MOBILITY SCENARIO-BASED PERFORMANCE EVALUATION OF PREEMPTIVE DSR PROTOCOL FOR MANET

Ramesh V[1] Subbaiah P.[2]

[1]Research Scholar, Sathyabama University, Chennai, TN, India.
[2]Professor in ICE, Sree Sai Ram Engg. College, West Tambaram, Affiliated to Anna University, Chennai, India.
Email: [1]v2ramesh634@yahoo.co.in, [2]subbaiah_nani@sify.com

Abstract

Ad hoc wireless networks are characterized by multi-hop wireless connectivity, infrastructure less environment and frequently changing topology. To analyze the performance of routing protocols in MANETs in the real world, a scenario based simulation analysis is required since there is a lack of necessary infrastructure for their deployment. Most of the earlier work done in this field have assumed the Random Waypoint model, which fails to capture the realistic movement of the nodes. In this paper, we describe a set of experiments conducted to analyze the performance of the Preemptive DSR routing protocol in a battlefield scenario. BonnMotion Software(Java based) is used to create and analyses mobility scenarios. Initially an explanation of the experimental metrics and the setup is described, followed by the scenarios used for our simulations. The results give an idea of how the Preemptive DSR protocol behaves in the given scenario and helps identify the metrics for optimal performance of the protocol.

Keywords—MANET, PDSR, battlefield, Packet Delivery Ratio, delay.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self configuring network of mobile nodes connected by wireless links, the union of which forms an arbitrary topology. The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology changes rapidly and unpredictably.

Proactive MANET protocols are table driven and will actively determine the layout of the network. Through a regular exchange of packets meant for network topology between the nodes of the network, a complete picture of the network is maintained at every node. Hence there is minimal delay in determining the route to be taken.

Reactive MANET protocols only find a route to the destination node when there is a need to send data. The source node will start by transmitting route requests throughout the network. The sender will then wait for the destination node or an intermediate node (that has a route to the destination) to respond with a list of intermediate nodes between the source and the destination. This is known as the global flood search, that in turn brings about a significant delay before the packet is transmitted. Since each of the proactive and reactive routing protocols suits well in oppositely different scenarios, there is good reason to develop hybrid routing protocol that is a mix of both proactive and reactive routing protocols. The hybrid protocol is applied to find a balance between the proactive and the reactive protocols.

II. DYNAMIC SOURCE ROUTING PROTOCOL

The Dynamic Source Routing (DSR) protocol is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes[8]. The DSR protocol allows source nodes to dynamically finds a route to any destination node in the ad hoc network. Each data packet sent has in its header the complete ordered list of nodes through which the packet must pass, and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. DSR cache the routing information for future use. DSR protocol contains two major phases, route discovery and route maintenance.

Route Discovery: It is the process by which a source node S needs to send a packet to a destination node D and hence obtains a route to D. Route Discovery is used only when source node S needs to send a packet to destination node D, it looks up its route cache to locate an unexpired route to the destination and if it fails, then it initiates the route discovery process through broadcasting a Route Request (RREQ) packet. Each node on receiving a RREQ packet, it rebroadcast the packet to its neighbors if it has not forwarded

already. Route Request packet (RREQ) contains <Destination Address, Source Address, route Record, Request ID> [8]. On receiving the RREQ packet the destination replies the RREQ packet the destination replies to the source with a Route Reply (RREP) packet. When an intermediate node detects that the link to the next-hop node towards the destination is broken, it immediately remove this link from the route cache and returns a route error message to the source node. The source node again activates a new route discovery. DSR works for small to medium size MANET when nodes speed is moderate and every node has enough battery power.

Its main feature is that every data packet follows the source route stored in its header. This route gives the address of each node through which the packet should be forwarded in order to reach its final destination. Each node on the path has a routing role and must transmit the packet to the next hop identified in the source route [8].

