Routing with AODV Protocol for Mobile ADHOC Network

M.Devi[1] and Dr.V.Rhymend Uthariaraj[2]

[1]*Research Scholar (I & CE), Anna University, Chennai-25, TamilNadu, India.*
sheeludevi@gmail.com
[2]*Director and Professor of RCC, Anna University, Chennai-25, TamilNadu, India*

Abstract **- One wireless network architecture that has received a lot of attention recently is the mobile ad hoc network (MANET).It is attractive because the network can be quickly deployed without the infrastructure of base stations. One main feature of MANET is that mobile hosts may communicate with each other through a sequence of wireless links (i.e., in a multihop manner). Mobile Ad hoc Networks are infrastructure less networks with dynamically changing topology. Several On-demand routing protocols have been proposed to facilitate the communication in these networks. Nodes of these networks function as routers, which discover and maintain routes to other nodes. The Ad hoc On-demand Distance Vector (AODV) is the widely used scalable protocol. But this shortest path algorithm prefers long hops, which results in routes with weak links. Hence route failure become frequent, even in case of less mobility, which degrades the network performance. In this paper we propose two modifications to the existing AODV. First to discover a reliable route (stable route), Next to minimize the delay in the re-route discovery. This reliable route discovery and seamless route maintenance mechanism will be implemented using GLOMOSIM (Global Mobile System Simulator) to obtain improvement in the network throughput.**

Index Terms **- Ad hoc networks, mobile computing, mobile networks, routing, and wireless communication.**

I. INTRODUCTION

1. MANET

Networking refers to some form of interaction among technological devices. Since their emergence in the 1970's wireless networks have become increasingly popular in the computing industry. There are currently two variations of mobile wireless networks [1].

The first is known as the" infrastructure network" (i.e. a network with fixed and wired gateways). The bridges for these networks are known as "base stations". A mobile unit within these networks connects to and communicates with the nearest base station that is within its communication radius. As the mobile travels out of range of one base station and into the range of another, a "handoff" occurs from the old base station to the new and the mobile is able to continue communication seamlessly throughout the network. Typical applications of this type of network are office wireless local area networks (WLANS)[2].

The second type of mobile wireless network is the infrastructure less mobile network, commonly known as the Ad-hoc network. [2]. [Ad-hoc refers to a Latin word meaning undetermined or unpredictable].

2. AODV

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the

source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

II. PROBLEM STATEMENT

Problem Statement –1

A RREQ is accepted only if its power level is above the threshold. Hence the hop size is reduced. Thus it leads to reliable route, which reduces route failures. For this we force the nodes to apply higher power threshold while forwarding RREQ packets.

Each node keeps track of its own threshold level. Each node categorizes the network as high threshold level or low threshold level based on the neighborhood changes perceived by the node. If the number of neighbor changes is high (exceeds a certain value), then the node threshold level is high. When a new packet is entered, a check is made of it exceeds the preset called the threshold level. If it exceeds, it is incremented in order to force an update. The threshold is used to decide when an update needs to be triggered.

Problem Statement –2

When a link failure occurs along a path, the route discovery algorithm must be reinvaded from the source to find a new path to the destination. No attempt is made to use partial route recovery, that is, to allow the intermediate nodes to attempt to rebuild the route themselves. That is, AODA do not specify intermediate node rebuilding. While this may lead to longer route reconstruction times since link failures cannot be resolved locally without the intervention of the source node, the attempt and failure of an intermediate node to rebuild a route will cause a longer delay than if the source node had attempted there building as soon as the broken link was noticed.

Hence to minimize the delay in the re-route discovery, we predict route failure by monitoring the signal strength. If it approaches the threshold level, the source is advised to find an alternate route or new route while continuing the packet forwarding. This helps to reduce delay in re-route computations, when the current route fails. The modifications explained above will result in improved route maintenance.

III. SIMULATION RESULTS

MOBILITY AND TRAFFIC MODEL

The random waypoint model is used to model mobility. Each node starts its journey from a random location to a random destination with a specific speed. Once the destination is reached, another random destination is targeted after a pause. Field configuration of 1000m x 1000m field with 50 nodes and 1500m x 1500m field with 100 nodes are used and each node uses the IEEE802.11 with a 250m transmission radius. The pause time is kept constant at 30 seconds for all our simulation experiments. Traffic source-destination pairs are spread randomly over the network and the number of source is varied to change the offered load in the network. The sending rate is set to 100 packets per second. Simulations are runs for 800 simulated seconds.

