International Journal on Wireless and Optical Communications
Vol. 3, No. 1 (2006) 83–100

NODE FRAGILITY VERSUS LINK FRAGILITY FOR ROUTE SELECTION IN MOBILE *AD HOC* NETWORKS

IMANE ALY SAROIT ISMAIL
Information Technology Department,
Faculty of Computers and Information, Cairo University,
5 Tharwat street, Orman, Giza, Egypt
iasi62@hotmail.com

Accepted 27 December 2005

A mobile *ad-hoc* network is a dynamically changing network of mobile devices that communicate without the support of a fixed structure. There is a direct communication among the neighboring devices, but non-neighboring devices requires a robust and intelligent routing strategy to ensure reliable and efficient communication. The performance of routing protocols depends on the quality of the routes chosen in terms of route longevity. A protocol that discovers better routes also features a reduced rate of route failures and lesser route discovery traffic. Thus an important aspect of the decision process is to compare and pick the more stable route. A Route Fragility Coefficient (RFC) metric was used to estimate routes' stability. In this paper, the link fragility metric is used to create a new metric called Node Fragility Coefficient (NFC) that is also used to estimate routes' stability. Comparing routing protocols using RFC and NFC metrics to select the more stable routes, simulation results prove that using NFC is much better, it leads to better throughput, average packet's delay, average number of hops/ packet, average consumed power/ packet, percentage number of route changes and percentage number of undelivered packets.

Keywords: *Ad hoc* routing-link; stability-route fragility-link; fragility-node.

1. Introduction

Mobile *ad hoc* networks — also called MANETs — promise to break many of the traditional requirements for building communication networks and make information exchange possible in a wide variety of situations. The *ad-hoc* wireless network is a network where no fixed infrastructure exists. Typical applications of MANET are outdoor special events such as conferences, communications in regions with no wired infrastructure support, in emergencies and natural disasters and in military operations [Toh, 2002; Kuladinithi, Görg & Allee; Perfkins, 2001].

In MANETs mobile devices randomly move and communicate over radio. If two mobile devices are in radio transmission range, they can communicate with each other directly. Otherwise, other mobile devices should forward packets between them; this requires a robust and intelligent routing strategy to ensure reliable and efficient communication [Toh, 2002; Kuladinithi, Görg & Allee; Perfkins, 2001; Mauve, Widmer & Hartenstein, 2001].

Mobile *ad hoc* networks pose many complex issues specially when used in a real time environment. In real time, packets reach the destination within certain time constraints. For this to be achieved the links of the network have to be maintained till all the packets get to the destination i.e. for the lifetime of the communication. Once a route has been established to the destination, the corresponding links are not dependable because of continuous motion of the nodes. Hence once a link breaks the routing protocols will take some finite time to form a new route or to hand-off to a new route. This finite time can be critical in most of the real time applications. Thus certain modifications have to be made to existing routing protocol to incorporate route maintenance without any lapse in time [Sujeetv].

A key factor deciding the performance of a routing protocol in mobile *ad hoc* networks is the manner in which it adapts to route changes caused by mobility; of course a less dynamic route lasts longer. A few routing protocols aim at establishing stable routes are found in [Geunhwi *et al.*, 2002; Gerharz *et al.*, 2003; Agarwal *et al.*, 2000; Agarwal & Das, 2003; Beongku & Papavassiliou, 2002; Tickoo, Raghunath & Kalyanaraman, 2003].

The Route Fragility Coefficient (RFC) metric was proposed in [Tickoo, Raghunath & Kalyanaraman, 2003] to compare routes in order to obtain more stable one. RFC uses signal levels to estimate the rate at which a given route expands or contracts. Expansion refers to adjacent nodes moving apart, while contraction refers to them moving closer. RFC combines the individual link contraction or expansion behavior to present a unified picture of the route dynamics. It has been demonstrated that lower the value of RFC, more static (less fragile) the route. So the RFC metric is used as a basis for route selection such that route discovery yields routes that last longer, and hence increase throughput while reducing control overhead.