Route Maintenance: Each node maintains a Route cache in which it stores every source route it has learned. When a node needs to send a data packet, it checks first its route cache for a source route to the destination. If no route is found, it attempts to find new route using the route discovery mechanism and hereby increases the control overhead and connection setup delay. To overcome these drawbacks we propose Preemptive Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks with Backup Route [6].

III. PREEMPTIVE DSR

We have proposed this algorithm in the earlier work[8].

Assumptions:

We assume that all nodes wishing to communicate with other nodes within the ad hoc network are willing to participate fully in the protocols of the network. Each node participating in the network should also be willing to forward packets for other nodes in the network.

We refer to the minimum number of hops necessary for a packet to reach from source to destination. We assume that he diameter of an ad-hoc network will be small(5 to 10 hops), but greater than 1. Packets may be lost or corrupted in transmission on the ad-hoc wireless network. A node receiving a corrupted packet can detect the error and discard the packet.

Nodes within the ad hoc network may move at any time without notice, and may even move continuously, but we assume that the speed with which nodes move is moderate with respect to the packet transmission latency and wireless transmission range of that particular network hardware in use. Preemptive DSR can support very rapid rates mobility, but we assume that nodes do not continuously move with high peed, because it may flood data packet in ad-hoc wireless networks. The wireless communications link between each pair of nodes will be bi-directional. But some time the wireless link between two nodes may be uni-directional also.

A. Route Discovery

Step 1: When a source node S wants to send a data, it broadcast the RREQ packet to its neighbor nodes.

Step 2: When an intermediate node on the route to the destination receives the RREQ packet, it appends its address to the route record in RREQ and re-broadcast the RREQ.

Step 3: When the destination node D receives the first RREQ packet, it starts a timer and collects RREQ packets from its neighbors until quantum q time expires.

Step 4: The destination node D finds the two (primary +Backup) best routes from the collected paths (Step 3) within the quantum q time.

Step 5: The destination node D sends RREP packet to the source node S by reversing (RREQ) packets which includes the two routes (Primary + Backup) for further communication.

B. Route Monitoring

Step 1: Each intermediate node on the route starts monitoring the signal strength.

Step 2: If signal strength falls below the specified threshold T, it will send a warning message “Path likely to be disconnected”, to the source node S.

C. The Source node S Communicates with destination node D

Step 1: The source node S starts Communicating with destination node D using primary path.

Step 2: On receiving the warning message from the intermediate node, it starts communicating destination node D with the backup route also.

Step 3: If source node S receives the acknowledgement form the destination node D go to step 4 else step 5.

Step 4: Preemption, switch over from Primary to Backup route.

Step 5: Initiates Route Discovery Process.

D. Prediction Mechanism

The main goal of our approach is to avoid sending unnecessary warning messages. In this work, we consider that anode is in an unsafe or preemptive region if the signal it receives from a predecessor node is below a threshold signal strength *Pt*. Once a node enters this zone, we make at least three consecutive measurements of the signal strength of packets received from the predecessor node, and predict link failure using the Lagrange interpolation. This interpolation has the following general form:

$$y = \sum_{i=0}^{n} \left[\frac{\prod_{\substack{j=0 \\ j=1}}^{n} (x - x_j)}{\prod_{\substack{j=0 \\ j=1}}^{n} (x_i - x_j)} \times y_i \right]$$

We store the power strengths of the three signals and their times of occurrence. When two consecutive measurements give the same signal strength, we store the time of the second occurrence. The expected signal strength *P* of the packets received from the predecessor node is computed as follows:

$$P = \left(\frac{t - t_1) \times (t - t_2)}{(t_0 - t_1) \times (t_0 - t_2)} \times P_0 \right) + \left(\frac{t - t_0) \times (t - t_2)}{(t_1 - t_0) \times (t_1 - t_2)} \times P_1 \right)$$

$$+ \left(\frac{t - t_0) \times (t - t_1)}{(t_2 - t_0) \times (t_2 - t_1)} \times P_2 \right)$$

Where P_0, P_1, P_2 are the measured power strengths at the measurement times t_0, t_1, and t_2, respectively. The time t is the sum of the time needed for discovering an alternative path (Discovery Period), the last measurement time t_2, and the average value of the measurement times t_0, t_1, and t_2. That is:

$$t = t_2 + \left(\frac{t_0 + t_1 + t_2}{3} \right) + \text{Discovery Period}$$

When *P* is lower than the minimum accepted power (-81 dB) a warning message is sent to the predecessor node. This node then starts a local repair procedure to find alternative paths to the destinations reached using the link to the node that sent the warning message.

