A LOCAL/GLOBAL STRATEGY BASED ON SIGNAL STRENGTH FOR MESSAGE ROUTING IN WIRELESS MOBILE AD-HOC NETWORKS

Tien-Chung Tien
Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, New York 14260

Shambhu J. Upadhyaya
Department of Computer Science and Engineering
State University of New York at Buffalo
Buffalo, New York 14260

ABSTRACT

Route switching is an important issue to connection-oriented communication that needs to maintain a route for a certain period. This paper suggests a new approach to ease the route switching problems in a network with higher migration rate of hosts. By monitoring the signal strength of messages, a host in a route that receives an incoming message can detect possible route fluctuations locally. As the average signal strength declines into a dangerous level, the host that receives the message will send an advance-warning message to the route source host. If the source host can find more stable routes locally, it will adapt a substitute route and will complete the process of adaptation before the breakdown of the original route actually occurs. If the route source host cannot adapt a new route locally, the source host will be forced to search for a new route by considering the entire network.

1. INTRODUCTION

The wireless mobile communication networks consist of various mobile processors units or mobile hosts, which may be the cell phones, the palmtops, notebook computers or any mobile utilities with capability of networked communication. The wireless mobile ad-hoc networks must dependent on their subordinate hosts to do the job of networking and therefore at least some of the mobile hosts in ad-hoc networks have to take the function of routers in order to enable message exchange among hosts. For a router with mobility, its position in the network topology is not fixed and will change as it migrates from its initial route.

In a wireless environment of message routing among mobile hosts, resources for mobile hosts such as battery power and frequency channels are limited. Besides these limited resources, the mobility characteristics of mobile hosts are quite different from the processor units of the wired networks. The greatest challenge for a wireless mobile ad-hoc network comes from its inherent characteristics of high uncertainty. Therefore, to deal with the routing problems within a wireless mobile network, one should resort to concepts that are different from traditional wired computer network architectures [IK96], [JCNK95], [PGH95].

In 1996, Johnson and Maltz proposed an algorithm of dynamic source routing (DSR) [JM96]. This routing algorithm is based on source routing with an improvement for dynamic environment. It is explicitly designed for use in the wireless environment of an ad-hoc network. Because it does not periodically broadcast routing advertisement, it greatly reduces the network bandwidth overhead and battery power consumption. In 1997, the proposed algorithm of signal stability-based adaptive routing (SSA) [DRWT97] tried to find the most stable route by analyzing the signal strength. The SSA algorithm has further improved the communication quality for message routing in a wireless ad-hoc mobile network. Besides the above the two algorithms, there have been many attempts from different researchers trying to solve some basic problems for such networks [IB94], [KCVP95], [CE95], [PB94], [DSB97].

The power-off or malfunction of some hosts in an established route (also called route hops) will interrupt message routing and cause routing failure. On the other hand, as an intermediate route hop migrates from a route, message transmission could suffer from route failure due to signal fading. Searching a substitute route after the initial route encounters a route failure will postpone all the following message transmissions, and decrease the throughput of the entire ad-hoc network. The process of route discovery is both making network throughput decline and delay the transmission of time-critical messages.

In the algorithms of dynamic source routing [JM96] and stability-based adaptive routing [DRWt97], source-destination pair hosts utilize a route until all message exchanges have ended or route-failure occurred. When message routing encounters link failure, such as network partition or route-hop breakdown, the route hop encountering message routing failure sends a routing-error message (REM) to source host to indicate the routing-error situation. The REM points out where and when the routing-error occurred. The source host then launches a process of route discovery under two conditions. 1) if the source host has got the routing-error message, 2) if routing-error message cannot reach the source host, it will wait for an acknowledgment message until a time-out expires and re-sends the same message

to the destination until a specified number of tries exceeds. This paper proposes a new scheme to improve the communication efficiency for ad-hoc networks under highly dynamic situations. In Section 2, the basic principle of the new routing scheme is given. Section 3 describes the global route adaptation strategy and Section 4 discusses the development of the new local route adaptation algorithm. Evaluation, results and a discussion appear in Section 5.

