A SECURITY SCHEME FOR MOBILE AD-HOC NETWORK USING VARIOUS ROUTING PROTOCOLS

[1] G.AMBIKA

[1]Assitant Professor, Dept.of.Computer science, Meenakshi Chandrasekaram College of Arts & Science Pattukkottai.

***ABSTRACT*−*A mobile ad-hoc network is gathering of mobile nodes which are design to converse each other without fix transportation and central coordination. Wireless networks are becoming more and more ubiquitous in recent years, ranging from Digital cellular telephony up to satellite broadcasting. Since in the MANET, routing protocols have no security mechanism. They are designed only to provide correct routing and have ability to adjust their dynamic changing condition. With the increasing demand and Penetration of wireless services, users of wireless networks now expect Quality of Service and performance comparable to what is available from fixed networks. So MANET is more venerable due to their routing behavior. Routing protocols are more affected by two way, first one is attacks from private node that do not belongs to network and also disrupted by presence of compromise nodes. In this paper three routing protocols aodv, dsr, and tora are compared. Opnet is used to simulate the performance of the routing protocols. Opnet modeler is one of the most popular products for modeling and simulating of computer network. We can solve the issue of attacks from private nodes by authentication techniques that provide mutual trust between nodes. In this paper, we proposed digital signature scheme to provide mutual trust between nodes.*

Keywords: Ad-hoc network, DSR, Routing security.

I. INTRODUCTION

The network dynamically setup temporary paths among themselves to forwarding data packets due to existence of temporary network without any fix infrastructure and centralize management. Since ad-hoc network routing protocols have not include any security mechanism at all so main security threads comes their routing protocols such as AODV, DSR, DSDV and OLSR. It means ad-networks are more venerable due to their routing behavior and characteristics of network. In the ad-hoc network, mobile nodes are not bound to any centralize control like base stations. In such type of network mobile nodes work not only as a host but also as a router. In the ad-hoc network routing protocol, each nodes allow to find multi-hop path to any other nodes in the network. Flexibility in MANET technology offers much application such as emergency services, geographical or terrestrial situations where we can establish communication without any fix base station. But these flexibility or characteristics such as dynamic topology, open medium and distributed cooperation are reason to be venerability in mobile ad-hoc network. Since in MANET, routing has important role to provide the security for entire network. Firstly, this paper will provide the little information regarding the routing protocols. The performance result of AODV, DSR and TORA will be presented. The result in this paper is based on fixed network topologies of 50 nodes. Performance of these routing protocols is shown using graphs and table at the end of the paper.

II.ROUTING ATTACKS:

First one is the passive attacks and second one is the active attacks. Passive attacks do not disrupt the operation of routing protocols, while active attacks disrupt the operation of routing protocols and engage modification, information interruption and fabrication.

2.1. *AODV (ad-hoc on-demand distance vector routing protocol)*

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. AODV avoids the counting to infinity problem. It defines three types of messages for working route request, route reply and route error.

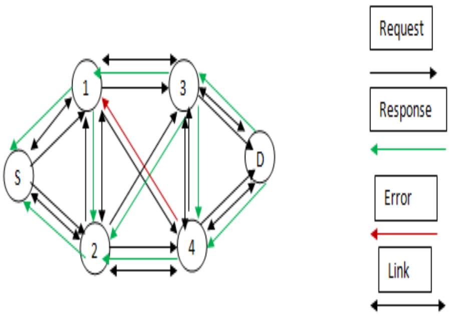
2.2.DSR (Dynamic Source Routing protocol)

It is a reactive routing protocol for ad hoc wireless networks. It also has on-demand characteristics. It is based on source routing. The node wishing to send a packet specifies the route for that packet. The whole path information for the packet traversing the network from its source to the destination is set in the packet by the sender. The two mechanisms are used in DSR route discovery and route maintenance. Route discovery finds the routs and route maintenance maintains the route using route error packet and acknowledgement.

