IMPROVED NETWORK CONNECTIVITY IN MANETS

B R Sujatha [1], M V Satyanarayana [2]
[1] Assistant Professor [2], Professor
Dept of E&C, Malnad College of Engg, Hassan
Email: brs_hsn@rediffmail.com

Abstract:

The growth in wireless communication technologies has resulted in a considerable amount of attention given to mobile adhoc networks. All mobile hosts in an adhoc network are embedded with packet forwarding capabilities. It is decentralized and is independent of infrastructure. Since mobile hosts in an adhoc network usually move freely, the topology of the network changes dynamically and disconnection occurs frequently. These characteristics require the routing protocols to find an alternative path towards the destination for data transfer. The existing on-demand routing protocols does the alternative path establishment only after the disconnection of links in the existing path. The data sent by the source during alternate path establishment period will be lost leading to incomplete data transfer. The network traffic will therefore increase considerably. This problem can be overcome by establishing an alternative path when the existing path is more likely to be broken, by sending a warning message to the source indicating the likelihood of disconnection. In this paper an attempt has been made to analyze a protocol that improves the network connectivity by preempting the alternative path before the existing link gets failed by monitoring the signal strength and 'age of the path'.

Keywords:

Mobile Adhoc Networks (MANETs), Dynamic Source Routing (DSR), Preemptive routing

1 INTRODUCTION

In recent days, connectivity with mobility is in great demand. This has given boost to lot of research in the field of adhoc networks. MANETs are self-organisable, infrastructure less, wireless, peer-peer, multi hop networks. They adopt distributed control in providing connectivity from the source to the destination. Therefore the mobile units themselves need to take the responsibility of discovering its nearest neighbors who are ready to route data packets to the destination. Co-operation among all the mobile nodes is very essential in such cases. [1, 2].Typical applications of these networks are outdoor events such as conferences, concerts and festivals, places with no network infrastructure, outdoor emergencies and natural disasters and military operations. A typical adhoc network is as shown in figure 1, which depicts its dynamic topology.

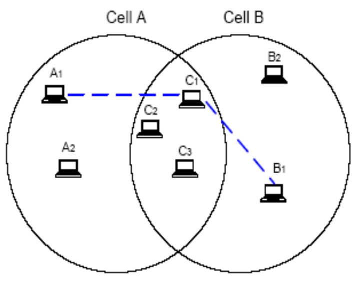

Fig 1 A Typical Adhoc Network

If a node A1 wants to send a data packet to node B1, it can do so via node C1, which is in the common range of both the nodes. However if C1 moves away and is beyond the range of A1, the link is broken and a different route has to be established.

In the literature, routing protocols are broadly classified into three categories viz proactive, reactive and hybrid protocols. Proactive protocols are also known as table driven protocols in which the route to each destination in the network is stored in tables. Hence when a data packet is to be transferred, the node will refer to its routing table to determine a route towards the destination [3, 4]. An example for this type of routing is Destination Sequenced Distance Vector (DSDV). In reactive protocols, which are also known as on demand routing protocols, the path towards the destination is discovered as and when it is required. DSR (Dynamic source routing) and AODV (Adhoc on demand vector) come under this category [5, 6, 7]. Hybrid protocols combine the advantageous features of both proactive and reactive protocols. CEDAR (Core Extracted Distributed Adhoc Routing) is one such protocol [8, 9].

On demand protocols are proved to perform better. But the major drawback of such protocols is that the alternate route discovery process is initiated only after the existing link has been reported as broken. This may considerably increase the network traffic as the data sent during the transition period will be lost and will have to be retransmitted [10]. This problem can be overcome by slightly modifying the existing on-demand protocols. Preemptive routing protocol is one such protocol [11, 12].

In preemptive routing, alternate route discovery process is initiated in anticipation of a link failure. This can be done by examining the signal strength continuously and the age of the path at regular intervals. Once the signal strength falls below a threshold or the age of the path increases beyond a threshold value, the process of route discovery will be initiated.

The rest of the paper is organized in various sections as follows. Section 2 highlights the previous works done on routing in MANETs, in particular Dynamic Source Routing (DSR). Section 3 describes the Preemptive routing protocol. Section 4 provides a comparison of the preemptive protocol with the traditional on-demand protocol using simulations. Finally section 5 gives the conclusion and the possible future work.

