A Reliable Multipath Routing Protocol in Mobile Ad Hoc Networks

Chi-Sheng Chiu Kuo-Feng Ssu Chih-Hsun Chou

Department of Electrical Engineering
National Cheng Kung University
Tainan, Taiwan

Abstract

This paper presents a reliable multipath routing (RMR) protocol to improve routing performance for ad hoc networks. The protocol uses a new loop-free route update scheme to accept backup paths that are longer-lived. Power information is also utilized so routing paths do not include nodes that are going to run out of battery. Furthermore, a dynamic route maintenance mechanism was developed to erase invalid backup routes preemptively. In order to reduce energy consumption, hosts can adjust the transmission power to send packets adaptively based on the mobility prediction. The RMR protocol was implemented on ns-2 and simulation results show that RMR outperformed both AODV and AOMDV.

Keywords*: mobile ad hoc networks, routing protocol, multiple paths, power failure.*

1 Introduction

A mobile ad hoc network is one type of wireless network that has no assistance of communication infrastructures, such as wireless access points and base stations. Instead of communicating via a centralized infrastructure, each host acts as a router to forward packets for other nodes. When a source node sends data packets to a destination node that is not within source's transmission range, the packets must be forwarded by its neighbors. The neighbors forward the packets to the destination hop by hop. For communication without help of infrastructure, it is important to establish routes between hosts in mobile ad hoc networks. Previous routing protocols for ad hoc networks can be roughly categorized as table-driven and on-demand. With the table-driven protocols, each host maintains all possible routes in its routing table. Each node needs to broadcast routing table advertisements in a period of time. When the topology of networks is changed, each node has to forward update information to maintain table consistency. The frequent updates may cause network congestion. Therefore, table-driven routing protocols are unsuitable for mobile ad hoc networks. On the other hand, with on-demand routing protocols, such as Dynamic Source Routing (DSR) protocol, Ad Hoc On-demand Distance Vector routing (AODV) protocol, source nodes build routes only when they really need to communicate with destination nodes [1, 2]. The protocols can reduce the control overhead compared to table-driven approaches.

Frequent route discovery in dynamic networks arises the routing overhead and end-to-end delay of packets. Many multipath protocols have been proposed to alleviate routing overhead and reduce transmission time. These protocols maintain potentially several paths between hosts that are found in the route discovery phase. Previous multipath protocols have several drawbacks. First, backup paths may be broken before a host uses them to forward packets. Switching to a backup path may cause more packet loss. Next, some protocols give up useful backup paths that are longer than the primary path. In addition, transmission power was not further reduced based on the exact distance between the sender and receiver.

This paper proposes a reliable multipath routing (RMR) protocol for mobile ad hoc networks. A mobility prediction method is adopted to calculate route expiration time (RET). Based on the information, a new loop-free route update scheme is used to obtain backup paths if they are longer-lived than the primary path. Moreover, a host removes the stale backup paths based on the route expiration time periodically. For the node failures due to power exhaustion, each mobile node measures its power expiration time periodically. If the node expiration time is lower than the threshold, a source node will not select the route containing the node in route discovery phase. Therefore, the selected routing paths will exclude the nodes that are going to run out of battery. A route maintenance mechanism is also implemented to remove invalid backup paths dynamically. A host that is going to run out of battery forwards route error packets to notify its upstream nodes. The source nodes can thus remove invalid paths immediately before they are broken. Finally, to consume power efficiently, a power control method is used to adjust the transmission power dynamically. With the RMR protocol, the mobility prediction can be used to measure the distance between two nodes so a host can adjust the transmission power to send packets appropriately.

This research was supported by National Science Council under contract NSC92-2213-E006-042.

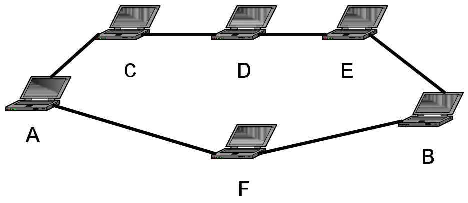

Figure 1. A drawback of loop-free scheme.