2 A NEW ROUTING SCHEME BASED ON SIGNAL STRENGTH

2.1 The Basic Idea

We utilize an advance-warning mechanism (AWM) to offer an advance warning service for message transmission. This mechanism monitors each routing link situation and responds to any possible route fluctuations before the actual link failure. By designing a routing algorithm with a local adaptation capability combining the signal strength monitoring with an advance warning mechanism to offer and maintain a stable communication service is a new attempt for message routing in a wireless ad-hoc mobile network. The AWM acknowledges possible route fluctuation by monitoring the signal strength from its neighborhood, including the previous hop and the next hop along a route. When a warning message is issued, a local route adaptation will be attempted and if it fails, it will go for global adaptation. That should give the source host enough time to make optimal decisions, whether it should still utilize the initial route or launch a route request procedure to find a new one, based on the information status before the route-failure actually occurs.

2.2 Signal Strength Determination

The wireless networks transmit signal over free space, and the average energy of message signal (s_{av}) will decrease by the inverse square of signal transmission range ($s_{av} \propto$ watts/meter^2). The fluctuation of signal strength could also come from other factors besides the hosts' movement, such as the low battery power of hosts and the geological effect. Because they also cause signal instability, the early warning concept still can be utilized in those cases. The signal strength determination is described in Fig. 2-1.

3 GLOBAL ADAPTATION STRATEGY

3.1 Route Discovery

Our route discovery scheme is based on the scheme of source routing algorithm [BG92] and the DSR [JM96]. Like the DSR and SSA [DRWT97] schemes, a source host will broadcast a route request message (RQM) to find a route to desired target host, if it does not have a usable cached route in its own routing table. The RQM will record each hop's address it passes until reaching the destination, and the medium access control (MAC) layer that controls the multiple accesses of transmission media of hosts follows the standard of IEEE 802.11 to avoid any possible messages conflicts.

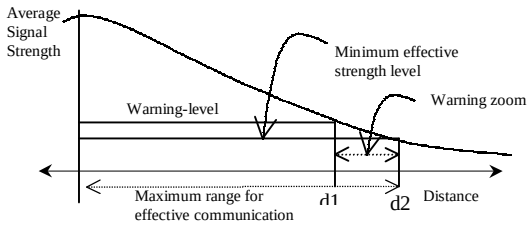

Figure 2-1. The horizontal axis is the separation between two hosts. The d2 is the maximum range for effective message communication. Beyond this point, the link will be highly unstable which might lead to communication interruption. The d1 is the experimentally decided warning point. The distance between d1 and d2 is warning range. Any separation or average signal strength between two hosts in this warning range will cause their local link maintenance mechanism to take actions.

In the routing table of each host, there is a warning mark number associated with each route and a warning mark associated with each neighborhood link. A counter is used to record how many warning links the RQM has encountered, and it starts with 0. Every host that receives RQM will analyze the signal strength of this message, and determine whether the incoming message has reached the warning point or not. If the incoming link declines to the warning point, a warning will be marked on this link of routing table, and the warning number counter on the RQM will be increased by 1. A host could receive several RQMs from different routes. It can re-broadcast first the first incoming RQM anyway, and re-broadcast later one with less number of warning marks if this host is not the destination. Hosts can also limit the maximum number of allowed warning mark (WM) of RQM. Receiver hosts will discard every RQM with higher WM number. The destination host could receive several RQMs from different routes but will choose the first incoming RQM with 0 WM number. Otherwise, one RQM with the least WM number will be the choice. By selecting the least WM number at each hop, the destination can find the most stable route. Destination host will send the source host a route reply message (RRM) to respond to the selected route.

3.2 Route Maintenance

Most proposed ad-hoc network algorithms adopt distributed network computing which means that each host will keep a local routing table. The local routing table reflects the network topology and it should be updated as the network topology changes. There are two major approaches to maintain the local routing table, one is active in which a host broadcasts link-checking message or sends beacons to poll its neighbor host at fixed periods and the other is passive in which a host listens to its neighborhood and updates the routing table

according to the result of eavesdropping [JM96] [DRWT97]. Our scheme adopts a combination to get advantages from both passive and active approaches. Polling will be done on a need basis. Based on that every host in an ad-hoc network listens to its neighborhood, a mechanism is setup to figure out a proper time to launch a link-checking message (LCM) to a specified neighbor host that has been silent too long. The mechanism of LCM will turn back a timer to 0, which counts up a time-out for a silent neighbor host and it starts from 0 after getting signal from this specified host, no matter whether it comes from the response of LCM or eavesdrops from neighbor's communication. Hosts will analyze every incoming message signal and update their local routing tables. The signal strength of every message will be analyzed; hosts will assign a warning mark on those incoming links that decline to warning-range. If a neighbor host is not silent within the maximum allowed time, then polling will not be necessary. Therefore, not only the battery power for LCM can be saved but also the network bandwidth.