2 PREVIOUS WORKS

Routing plays a vital role in MANETs. The dynamic nature of the network along with the wireless communication poses many challenges on the routing protocols. Many proposed routing protocols for adhoc networks operate in an on-demand fashion. Dynamic Source Routing (DSR) is a routing protocol adapted for MANETs with dynamic topology due to frequent movement of the nodes in the network [13]. DSR has two phases viz. route discovery and route maintenance.

2.1Route Discovery

This is a process of determination of a suitable route to the destination. To perform route discovery, the source node broadcasts a *route request* packet with a recorded source node addresses. Each node that hears the route request forwards the request (if appropriate), adding its own address to the recorded source route field in the packet. The route request packet propagates hop-by-hop outwards from the source node until either the destination node is found or until another node is found that can offer a route to the destination [13].

A node will forward the route request if it is not the destination node and if it is not already listed as a hop in the route. When a node wishes to send a packet, it examines its own route cache and performs route discovery only if no suitable source route is found. Further, when a node receives a route request for which it has a route in its cache, it does not propagate the route request but instead returns a *route reply* to the source node. The route reply contains the full concatenation of the recorded route from the source and the cached route leading to the destination. Naturally, if a route request packet reaches the destination node, the destination node returns a route reply packet to the source node with the full source to destination path listed.

2.2 Route Maintenance

Conventional routing protocols integrate route discovery with route maintenance by continuously sending periodic routing updates. If the status of a link or node changes, the periodic updates will eventually reflect the change in all other nodes, presumably resulting in the computation of new routes. If a node along the path of a packet detects an error, the node returns a *route error* packet to the sender. The route error packet contains the addresses of the nodes at both ends of the hop in error. When a route error packet is received or overheard, the 'hop in error' is removed from any route caches and all routes which contain this hop must be truncated at that point. Route maintenance can also be performed using end-to-end acknowledgments rather than the hop-by-hop acknowledgments described above [13].

In DSR, an alternative path discovery is initiated only after the path disconnection due to a link failure. This will result in loss of a number of data packets. Therefore there is a need to modify the conventional DSR protocol.

3 PREEMPTIVE ROUTING

Conventionally, a change of path occurs in networks when: (i) a link along the path fails or (ii) a shorter path is found. A link failure results in multiple retransmissions being required to detect the failure and a new path has to be found and used as in on-demand routing. In MANETs, as the network topology frequently changes, path disconnections occur and this proves to be very costly.

As soon as a chance of link failure is identified, the preemptive routing invokes the routing algorithm to discover an alternative path before the actual link failure occurs. Thus, the connectivity of the network can be improved. This technique is similar to the soft handoffs in mobile telephone networks. The route maintenance algorithm is as follows:(i) Detect the path which is more likely to be broken (ii) Invoke routing algorithm to discover an alternate path. (iii) Continue the transmission with the new path [14].

The key factor in the algorithm is to decide, when to rediscover a new path. This can be done on the basis of the quality of the path which may incorporate several criteria such as signal strength, age of the path, the number of hops to the destination etc. In this paper, we have considered two 'path quality' parameters viz the *signal strength* and the *age of the path*. As the link failures in adhoc networks can be attributed to node's mobility, signal strength measurement provides estimate of nodes ability to converse with each other. However, signal variations due to fading and other temporary disturbances may generate erroneous signals resulting in unnecessary new path discoveries and increasing the path overheads. The other parameter, the *age of the path* also plays a vital role in deciding the maintenance of existing paths. As the age of the path increases (under conditions of low mobility) with the same set of nodes participating in data transmission, there are chances of these nodes failing because of battery drain. Hence, if the age of the path increases beyond a threshold, inspite of the path being active, an alternate path with more number of nodes (may or may not be) has to be discovered to avoid the total drain of the batteries of the intermediate nodes. Although this method increases the network control traffic required for new path discoveries, it improves network connectivity.

3.1 Generating the Warning Message based on Signal Strength

The threshold value selected to generate warning plays a vital role in defining the efficiency of this algorithm. If the value is too small, there may not be sufficient time to discover a new path before the existing link is broken. On the contrary, if it is too high then unnecessary route discoveries will be done increasing network control traffic. Hence, a trade off has to be made in deciding an optimal threshold value for new path/route discovery.

A Preemptive region is defined around every node as shown in the figure 2 for node A. As soon as node C enters the preemptive region, a warning message is sent to the sender node A. Then the node A initiates a route discovery process. With the establishment of a new route, data transmission is continued along this new route. The time required to discover a new path can be termed as recovery time T_{rec}. Hence the time between the warning and the path break T_{warn} should be atleast or slightly greater than T_{rec}.

