

Preemptive Routing Algorithm to Reduce Link Breakage and Routing Overhead for Ad-Hoc Networks Using PRM

Anjaneyulu K
Asst.Prof & HOD-MCA
Sai Institute of Technology & Science
Rayachoty, Kadapa(dt).

Ramana V V
Assoc.Prof. & HOD,CSE
Sri Sai Institute of Technology & Science
Rayachoty, Kadapa(dt).

Mohammad Rafi G
M.Tech(CSE)
Sri Sai Institute of Technology & Science
Rayachoty, Kadapa(dt).

Abstract- Dynamic Source Routing Algorithm is simple and best suited for high mobility nodes in wireless ad hoc networks. Due to high mobility in ad-hoc network, route may not exist for long time. Hence, DSR algorithm finds an alternative route when the existing communicating route goes down. It becomes a time consuming process if the communicating route fails frequently. In order to avoid this, we propose a modification to the existing DSR protocol. The source node can perform a pro-active route rebuild to avoid disconnection. Intermediate nodes in the route continuously monitor the signal strength at the time of communication, based on a predefined threshold signal value. Intermediate node sends a message to the source. If source receive this message it starts using backup route and if back route also fails then it finds alternative route. The backup route will minimize the time consuming process of finding an alternative route to some extent. Experiments demonstrate that adding link breakage prediction to DSR can significantly reduce the total number of dropped data packets (by at least 25%). Simulation results shows the probability of the communication breakage decreases when parallel routes are used and comparisons between DSR and Modified DSR(Preemptive Version) with respect to no. of broken paths and routing overhead.

Keyword: *ad-hoc network, Dynamic Source Routing Algorithm, Preemptive Version.*

I. INTRODUCTION

There are currently two variations of mobile wireless networks. The first is known as infrastructure network. 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 unit travels out of range of one base station into the range of another, a "handoff" occurs from the old base station to the new, allowing the mobile to be able to continue communication seamlessly throughout the network. Typical applications of this type of network include office wireless local area networks (WLANs). The second type of mobile wireless network is the mobile ad-hoc network or MANET. Unlike infrastructure network, this type of network needs no base station. Mobile nodes communicate to each other by either directly or through intermediate nodes. Ad-hoc network becomes popular since it can be applied in many situations, such as emergency search-and-rescue operations, classroom, meetings or conference and many more. To facilitate communication within the network, routing protocols used to discover routes between nodes. Building a MANET routing protocol is not an easy job, since efficiency and correctness becomes the main concern. Some approach had been proposed to make routing protocol becomes efficient and correct. Routing protocols in MANET, generally, can be categorized as table-driven and on-demand.

II. ROUTING PROCEDURE

DSR algorithm is simple and best suited for high mobility nodes in wireless ad hoc networks. Due to high mobility in ad-hoc network, route may not exist for long time. Hence, DSR algorithm finds an alternative route when the existing communicating route goes down. It becomes a time consuming process if the communicating route fails frequently. In order to avoid this, we propose a modification to the existing DSR protocol. In this paper, we add a link breakage prediction algorithm to the Dynamic Source Routing (DSR) protocol.

The mobile node uses signal power strength from the received packets to predict the link breakage time, and sends a warning to the source node of the packet if the link is soon-to-be-broken. The source node can perform a pro-active route rebuild to avoid disconnection. Intermediate nodes in the route continuously monitor the signal strength at the time of communication, based on a predefined threshold signal value. Intermediate node sends a message to the source node that the route is likely to be disconnected, if signal strength falls below the threshold value. If source

receive this message it starts using backup route and if back route also fails then it finds alternative route. Experiments demonstrate that adding link breakage prediction to DSR can significantly reduce the total number of dropped data packets (by at least 25%).

Dynamic Source Routing

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. It is based on the concept of source routing, a routing technique in which the sender of the packet determines the complete sequence of the nodes through which to forward the packet. The sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. When a mobile node wants to send a packet to some destination, it first checks its route cache to determine whether it already has a route to the destination. If it has one, it will use this route to send the packet. Otherwise, it will initiate route discovery by broadcasting a route request packet. When receiving a request packet, a node appends its own address to the route record in the route request packet if it did not receive this request message before, and re-broadcasts the query to its neighbors. Alternatively, it will send a reply packet to the source without propagating the query packet further if it can complete the query from its route cache. Furthermore, any node participating in route discovery can learn routes from passing packets and gather this routing information into its route cache. When sending or forwarding a packet to a destination, Route Maintenance is used to detect if the network topology has changed such that the link used by this packet is broken. Each node along the route, when transmitting the packet to the next hop, is responsible for detecting if its link to the next hop has broken. When the retransmission and acknowledgement mechanism detects that the link is broken, the detecting node returns a Route Error packet to the source of the packet. The node will then search its route cache to find if there is an alternative route to the destination of this packet. If there is one, the node will change the source route in the packet header and send it using this new route.

