On-Demand Routing in Mobile Ad-Hoc Network

Humayun Bakht,
Contributing Editor, ZATZ Publishing USA, humayunbakht@yahoo.co.uk

Abstract

MAODDP is an on-demand protocol which establishes route and delivers data one after the other. The key feature of MAODDP is the integrated approach of addressing various routing related issues. Unlike some other protocols of similar type, MAODDP has its own security and power saving mechanisms. This paper besides security present simulation based evaluation of MAODDP power saving mechanism..

A series of experiments were conducted to monitor power conserving ability of MAODDP. MAODDP showed an impressive performance in conserving available power by saving 22% more memory with an increased data delivery of 5% in power saving mode.

***Keywords**: MANET; Routing; MAODDP; Power Aware Routing; Secure Routing*

1. Introduction

Mobile nodes in mobile ad-hoc networks operate on low battery power. That makes power conservation an important challenge in mobile ad-hoc networks. Most of the protocols that have been reported propose routing without considering their affects on some other routing related issues. The current protocols for mobile ad-hoc networks can generally be categorized into one of two types: pro-active and re-active protocols types.

Pro-active protocols[1, 2] establish routes via continuously evaluating the known routes and attempting to discover new routes, thus trying to maintain the most up-to-date view of the network. In pro-active protocols, nodes need to be in either receiving or sending mode throughout the network life. This approach adds a considerable burden on available power. Reactive protocols [3-6] determine the route only when required, that is, when a packet needs to be forwarded. In this instance, the node floods the network with a route-request and builds the route on demand from the responses it receives. Reactive protocols do not require nodes to be awake all the time but too many query packets could yield the same effects as in pro-active protocols.

There are protocols which [7] are specifically designed to conserve battery power. MAODDP[8-10] follows an integrated approach of addressing various routing related issues by offering broad routing solution with power conservation. MAODDP, unlike some other protocols[10] has its own security and power saving mechanism. Rest of this paper has been organized as follows. In section 2, an introduction to MAODDP security and power aware mechanism is presented. In section 3, simulation environment is defined. In section 4, evaluation results and observations are presented. Conclusions are given in section 5 and references are listed in section 6.

2. Mobile Ad-hoc On Demand Data Delivery Protocol (MAODDP)

Mobile Ad-hoc on Demand Data Delivery Protocol adopts an intermediate approach by building routes and delivers data at the same time one after the other [11]. MAODDP builds routes using a route query and data delivery process. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route query and data delivery (RQDD) packet. Nodes receiving RQDD update their routing tables for the source node and set up backwards pointers to the source node in the routing tables.

A node receiving a RQDD, if it is the destination node, issues an acknowledge (ACK) back to the source node. If it is an intermediate node, which has a route to the destination, it forwards

RQDD to the destination. Any further RQDD with the same sequence number and broadcast ID is dropped by the intermediate nodes without action.

Once the source node received the acknowledge packet, it can begin to forward data packets to the destination using the same route. If the source node later received any updated route with a smaller hop count, it updates its routing table for that destination. On the other hand if the source node does not hear anything back from the destination within a set time limit, it considers the previous attempt as unsuccessful. Source nodes in this case can rebroadcast RQDD with a new sequence number and broadcast ID.

2.1. Security

MAODDP deal security at an intermediate level. However, implementation of the protocol allows for other security mechanisms e.g. [12] to integrate within the protocol structure. MAODDP security mechanism as mentioned in[11] uses trusted certificate server C, whose public keys known to all valid nodes. Two or more mobile nodes collectively can act as a trusted server. Keys are priority generated and are exchanged through mutual relationship between C and each node. Each node obtains a certificate with exactly a single key from the trusted certificate server on joining the network.

The certificate details different aspect of connecting node such as node addresses, a public key and a time stamp T1 and T2. T1 defines the certificate issue time and T2 stands for the expiry time of the certificate. These certificates are authenticated and signed by the server C. The goal of communication between source and the destination is to make sure that data is reached safely at the destination. MAODDP allocated public key to all the mobile nodes at the joining of the network. Public key contains a certificate and expiry time. For each RQDD the receiver node extracts the public key from the certificate ‘C’ to validate the signature and to make sure that the certificate is not expired and is still valid. The same procedure is repeated in forwarding ACKs from the destination to the source node.