IV. PERFORMANCE EVALUATION OF PREEMPTIVE DSR IN A BATTLEFIELD SCENARIO

As explained earlier, the Preemptive DSR routing protocol uses a combination of table-driven and reactive methods to achieve optimal performance. It has been found previously, that PDSR achieves a higher packet delivery fraction and lower latency than the table-driven protocols. Further, it also adapts well to node mobility and link changes. In the following sections we describe the experiments carried out to analyze the performance of PDSR in a battlefield scenario. It is found that PDSR achieves high packet delivery fraction, low end to end delay and normalized routing loads in medium size networks with lower mobility of nodes.

Experimental Setup and Metrics

The ns-2 simulator was used for the experiments. We now describe the traffic pattern, the scenario description and the metrics that were used for the experiments.

(i) The traffic pattern

The parameters used were as follows –

Table 1. Traffic pattern

Type of traffic	Constant Bit Rate
Packet Size	512 bytes
Packet Rate	4 pkts/sec
Maximum number of connections	20

(ii) Scenario description

BonnMotion is a Java software which creates and analyses mobility scenarios. It is developed within the Communication Systems group at the Institute of Computer Science of the University of Bonn, Germany, where it serves as a tool for the investigation of mobile ad hoc network characteristics. The scenarios can also be exported for the network simulators ns-2, ns-3, GloMoSim/QualNet, COOJA, MiXiM, and ONE. Several mobility models are supported, namely

- the Random Waypoint model,
- the Random Walk model,
- the Gauss-Markov model,
- the Manhattan Grid model,
- the Reference Point Group Mobility model,
- the Disaster Area model,
- the Random Street model,
- and more.

It generates the movements of nodes in an ad hoc network as a trace file which can be imported into ns-2.

The following metrics were used to depict a battlefield scenario.

Table 2. Parameters for the battlefield scenario

Dimensions	2000*2000
Mobility Model	Reference Point Group Mobility Model (RPGM)
No. of nodes	50
Min. speed	1 m/s
Max. speed	5 m/s
Average number of nodes in a group	10
Probability of group change	0.01
Pause time	60 sec

(iii) Metrics

The following metrics are used for performance evaluation.

(a) Packet Delivery Fraction (PDF)

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation.

$$PDF = \frac{\text{number Of Received Packets}}{\text{number Of Sent Packets}}$$

This estimate gives us an idea of how successful the protocol is in delivering packets to the application layer. A high value of PDF indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance.

(b) Normalized Routing Load (NRL)

This is calculated as the ratio between the no. of routing packets transmitted to the number of packets actually received (thus accounting for any dropped packets).

$$NRL = \frac{\text{number Of Routing Packet Sent}}{\text{number Of Data Packets Received}}$$

This metric gives an estimate of how efficient a routing protocol is since the number of routing packets sent per data packet gives an idea of how well the protocol maintains the routing information updated. Higher the NRL, higher the overhead of routing packets and consequently lower the efficiency of the protocol.

(c) Average end to end delay (AED)

This is defined as the average delay in transmission of a packet between two nodes and is calculated as follows-

$$AED = \frac{\sum_{i=0}^{n} (\text{time PacketReceived}_i - \text{time Packet Sent}_i)}{\text{total Number Of Packets Received}}$$

A higher value of end-to-end delay means that the network is congested and hence the routing protocol doesn't perform well. The upper bound on the values of end-to-end delay is determined by the application. For example multimedia traffic such as audio and video cannot tolerate very high values of end-to-end delay when compared to FTP traffic.