This indicates that this algorithm selects routes based on the signal threshold between nodes. This route selection criterion has the effect of choosing route that have stronger threshold. Similarly continuous monitoring the signal strength of the neighboring nodes and if the chosen path has a high threshold level, then the packets arrive at the destination in the same way. If they arrive at a node with weak threshold level the packets with smaller values are dropped. When a failed link is detected within the network, the intermediate nodes send an error message to the source to the source indicating which channel has failed. Then the source initiates route search process to find a new path to the destination.

BASIC CONFIGURATION FILE

The main configuration parameters for setting up a scenario are defined in the CONFIG.IN file. These parameters are the following:

Simulation Time : Maximum Simulation time

Seed : It is a random number used to initialize part of the seed of various randomly numbers in the simulation.

Terrain Dimensions : Terrain area simulated in meters.

Number of Nodes : Number of nodes being simulated.

Node Placement : Represents the node placement strategy.

Mobility : Represents the mobility model.

The NODE PLCEMENT parameter can be assigned the following values:

RANDOM (nodes are placed randomly within the physical terrain), UNIFORM (based on the number of nodes in the simulation, the physical terrain is divided into a number of cells. Within each cell, a node is placed randomly), GRID (node placement starts at 0,0 and are placed in grid format with each node GRID-UNIT away from its neighbors, the number of nodes has to be square of an integer) and FILE (position of nodes is read from NODE-PLACEMENT-FILE). If the MOBILITY parameter is said to be NONE then there is no movement of nodes in the model.

Propagation Limit : Signals below this parameter (in dBm) are not delivered. This value must be smaller than RADIO-RX-SENSITIVITY+RADIO-ANTENNA-GAIN of any node in the model. Otherwise, simulation results may be incorrect. Lower value should make the simulation more precise, but it also makes the execution time longer.

Propagation-path loss: Specifies the path loss model.

Noise Figure Temperature: Temperature of the environment (in K)

Radio Type: Radio model to transmit and receive packets

Radio Frequency: Frequency in Hertz.

Radio Bandwidth: Bandwidth in bits per second.

The PROPAGATION PATH LOSS parameter specifies the path loss model. Models available in GlomoSim are FREE-SPACE and TWO-RAY model. The values of the RADIO-TYPE parameter are: RADIO-ACCNOISE refers to the standard radio model while RADIO-NONOISE refers to the abstract radio model.

RADIO-Rx-Type: specifies the packet reception model.

Radio-TX-Power: Radio transmission power (in dBm)

Radio-Antenna-Gain: Antenna Gain (in dB)

Radio-Rx-Sensitivity: Sensitivity of the radio (in dBm)

Radio-Rx-Threshold: Minimum power for received packet (in dBm)

In the RADIO-Rx-Type parameter, when the SNR-BOUNDED parameter is used, if the signal to Noise Ratio (SNR) is more than RADIO-RX-SNR-THRESHOLD (in dB), it receives the signal without error. Otherwise the packet is dropped. RADIO-RX-SNR-THRESHOLD needs to be specified. The default values of the last two parameter are:

Radio-Rx-Sensitivity : -91.0

Radio-Rx-Threshold : -81.0

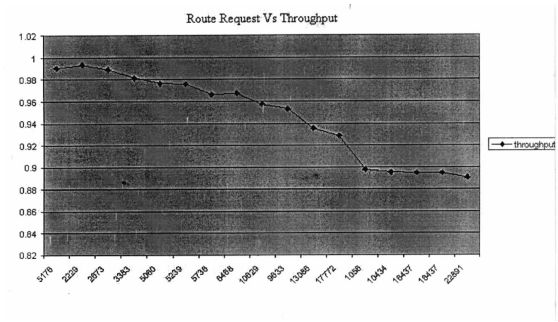
MAC protocol : Definition of Medium Access Protocol

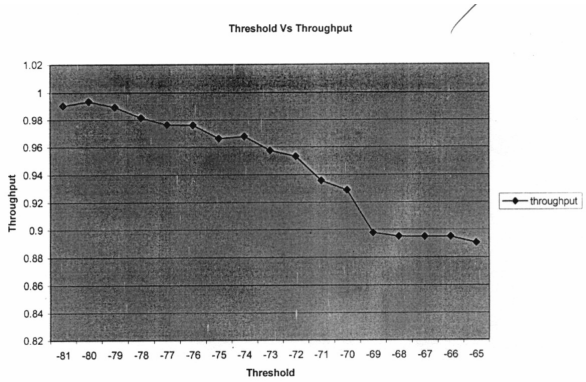
Promiscuous Mode : It is set to YES if nodes want to overhear destined to the neighboring node.