This mechanism is called "salvaging" a packet. When a Route Error packet is received or overheard, the link in error is removed from the local route cache, and all routes which contain this hop must be truncated at that point. The source can then attempt to use any other route to the destination that is already in its route cache, or can invoke Route Discovery again to find a new route.

Disadvantages

When the retransmission and acknowledgement mechanism detects that the link is broken, the detecting node returns a Route Error packet to the source of the packet. 2. When a Route Error packet is received or overheard, the link in error is removed from the local route cache, and all routes which contain this hop must be truncated at that point. The source can then attempt to use any other route to the destination that is already in its route cache, or can invoke Route Discovery again to find a new route 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.

III. PROACTIVE ROUTE MAINTENANCE

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 the diameter of an ad-hoc network will be small(5 to 10 hops), but greater than 1. Packets

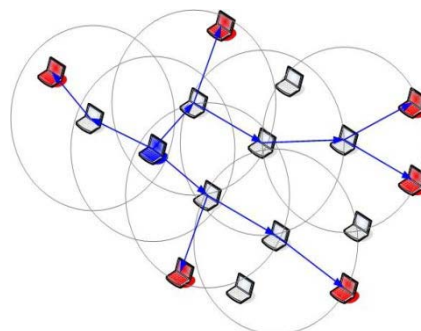


Figure 1: Proactive Route Maintenance in MANET

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. The GPS and signal strength methods both use physically measured parameters to predict the link status. The signal strength method only consumes receiving node's computing power, and does not depend on any additional device. It is used in this paper. At first we assume that the sender power level is constant. Received signal power samples are measured from packets received from the sender. From this information it is possible to compute the rate of change for a particular neighbor's signal power level. Because the signal power threshold for the wireless network interface is fixed, the time when the power level drops below the acceptable value can be computed. Characteristics of PRM include: Freshness. All nodes near an active route have the up-to-date routing information. Broken paths are eliminated, new paths recognized, and non-optimal paths replaced by optimal ones. Robustness. An active node that is forwarding data packets usually maintains several fresh alternative paths. After one path fails, the data packet is usually forwarded via another path without causing packet loss or extra delay.

PRM will resort to a route discovery operation only after all alternative paths have failed. Lightweight maintenance, Unlike in existing proactive routing protocols, the route maintenance is confined to those small areas surrounding active routes, where control packets make only a small portion of data transmission. As the lifetime of a route is lengthened, the overhead of the proactive route maintenance can be compensated by the less frequent route discovery operations. The proposed Concept is illustrated using the following example.

IV. MULTIPLE ROUTES

The Use of multiple routes parallel, instead of a single route at a time, can be to improve the ongoing communication between the two ends. The source node will use each of these routes alternatively to send packets to the destination node. Use of multiple routes reduces the dependency on a single route, which results in more stable communication. This is because, if a single route fails, we need to again initiate the Route Discovery process. However, if multiple routes are used, when one route fails, another route can be used. Only when all the routes fail, the Route Discovery is to be done to search a new route. Here it should be noticed that the use of multiple routes is different from the backup route theory of DSR. In the backup route approach, the source node uses the primary route for communication and keeps a backup (secondary) route in its route cache. Whenever the primary route fails, the backup route is used. The problem with this approach is that, while the source is still using the primary route, the backup route might fail and the source would remain unaware of that. If after some time the primary route fails and the source node switches to the backup route, it discovers that the backup route has been already broken. But if multiple routes are used in parallel, the source node will be informed of the route failure immediately whenever it occurs. Thus, the source node will never attempt to use a stale route.

Algorithms and Flowcharts

Proactive Routing Design Algorithm

When a source node S want to send message to the destination node D, it initiates route discovery by broadcasting the RREQ packet to its neighbors (A, E, F) as shown in Fig 3. The intermediate nodes (A, E, F) on receive the RREQ packet rebroadcast the packet to its neighbors by appending its id in the route record of the RREQ packet. Similarly, other intermediate nodes also forward the RREQ packet to the destination. When the destination node D receives two or more RREQ packets from the same source through different routes, it finds the two best routes based on the no of hops. The route which has least number of hops. The route which has least number of hops it becomes primary<S, F, G>, and second least number of hops route becomes backup route<S, A, B, C>. The destination node D sends Route Reply (RREP) packet using the Primary (<S, F, G>) and Backup (<S, A, B, C>) route as shown in the following Fig. Each RREP packet contains the Primary as well as the Backup route information. When source node S receives first RREP packet form destination, it treats this is the primary route and wireless communication is more error prone compared to wired network. To improve the reliability we are sending route reply (primary + backup routes information) through the primary and the secondary route. If any one packet gets corrupted at the time of transmission, source must be able to use the other packet.