In this paper, the individual link fragility factor metric from [Tickoo, Raghunath & Kalyanaraman, 2003] was used to create the Node Fragility Coefficient (NFC) metric. NFCs are used to describe how dynamic a route is; more static routes have lower values of NFC. A new routing protocol proceeding in three phases is proposed:

- First, every node broadcasts a “HELLO” packet to all nodes in its transmission range every time period (ΔT).
- Second, on receiving a Route Request (RREQ) packet (containing accumulated NFC and hop counters) each node on the route computes its NCF using the link fragility of the virtual links connecting it to all nodes in its transmission range at this moment. The result is then added to the NFC counter in RREQ, also the hop counter is incremented by 1.
- Third, the destination collects multiple RREQs with different NFCs and hop counters. It employs a function of the number of hops and the value of NFC for the routes represented by each RREQ, to choose the RREQ representing the best route and replies to it.

This remainder of this paper is organized as follows. Section 2 defines routing in mobile *Ad hoc* networks. In Sec. 3, calculation of the Route Fragility Coefficient (RFC) metric is illustrated. The new proposed metric, Node Fragility Coefficient (NFC) is derived in Sec. 4, together with the proposed algorithm. Comparison between routing protocols using RFC and NFC metrics is done using simulation programs, results are presented in Sec. 5. Conclusions and future trends are discussed in Sec. 6.

2. Routing in Mobile *Ad Hoc* Networks

A wireless *ad hoc* network (MANET) is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. Each node in a wireless *ad hoc* network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, so the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. Hence, there is a need for efficient routing protocols to allow the nodes to communicate over multihop paths consisting of possibly several links in a way that does not use any more of the network "resources" than necessary [Sujeetv].

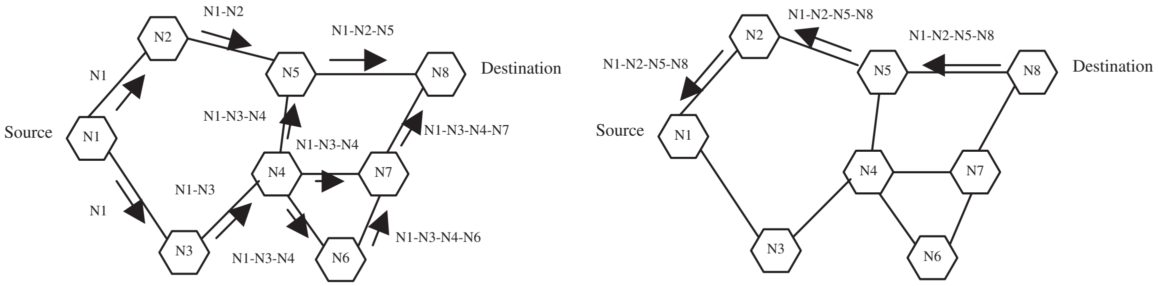
The basic assumption in an MANET is that, any two nodes willing to communicate may be outside the wireless transmission range of each other but may be able to communicate in multiple hops, if other nodes in the network are willing to forward packets for them. The mobile nodes would be arbitrarily located and would be moving in a dynamic manner.

Node mobility and the lack of topological stability make the routing protocols previously developed for wireline networks unsuitable for *ad hoc* networks. The *ad hoc* network routing protocols can be roughly divided into three categories: proactive, reactive, and hybrid [Toh, 2002; Kuladinithi, Görg & Allee; Perfkins, 2001; Mauve, Widmer & Hartenstein, 2001].

A proactive routing protocol, also called a table-driven protocol, requires that each node maintains an up-to-date routing table, such that a route is readily available when data packets need to be sent out. Periodical dissemination of routing information is done every ΔT seconds. If ΔT is too large, the outdated routing information may cause extra delay and packet loss. If ΔT is too small, a huge overhead may use up system resources and causes large delays and serious packet loss. Routing protocols such as DSDV, STAR, CSGR, and WRP are examples of proactive protocols [Toh, 2002; Kuladinithi, Görg & Allee; Perfkins, 2001; Mauve Widmer & Hartenstein, 2001].

In reactive routing protocols, also called on-demand protocols, a node is not required to maintain a routing table, but instead a route query process is initiated whenever it is needed. This route is used until communications stop. Route recovery means finding a new route only when the old one breaks. A reactive protocol avoids the control message overhead incurred in building routing tables, which may never be used before the routes become obsolete due to topology changes. These routing protocols have no overhead, but they have longer delay since data packets must wait before a route is discovered or recovered. Routing protocols such as AODV, DSR, TORA, SSR, LAR and PAR are examples of reactive protocols [Toh, 2002; Kuladinithi, Görg & Allee; Perfkins, 2001; Mauve, Widmer & Hartenstein, 2001].