2 Related Work

AOMDV establishes multiple loop-free and link-disjoint paths without transmitting any extra routing packets [3]. An intermediate node forwards the duplicated RREQ packets with the hop count that is not larger than the primary path. The hosts only accept backup paths that are equal or shorter than the primary path. The scheme guarantees a host to find loop-free multiple paths. However, the scheme may discard some potential paths. For example (see Figure 1), a source node A wants to create routes to a destination node B. There are two disjoint routes, A-C-D-E-B and A-F-B. If A-F-B is found first, the route A-C-D-E-B will not be inserted in the multiple route list due to its larger hop count. Typically, the first found path is the shortest so many useful (loop-free) paths are discarded.

A mobility prediction mechanism uses location information to calculate the disconnection time of routes [4]. Location information provided by the GPS is piggybacked in routing packets. With coordinates, velocity, movement direction of two nodes, the link expiration time (LET) can be computed. Based on the information, the route expiration time (RET) can be measured using the minimum of the LETs along the route. A host selects the longest-lived route to reduce the possibility of rebuilding routing paths. The preemptive routing protocol uses the signal power strength to predict the link stability [5]. When a node moves into the preemptive region, a warning packet is sent to upstream nodes for route discovery.

Several energy-aware routing protocols were proposed. The essence of the protocols is to distribute power consumption evenly. Minimum Total Transmission Power Routing (MTPR) is one of the protocols that uses a formula to derive total transmission power for the routes [6]. With the information, a source can obtain a route with minimum total transmission power from all possible routes. Minimum Battery Cost Routing (MBCR) utilizes the remaining battery capacity of each host to select routes [7]. The Minimum Drain Rate (MDR) uses both energy drain rate and remaining battery capacity to determine which routes to select [8]. In order to reduce the transmission power, Power Control Routing (PCR) divides transmission power into N levels [9]. A host can choose the suitable transmission power for sending packets.

3 Reliable Multipath Routing

3.1 Node Expiration Time Prediction

Node failures are caused by many factors, such as crashes, shutdown of hosts, power exhaustion, and so on. Due to limited battery capacity, the power exhaustion is a major factor that may leads node failures. Therefore, power exhaustion is a possible indication that can be used for predicting the node expiration time. The node expiration time can be estimated by the future power drain rate and the remaining battery capacity. The future power drain rate could be predicted as an exponential average of the previous power drain rate. D_{t+1} is the predicted value for future power drain rate and D_t represents the previous average power drain rate from beginning to t_{th} second. In order to save memory space, a host only stores the information from $(t-j)_{th}$ to t_{th} seconds. The corresponding prediction function can be defined as:

$$D_{t+1} = \alpha \sum_{n=0}^{j} (1-\alpha)^n D_{t-n} \tag{1}$$

In the formula, D_i can be derived like this:

$$D_i = \frac{C_0 - C_i}{t_i} \tag{2}$$

C_i is the remaining battery capacity at i_{th} second, C_0 is the initial battery capacity, and t_i represents the interval from beginning to i_{th} sec. In formula (3.1), D_{t+1} is composed the recent and past power drain rate and parameter α is related with weight of the recent and past information. This value can be used to control the weight between recent history and past history. When α becomes larger, it means that the recent history's weight becomes higher. On the contrary, the past history's weight becomes higher. Let C_{now} be the current remaining battery capacity, the formula can be derived:

$$T_{expire} = \frac{C_{now}}{D_{t+1}} \tag{3}$$

In the RMR protocol, each host should keep track of its power information periodically.

3.2 Node Expiration Time Prediction

In most existing wireless networks, the transmission power is set as a constant. Like Lucent's WaveLAN, the radio propagation range is defined as 250 meters. Nevertheless, the constant transmission range may cause waste of the battery capacity. To save energy consumption, a mobile host should change its transmission power adaptively according to the distance to the receiver. The following is an equation for the relation between transmission power and distance:

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \tag{4}$$

P_t is the transmitted signal power and P_r is the received signal power. L is the system loss (L ≥ 1) and λ is the wavelength. G_t and G_r are the antenna gains of the transmitter and the receiver respectively. In normal situation, G_t and G_r are always constants. Based on communication theory, the signal power of a packet should decay when the packet is transmitted. At the physical layer of each wireless node, there is a receiving threshold. If signal power of a received packet is below the receiving threshold, the packet cannot be decoded correctly. Therefore, it is marked as an error packet and dropped by the MAC layer. Due to constant receiving threshold, P_t can be adjusted for power saving when the distance is lower than 250m.