4 LOCAL ROUTE ADAPTATION STRATEGY

In this Section, we consider 3 cases of route hop migration behavior. In each model, the nth hop always represents the leftmost hop that detects the migration movement of an intermediate hop.

4.1 Case 1: Migration Affecting Outgoing Link

This is the case where a route hop's migration movement affects its out-going link transmission to next hop but does not affect the incoming link. In this case, the next hop can detect that its incoming link is entering into warning level. Fig. 4-1 shows that the (n-1)th route hop is migrating away from nth hop, and the nth hop detects that the link between (n-1)th hop and nth hop is stepping into warning level.

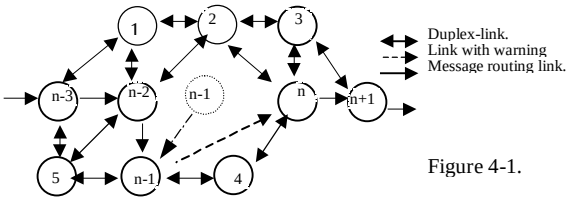

Figure 4-1.

Case 2: Migration Affecting Incoming Link A route hop's migration movement affects its incoming link from previous hop but does not affect out-going link to next hop. This migrating hop can detect if incoming link is entering into warning level. Fig. 4-2 shows that the nth route hop is migrating away from (n-1)th hop, and the nth hop detects that the incoming link from (n-1)th hop is entering into warning level.

Case 3: Migration Affecting Both Incoming and Outgoing Links A route hop's migration movement affects both incoming and outgoing links simultaneously as shown in Fig. 4-3. The (n-1)th route hop is migrating away from both (n-2)th hop and nth hop. It can detect that the incoming link from (n-2)th hop is entering into warning level. Meanwhile, the nth hop also detects that the incoming link from (n-1)th hop is entering into warning level.

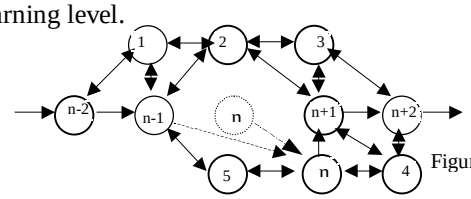

Figure 4-2.

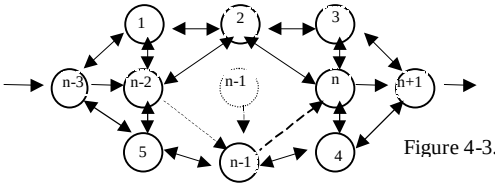

Figure 4-3.

From these models, it is seen that the links affected by a migrating hop are (n-2)th to (n-1)th and (n-1)th to nth, and the hops which could be potentially involved in this event of migration are (n-2)th, (n-1)th, and nth hops. The least number of hops that could be affected is 2 for case 1 and case 2, or 3 for case 3. Therefore, the (n-1)th hop and (n-2)th hop will be the prime hops to make the decision for local route switching. It is important to recognize every hop's relative position (RP) in a route. And, in order to recognize the position of link in a route which encounters a warning condition, the list of cached routes in each host's routing table arranges hops' addresses by sequence ordering. The source host is assigned at the most significant position and the destination host is at the least significant position. By this position ordering, each hop can recognize its relative position among the route hops. From this position relationship, a hop can acknowledge itself belonging to the forward part or backward part of a routing message at each link along a route as shown in Fig. 4-4.

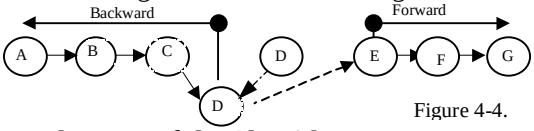

Figure 4-4.

