequence numbers.

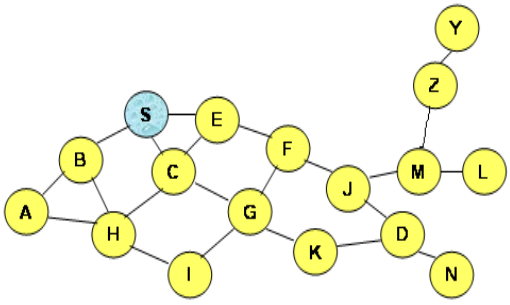
AODV is a reactive routing protocol designed for ad hoc mobile networks. AODV establishes routes using request and reply messages. When any node has packets to send, at first it searches for the routes to the destination. If the node doesn't have any routes to the destination, it broadcasts route request packet (RREQ) over the network. After receiving RREQ packet, the intermediate nodes update their routing table with the address of the node from which it gets first RREQ broadcast messages and hence it sets a reverse path to that node.

The nodes that receive RREQ packets send back RREP packet, if it is a destination node or it has a route to the destination node. After receiving the RREP packets, source node starts to forward the data packets through that path which has minimum hop count. The route will be maintained periodically till the data packets travelled along this path from source to destination. When any node of that path detects the link failure immediately informs the source node by sending route error message so that the sender node stops sending the data packets.

AODV has three main process: Route Discovery, Route Maintenance, and update energy level

A Route discovery in AODV

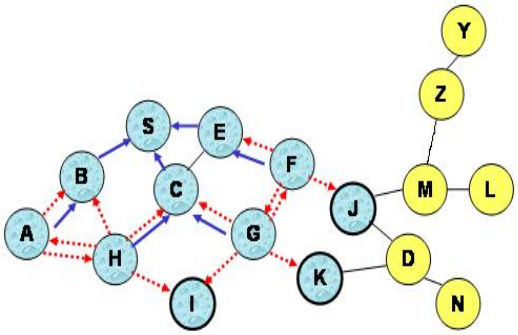
Route Discovery allows any host in the ad hoc network to dynamically discover a route to any other host in the ad hoc network, whether directly reachable within wireless transmission range or reachable through one or more intermediate network hops through other hosts. An example route discovery model show in fig.2



Represents a node that has received RREQ for D from S.

Figure 2: Route Discovery in AODV

There are two types of route discovery will be performed in the AODV protocol using direct and indirect observation. A host initiating a route discovery broadcasts a *route request* packet which may be received by those hosts within wireless transmission range of it. The route request packet identifies the host, referred to as the *target* of the route discovery, for which the route is requested.



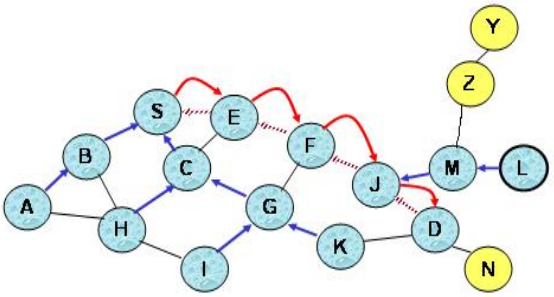
Represents Transmission of RREQ.

Represents links on reverse path.

Figure 3: Propagation of RREQ Message

Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once. Node D does not forward RREQ, because Node D is the intended target of RREQ. The node receive that packet checks their routing table whether destination node is available or not,if not it rebroadcasts the packet otherwise it send route reply packet to the source node.

If the route discovery is successful the initiating host receives a *route reply* packet listing a sequence of path through which it may attain the point. Forward links are Set-Up when RREP travels along the reverse path. Routes are established on demand and destination sequence numbers are used to find the latest route to the destination.



Represents a link broken on the forward path.

Figure 4: Propagation of RREP Message

B Route maintenance

It monitors the operation of the route and informs the sender if there is any routing error. If the status of a link or router changes, the changes are update in entire routers participate in the network. Route maintenance can also be performed using end-to-end acknowledgements rather than the hop-by hop acknowledgements.

Route Maintenance is possible. In hop-by-hop acknowledgements, the particular hop in error is indicated in the route error packet, but with end-to-end acknowledgements, the sender may only assume that the last hop of the route to this destination is in error.

C Update energy level

Nodes will periodically share their energy level continuously. Source will update the energy and compare which route has high residual energy. After comparing residual energy level, source will select different route for data forwarding. It will continue till end of the communication.

D Black hole attacks

A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. There is a risk for the attacker to be identified as a misbehaving node by the neighbor nodes if there is any monitor mechanism for watching nodes behavior. So sometimes attacker does not drop the packets, but change the information in the packet coming from the source keeping the other information of other nodes intact.

