MANET Routing Protocol Features

S.Gayathri, Assistant Professor

S.Samundeeswari, Professor

Naveen.M, UG student

Department of Computer science Enginnering

PRIST University

Abstract

Mobile Ad-hoc network(MANET) is the type of network which can change locations and configure itself on the fly. In this paper, we discuss a scenario and methodology for solving the wormhole routing attack. To implement the proposed algorithm and requirements, we use route discovery and route failure to maintain the route. Major drawbacks of MANET is that as it is an infrastructure-less network, created on the fly, where each node can also function as a router. We combined a introduce unique security feature for On-Demand routing protocols both in it's multicast and unicast avatars.

Keywords: Trust, MANET, TABR, AODV

I INTRODUCTION

Mobile ad hoc networks are a network which consists of nodes that are independent, from their topologies dynamically and use the wireless medium to communicate. The nodes cannot be dictated to cooperate by a central administrative authority as there is no such authority in the case of MANETs. Implementation of wireless and mobile communication networks has instrumental growth in last few years. One of the basic characteristics of MANET is that it is an infrastructure less network, so there is an absence of specified nodes for operations related to network management, as there are in the normal routers in the fixed and wired networks. Routing protocols are a necessary evil in MANETs. They are responsible for identifying the optimal route from a source node to a destination node in a particular MANET. Thus, a network –layer protocol that is designed for self-configuring networks should have rules that are enforced for connectivity and security requirements to make sure that the higher layer protocols are operating at an optimum level. The basic mobile ad hoc network depends on some fixed accesses point or another mobile node (in case of MANETs) for communication via sending and capturing packets. When one compares wired ad hoc networks with MANETs, wired networks have a proper infrastructural set up for sending, forwarding and capturing packets. Routing protocols in MANETs are generally classified as proactive and reactive. Trust plays a vital role in MANET routing in providing reliable and efficient routing. The idea of using the trust to mitigate security threads has been an important area of research. The trust-based routing is one way to form cooperation among nodes for establishing efficient routing between nodes.

Characteristic of an Ad-hoc network

- Collection of mobile nodes forming a temporary network
- Network topology changes frequently and unpredictably
- No centralized administration or standard support services
- The host is also functioned as a router
- Ad-hoc an application requirements provide to the 10G EPON T.F information on actual deployments by service providers requirements worldwide regarding distance split ration, power budgets installed optical transceiver characteristics, video overlay characteristics,co-existence with deployed EPONs, and their response to the need to deploy blocking filters for co-existence.

This will be accomplished through surveying service providers and analysis of those replies. Such information will be used by this Ad-hoc to formulate positions on wavelength plans and optimal power budget.

II Types of Ad-hoc network

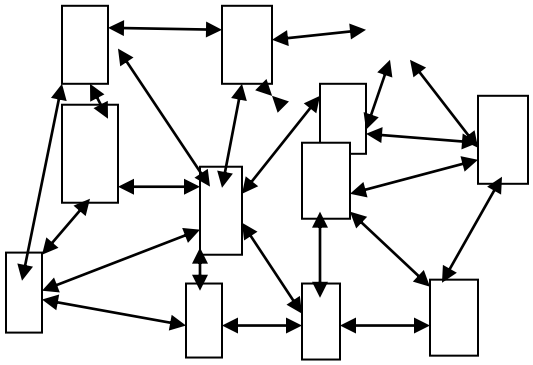

Fig 1: Mobile Ad Hoc Network

1. Wireless Mesh Network

Formed to provide an alternate communication infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraints and the requirements of network planning of the cellular network.

2. Wireless Sensor Network

The network used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.

III .Spectrum Requirement at nodes in MANET

- Each MANET nodes has smaller frequency requirements than that of a fixed infrastructure network.
- A node can act as a router for all the packets and it can also move to another node.
- MANET enables spectrum reuse