3.2. Power Saving Mode

MAODDP allows mobile nodes to switch in between one of two modes: sleep state or active state. Nodes are required to be awake only during the active transmission and are allowed to go into sleep mode if are not the receivers or the senders of packets. Moreover with the addition of a specific listening time (LT) each node can switch back into listening mode after a time period of (LT). Under active mode, if the node does not find itself in an active transmission it can switch back into sleep mode.

MAODDP defines a number of other different functions. Joining message allows mobile nodes to establish an ad-hoc network or a mobile node to join an existing ad-hoc network. Route Query Data Delivery process calls each time when a node wants to broadcast a Route Query Data Delivery (RQDD). Broadcast Acknowledge process enables broadcasting acknowledge messages (ACK) for the source of RQDD and Broadcast Route Error is to broadcast route error messages. MAODDP supports multicasting and has its own secure mechanism for securing data transmission.

3. Simulation Environment

Each set of experiments comprises of nine different tests. Seven sets of experiments were conducted over SWANS under SuSE Linux 10.1 operating environment. Six of these sets were conducted under power saving mode and the last one without power saving mode.

It is not possible in SWANS to carry out simulation that can highlight direct power consumption of mobile nodes. However, some of the understood concepts could be utilized to draw conclusions. It can be understood that if the nodes are not in sleep states, it will increase its message activities. In terms of protocol functioning it is expected to see more broadcast RQDD and ACK in simulation cycle. Moreover, bandwidth consumption is likely to increase. If no power saving mechanism is available the chances are that the nodes will be engaged continuously in replying to different messages which otherwise could be re-route to some other node. These two factors are measured against those obtained in power saving mode. In this regard different readings from each of the first six sets of experiments have been taken. In table 3.1 all those readings are collected while in table 3.2 all readings for the same simulation parameters in no power saving mechanism are recorded. To obtain such readings a manual procedure was followed. Code that deals with MAODDP power aware operation was disabled and whole simulator was recompiled before running simulations for the selected readings.

Simulation environments were generated via selection of one of many input parameters. Details of each of these parameters and how they were used are as follows:

Nodes were placed mainly in a grid type area of 5m x5m to 30m x 30m within a two dimension fixed field size of 500m x 500 m. However, in one set of experiments nodes were placed randomly within the same fixed field as described above. Nodes were selected from the range of 25 to 450 mobile nodes. All simulation starts at 10 seconds with a fixed resolution time of 60 seconds. MAODDP was evaluated both for short and long simulations run therefore simulation stop time was chosen from the range of 600 to 800 seconds. A fixed pause time of 10 seconds was used for all the simulation. In some sets, mobility was defined as static and for the others different mobility models were used.

Packet loss for most of the experiment defined as default. Adding packet loss to the simulation does not really test anything new, since the simulations already have packet loss even without specifying it. Following mobility models were used in some of the experiments.

Random Walk: In Random Walk Mobility model mobile nodes moves in turn.

Random Way Point: Random Way Point model is an extension of the random walk model. In this model each node at the beginning of its turn first moves to a new position selected at random in the unit square.

Teleport Model: This was another model which was used in some of the simulation experiments.

Definitions and explanations of conclusions drawn from the simulation results are as follows:

Data delivery defines the ratio between the number of ACK sent and broadcasted RQDD.

Route formed: Defines number of new routes added.

Elapsed time defines the time between simulation start time and simulation stop time.

Memory saved is the difference of total memory and memory used in a simulation cycle.