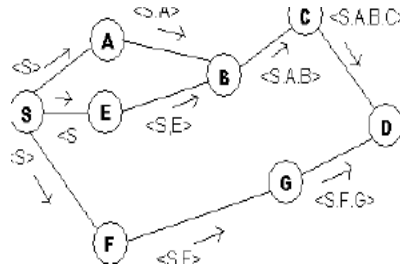


Figure 2: Proactive Routing Design

Route Discovery Broadcasting Using RREQ

When a source node S want to send message to the destination node D, it initiates route discovery by broadcasting the RREQ packet to its neighbors (A, E, F). The intermediate nodes (A, E, F) on receive the RREQ packet rebroadcast the packet to its neighbors by appending its id in the route record of the RREQ packet. Similarly, other intermediate nodes also forward the RREQ packet to the destination. When the destination node D receives two or more RREQ packets from the same source through different routes, it finds the two best routes based on the no of hops. The route, which has least number of hops. The route which has least number of hops it becomes primary<S, F, G>, and second least number of hops route becomes backup route<S, A, B, C>. The destination node D sends Route Reply (RREP) packet using the Primary (<S, F, G>) and Backup(<S, A, B, C>) route as shown in the following Fig. Each RREP packet contains the Primary as well as the Backup route information. When source node S receives first RREP packet form destination, it treats this is the primary route and wireless communication is more error prone compared to wired network. To improve the reliability we are sending route reply (primary + backup routes information) through the primary and the secondary route. If any one packet gets corrupted at the time of transmission, source must be able to use the other packet

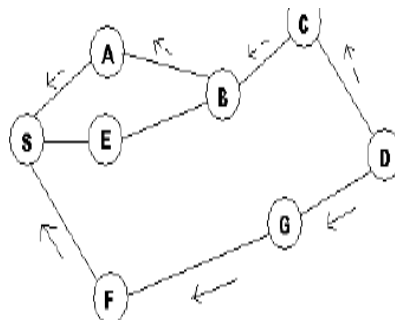


Figure 3: Route Discovery Broadcasting Using RREQ

Route Discovery Algorithm

- 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.

Primary Route Design

Primary Route:
 {<S.F.G> + {<S.A.B.C>}}
 Backup Route: {<S.A.B.C>+{<S.F.G>}}

The communication between the source node S and destination node D commence using the primary path<S, F, G>. During communication, the node F starts moving away from S. When the signal strength of node F falls below

threshold T, it sends a warning message “Path likely to be disconnect” to source node S. As soon as S receives the warning message, it starts using the Backup route along with primary route. Whenever destination node receives the data packets from the source node through two different paths (Primary + Backup), it sends acknowledgement through both the paths. If source node S receives an acknowledgement from the destination node through the Backup route, it makes preemptive switch over to the Backup route; otherwise S initiates the route discovery process.

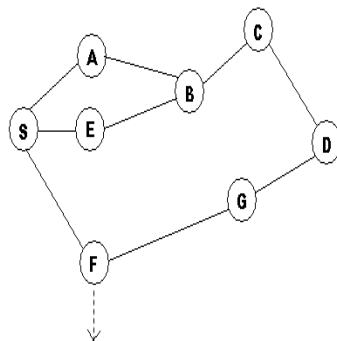
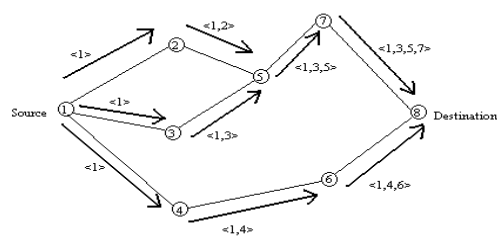
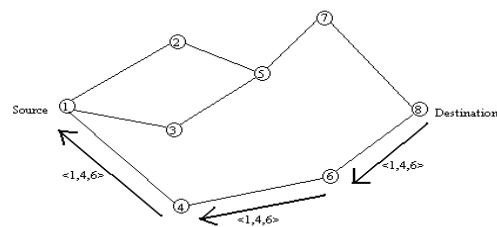


Figure 4: Primary Route Design

Route Maintenance



(a) Building Record Route during Route Discovery



(b) Propagation of Route Reply with the Route Record

Figure 5: Route Maintenance

The next step is the maintenance of these routes which is equally important. The source has to continuously monitor the position of the nodes to make sure the data is being carried through the path to the destination without loss. In any case, if the position of the nodes change and the source doesn't make a note of it then the packets will be lost and eventually have to be resent.