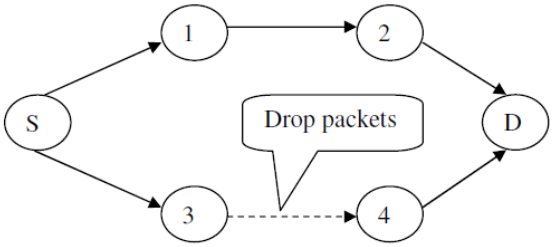


Figure 5: Black hole attack

In black hole attack, attacker first involved itself in routing by rushing attack and then capture all the packets coming from the source to a particular destination and drops all the packets destined for that destination. There is a risk for the attacker to be identified as a misbehaving node by the neighbor nodes if there is any monitor mechanism for watching nodes behavior. So sometimes attacker does not drop the packets, but change the information in the packet coming from the source keeping the other information of other nodes intact.

E Black hole removal process

Actions by Source node on receiving the RREP

Step 1: If the RREP is received only to the Destination & not to the Restricted IP(RIP), the node carries out the normal functioning by transmitting the data through the route.

Step 2: If the RREP is received for the RIP, it initiates the process of black hole detection, by sending a request to enter into promiscuous mode, to the nodes in an alternate path (i.e. neighbors of next hop for RIP).

Step 3: The feedback sent by the alternate paths are analyzed to detect the black hole & this information is propagated throughout the network, leading to the revocation of the Black Holes certificates.

In general, detection mechanisms that have been proposed in to

1) Proactive detection schemes that regularly detect the nearby nodes to check if the node is malicious node or normal node. It detects the malicious node regularly so its resources are wasted. The main advantage is to prevent or detect the attack in its initial stages.

2) Reactive detection schemes are used to detect the malicious node during the significant drop in the packet delivery ratio. The resource wastage is reduced because it can monitor the route during the packet loss.

SYSTEM DESIGN

A Data unit

Data Unit is used to process the data. It is used to Store and retrieve the data.

B Route discovery

It is used to discover the new route to send the data packets. Route Discovery allows any host in the ad hoc network to dynamically discover a route to any other host in the ad hoc network.

C Route maintenance

Route Maintenance is used to maintain and recover in case of failure occur in route. Route Discovery and Route Maintenance are combined to allow nodes to discover and to maintain source routes to arbitrary destinations in the ad hoc network.

D Routing manager

Routing Manager is used to manage all the activities in the network. It is used to transmit and receive the data in the network.

E Behaviour analyzer

It is used to analyse the behaviour of the node.To Check whether the node is good or bad.

F Route cache

To update those network are participated in route.It can store the all node details including the hacker node.

G Architecture of trust model

The source node sent route request from all the neighbor nodes using direct and indirect observation method. The destination node sends route reply based on energy level. Finally select best route path and data will be forward.

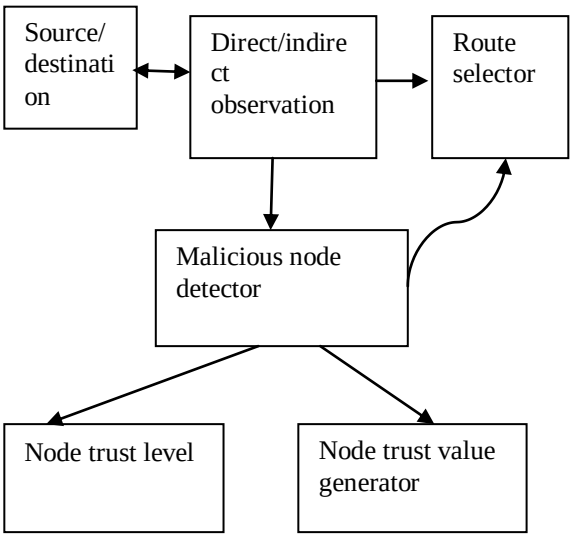


Figure. Architecture of trust mode

CONCLUSION

The security of MANET is improved by trust management scheme. The modified AODV protocol evaluates the trust values of nodes. Trust values are used to identify the modified packets. The solution is simulated the global mobile simulator and is fond to achieve the required security with minimal delay.

REFERENCES

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai,Defending Against Collaborative Attacks By Malicious Nodes In MANETs:A cooperative Bait Detection Approach,2014. page number:1-11.

[2] A.Baadache and A.Belmehdi,"Avoiding blackhole and cooperative blackhole attacks in wireless adhoc networks,"Intl.J.Comput.Sci. Inf.Security, vol. 7, 1, 2010.Page number : 35-43 .

[3] K.Vishnu and A.J Paul, "Detection and removal of cooperative black/gray hole attack in Mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, 2010.page number: 28–32.

[4] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen,"CBDS:A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl.Conf.WirelessCommun.,VITAE,Chenai,India,Feb.28–Mar.,03,2011,page number: 1–5.

[5] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,Jan. 1999. (Last retrieved March 18, 2013).page number:1-6.

[6] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc.WiSec, 2009,page number:103–110.