Number of Nodes	RQDD Sent	ACK received	Data Delivery %	Routes Formed	Bandwidth Saved
25	460	357	77.60	46	96.94
50	1249	1249	100	144	97.07
100	2435	2374	97.49	349	99.74
250	10553	8796	83.35	1056	97.69
350	13541	11153	82.36	1356	97.64
450	18409	12777	69.40	1842	97.13
	7774.5	6117.67	Avg(85.03)	798.83	97.13%

Table 3.1 Results chart with power saving mode

Number of Nodes	RQDD Sent	ACK Received	Data delivery	Routes Formed	Bandwidth Saved %
25	517	350	67.698	52	46.44
50	1256	1256	100	126	52.56
100	2496	2402	96.23	251	53.58
250	10887	8219	75.49	1090	56.96
350	14015	11024	78.65	1402	56.63
450	17789	11265	63.32	1767	97.23
	7826.66	5752.66	Avg(80.23)	781.33	61.07 %

Table 3.2 Results chart without power saving mode

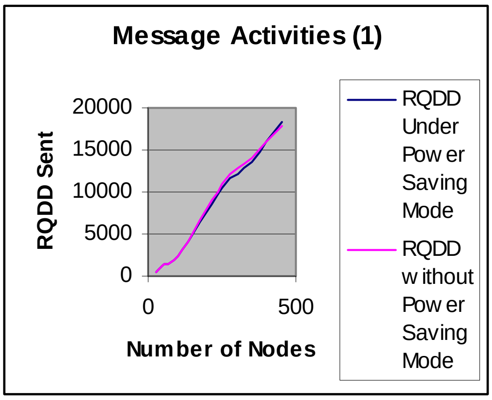
4. Evaluation Results

In the light of all the evaluation results, it can easily be seen that MAODDP performance was impressive in respect of power consumption. Simulation environment for these experiments were created in a manner which can best reflect the nature of mobile ad-hoc network communication pattern.

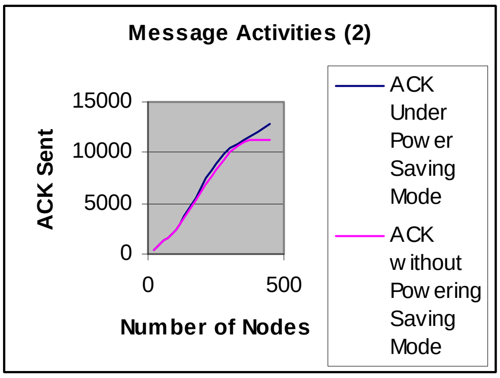
Evaluation experiments were run with different mobility models. Results showed that highest message activity in terms of broadcasted RQDD was recorded in the random waypoint model. It might be due to limited and specific communication pattern of mobile nodes of this model.

In general, message activities both in terms of broadcasting RQDD and sending ACK were quite high as shown in graph (1) and graph (2) respectively. Statistics of table 3.1 and table 3.2 shows an increase of 1 % in broadcasted RQDD. In graph (1) it can be observed that more RQDD were broadcast without power saving mode then under power saving mode. This further explains that without having the power saving mechanism, node performance could drop. Results showed 5% increase in data delivery under power saving mode as it is shown in graph (3). It can be assumed that this 0.1% broadcast packets might be the one's who were broadcast before. This further supports power aware operation of MAODDP as it could be helpful in avoiding dealing with the same packets again. This assumption also can be supported with the fact that more routes were established under power saving mode (table 3.1) than when it was off (table 3.2). Graph (4) presents a comparison of route formation in between two modes. It can be seen that the probability of new route formation increased with the addition of mobile nodes.

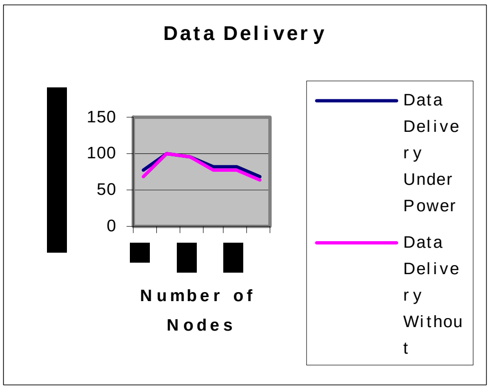
Among the three mobility models used, teleport proved to be most memory conserving. Statistics of table 3.1 and 3.2 shows that MAODDP saved almost 22.05 % available memory in power saving mode. A graphical comparison in terms of memory saved is shown in graph (5).