Ad Hoc Testing

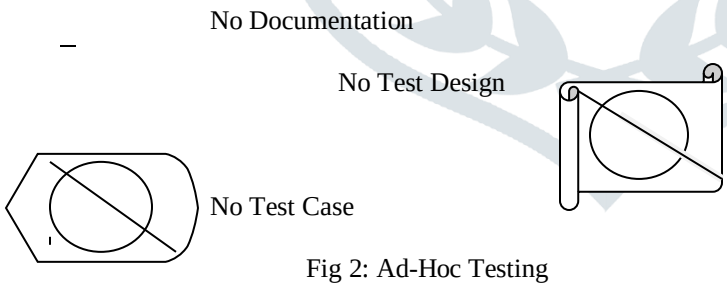

Fig 2: Ad-Hoc Testing

Types of Routing Protocols

1. PROACTIVE : DSDV, OLSR, CGSR, WRP
2. REACTVE : AODV, LMR, TORA, DSR
3. HYBRID : ZRP, BGP, EIGRP

IV. PROPOSED ALGORITHM AND IMPLEMENTATION REQUIREMENTS

A. Hardware and Software Requirements

- Intel or any other processor with a minimum of 2 GHz processing speed.
- RAM 256 MB or above.

- Hard Disk Capacity 2 GB or more.
- Windows 7 Home or Higher version.
- JRE 1.7 or higher and JDK 1.7 or higher version.
- NETBEANS or ECLIPSE IDE installed in the system for implementation only.
- Dynamic Ad-Hoc routing Simulator-created using JSIM and SWING JAVA libraries. Purely JAVA based tool. Implemented in pure JAVA.

V. PROPOSED WORK

The biggest challenge in mobile Ad hoc network is routing due to the dynamic nature of nodes. In spite of this vibrant topology, nodes communicate with each other and exchange data on the network. Ant colony optimization is used to optimize the routes selected for routing and along with trust which provides more efficient routing. The various phases of proposed TABR and its algorithm are described in the following sections.

Phases of TABR

In the proposed TABR for MANETs, the network agents(ants) are only transmitted on demand and are flooded through the entire network in a similar process as AODV. The routing table entries stores pheromone concentrations, which are transformed into probabilities later on.TABR works in three phases which are discussed in the following section.

Phase 1.Route Maintenance

Data packets are used to maintain the path, so no overhead is introduced but still, nodes have to be checked for updated trust values. Once the Bands have established the pheromone tracks for the source and the destination node, subsequent data packets also increased the pheromone value. Pheromone and trust value keeps on changing. When a node relays a data packets toward destination to a neighbor node, it increases the pheromone for that entry. The same happens in the opposite direction. The evaporation process is simulated by regular decreasing of the pheromone values.

Phases 2. Route Discovery

In the third phase, the Route Discovery Phase, new paths are discovered. The creation of new Adjustment of AODV Route Discovery Process for Fairness We improve the AODV route discovery process to achieve fairness. The problem of AODV route discovery is the rule of discarding already received RREQ packets via another route. The aim of our change is to construct paths that are appropriate to achieve fairness. FRAODV evaluates each path of RREQ packets in the route discovery process and broadcasts the RREQ packets based on the evaluation. FRAODV does not discard paths that might be suitable for adjusting the FV, and such a route is constructed as an available path. We show the detail of FRAODV route discovery process. The change from ISK protocol is that RREQ forwarding is decided by FV of the path to prevent discarding useful paths to achieve fairness. 1) Route discovery algorithm of FRAODV

1. This process is the same as AODV.

2. This process is the same as AODV with the exception of calculating FV in the packet header. A node that receives the RREQ packet adds the routing information to the routing table, compares FV and checks whether its destination node is itself. If it is not the destination and it has not yet received an RREQ packet with the same RREQ ID, it records the FV of the RREQ in the node, writes its node ID and adds its FV to the FV in the RREQ packet, and broadcasts the RREQ packet. If it has already received an RREQ packet with the same ID, it compares the FV in the newly received RREQ and already recorded FV

in the node. If the FV of newly received RREQ is smaller than the recorded FV in the node, it replaces the recorded FV in the node and broadcasts the RREQ packet, otherwise, the node silently discards the newly received RREQ.

3. This process is the same as AODV with the exception of replying the RREQ and adding the value of FV in the RREP packet header. An RREP has the value of FV that is the summation of FVs of the nodes in the path. If a node that receives the RREQ packet is the destination node, it checks the FV and recorded FV. If the FV of newly received RREQ is smaller than the current path's FV in the node, the node generates the RREP packet and send to the source node.

4. The source node selects the route of the first received RREP. If the node receives an RREP packet whose FV is smaller than the currently selected path's FV, the node selects the path of the newly received RREP packet.