Route Monitoring Algorithm

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.

Multiple Routers Data Transmission

The path selection, maintenance and data transmission are consecutive process which happen in split seconds in real-time transmission. Hence the paths allocated priority is used for data transmission. The first path allocated previously is now used for data transmission. The data is transferred through the highlighted path. The second path selected is now used for data transmission. The data is transferred through the highlighted path. The third path selected is used for data transmission. The data is transferred through the highlighted path.

Algorithm for 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 with 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 go to step 5.

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

Step 5: Initiates Route Discovery Process.

Flowchart:



Figure 6: Flow chart

V. RESULT ANALYSIS

The results shows the probability of the communication breakage decreases when parallel routes are used and comparisons between DSR and Modified DSR(Preemptive Version) with respective to no. of broken paths and routing overhead. The analysis is represented in the following tables:

Table 1: Comparison Based on Broken

Preemptive Ratio	Number of Broken Paths			
	DSR High Mobility	DSR Low Mobility	PDSR High Mobility	PDSR Low Mobility
0	240	140	-----	-----
1	240	140	50	05
1.2	240	140	40	03
1.4	240	140	30	03
1.6	240	140	25	02
1.8	240	140	20	01
2	240	140	10	0

Table 2 : Comparison Based on Packets Sent

Preemptive Ratio	DSR Packets sent			
	DSR Low Mobility	DSR High Mobility	PDSR Low Mobility	PDSR High Mobility
0	-----	-----	-----	-----
1	1500	1000	3000	2000
1.2	1500	1000	3400	2500
1.4	1500	1000	4000	2600
1.6	1500	1000	4200	2800
1.8	1500	1000	4800	2900
2	1500	1000	4900	3000

VI. CONCLUSION & FUTURE ENHANCEMENT

Reactive ad hoc routing algorithms initiate route discovery only after a path breaks, it has significant control overhead for detecting the disconnection and re-construction of a new route. DSR with PRM mechanism detects early about the link that is likely to break soon, and hence it uses a backup path before the existing link fails.

The paper explains the preemption of Primary to Backup route by the source node S, whenever the signal strength of the primary route falls below the threshold value T. The modified DSR will improve the communication reliability between the source and destination node even if the mobility is high. In addition, Proactive routing improves the overhead of rediscovering route whenever the primary route fails.

Its future enhancements are, Modified DSR protocol will be extended to transfer messages to the destination system even though it is not in the coverage area of the source node through the router. This protocol also will be extended to handle the cases where the routers failed while data packets are travelling.

REFERENCES

1. V.Ramesh,Dr.P.Subbaiah,K.Sangeetha Supriya, "Global Journal of Computer Science and Technology" Vol. 9 Issue 5 (Ver 2.0), in Proc. IEEE INFOCOM January 2010.
2. Siva Ram Murthy, B.S, Manoj, "Routing Protocols for Ad Hoc wireless Networks," in Ad Hoc wireless networks: Architectures and Protocols, Chapter 7. Pearson.
3. Publication. Hongbo Zhou, "A Survey on Routing Protocols in MANETs," Technical. Note March 2003.

4. Elizabeth M. Royer, University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE personal communications, April 2007.
5. David B. Johnson, Davis A. Maltz, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks” October 1999 IETF Draft.
6. SM. Jiang, DJ. He and JQ. Rao, “A Prediction- Based Link Availability Estimation for Mobile Ad-Hoc Networks. Proceedings of IEEE INFOCOM, pages 1745-1752, Vol.3, April 2001.
7. Nasipuri, R. Castañeda, and S. R. Das, “Performance of multipath routing for on-demand protocols in ad hoc networks,” ACM/Kluwer Mobile Networks and Applications (MONET) Journal, vol. 6, no. 4, pp. 339–349, Apr. 2001.
8. M C Domingo, D Remondo and O. Leon, “A Simple Routing Scheme for Improving Adhoc Network survivability”, GLOBECOM, IEEE,2003.
9. T. Goff, N.B. Abu-Ghazaleh, D.S. Phatak and R. Kahvecioglu, “Preemptive Maintenance Routing in Ad Hoc Networks”, journal of parallel and Distributed Computing, Special Issue on Wireless Mobile Communication and Computing’03.
10. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, “A Performance Simulation for Route Maintenance in Wireless Ad Hoc Networks”, ACM,2004