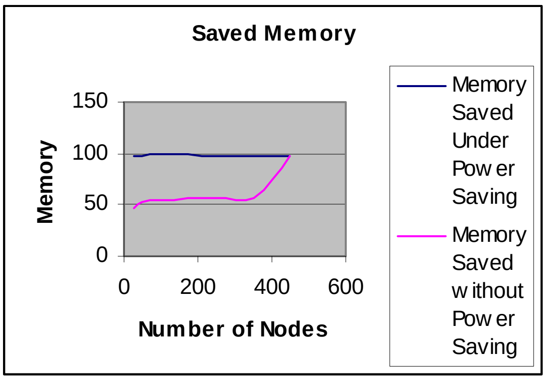
Graph (1) Message Activities (1)



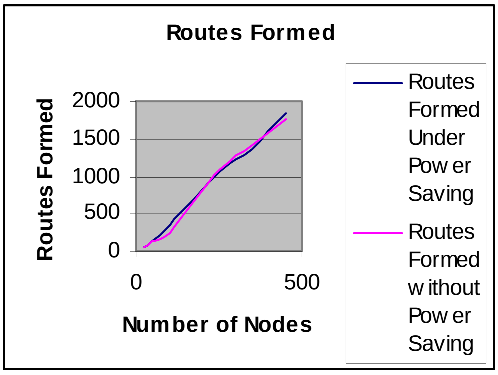
Graph (2) Message Activities (2)



Graph (3) Data Delivery



Graph (4) Routes Formed



Graph (5) Saved Memory

5. Conclusions

This paper presents a brief discussion on security and power saving mechanisms of MAODDP. A series of experiments were conducted to measure the power saving efficiency of MAODDP. MAODDP showed an impressive performance in respect of conserving available power. Results showed an increased of 5% in data delivery with 22% memory were saved with a higher capability of new route formation of MAODDP. In future we will be conducting evaluation tests to monitor scalability factor of MAODDP. We are committed to share our research finding with the ongoing research in this area.

6. References

[1] S.Kannan, John E Mellor, and D.D.Kouvatsos, *Investigation of routing in DSDV*. 4th Annual Post-Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, Liverpool UK, 2003.

[2] G. Pei, M. Gerla, and T.-W. Chen, *Fisheye State Routing in Mobile Ad Hoc Networks.* Proceedings of Workshop on Wireless Networks and Mobile Computing, 2000.

[3] Charles E. Perkins and Elizabeth M. Royer, *Ad-hoc On-Demand Distance Vector Routing.* Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999: p. pp. 90-100.

[4] Elizabeth M. Royer and Charles E. Perkins, *Multicast Ad hoc On-Demand Distance Vector routing (MAODV).* Internet Draft, draft-ietf-manet-maodv-00.txt.

[5] Humayun Bakht, Madjid Merabti, and Robert Askwith, *Mobile Ad-hoc On Demand Data Delivery Protocol.* 3rd Annual Post-Graduate
Symposium on the Convergence of Telecommunications, Networking and Broadcasting, 2002.

[6] Elizabeth M. Royer and Charles E. Perkins, *Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol.* Proceedings of MobiCom '99, 1999.

[7] Y. Tseng, C. Hsu, and T.Hsieh, *Power-saving protocols for IEEE 802.11-based multi-hop ad hoc networks.* Computer Networks, October 2003. **43**(3): p. 317 - 337.

[8] R.L. Gilaberte and L.P. Herrero. *Routing Protocols in Mobile Ad-Hoc Networks*. in Communication Systems and Networks. December, 2005. Benidorm,Spain.

[9] M.Saleem and M.A.Sheik, Empirical Analysis hoc Routing Protocols for Hybrid Sensor Networks. *International Conference on Electrical Engineering(ICEE),* April 2007.

[10] David B. Johnson, David A. Maltz, and Josh Broch, *DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks.* Ad Hoc Networking, 2001.

[11] R.L.Gilaberte and L.P.Herrero, *A Secure Routing Protocol for Ad hoc Networks Based on Trust*. International Conference on Networking and Services (ICNS '07),2007.

[12] W. Wang, Y. Lu, and B. Bhargava. On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks. in IEEE International Conference on Pervasive Computing and Communications. March 2003. Dallas-Fort Worth, Texas,USA.

Article received: 2009-11-06