Our protocol assumes that a mobile host can obtain location information about its neighbors. The host can compute the distances to all its neighbors, and then it can adjust its transmission power dynamically. Assume that *d* is the distance to a neighbor and P_t is the transmission power for transmitting 250m.

$$P_{adjusted} = \frac{P_t \times (d + \phi)^2}{250^2} \quad (5)$$

$P_{adjusted}$ is the adjusted transmitted signal power. ϕ is a parameter to increase the predicted distance to neighbor. If $(d + \phi)$ is more than 250, it will be replaced by 250. The chance that the neighbor is not within the predicted transmission range can be reduced.

3.3 Protocol Overview

3.3.1 Assumptions

Each host in the mobile ad hoc networks is equipped with GPS. Location information is piggybacked in routing and data packets. To predict node expiration time, each host should have the ability to read the remaining battery capacity from the power management components. Each host can calculate its expiration time to determine whether it is about to run out of power.

3.3.2 Data Structure

In the RMR protocol, each mobile host maintains a multiple path routing table. Each entry of the table contains following information: destination address, next hop address, hop count, sequence number, route expiration time, maximum route expiration time, and a pointer to the list of backup paths. The value of sequence number is for determining the freshness of routes. The list of backup paths is used to store all redundant paths. If there is only a primary path, the value of the pointer to the list of backup paths is NULL. Each element of the backup list contains next hop address, hop count, and route expiration time (RET). The value of route expiration time represents the stability of paths. A route with longer route expiration time is more stable. The "maximum route expiration time" is used to compute loop-free multipath. The maximum route expiration is set as zero initially. When backup paths are found, value of the field is set as the maximum RET among multiple paths.

3.3.3 Calculate Multiple Loop-free paths

In single path on-demand routing protocols, duplicate route request (RREQ) packets are discarded so some paths cannot be found. In order to obtain all potentially useful multiple paths, all duplicate RREQ copies should be processed. However, using all duplicate RREQ copies to obtain multipath may cause routing loops. The RMR uses a new route update scheme to avoid routing loops.The route update scheme in some previous multipath routing protocols restricts a host to accept only backup paths that are equal or shorter than the primary path. To solve the problem, the field "maximum route expiration time" (described in Section 3.3.2) is added in routing tables. The field is set as zero in the beginning. When a path with longer route expiration time is found, the maximum route expiration time is updated. The maximum route expiration time is utilized to eliminate all possible routing loops. The route update scheme is as follows:

1. A host keeps only routes with the highest destination sequence number.

2. For the same sequence number, a host accepts a route from its neighbor if it has a larger route expiration time than the maximum route expiration time in routing table or it has smaller hop count.

Rule 1 is the same as traditional single path routing protocols. A host only maintains the freshest routes. Rule 2 can help a host to find more useful paths and to prevent the occurrence of routing loops. A path with routing loops must be longer than a normal one. The value of RET in an RREQ must be smaller when the packet is flooded hop by hop because the value is replaced with a smaller LET. Therefore, a route that has larger route expiration time than the maximum route expiration time should not cotain routing loops. Meanwhile, a host can insert longer-lived backup paths into its backup path list. The route update strategy is described in Figure 2.

3.3.4 Route Discovery

In route discovery process, both mobility prediction and power failure prediction are applied to select backup paths. The route discovery process has two major phases: route request phase and route reply phase. The route discovery process will be initialed when a route is requested by a source node and there is no information about the route in its routing table. First, the source node generates an RREQ and then floods the packet to networks. The RREQ includes following fields:

Source address (the IP address or the host ID of the node that issues the RREQs), Destination address (the IP address or the host ID of destination), Hop count (length of routing path), Broadcast ID (the value can identify an RREQ uniquely), Sequence number (the

```
Definitions:
    rt1: the route entry to node S
    rt2: the route entry to node D
    src_seqno: the source sequence number in the
               routing packet
    dst_seqno: the destination sequence number in the
               routing packet
    seqno: the sequence number in the routing table
    ret: the route expiration time in the routing packet
    mret: the maximum route expiration time in the
          routing table
    rq: a route request packet from the source S to
        the destination D
    rp: a route reply packet from the destination D to
        the source S

procedure route_update
begin
    For an intermediate node receives rq
    if ($rq.src\_seqno > rt1.seqno$) then
        erase the multipath list;
        $rt1.mret \leftarrow 0$;
        insert the new path into the multipath list;
    else if ($rq.src\_seqno = rt1.seqno$)
        if (($rq.hopcount < rt1.hopcount$) or
        ($rq.ret > rt1.mret$)) then
            insert the new path into the multipath list;
        endif
    else
        drop the packet rq;
    endif

    For an intermediate node receives rp
    if ($rp.dst\_seqno > rt2.seqno$) then
        erase the multipath list;
        $rt2.mret \leftarrow 0$;
        insert the new path into the multipath list;
    else if ($rp.dst\_seqno = rt2.seqno$)
        if (($rp.hopcount < rt2.hopcount$) or
        ($rp.ret > rt2.mret$)) then
            insert the new path into the multipath list;
        endif
    else
        drop the packet rp;
    endif
end
```