4.2 Development of the Algorithm

As a receiver detects that an incoming link is at the warning level, it will do two things: 1) send a local warning message (LWM) backward to sender which can be done either by locally broadcasting or by affixing a link warning (LW) to acknowledgement. 2) increase the warning number by 1 at the header of the transmitted message. Thus, the destination host gets informed that some link in this route is under warning. By checking the warning number at the header of incoming message, the destination host can monitor the conditions of all the links of a route.

4.2.1 Rules for Local Broadcasting For the local broadcasting, the LWM transmission follows certain

rules and regulations such that the set of available potential substitutes at local region is small.

1. The LWM contains both addresses of sender-end and receiver-end, and addresses of all route hops.
2. Any forward hops with RP > n+1 that receive LWM just discard it to avoid unnecessary overhead in the network.
3. The LWM has a maximum hopping number.
4. The sender-end hop of a warning link will discard the LWM received directly from the receiver-end hop.
5. If any backward hop with RP < n-2 receives a LWM without affixing any potential substitute candidate, it just discards this message.
6. After broadcasting a LWM to its neighborhood, the nth hop will listen to its neighbor to confirm this message broadcasting. If no response, it can either re-broadcast this LWM or just stop this local broadcasting.
7. The action of re-broadcasting is limited to a specified number of tries.

Rules 2 and 3 limit the potential substitute at local regions of the network. Rules 4, 5, and 7 are to reduce unnecessary transmission overhead. Rule 6 is to make sure that any possible existing neighbor hosts of the receiver-end hop of a warning link will receive LRQM. Consider that the communications links between hosts may not always have duplex capabilities, and some links may just offer one-way communication. Thus, there are two possibilities for the results of the LWMs reaching at backward hops of local route discovery. Therefore there are two different approaches to deal with both cases of links with two-way communication capability and one-way communication capability. In the following we discuss only the former case.

4.2.2 An Available Local Substitute Found by the LWM The LWM message include entire route hops' addresses, which allow the neighborhood of the sender-receiver pair to check if their routing tables have a potential candidate for such local substitute route. A potential candidate should conjoin two intermediate hops of that initial route, and should not let the warning link still to be an intermediate part of this new route. By presetting the number for an acceptable local substitute, the potential candidates can be limited. If all links between neighbor hosts offer duplex communications, the LWM can find local substitutes. To decide which substitute is adopted from several possible candidates, certain rules and regulations are defined. This will avoid any potential route-found message competition.

1. If a neighbor host has more than one potential local substitute at its routing table, it should choose the one with the least number of replacement hops.
2. If a neighbor host receives a LWM affixed with a candidate with replacement hops less than or equal to its own potential candidates at routing table, this host will stop re-transmitting this LWM.
3. If a neighbor host receives a LWM affixed with a candidate with larger number of replacement hops than its own potential candidates, it will replace it by its own candidate to retransmit.
4. In order to limit the number of potential candidates reaching a hop with RP <= n-1, the first incoming candidate with replacement hops less than or equal to that of the initial route will be chosen as the substitute.
5. If several backward route hops, RP <= n-1, have chosen their own candidates, the hop with the smallest RP and with the hopping number less than or equal to that of the initial route will be the one to do local route-switching.

4.3 An Illustration

To see how to apply these regulations, we consider a simple example by using model 1. In model 1, as the nth hop detects that the link of (n-1)th to nth is at warning level (Fig. 2-3), it broadcasts a LWM with maximum hopping number equal to 2 (MHN = 2) to its neighborhood. The (n-1)th and (n+2)th hop will discard this message, but the (n+1)th hop will retransmit it. The neighbor hosts of the nth, the MH 2, MH 3, MH4, and (n+1)th hops will check the route record that came with this LWM. MH 3 will discard this LWM from (n+1)th hop for it has received once from nth hop. MH 3 also will discard and stop to retransmit this LWM affixed with MH 2's proposed candidate, for MH 2 has smaller hopping number of proposed candidate than its own proposed candidate. MH 2 will discard and stop re-transmitting this message affixed with MH 3's proposed candidate, for MH 3 has larger hopping number of proposed candidate, -- (n-2)th - MH 2 – MH 3 - nth --, than its proposed candidate. MH 2 will retransmit the LWM from nth hop and affix its own proposed candidate with this message, -- (n-2)th – MH 2 – nth --. MH 4 will discard and stop re-transmitting the LWM affixed with MH 2's proposed candidate, for its proposed candidate, -- (n-2)th – MH 4 – MH 2 – n --, has larger hopping number than that of MH 2's. As the LWM affixed with the MH 2's proposed candidate reaches at the (n-2)th route hop, the (n-2)th hop will immediately select this substitute to be its proposed candidate, for it has the same hopping number as that of the initial route. The MH 4 will affix its proposed candidate with this LWM from nth hop, -- (n-2)th – (n-1)th –MH 4 – nth --, and retransmit it. The (n-1)th route hop will accept MH 4's candidate to be its proposed candidate, for this substitute is the only one reaching at (n-1)th hop. Then, both the (n-2)th hop and (n-1)th hop has its own proposed substitute candidate. Because by limiting the MHN to 2, the possible hops that received the LWM are (n-2)th and (n-1)th in this example. And the (n-2)th hop's RP and