(iv) Research methodology

Three parameters in the battlefield scenario were varied - pause time, the total number of nodes and average number of nodes in a group and their impact on the three metrics described above were studied. The results are discussed in the next section.

V. RESULTS

(i) Effect of varying the number of nodes

The number of nodes was varied from 50 to 100 and the effect on PDF, NRL and AED was studied. The results can be found in table 3 and figures 1, 2 and 3.

It is found that the packet delivery fraction decreases as the number of nodes in the network increases. This is due to the fact that as number of nodes increases, the congestion in the network also increases and hence the number of lost packets due to retransmission also increases. Further, since PDSR uses a table driven approach, the processing delay at the nodes also increases with an increase in the size of the network thereby accounting for the higher end-to-end delay. The normalized routing load increases with an increase in number of nodes due to an increase in the routing packets in the network.

Table 3. Effect of varying the number of nodes

No. of Nodes	Packet Delivery Fraction (%)	Average End-end delay (sec)	Normalized Routing Load
50	99.91347	0.006527167	0.2460694
60	100	0.006546792	0.2977803
70	100	0.013576984	0.42168674
80	99.94656	0.032688957	0.47558385
90	99.96	0.010168137	0.49618322
100	99.873	0.010737591	0.553427

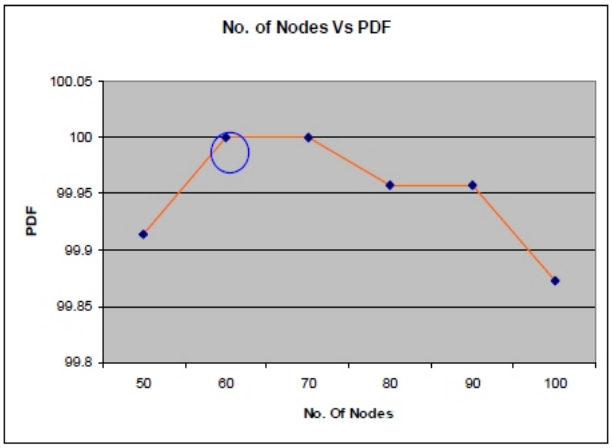

Fig. 1. Effect of varying the number of nodes on the pause time

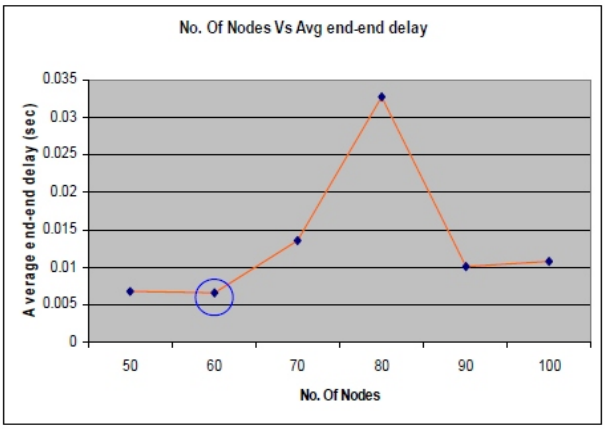

Fig. 2. Effect of varying the number of nodes on the Average end-end delay

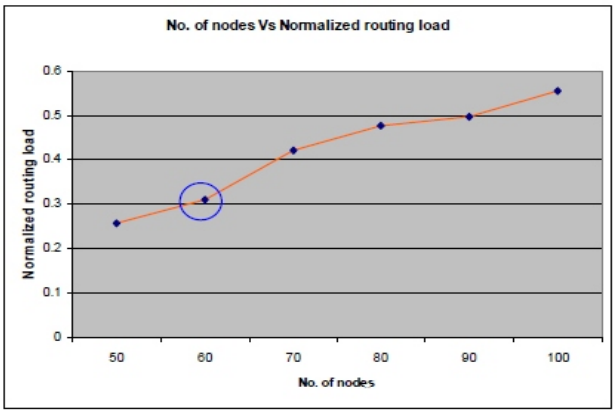

Fig. 3. Effect of varying the number of nodes on the Normalized Routing Load

The blue circles in figures 1, 2 and 3 represent the "optimal points" which corresponds to the highest PDF, lowest end-to-end delay and the lowest normalized routing load. It is found that for 60 nodes we achieve this optimal point.