Figure 2. Algorithm for route update.

current sequence number of the originator), Location information (the velocity, position, and movement direction of the source), Route expiration time (the predicted lifetime of a reverse path) and TTL (the lifetime of an RREQ).

The RREQs are propagated to neighbors within the source's transmission range. They also broadcast the packets to their neighbors. The process is repeated until the destination receives the RREQ. When an intermediate node receives the RREQ, it performs the following process:

1. The node measures its node expiration time (NET) first. If the node expiration time of a host is lower than threshold, the host will discard the RREQ. The node will run out of battery soon so the routes with the node will be broken quickly. Therefore, the routes that are going to expire can be avoided.

2. The node decreases TTL of the RREQ by one. If the TTL is smaller than zero, the host will drop the RREQ.

3. The node reads the location information from the RREQ. It calculates the link expiration time (LET) to the previous node. If the link expiration time is smaller than the route expiration time (RET) stored in the RREQ, it will replace the RET by LET.

4. In order to transmit route reply packets to the source, the node builds a reverse path to the source based on the route update rule. If the path conforms to the route update rule, the node will insert the path to its multiple path list. Otherwise, the node will ignore the path and discard the RREQ.

5. The node determines whether the RREQ is redundant or not by checking the pair (source address, broadcast ID). If the RREQ is not redundant, the node will refresh the location information of the RREQ and forward the packet to neighboring nodes. On the other hand, it will drop the RREQ.

When the destination receives the route request packet, it sends route reply (RREP) packet to the source along the reverse paths created previously. The RREP includes the following fields:

Source address (The IP address or the host ID of the node that originates the RREQs), Destination address (the IP address or the host ID of the node that initiates the route reply packets), Hop count (The number of hops from the destination to the node that handles the RREP), Destination sequence number (the destination sequence number that represents the freshness of a route), Location information (the velocity, position, and moving direction of the sender) and Route expiration time (the predicted lifetime of a route).

The destination sends RREPs to next nodes of reverse paths. They also forward the packet to next nodes until the source receives the RREP. During processing route reply packets, each intermediate node performs the following process:

1. The node reads the location information from the RREP and calculates the link expiration time (LET) for the sender. If the link expiration time is smaller than the route expiration time (RET) stored in the RREP, the LET will replace the RET. Therefore, the expiration time for the forward paths can be obtained.

2. If the path conforms to the route update rule, the node will insert the path to its forward path list. Otherwise, the node will ignore the path and discard the RREP.

3. The node creates or updates the entry of neighbor table based on the location information stored in the RREP. It also stores the timestamp in its neighbor table.

4. The node determines whether the RREP is redundant or not by checking the matrix (destination address, source address, and destination sequence number). If the RREP is not redundant, the node will refresh the location information of the RREP. On the other hand, it will drop the RREP.

5. The node forwards the RREP to next nodes of reverse paths.

After the process, the source obtains information about multiple paths and selects a path set. The RMR protocol selects the shortest path as primary path. If there are more than one shortest paths, a host will select the path that is found first. When the primary path is broken, a host switches data traffics to the shortest backup path. During data transmitting, a host measures the distance to the next hop based on the location information stored in its neighbor table. According to the distance, the host can adjust the transmission power dynamically. Additionally, to improve the availability of backup paths, a host removes the stale backup paths based on the predicted lifetime periodically.

3.3.5 Route Maintenance Strategy

Link failures in ad hoc networks are caused by mobility, congestion, packet collisions, node failures, and so on. In the RMR protocol, the link layer feedback from IEEE 802.11 is utilized to detect link failures. If a node sends packets along the broken link, it will receive a link layer feedback. When a node detects a link break, it broadcasts route error (RERR) packets to its neighbors. The neighbors then rebroadcast the packets until all source nodes receive the packets. If a source node receives the RRER, it will remove every entry in its routing table that uses the broken link. Differing from single path routing protocols, the route error packets should contain the information not only about the broken primary path but also the broken backup paths. When the source node receives the RERRs, it removes all broken routing entries and uses the shortest backup paths as primary paths. The source node initiates a route discovery process when all backup paths are broken.