Phase 3 Route Failure Handling

A route failure is recognized through a missing acknowledgment on the MAC layer and to deactivate that link by resetting the pheromone concentration to 0. Then, the routing table is checked for different links towards the destination and the packet gets relayed accordingly. If a message has to take a long path towards a target it lasts long until the sender is able to realize that the packet was lost. First, an attempt is made to send the packet over an alternate route; otherwise, it is returned to the previous hop expecting that there exists an alternate route in the network.

VI. Experimental Results

Optimization helps search packets or data packets to favorably move towards the destination by improving the pheromone concentration on the trusted paths. However, it reduces the pheromone concentrations on the paths which are not on the way towards the destination node. With optimization introduced these algorithm assigned a new name as TABR, i.e, Trust ANT Based Routing in MANETs. The simulation parameters used for TABR implementation are shown in table 2. The simulation results obtained from the execution of TABR is compared with the simulation results obtained from the execution of AODV, DSR, and an Ant-based protocol HOPNET. The experiments results were obtained against different no of nodes and different pause time. The proposed TABR shows good improvement in QoS metrics. PDR and Throughput

A. Packet Delivery Ratio

The calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in the trace file. In general, PDR is defined as the ratio between the received packets d packets by the source.

B. Throughput

TABR is on middling 12% better than AODV,20% better than DSR and 7% better than HOPNET in terms of middling throughput as shown in fig 1.since the likelihood of finding an efficient route for TABR is higher than that of AODV, DSR and HOPNET

C. Delay

TABR out forms AODV and HOPNET in delay as shown in figure5.The middling delay for AODV and HOPNET is around 0.18 and reduces when to pause time increases. The key reason for this close delay time is the additional works (trust and ant agents) to be carried out by the proposed TABR**.**

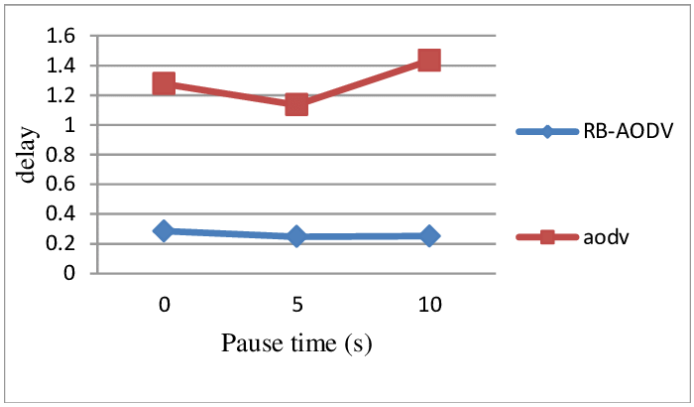

Fig 3 : Throughput

7. Conclusion

Mobile Ad-hoc network(MANET) is the type of network which can change locations and configure itself on the fly. In this paper we discuss about a scenarios and methodology for solving warmhole routing attack. To implement the proposed algorithm and requirements, we use route discovery and route failure to maintain the route. Major drawbacks of MANET is that as it an an infrastructure-less network created on the fly, here each node can also function as a router. We combined introduced a unique security feature for On-Demand routing protocols both in it's a multicast and unicast avatars. An application of ad hoc network ,requirements, characteristics, experimental results in ,packet delivery ratio, throughput and delay of ad hoc netwoks are explained.

8. REFERENCES

[1] R. Singh, P. Singh and M. Duhan, "An Effective Implementation of security based algorithmic approach in mobile Adhoc networks.", Human-Centric Computing, Springer Open-Access Journal, E4:7 (2014). http://www.hcis-journal.com/content/4/1/7

[2] W.Chen Wu, H.Twu Liaw, "A study of High Secure and Efficient MANET Routing Scheme.", Journal of Sensors, Hindawi Publishing, Vol.1 (2015). http://dx.doi.org/10.1155/2015/365863

[3] R. Dilli, P. Chandra Sekhar Reddy, "Implementation of security features in MANETs using SHA-3 Standard Algorithm." ICCSISSS, Vol.1 (2016).

[4] R.K. Singh, P. Nand, "Literature Review of Routing Attacks in MANET", ICCCA, Vol.1 (2016).

[5] M.A. Abdelshafy, P. J. B King, "Analysis of security attacks on AODV routing", IEEE, E1:2, pp 290-295 (2013).