Hybrid flat protocols were proposed to combine the benefit of both approaches. ZRP [Toh, 2002] and SHARP [Ramasubramanian, Haas & Gün Sirer, 2003] are examples of hybrid protocols.



(a) Propagation of the route request

(b) Propagation of the route reply

Fig. 1. Route discovery in DSR.

As mentioned, the reactive routing algorithms consists of two phases, the first one is the route discovery which is executed upon demand, only when a source node needs to send a packet. The second one is the route recovery and maintenance which is executed only when a route is broken, however, these last procedures consume many resources. So it is important to use stable routes to minimize the need for route recovery.

In order to explain how route discovery process is done in reactive protocols, consider the route discovery process used for DSR reactive routing protocols (Fig. 1): The source initiates a route discovery packet (route request; RREQ) and broadcast it to the network. All the nodes in its range get the packet. These nodes make an entry of their own address in the packet and again broadcast the packet to the nodes in their range. If a packet reaches a node whose entry is already in the packet, then the packet is discarded. However when the destination gets the route discovery packet, it has a sequence of all the nodes, which the packet has traveled along to the destination. The destination now returns a route reply packet through the same route back (back track). Similar approaches; also based on RREQ distribution is used for the other protocols.

The obvious drawback of all route discovery approaches is the increased traffic due to continuous position update and link update packets sent by the nodes when a node is continuously changing its direction, e.g. a car takes a small turn.

The performance of routing protocols depends on the quality of the routes chosen in terms of route longevity. A protocol that discovers better routes also features a reduced rate of route failures and lesser route discovery traffic. Thus an important aspect of the decision process is to compare and pick the "better" route; this route consists of nodes that "stay together" while being mobile for as long as possible.

In order to maintain continuous connectivity of the routes, the lifetime of each link has to be predicted. The source node has to know when a particular link will break and just before that the source either discovers a new route or hands over to an alternative route.

To minimize route breaking, it is important to find a route that endures longer time. Shortest path route has short lifetime especially in highly dense *ad-hoc* wireless networks. Some routing protocols such as RABR [Agarwal *et al.*, 2000], DRM [Agarwal & Das, 2003], entropy based model [Beongku & Papavassiliou, 2002] and RFC [Tickoo, Raghunath & Kalyanaraman, 2003] protocols are considering the link stability, trying to find more stable route. The second and third protocols need to use the Global Positioning System (GPS) while the other two do not need that.

3. Route Fragility Coefficient

A key factor deciding the performance of a routing protocol in mobile *ad hoc* networks is the manner in which it adapts to route changes caused by mobility, of course, a less dynamic route lasts longer. The Route Fragility Coefficient (RFC) metric was proposed in [Tickoo, Raghunath & Kalyanaraman, 2003] to compare routes. RFC estimates the rate at which a given route expands or contracts. Expansion refers to adjacent nodes moving apart, while contraction refers to their moving closer. RFC combines the individual link contraction or expansion behavior to present a unified picture of the route dynamics. It has been demonstrated that lower the value of RFC, more static (less fragile) the route. RFC metric was used as a basis for route selection so that route discovery yields routes that last longer and hence increases throughput while reducing control overhead.

In order to compute this metric the rate at which the separation between each adjacent pair of nodes in the route is increasing (expansion) or decreasing (contraction) was estimated. A measure of such an expansion or contraction is given by the relative speed of the nodes.

This section is divided in three subsections, first the techniques used to estimate relative speed of a pair of nodes are discussed, then discussion of how to combine these measurements to get a single number representative of the whole route; the RFC. Finally, the distributed routing algorithm using the RFC metric is illustrated [Tickoo, Raghunath & Kalyanaraman, 2003].

3.1. *Estimating relative speed*

Consider a node n_1 receiving packets from a node n_2. Let t_1 and t_2 be the times at which the last two packets from n_2 were received. Denote the received power for these packets as P_1 and P_2. Consider two possible situations, the nodes are moving closer ($P_1 > P_2$) or are moving apart ($P_1 < P_2$).

