PATH DETERMINATION AND OPTIMIZING: MANET

Ashish Joshi[1], Deepak Painuli[2]
[1]Department of Computer Science and Engineering, THDC-IEHT, NEW TEHRI
[2]Assistant Professor, Quantum School of Technology, Roorkee, India

Abstract

Routing and Security in Mobile Ad-HOC network (MANET) haven been a major challenge in recent days in the terms of route selection and security of data transmitted. A large number of promising path determination algorithm already exist as nodes are mobile and they dynamically exchange data among themselves. As the nodes are not static major problem arises in transmission range, multi-hopping, route discovery. This paper presents a comparative analysis of algorithm currently existing and tempts to provide an algorithmic solution.
Keywords: MANET, Ad-HOC networks, protocols, wireless, hops

I. INTRODUCTION

MANET (Mobile Ad-HOC) networks are those networks that do not possess a fixed infrastructure or wired backbone. In these types of networks, the nodes act like routers and are responsible for forwarding the data from one node to another resulting in wireless network kind of infrastructure. Initially some algorithms are applied for determination of path in this type of scenario. As a result, we will obtain a virtual path along the connected nodes in dynamic scenario.

Since all the nodes in mobile ad HOC network are in moving state so topology determination like in case of wired networks is quite typical as in the latter case all the nodes are static. Henceforth resulting in problem of path determination as each node has its own limitation in Hardware.

Because of mobility concept several other issue again arises like path may break in between as certain node may become out of range in between thereby resulting in route break. If path determination in a wireless dynamic scenario is repeated many times bandwidth is consumed and changes of getting errors in data transmission algorithms is increased to a great extent.

II. RELATED WORK

Huge number of work have been already done in field of path determination and security. Major protocols have been classified into two categories Proactive and reactive. Reactive protocols are in those category whose routing tables are dynamically exchanged. DSR (Dynamic Source Routing) has been a very ideal for routing in multi hops networks. DSR facilitates source routing Network can organize and configure itself for wireless networks. DSR has two phases as route discovery and route maintenance. Route discovery phase is related to formation of route in multi- hop networks whereas route maintenance phase is related to maintain path during the transmission process. Other protocols include AODV, DSDV [1] and TORA [2]

Sung-Ju Lee and Mario Gerla proposed AODV-BR [3] routing protocol. It uses same route almost discovery process as AODV [4]. It searches a route by flooding a route request (RREQ) packet if there is no route present. Packets have a unique ID so that nodes in between (in case of multi hops) can detect and drop duplicates.

III. PROPSED SCHEME

We propose a following scheme for communication within the MANET (in certain region e. g office schools business organizations etc) to avoid path congestion and provide security to the network.

Algorithm:

Step1: Apply process as:

    a. Assign the leader of network either by voting or by size of participating nodes.

Maximum the size of node it will be chosen as a leader.

b. Leader will Sent request to sent the public key to all nodes participating in the network

c. Form a table structure

IP	Key	Next hop	alternate

Table1:

The ip is the IP of participating nodes key is referring to public key of particular nodes next hop is referring to nearest node usually calculated by Manhattan distance/ Dijakastras/bellman ford also can be applied for all the nodes. The node having least distance is selected as next hope the next node having next least distance is kept as alternate node. To be updated periodically on timestamp basics.

Leader will distribute it to all parties in network by flooding in a fixed duration of time.

Step 2: Select the sender and receiver in the network

Step 3: Sender the required to encrypt the data with the public key available of the receiver end.

Step 4: Send the packet through next hop if ack is not received within certain period sent ithrough alternate route.

Step 5: Decrypt the process at the receiver's end This setup aims to provide a cheap and secure communication to smaller ranges involving distributed, cryptographic measures.

REFERENCES

[1] C. E. Perkins and P. Bhagwat. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers, In ACM SIGCOMM, pages 234-244, 1994.

[2] Vincent D. Park and M. Scott Corson. Temporally Ordered Routing Algorithm (TORA) Version 1: Functional Specification. Internet-Draft,draft-ietf-manet-tora-spec-01.txt, Aug 1998.

[3] S.J.Lee, M.Gerla, "AODV-BR: Backup Routing in ad hoc networks", IEEE WCNC, September 2000.

[4] C.E. Perkins, E.M. Royer, "*Ad-hoc On-Demand Distance Vector* Routing", Proceedings of IEEE WMCSA, Feb 1999.

[5] N.Jaisankar and R.Saravanan,' An Extended AODV Protocol for Multipath Routing in MANETs IACSIT International Journal of Engineering and Technology, Vol.2, No.4, August 2010