the hopping number of its proposal is smaller than that of (n-1)th hop, this candidate of – (n-2)th – MH 2 – nth – will be the local substitute automatically. The (n-2)th hop will switch following data messages to this new substitute route. The other models can also utilize the same process to find a local substitute for initial route.

5. EVALUATION AND DISCUSSION

In this section, we evaluate this proposed algorithm of local/global strategy based on signal strength by calculating the latency needed for route switching when a routing-failure occurs. In the early part, the problem of route failure without local adaptive capability is discussed. First we analyze the latency for both the global adaptation and the local adaptation algorithm, without utilizing the advance-warning mechanism. After that we will add the advance-warning mechanism with the local adaptation to see how much improvement can be obtained. This evaluation verifies that our proposal has the potential to handle route switching seamlessly for communication services at a mobile wireless ad-hoc network that has the characteristic of high migration rate of mobile hosts.

We derive a simple function to estimate the latency for a route switching for the global adaptation strategy. Assume that the network topology is dense enough such that it is possible to find at least one neighbor host around each hop along a variable route, and also that it is possible to find at least one substitute either at global or local region. Though, these evaluations are based on an ideal-operating environment, it still can reflect the essentials of the problem. The total latency for the route switching at local region from detecting a route failure to renewing data message routing can be expressed as: Total latency = Latency for routing REM (T_{REM}) + Latency for routing RQM (T_{RQM}) + Latency for routing RRM (T_{RRM}), where REM = route error message. And these three types of routing latency can be expressed individually by the following functions: $T_{REM} = T_{Time\text{-}out} + \sum (T_{REM\text{-}processing} * N_{REM\text{-}passed}) + \sum (T_{REM\text{-}transmission} * N_{REM\text{-}passed})$;

$T_{Time\text{-}out}$: Time-out latency for route failure confirmation at nth hop. $N_{REM\text{-}passed}$: Number of hops of REM passed. $T_{REM\text{-}processing}$: Latency for REM processing at a host. $T_{REM\text{-}transmission}$: Latency for REM transmitting over free space. $T_{RQM} = \sum (T_{RQM\text{-}processing} * N_{RQM\text{-}passed}) + \sum (T_{REM\text{-}transmission} * N_{REM\text{-}passed})$;

$N_{RQM\text{-}passed}$: Number of hops of RQM passed. $T_{REM\text{-}processing}$: Latency for REM processing at a host. $T_{RQM\text{-}transmission}$: Latency for RQM transmitting over free space. $T_{RRM} = \sum (T_{RRM\text{-}processing} * N_{RRM\text{-}passed}) + \sum (T_{RRM\text{-}transmission} * N_{RRM\text{-}passed})$;

$N_{RRM\text{-}passed}$: Number of hops of REM passed. $T_{RRM\text{-}processing}$: Latency for REM processing at a host. $T_{RRM\text{-}transmission}$: Latency for RRM transmitting over free space.