However, a link failure cannot be detected unless a packet is sent along the link. To solve the problem, a dynamic route maintenance mechanism is used to detect failures preemptively in the RMR protocol. When a host receives a data packet from its neighbor, it computes the link expiration time (LET) of the link. If the host finds that the value of LET is lower than threshold, the host will send RERRs to the source nodes. Additionally, each host calculates its power expiration time periodically. When the host finds that the value of node expiration time is lower than threshold, it will forward RERRs to its neighbors to notify that the node is going to run out of battery. With above schemes, a host equips capability to remove the invalid backup paths preemptively and reduce packet loss caused by invalid backup paths.

4 Performance Evaluation

4.1 Simulation Environment

The RMR protocol was evaluated using the ns-2 simulator version 2.1b9a [10]. In the simulation, the IEEE 802.11 distributed coordination function (DCF) was used as the medium access control protocol. The physical radio characteristics of each wireless host were based on Lucent's WaveLAN. WaveLAN was direct spread spectrum radio and the channel had radio propagation range of 250 meters and capacity of 2 Mb/sec.

The AODV, AOMDV, and RMR were compared in the simulation. The AOMDV, an extension of AODV, was also implemented because it was not included in the NS2. The simulation model was consisted of 50 mobile nodes randomly distributed in an 1500*300 rectangular area. The traffic pattern consists of 30 constant bit rate (CBR) sources sending 512 byte packets at a constant rate 4 packets per second. The random waypoint model was used to perform node movement. Each node selected a random destination in the observed area and moved to the position with a specified speed. When a node moves to the destination, it will stop moving for a predefined pause time. The node will then move to another location. In the simulation, the pause time was modelled as normal distribution and the mean value was 60 seconds. Besides, the velocity of each node was also normal distributed. The movement patterns were generated by using 6 different average velocities: 0, 2.5, 5, 10, 15, 20 m/s. The total simulation time was 900 seconds.

4.2 Simulation Results and Analysis

The following metrics were used to evaluate the three routing protocols:

- Average number of paths: The average number of paths that are found in each route discovery process. The paths includes both a primary path and backup paths. The metric represents the ability to find multiple paths.

- Successful rate of backup paths: This metric is defined as a probability of switching data traffics to the backup paths successfully. With the metric, the efficiency of backup paths for multipath routing protocols can be compared.

- Packet delivery ratio: The number of data packets delivered to the destinations to the number of data packets sent by the sources.

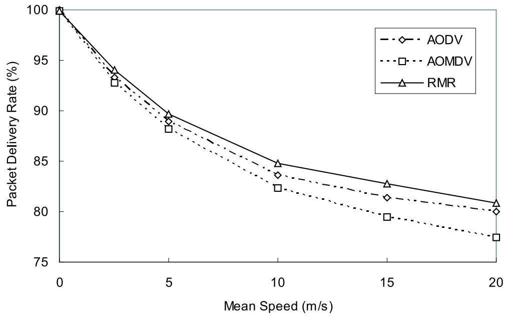

Figure 3. Packet delivery ratio.

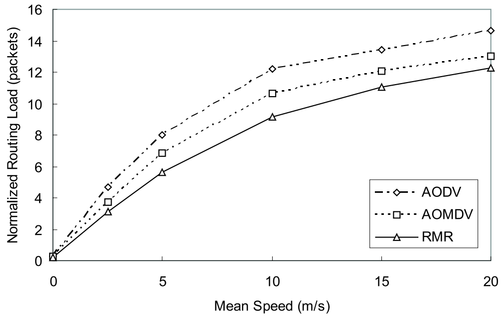

Figure 4. Normalized routing load.

- Normalized routing load: The number of routing packets transmitted per data packets delivered. This metric indicates the efficiency of routing protocols.
- End-to-end delay: Average time between data packets received by the destinations and data packets sent by CBR sources. The data were collected only for successfully delivered packets. The delay is determined by many factors, such as buffering during route discovery, queuing at the interface queue, and routing paths between two nodes.
- Throughput: The total size of data packets that are received in CBR destinations per second. It represents whether the protocols make good use of network resources or not.
- Normalized energy consumption: The value of energy consumption per data packets delivered. The metric indicates the efficiency of energy consumption.