(ii) Effect of varying the pause time

The effect of varying the pause time on the three metrics are shown in table 4 and the corresponding graphs are shown in figures 4,5 and 6. It can be inferred that as pause time varies, the packet delivery fraction also increases. This is due to the fact that as pause time increases, the relative mobility of the nodes decreases, and hence the congestion also decreases in the network. The end-to-end delay also decreases as the pause time is increased. This can be explained as follows – as the pause time increases, the network topology is relatively stable and hence the number of stale routes in the routing tables decreases. Thus route

discovery and maintenance take less time. This also reduces the number of routing packets in the network, thereby decreasing the NRL.

Table 4. Effect of varying the pause time

Pause Time (sec)	Packet Delivery Fraction (%)	Average End-end delay (sec)	Normalized Routing Load
10	99.87218	0.006748153	0.25597268
20	99.96	0.006743255	0.25531915
30	99.924	0.006523045	0.25412962
40	100	0.010312819	0.27754056
50	100	0.010314601	0.2742616
60	99.9132	0.006738278	0.2570694

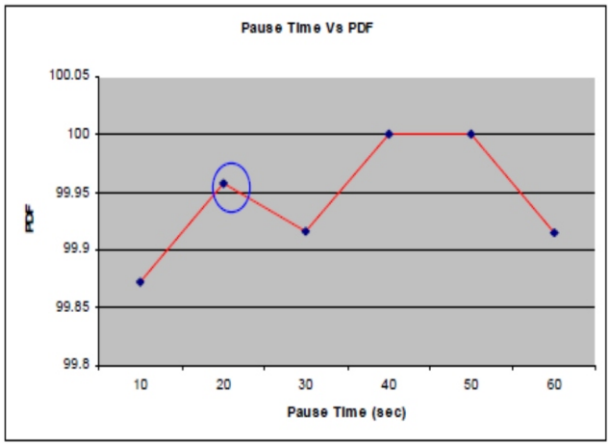

Fig. 4. Effect of varying the pause time on PDF

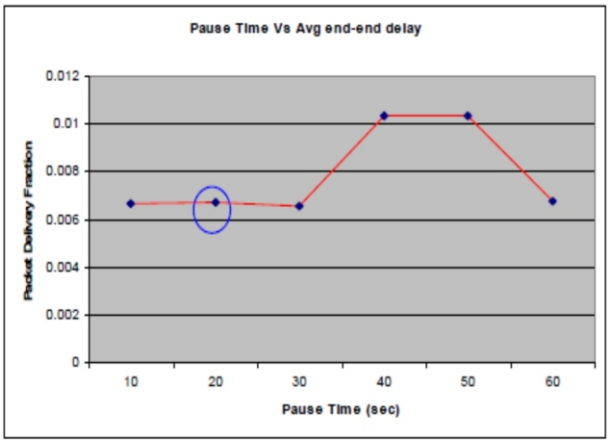

Fig. 5. Effect of varying the pause time on average end to end delay

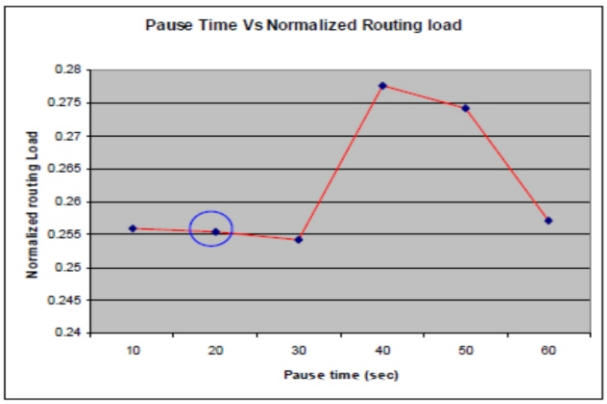

Fig. 6. Effect of varying the pause time on NRL

From figures 4, 5 and 6 it can be inferred that for a pause time of 20 sec (represented by a blue circle), we obtain optimal values for the three metrics.