Also, assume that a duplex communication is available between hosts in this example network that allows a routing-error message sending backward directly to the source host from a route hop that encountered routing failure The RQM and RRM will pass through the same hops for a route discovery processing. The message transmission over free space costs little latency compared with that of the message processing latency at hosts. So it could ignore the transmitting latency without affecting this evaluation much. Further, assume that the latencies for these three types of message processing (REM, RQM, and RRM) are the same and is a constant for every host in the network. Then, the total latency to renew the data message routing for hosts encountering route failure will be: $T_{Total\ Latency\ for\ global\ adaptation} = T_{Time\text{-}out} + \sum (T_{Message\ processing\ at\ a\ host} * N_{REM\text{-}passed}) + \sum (T_{Message\text{-}processing\ at\ a\ host} * 2 * N_{RRM\text{-}passed})$;$T_{Total\ Latency\ for\ global\ adaptation} = T_{Time\text{-}out} + T_{Message\ processing\ at\ a\ host} * (\sum N_{REM\text{-}passed} + 2 * \sum * N_{RRM\text{-}RQM\text{-}passed})$.

From the above function, it is clear that the values of $N_{REM\text{-}passed}$ and $N_{RRM\text{-}RQM\text{-}passed}$ will decide how much is the total latency. The $N_{REM\text{-}passed}$ variable is irrelevant for the case that the REM will not reach at the source host. However, the $T_{Time\text{-}out}$ setting at source host should allow the maximum duration for message routing processing from destination to source host ($T_{Time\text{-}out\ at\ source\ host} = T_{Message\ processing\ for\ a\ host} * N_{Total\text{-}\ hops}$). That duration will be the same as that of the worst case of the REM passing through all hops. For the local adaptation algorithm without advance-warning (AW) mechanism, following the same assumptions, the total latency to renew a data message routing would be: $T_{Total\ Latency\ for\ local\ adaptation\ without\ AW} = T_{Message\ processing\ at\ a\ host} * \sum (N_{LWM\text{-}passed})$; The $N_{LWM\text{-}passed}$ variable decides the total latency needed to renew a data message routing, and it is a limited small number. Then, considering a minimum common hopping number that could satisfy three possible migration models simultaneously; Common_min_HN = Maximum {min_HN_Model 1, min_HN_Model 2, min_HN_Model 3} = Maximum {2, 3, 2} = 3; So, the minimum hopping number that can satisfy three possible migration models simultaneously is 3. In local adaptation with advance warning mechanism, the warning duration is strongly dependent on operating environment. If this duration is set to be larger than the total latency needed to renew the data message routing, the total latency will be zero, $T_{Total\ Latency\ for\ local\ adaptation\ with\ AW} = 0$, for the new local adaptation strategy with advance warning. So, the minimum interval for warning duration is:

$T_{Total\ Latency\ for\ local\ adaptation\ with\ AW} = 0 = T_{warning\ duration} - T_{Message\ processing\ at\ a\ host} * \sum (N_{LWM\text{-}passed})$;

$T_{warning\ duration} = T_{Message\ processing\ at\ a\ host} * \sum (N_{LWM\text{-}passed})$;

$T_{warning\ duration} = 3 * T_{Message\ processing\ at\ a\ host}$;

Thus, the minimum boundary value for setting the warning duration is equal to $3 * T_{Message\ processing\ at\ a\ host}$.

Fig. 3-1 and fig. 3-2 show the results of the evaluation. These evaluations show that routing algorithms without local adaptation capability will spend considerable time on waiting for the route switching to be completed as a route failure occurs. By introducing our proposed algorithm, the efficiency for route switching can get a real improvement if a local substitute is available. It is possible to avoid unnecessary searching for local substitute if the local routing table at each host has perfect maintenance. In other words, a route hop just needs to check its own local routing table when encountering route failure and know whether or not a neighbor host is available. If there is no available neighbor host, this hop can abandon the local adaptation attempt and send a warning message directly to source host. During the period of warning message routing to source host, the initial route can continue data message transmission. Thus, in the worst case, this proposed global adaptation algorithm still could reduce the latency for route switching at the global region.

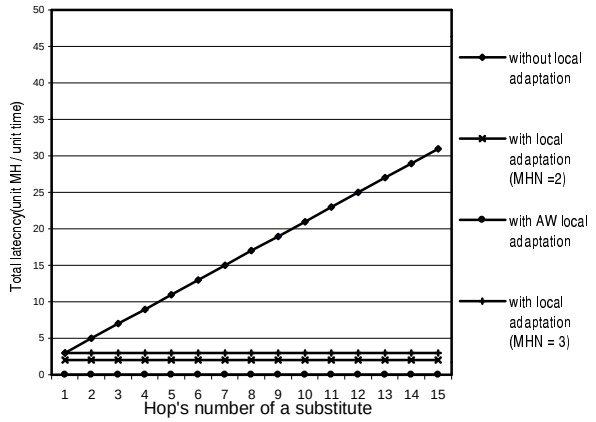

Figure 3-1. Total latency to renew the data message routing as the second hop encounters route failure in a route with n hops.