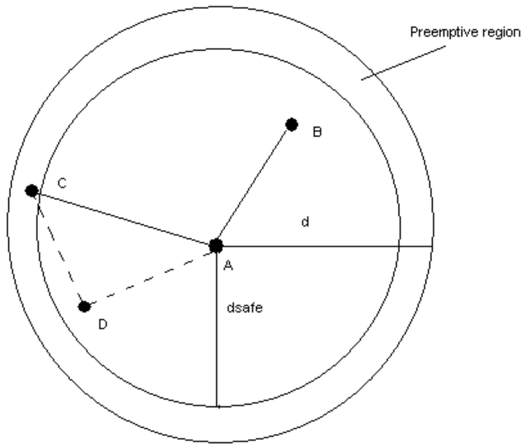

Figure 2: Preemptive Region

In order to determine the optimal range, it is necessary to exchange the location and velocity information of the nodes amongst all the nodes depending on the receiver signal power. The receiver signal power,

$$P_r = P_0 / r^n$$

at a distance r from the transmitter, where P_0 is the transmitted power and path loss exponent n is typically between 2 and 4.

The minimum power receivable by the device is the power at the maximum transmission range,

$$P_d = P_0 / d^4$$

Similarly, the preemptive signal power threshold is the signal power at the edge of the preemptive region. In addition, for a preemptive region of width of w, the signal power threshold is

$$P_{safe} = P_0 / d^4_{safe}$$

Where d_{safe} is equal to (d- w) and w=relative speed*T_{warn}

The preemptive ratio α is defined as $\alpha = P_{safe} / P_d = range / (range - w)$

In reality, the received signal power may experience sudden fluctuations due to channel fading and multipath effects which will trigger a false warning, causing unnecessary route request floods. This may result in lower quality routes being initiated and also increasing the routing overheads. In cellular networks, an exponential average of the signal power is used to verify that the signal power drop was not due to fading. However, if the traffic is bursty or infrequent, the preemptive region may be fully crossed by the time enough packets are received to drop the average below the threshold. Therefore quicker power estimates can be achieved by sending a warning whenever the instantaneous power drops below the threshold and checking the warning packet received power when it is received by the source. If the warning packet power is also below the threshold, there is a good probability that the warning is real.

3.2 Generating the Warning Message based on 'Age of the Path'

With transmissions being done along the same path, relay nodes will experience a continuous drain of their battery power for the same source destination pair which may result in path failure. Therefore alternate route discoveries are required before the onset of failure.

Nodes keep a record of their most recent encounter times with all other nodes. With a path discovery being made, the source node sets a timer. The preemptive warning is generated based on two parameters- Age of the path defined as the time difference T_{age} between the transmissions of two consecutive route discovery packets from the source to the same destination and threshold value Γ is defined for the age of the path. As long as T_{age} is lesser than Γ, data transmission can be continued on the same path. When the timer value exceeds the threshold Γ, a warning message is generated leading to a new path discovery. However this new path may or may not be the shortest path to the destination. The choice of the threshold depends on node density of the network. If the node density is small with lesser number of paths available, Γ must be large.

4 SIMULATION RESULTS

The following assumptions were made for carrying out simulation [15, 16].

- The discrete event network simulator NS-2 has been used for analysis and comparison of the adhoc routing protocols.
- The mobility model uses the *random waypoint model* in a rectangular field.
- The mobile node movement is restricted to a square cell of 600 X 600m containing 70 nodes.
- A 512-byte User Datagram Protocol (UDP) generated by a constant bit rate (CBR) traffic source is used.
- Simulation lasts for 600 seconds.

A comparison of preemptive routing with the traditional DSR algorithm is discussed here.