(iii) Effect of varying the average number of nodes

The effect of varying the average number of nodes on the three metrics is shown in table 5.The graphs for the three metrics are shown in figures 7,8 and 9.

Table 5. Effect of varying the average number of nodes

Age No. of Nodes	Packet Delivery Fraction (%)	Average End-end delay (sec)	Normalized Routing Load
5	100	0.011443271	0.2754056
6	99.96	0.015179819	0.2982732
7	99.924	0.006548823	0.25467707
8	100	0.006707324	0.2575447
9	99.87288	0.018596672	0.3182011
10	99.921	0.006738278	0.2530694

From figure 4.9 it can be inferred that the PDF decreases as the average number of nodes in a group is decreased. This is due to the face that as the average number of nodes increases, the density increases, thereby causing more congestion in the network. Since PDSR uses HELLO messages for neighbor detection, as the node density increases, the number of such packets also increases, thereby decreasing the PDF.

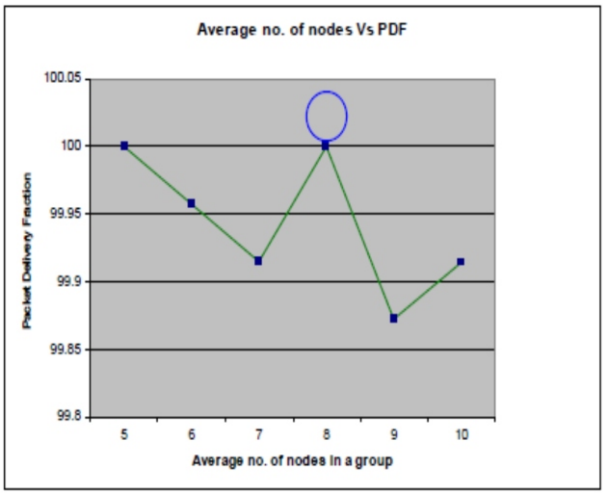

Fig. 7. Effect of varying the average number of nodes on the PDF

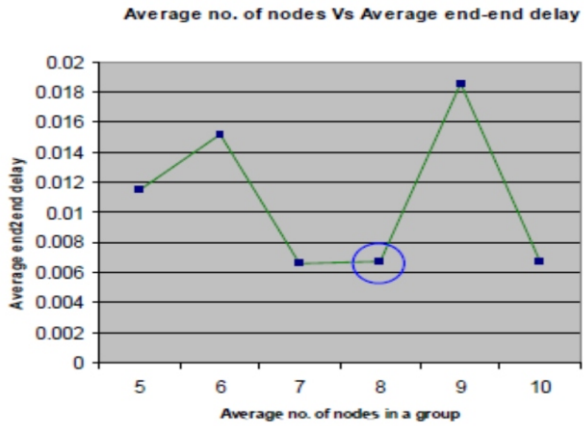

Fig. 8. Effect of varying the average number of nodes on the AED

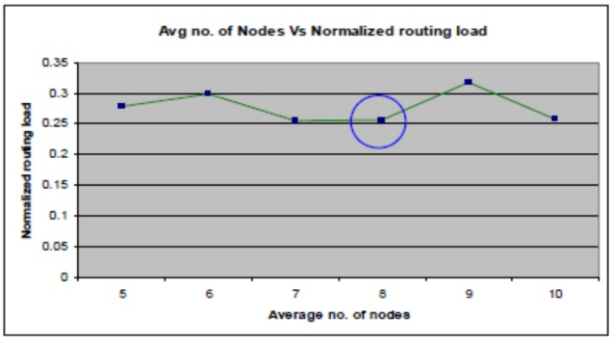

Fig. 9. Effect of varying the average number of nodes on the NRL

The effect of increasing the average number of nodes on the average end-to-end delay is shown in figure 8. It is found that the delay decreases the density increases, thereby indicating that PDSR scales well to the network density. Further by not using source routing, it achieves lower latency due to a lesser packet overhead.