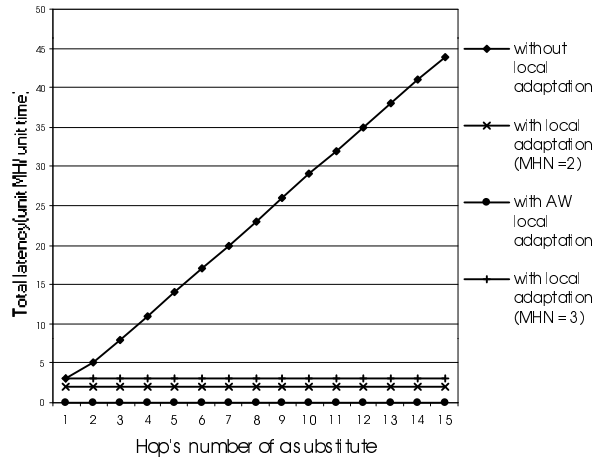

Figure 3-2. Total latency to renew the data message routing as the (n-1)th hop encounters route failure in a route with n hops.

As part of future work, the essential characteristics of mobile hosts of ad-hoc networks will be further studied. In a real world, the migration of mobile hosts is common. So, a routing algorithm for such network should have enough capabilities to adapt possible topology change, no matter if the topology is stable or dynamic. Through the investigation about these essential characteristics, a more robust and practical routing algorithm for mobile wireless ad-hoc network can be setup. Our research will consider simulation and the determination of success rate in route switching using the proposed technique under more realistic topological setting.

Reference:

[CE95] M. Corson, and A. Ephremide, " A Distributed Routing Algorithm for Mobile Wireless Networks" ACM J. Wireless Networks, 1, p. 61-81, Jan. 1995.

[DRWT97] R. Dube, C. Rais, K. Wang, and S. Tripathi. "Signal Stability-Based Adaptive Routing for Ad Hoc Mobile Networks". IEEE Personal Comm., p. 36-45, Feb. 1997.

[DSB97] B. Das, R. Sivakumar, and V. Bharghavan. "Routing in ad-hoc networks using a virtual backbone". ACM SIGCOMM '97, p. 1-20, Jan. 1997.

[IB94] T. Imielinski, B. Badrinath. "Mobile Wireless Computing", Comm. of the ACM, p. 18-28, Vol. 37, No.10, Oct 1994.

[IK96] T. Imielinski and H. Korth. "Introduction to Mobile Computing", Kluwer Acad. Pub., p. 1-43, 1996.

[JCNK95] B. Jabbari. G. Colombo, A. Nakajima, and J. Kulkarni, "Network Issues for Wireless Communications". IEEE Comm. Magazine, p. 88-98, Jan. 1995.

[JM96] D. Johnson and D. Maltz. "Dynamic Source Routing in Ad-Hoc Wireless Networks", Kluwer Academic Publishers, p. 153-181, 1996.

[KCVP95] P. Krishna, M. Chatterjee, N. Vaidya, D. K. Pradhan. "A Cluster-Based Approach for Routing in Ad-Hoc Networks". Proc. of the 2nd USENIX,p.1-10, 1995.

[PGH95] J. Padgett, C. Gunther, and T. Hattori. "Overview of Wireless Personal Communications". IEEE Comm. Magazine, p. 28-41, Jan. 1995.

[PB94] C. Perkins and P. Bhagwat. "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Computer Comm. Re.,24, 4 (ACM SiGCOMM 1994), p. 234-244, 1996.

Ting-Chung Tien received the B.S. degree in Physics from the Tankang University, Taiwan and M.S. in Electrical Engineering from SUNY-Buffalo, NY. His research field is wireless mobile computer networks.

Shambhu J. Upadhyaya received his Ph.D. in Electrical & Computer Engineering from University of New Castle, Australia in 1987. His research interests are fault diagnosis, fault tolerant computing, distributed systems and computer security.