4.2.1 Without Node Failures

Power failure was not considered in the first set of simulations. Every node functioned correctly during the simulation. The Table 1 shows the average number of paths and the successful rates of backup paths for both AOMDV and RMR. The RMR found more routing paths in each situation because not only shorter paths were accepted but also longer-lived paths. Moreover, the successful rates of backup paths in RMR were higher than AOMDV in each scenario because RMR removes stale backup paths periodically. The results proved that RMR provided more reliable paths than AOMDV when a host switched data traffics to backup paths. Figure 3 compares the packet delivery ratios for the three protocols. Though AOMDV provided backup routing paths, the packet delivery ratio of AOMDV was lower than AODV. AOMDV did not guarantee all backup routing paths were useful so mobile hosts may switch data traffics to broken backup paths. With RMR, each host used the mobility prediction method to build backup paths that had longer predicted route expiration time than the primary path. The dynamic route maintenance also helped each host to erase invalid backup paths. Therefore, the packet delivery rates in RMR were higher than AOMDV.

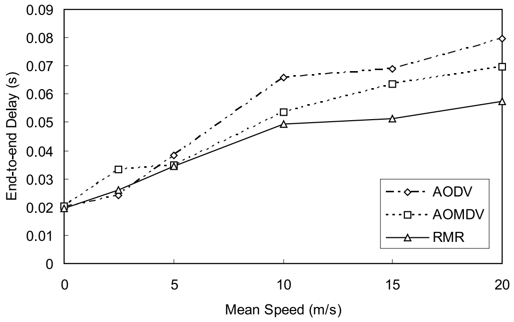

Figure 5. End-to-end delay.

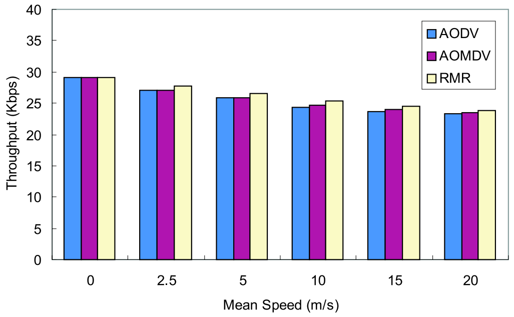

Figure 6. Throughput.

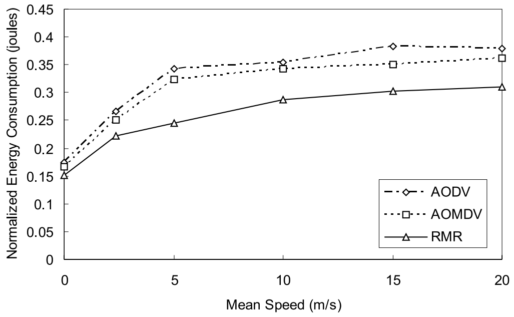

Figure 7. Energy consumption.

In Figure 4, the normalized routing load of both mulipath protocols was smaller than AODV. The RMR provided more and reliable backup paths so its normalized routing load was lower than AOMDV. Figure 5 shows the advantage of multipath routing protocols for reducing the end-to-end delay. Instead of initiating a new route discovery, using backup paths eliminated

Table 1. Average Number and Successful Rate for Backup Paths

Mean speed	2.5 (m/s)		5 (m/s)		10 (m/s)		15 (m/s)		20 (m/s)	
Metric	Number	Rate	Number	Rate	Number	Rate	Number	Rate	Number	Rate
AOMDV	2.168	0.762	2.119	0.700	2.155	0.589	2.148	0.529	2.056	0.490
RMR	2.393	0.926	2.351	0.909	2.446	0.848	2.426	0.810	2.367	0.752

Table 2. Power Consumption Model of Lucent IEEE 802.11 WaveLAN Card

Packet type	Energy consumption (μW)
broadcast send	1.9 × *PacketSize* + 250
point-to-point send	1.9 × *PacketSize* + 420
broadcast receive	0.50 × *PacketSize* + 56
broadcast send	0.42 × *PacketSize* + 330