Figure 8 shows the effect of varying the average number of nodes in a group on the routing load. In general, PDSR has less routing overhead achieving a peak load of about 0.32 when the average number of nodes in a group is 9 (represented by blue circles in the graphs). From the graphs, it can be inferred that the optimal point corresponds to 8 nodes per group.

V. CONCLUSION

For the battlefield scenario, PDSR has found to perform well for lower pause times (20 sec), higher density of nodes (9 per group) and smaller networks. As the network size increases, the performance drops due to a table-driven approach. However, since it does not use source routing, it has a much lower end to end delay for In order to analyze the performance of routing protocols in practice, such a scenario-based approach is vital. It also helps identify the suitable routing protocol for an optimal network size, the mobility of the nodes, the network density and a given traffic pattern.

A more comprehensive study of other routing protocols such as DSR, TORA, DSDV, etc. is needed to choose the right protocol for a given scenario.

REFERENCES

[1] C. Siva Ram Murthy, B.S. Manoj, "*Ad Hoc Wireless Networks : Architectures and Protocols", Prentice Hall publishers, May 2004, ISBN 013147023X*

[2] C.-K. Toh, "*Ad Hoc Mobile Wireless Networks: Protocols and Systems", Prentice Hall publishers, December 2001, ISBN 0130078174*

[3] Haas Z.J, " *A new routing protocol for the reconfigurable wireless network". In Proceedings of the 1997 IEEE 6th International Conference on Universal Personal communications, ICUPC '97, San Diego, CA, October 1997; pp.562--566.*

[4] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding royer. *"A Secure Routing Protocol for Ad Hoc Networks" (ARAN) In International Conference on Network Protocols (ICNP), Paris, France, November 2002.*

[5] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, "*Mobile Ad Hoc Networking*", ISBN: 0-471-37313-3, Wiley-IEEE Press: *Chapter 12: Ad hoc networks Security Pietro Michiardi, Refik Molva*

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "*Routing Security in Wireless Ad Hoc Network*," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[7] Yih-Chun Hu, David B. Johnson, Adrian Perrig. *"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp: 3-13, Jun 2002.*

[8] V.Ramesh, Dr.P.Subbaiah, K.Sangeetha Supriya "Modified DSR (Preemptive) to reduce link breakage and routing overhead for MANET using Proactive Route Maintenance (PRM)" in the Global Journal of Computer Science and Technology, vol.9, issue 5, January 2010, pp 124-129.

Mr.V. Ramesh received his B.Tech from N.B.K.R.I.S.T, Vidyanagar, AP in Computer Science & Engineering and M.Tech in IT from Sathyabama University, Chennai. Presently he is working as Associate Professor in the department of Computer Science & Engineering at Sree Vidyanikethan Engineering, Tirupati, AP. He has published several papers in various International & National Conferences and Journals. Presently he is pursuing his Ph. D in the field of Ad-hoc networks at Sathyabama University, Chennai. His research interests include Operating Systems, Computer Networks and MANETs.

Dr P. Subbaiah received M.Tech(D.S.C) from JNTU and Ph. D from S.K University, Ananthapur in the area of fault tolerant systems. He has published several papers in international, national conferences and journals. He guided 6 research scholars. Presently he is working as Professor in ICE, Sree Sai Ram Engg. College,West Tambaram, Affiliated to Anna University, Chennai, India. His research interests include Mobile ad-hoc networks, Digital image processing and VLSI design.