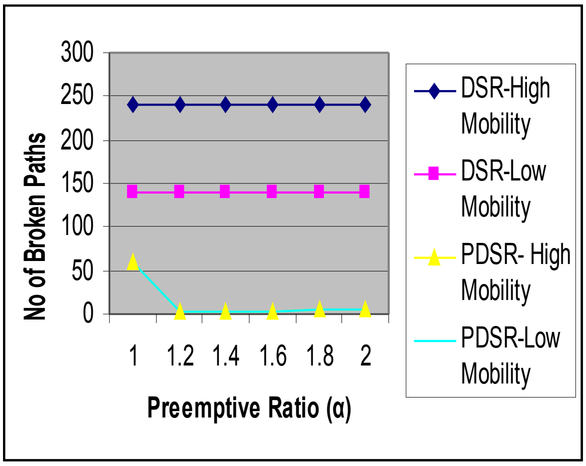

Figure 3: Comparison wrt to Broken Paths

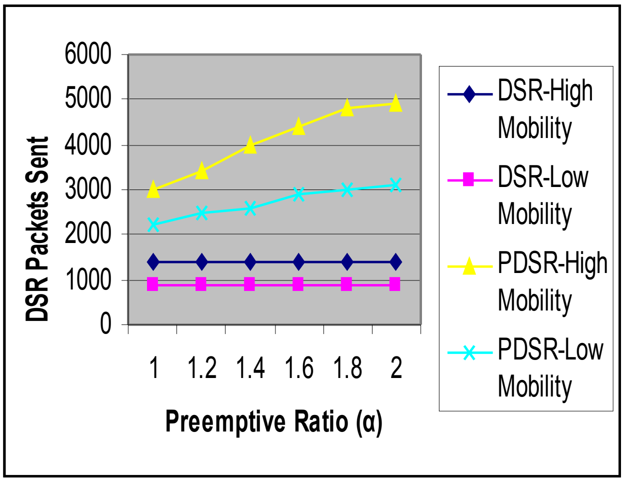

Figure 4: Comparison wrt to Routing Overheads

The direct effect of preemptive routing can be seen by examining the number of broken paths (Figure 3). The horizontal lines on each figure correspond to conventional DSR (with no modifications whatsoever) under high mobility and low mobility conditions.

Figure 4 shows the overhead of PDSR compared to DSR. While the overhead is higher, it can be noted that most of the overhead was experienced also by the non-preemptive version of PDSR but with increased network connectivity.

The effect of number of active nodes with respect to the simulation time is as shown in figure 5. It can be seen that if the threshold is small, number of active nodes will be more as new routes will be initiated before the node's battery gets drained completely.

.

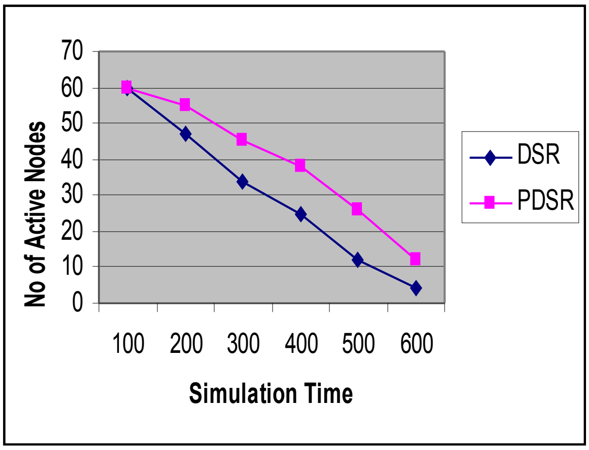

Figure 5: Comparison wrt to Number of Active Nodes

The effect of packet loss with reference to various node densities is as shown in the figure 6. It is clear that at low node densities the packet loss will be more as there will be less chances of having an alternative path using the available limited number of nodes. As the node density increases there will be more routes possible for the same destination resulting in the decrease in the packet loss.

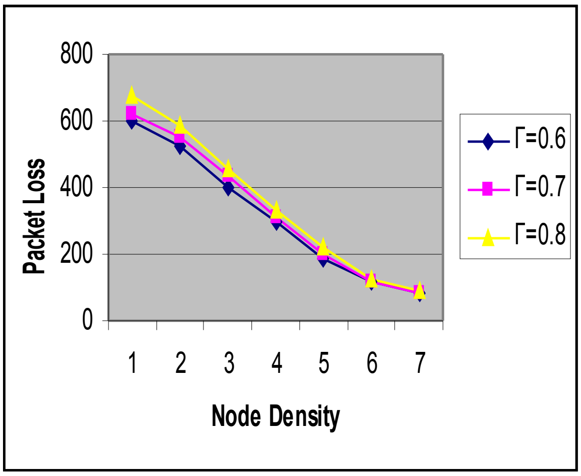

Figure 6: Comparison wrt to Packet Loss

5 CONCLUSIONS

In this paper, an attempt has been made to improve the data connectivity in the network by preemptively selecting an alternate path as soon as the signal strength falls below the threshold value and the age of the path exceeds the predefined threshold. An analysis of preemptive protocol is made with the DSR algorithm.