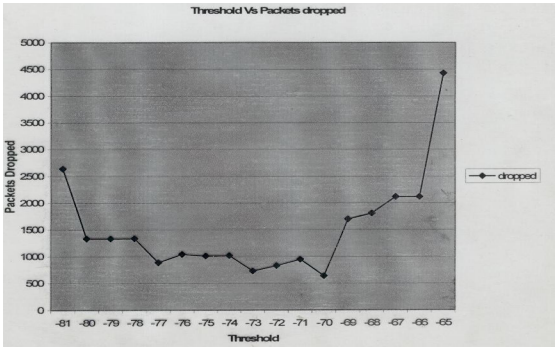
Network Protocol : Definition of the network protocol.

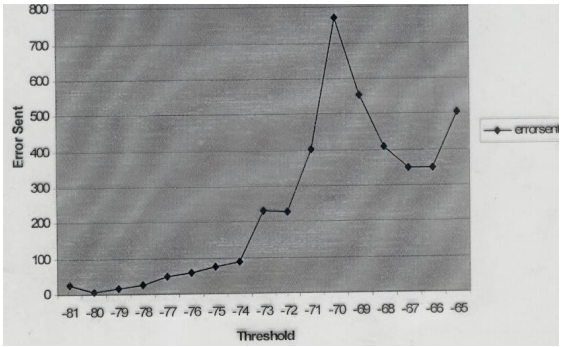
Routing Protocol : Definition of the routing protocol.

App-config-file : Specifies the file that sets up applications such as FTP, CBR and TELNET.









IV. CONCLUSION

With the advent of Ad hoc wireless, there are more and more demands on them to take advantage of the flexibility and provide easy access to the internet, but still have the stable and high performance

characteristics of the traditional wired network. In this paper we proposed modifications of the AODV protocol for dynamic ad-hoc networks. With this modification, they can achieve loner lifetime with stable route without any central information about topologies or traffic demands. The advantage of this approach is that the nodes require no addition information required in other protocols designed for reducing power consumption in MANETs. Thus the route can be efficiently served by using this modification. The modifications are implemented using GloMoSim Simulator.

REFERENCES

1. YU-Chee Tseng, Senior Member, IEEE, Yue- Feng LI, and Yu-Chia Chang "On

   Route Lifetime in Multihop Mobile Ad Hoc Networks"– IEEE Transmission on Mobile Computing. December 2003.

2. "On Security Study of Two Distance Vector Lrouting Protocols for Ad Hoc Networks" - Weichao Wang, Yi Lu, Bharat Bhargava CERIAS and Department of Computer Sciences, Purdue University, March 2003.

3. Chris Ellis, Senior Associate – "Leveraging IPV6 Capabilities to Facilitate the

   deployment of Mobile Ad Hoc and Sensor Networking" – December 2004.

4. Jie, Wu, Senior Member, IEEE, and Fei Dai, Student Member, IEEE."Efficient

   Broadcasting with Guaranteed Coverage in Mobile Ad Hoc Networks" IEEE Transmission on Mobile Computing. June 2005.

5. PARSEC User Manual For PARSEC Release 1.1 Revised in September 1999

   developed by members of the UCLA Parallel Computing Laboratory Mineo Takai, Jay Martin, Richard Meyer, Brian Park, Ha Yoon Song

6. Djenouri, D., Khelladi, L., and Badache, N. A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys & Tutorials., 7, 4 (2005), 2--28.

7. Wu, J. and Stojmenovic, I. Ad hoc networks. Computer., 37, 2 (2004), 29--31.

8. Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. Security in mobile ad hoc networks challenges and solutions. IEEE Wireless Communications., 11, 1 (2004), 38--47.

9. Royer, E. M. and Toh, C. K. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications., 2, 6 (1999), 46--55.

10. Deng, H., Li, W., and Agrawal, D. P. Routing security in wireless ad hoc networks. IEEE Communications Magazine., 40, 10 (2002), 70--75.