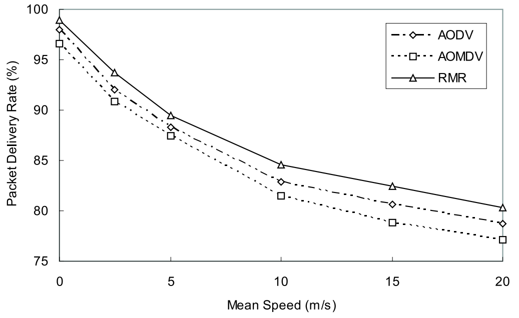

Figure 8. Packet delivery ratio.

the overhead and delay of the route discovery process. The RMR performed better than both AODV and AOMDV due to more reliable backup paths. The AOMDV did not perform stably and had larger delay than AODV when mean speed was low. Broken backup paths led to local repair processes for building a new route from the intermediate nodes to the destinations so the end-to-end delay for AOMDV was affected. Figure 6 is a comparison for the throughput of the protocols. Due to smaller number of routing packets, the RMR could save the bandwidth of mobile hosts for sending control messages so the RMR made good use of network resources. Besides, due to the smaller end-to-end delay, the RMR transmitted more data packets than AODV and AOMDV during the simulation time. Therefore, the RMR produced more throughput than AODV and AOMDV. Figure 7 illustrates that RMR consumed energy more effectively than AODV and AOMDV. Though AOMDV can reduce the number of routing packets, it only performed a little better than AODV. The RMR reduced the transmission energy by the power control method and had fewer routing packets so the normalized energy consumption was further enhanced.

4.2.2 With Node Failures

The initial energy for each node was modelled using normal distribution and the mean value was 30 joules. Based on the Lucent IEEE 802.11 WaveLAN's specification, the linear power consumption model coefficients for data sending, receiving are shown in Table 2. In the end of the simulation, about ten nodes ran out

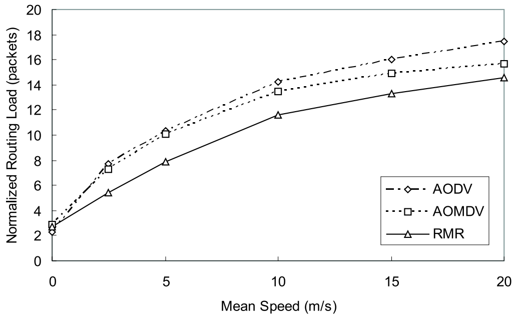

Figure 9. Normalized routing load.

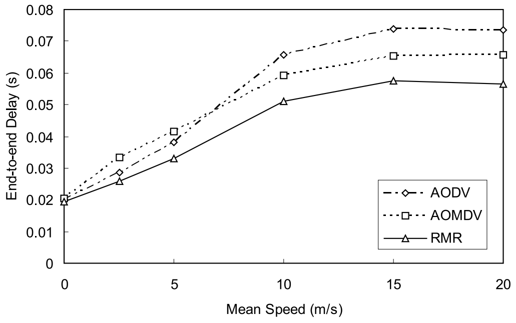

Figure 10. End-to-end delay.

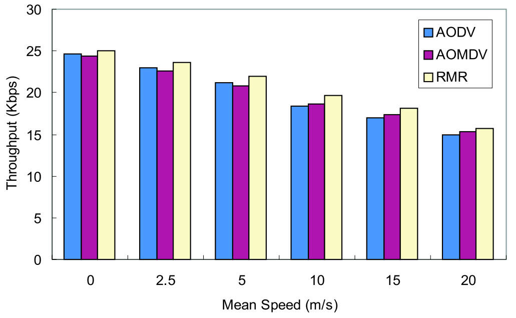

Figure 11. Throughput.

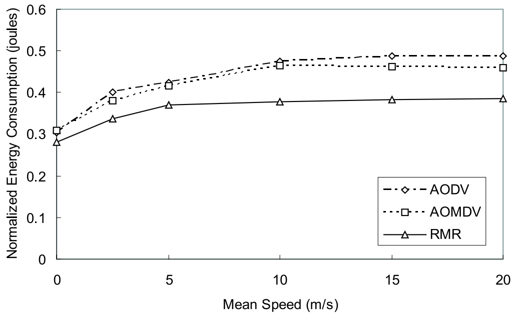

Figure 12. Energy consumption.

Table 3. Average Number and Successful Rate for Backup Paths

Mean speed	2.5 (m/s)		5 (m/s)		10 (m/s)		15 (m/s)		20 (m/s)	
Metric	Number	Rate	Number	Rate	Number	Rate	Number	Rate	Number	Rate
AOMDV	1.742	0.731	1.829	0.682	1.794	0.571	1.913	0.514	1.845	0.486
RMR	1.943	0.919	2.036	0.904	1.973	0.852	2.113	0.807	2.104	0.763

of battery. Therefore, there were some link failures caused by node failures.