The performance of the preemptive algorithm is dependent on the preemptive ratio α. It is clear from the analysis that preemptive algorithm performs better than DSR. But the offered load on the network is more in preemptive protocol as continuously the signal strength and the age of the path has to be examined and warning messages are to be sent back immediately.

As a part of future work, this algorithm can be implemented over energy aware routing protocols available in the literature.

ACKNOWLEDGEMENT

The authors would like to thank everyone, including the anonymous reviewers.

REFERENCES

[1] B. Cameron Lesiuk, *"Routing in Adhoc Networks of Mobile Hosts"*, MECH 590, Directed studies with Dr.Gerard McLean, December 2, 1998

[2] Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, *"A Review of Routing Protocols for Mobile Adhoc Networks",* Elsevier, Ad Hoc Networks 2004

[3] C Siva Ram Murthy and B S Manoj, *"Adhoc Wireless Networks-Architectures and Protocols"*, Pearson education, 2004

[4] Ismail Ari, Neelu Jethani, Aniruddha Rangnekar, Sushma Natarajan, *"Performance Analysis and Comparison of Adhoc Routing Protocols"*, IEEE transaction on Mobile Computing, 2000

[5] Elizabeth M. Belding-Royer, Charles E. Perkins, "*Evolution and Future Directions of the Adhoc On- demand Distance Vector RoutingPprotocol*", *Elsevier, Adhoc Networks* 2003

[6] C E Perkins and E M Royer, *"On- demand Distance Vector Routing"*, Proceedings, IEEE workshop on mobile computing systems and applications, February, 1999

[7] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, *"A Performance Simulation for Route Maintenance in Wireless Ad Hoc Networks"*, ACM,2004

[8] B R Sujatha, K S Shivaprakasha, Siddiq Iqbal, M V Satyanarayana, "*A Comparative Study of Routing Protocols in Mobile Adhoc Networks*", Proceedings of National Conference on VLSI design, Signal processing and Communication, NCVSPCom-2007,pp 148-151

[9] T. Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj, C. Siva Ram Murthy," *Quality of service Provisioning in Ad hoc Wireless Networks: A Survey of Issues and Solutions*", Ad Hoc Networks 4 (2006) 83–124, Elsevier

[10] K S Shivaprakasha, B R Sujatha, Siddiq Iqbal, *"Performance Analysis of Routing Protocols in MANETs"*, Proceedings of National Conference on Recent Trends in Electronics and Communication, Kurnool, AP, pp 35-39

[11] T. S. Rappaport, "*Wireless Communication Systems",* Prentice Hall, 1996.

[12] M C Domingo, D Remondo and O. Leon, *"A Simple Routing Scheme for Improving Adhoc Network Survivability"*, GLOBECOM, IEEE, 2003

[13] D B Johnson and D A Maltz, *"DSR-The Dynamic Source Routing Protocol for Multihop Wireless Adhoc Networking"*, Charles E, Perkins,Addison Wesley,2001

[14] Tom Goff, Nael B. Abu-Ghazaleh, Dhananjay S. Phatakand Ridvan Kahvecioglu *"Preemptive Routing in AdHoc Networks"*, ACM SIGMOBILE 7/01 Rome, Italy

[15] NS-2: Network Simulator

[Courtesy: http:// www.isi.edu/ nsnam/ns/]

[16] Kevin Fall Kannan Varadhan, "*The ns Manual*"
[Courtesy: http://www.isi.edu/nsnam/ns/ns-documentation.]

Authors

Ms. Sujatha.B.R is a Ph.D student and also working as Assistant Professor in the Department of Electronics and Communication at Malnad College of Engineering, Hassan, India. She received her ME degree in Electrical Communication Engineering from Indian Institute of Science, Bangalore and BE degree from University of Mysore. Her research spans Wireless Communication, Computer Networks and Ad Hoc Networks.

Dr. M V Sathyanarayana is Professor in the Department of Electronics and Communication at Malnad College of Engineering, Hassan, India. He received his Ph.D degree in Electrical Communication Engineering from Indian Institute of Science, Bangalore, MTech from National Institute of Technology, Karnataka and BE degree from University of Mysore. His research spans Optical Communication, Computer Networks, Ad Hoc Networks and Data Mining.