2.3. Routing protocols of MANET

Basically many routing protocols are developed for mobile ad-hoc network which are designed to established route between sources to destination. But they are classified into two categories. *Table driven or proactive routing protocols:* In proactive or table driven routing protocols each node have maintain up-to-date routing information to each and every other nodes in the network. These types of protocols need every node to keep one or more table to store information about its neighbor and dynamic change in network topology during routing. *On demand:* In on demand or reactive routing protocols have each node have maintain routing information about active route only as when needed. These protocols are designed to reduce routing overheads in table driven protocols. On demand of route, when source node wants a route to destination for transmitting data packet, a route discovery process is initiated. There are mainly three routing protocols for a MANET, AODV (ad-hoc on demand distance vector), DSR (dynamic source routing), and DSDV (destination sequence distance vector). AODV is reactive routing protocols in which route discovery process is initiated to create route from source to destination when they are needed. Maintenance process at each node is based on time in which if the routing entry is not recently used, it will be expire. DSDV proactive routing protocol is based on Bell- Ford routing algorithm. In this, every node maintain a routing table about all possible routes to destination. DSR maintain routes in its table of which it is aware in route cache.

Since there are no dedicated routers, every mobile node is expected to route packets on behalf of other nodes. Nodes often transform their location in network. So, some fusty routes are produced in the routing table which leads to unnecessary routing overhead. So a HELLO message is being sent from source using AODV protocols to maintaining the link breakage and removing the unnecessary information from its routing table on occurring of ERROR messages.



In case first, when source node want to send a data to destination then there is need of routing protocols which is used to discover arouse to destination. We have chosen AODV routing protocol for establishment of route to destination. It is initiated on demand of data by source when source want to send data to any destination. Source node sends request packets to their neighbors with a destination IP address. Intermediate node response when they receive their request otherwise sends an error message to source.

III. NETWORK LOAD

Network load define the total load on WLAN. Different applications have different effect on network load. Network load also depends upon the type and size of data. For example, for real time applications load will be high as compare to other type of data.

3.1. Delay

From the analysis it is clear that AODV has minimum delay as compared to other protocols. Minimum delay means that better output. On the other hand, DSR has more delay as compare to AODV due to large number of nodes. TORA experiences lengthy delay while waiting to determine a new route. TORA and AODV have the lowest delay as compared to DSR.

3.2. Throughput

The average rate at which the data packet is delivered successfully from one node to another over a communication network is known as throughput. The throughput is usually measured in bits per second. A throughput with a higher value is more often an absolute choice in every network. Mathematically, throughput can be defined by the following formula.

How to check route validation and availably:

: In request packet, a time interval is set for response message to source when request is send by the source to destination. If response messages are received by source in this time interval with same hop-count in their routing table. Then route is valid and available else route is not valid. If time is out then an error message is send to source and source node choose another path with available highest sequence no. and minimum hop count.

VI. CONCLUSIONS

A security scheme for Mobile ad-hoc network with reduced routing overhead based on digital signature. In this scheme, a key is used by all offices in team member. This key generates digital signature using encryption technique and verifies the digital signature after decrypt the digital signature. The simulation model was developed on OPNET which allowed the simulation of fixed nodes. Several scenarios were implemented. The fixed node topology was compared against 50 nodes. AODV routing protocol showed that it has the highest throughput and lowest delay as compared to DSR and TORA.

V. REFERENCES

[1] L.Pengwei and X.Zhenqiang, *Security Enhancement of AODV against Internal Attacks*, International Conference on Information Science and Engineering (ICISE), Vol. 2, pp 584-586, 2010.

[2] A.Das, S.S.Basu and A.Chaudhuri, *A Novel security scheme for wireless Ad-hoc network*, International Conference on Wireless Communication Vehicular Technology, Information theory and Aerospace and Electronic System technology, Vol. 2, pp 1-4, 2011.

[3] DENG Hongmei, L I Wei and D P Agrawala, *Routing Security in Wireless Ad Hoc Networks*, International Journal of IEEE, Communication Magazine, Vol. 40(10), pp 70-75, 2002.

[4] Parulpreet Singh, Ekta Barkhodia, Gurleen Kaur Walia, *Performance Study of Different Routing Protocols(OLSR, DSR, AODV) Under Different Traffic Loads and with Same Number of Nodes,* of Electronics & Communication, LPU, Phagwara, Vol. 3, Issue 1, Jan.- March 2012

[5] Park, V., Corson, S., *Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification,* IETF MANET Working Group Internet Draft. Draft-item-manet-TORA-spec-03.txt. November 2000.

[6] Deep Kaur and Kirandeep Kaur "*QoS in WLAN using IEEE 802.11e (Survey of QoS in MAC layer Protocols)"* of SBS College of Engineering and Technology, Ferozepur, India, 2012 IEEE DOI 10.1109/ACCT.2012.93