In Table 3, the average number of paths for each protocol was smaller than the results without node failures. Node failures decreased the density of mobile hosts so fewer nodes could help to establish multiple routing paths. However, the successful rates of RMR using node failure prediction were almost the same compared to prior results. In Figure 8, the packet delivery ratio for both AODV and AOMDV decreased compared to the previous results. Based on Table 3, due to node failure prediction method and dynamic route maintenance, the packet delivery ratio of RMR was better than AODV and AOMDV. The performance of the RMR was not much affected by the faulty nodes.

The AOMDV performed a little better than AODV (see Figure 9). With node failure prediction, RMR outperformed AODV and AOMDV in all varying speeds. With the RMR, a source node could avoid selecting a path with nodes that were going to run out of energy so the paths were more reliable than AOMDV. Figure 10 shows that RMR had the best end-to-end delay with all different speed settings. With the RMR, some local repair processes were avoided due to node failure prediction. AOMDV did not always perform better than AODV due to some useless backup routing paths. Figure 11 illustrates that RMR had the best performance among these protocols. Due to lower routing load and end-to-end delay, RMR could transmit more data packets. In our simulation, the RMR saved more energy than other protocols (see Figure 12). With the power control method, the RMR can reduce the transmission power. Additionally, the RMR had few routing load among these protocols so some energy consumption caused by routing packets can be avoided.

5 Conclusion

The RMR protocol was developed for providing more reliable backup paths in mobile ad hoc networks. The higher reliability of the backup paths improves routing performance. The RMR protocol utilizes both mobility prediction and power failure prediction to select longer-lived backup paths. The dynamic route maintenance scheme also removes invalid paths caused from power failures and link failures. Moreover, the RMR uses power control method to reduce required transmission power.

Simulation results showed that the RMR can locate more backup paths than the AOMDV. The successful rates of the RMR were about 30% higher than AOMDV. Because the RMR provided more available backup paths, the routing load of the RMR was smaller than both AODV and AOMDV. For end-to-end delay, the RMR performed 30% faster than AODV 20% faster than AOMDV. Due to smaller number of routing packets and smaller end-to-end delay, the RMR achieved best throughput. Finally, the RMR reduced 20% energy consumption compared to both the AODV and AOMDV.

References

[1] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, vol. 353, pp. 153–179, 1996.

[2] C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," *Proceedings of IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, Feb. 1999.

[3] M. K. Marina and S. R. Das, "Ad hoc On-demand Multipath Distance Vector Routing," *Review of ACM SIGMOBILE Mobile Computing and Communications*, pp. 92–93, July 2002.

[4] W. Su, S. J. Lee, and M. Gerla, "Mobility Prediction in Wireless Networks," *Proceedings of the IEEE International Conference on Military Communications*, pp. 491–495, Oct. 2000.

[5] T. Goff and N. B. Abu-Ghazaleh, "Preemptive Routing in Ad Hoc Networks," *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking*, pp. 43–52, July 2001.

[6] K. Scott and N. Bambos, "Routing and Channel Assignment for Low Power Transmission in PCS," *Proceedings of IEEE International Conference on Universal Personal Communications*, pp. 498–502, Oct. 1996.

[7] S. Singh, M. Woo, and C. Raghavendra, "Power-aware Routing in Mobile Ad Hoc Networks," *Proceedings of Annual International Conference on Mobile Computing and Networking*, pp. 181–190, Oct. 1998.

[8] D. Kim, J. J. Garcia-Luna-Aceves, K. Obraczka, and P. M. J. Cano, "Power-Aware Routing Based on the Energy Drain Rate for Mobile Ad Hoc Networks," *Proceedings of International Conference on Computer Communications and Networks*, pp. 565–569, Oct. 2002.

[9] K. Tsudaka, M. Kawahara, A. Matsumoto, and H. Okada, "Power Control Routing for Multi Hop Wireless Ad-hoc Network," *Proceedings of IEEE GLOBECOM*, pp. 2819–2824, Nov. 2001.

[10] K. Fall and K. Varadhan (editors), *The ns Manual (ns Notes and Documentation)*. The VINT project, www.isi.edu/nsnam/ns/ns-documentation.html, Feb. 2002.