3.1.1. *Nodes moving apart*

Figure 2 indicates two nodes n_1 and n_2, with d_1 and d_2 being distances corresponding to the positions of node n_2 at received powers of P_1 and P_2 at time t_1 and t_2 respectively. To estimate the relative speed of the nodes, we do not need the exact position of the two nodes. This is represented by the two circles indicating all the possible positions in which

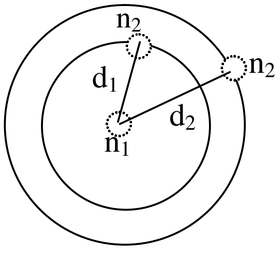


Fig. 2. Nodes moving apart.

n_2 can lie with respect to n_1 position. Assuming a free space path loss model, we have:

$$P_i = \frac{K}{d_i^2},$$

then;

$$\frac{d_i}{\sqrt{K}} = \frac{1}{\sqrt{P_i}}; \tag{1}$$

where K denotes a constant that depends on the antenna gains of the two nodes and the wavelength of the transmission.

Since the nodes are assumed to be moving with a constant velocity in a piecewise linear manner, we can then write the following.

$$\frac{d_2 - d_1}{\sqrt{K}} = \frac{1}{\sqrt{P_2}} - \frac{1}{\sqrt{P_1}}. \tag{2}$$

So the following equation allows computing the relative speed v, normalized by the constant K.

$$\frac{v}{\sqrt{K}} = \frac{1}{(t_2 - t_1)}\left(\frac{1}{\sqrt{P_2}} - \frac{1}{\sqrt{P_1}}\right). \tag{3}$$

3.1.2. *Nodes moving closer*

For the case where $P_2 > P_1$, i.e. n_2 is moving closer to n_1 in Fig. 3, a similar analysis holds. Assuming the node moves in a straight line. Note that the node n_2 will stay in the range of n_1 for a longer time if it moves along a radial direction. The worst-case is when n_2 starts moving away from n_1 just after time t_2.

The line segment |BC| represents such a path:

$$|BC| = \sqrt{d_1^2 - d_2^2}.$$

We then obtain the relative v, normalized by the constant K.

$$\frac{v}{\sqrt{K}} = \frac{\sqrt{d_1^2 - d_2^2}}{(t_2 - t_1)} = \frac{1}{(t_2 - t_1)}\sqrt{\frac{1}{P_1} - \frac{1}{P_2}}. \tag{4}$$

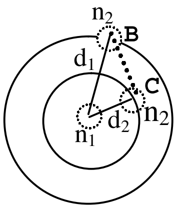


Fig. 3. Nodes moving closer.

3.2. *Routing protocol based on route fragility coefficient*

Using Eqs. (3) and (4), we have the means to compute an estimate of the relative speed (normalized by a constant) with just the received power measurements. Equipped with a measure of expansion and contraction of the link between a pair of nodes, in order to combine these values to obtain a single metric for a route R;

- Let E denote the set of node-pairs (n_k, n_j) such that they are adjacent nodes in R and are moving apart. Using Eq. (3), the Cumulative Expansion Metric is given by:

$$CEM = \sum_{i \in E} \frac{v_i}{\sqrt{K_i}}. \tag{5}$$

- Let C denote the set of node-pairs (n_k, n_j) such that they are adjacent nodes in R and are moving closer. Using Eq. (4), the Cumulative Contraction Metric is given by:

$$CCM = \sum_{i \in C} \frac{v_i}{\sqrt{K_i}}. \tag{6}$$

Observe that CCM and CEM are positive quantities and higher values indicate that the route is more dynamic (more fragile). In order to capture these two measures in a single metric, we consider a weighted sum. Note that; a contracting link (neighbors moving closer) lasts longer than an expanding link. Thus a weighted sum would have to penalize expansion more than contraction.

In order to obtain this combined metric; consider a pair of nodes n_1 and n_2 which are in each other's range at some point in time. Let d_1 indicate the distance between the nodes when they are closest. We can divide the period in which they are within range, into two parts — one, comprising of the time when they drawing closer till d_1; two, comprising of the time when they are moving apart. On the average we can consider these two distances to be equal. Thus, a contracting link eventually transforms into an expanding link, staying alive for approximately twice the time as compared to a link currently detected to be expanding. Hence we propose the following combined metric, which we call the "Route Fragility Coefficient" (RFC):

$$RFC = CCM + 2 * CEM. \tag{7}$$

This reflects the intuition that an expanding link is roughly twice as bad as a contracting link.

In general, the average lifetime of a path decreases with its length. The reason for this is that longer paths have a higher probability of including a short lived link. For the stability metrics, the probability of making a wrong selection increases with every additional hop. Although stable paths are identified by the different stability metrics; which are usually not the shortest paths, the length of a route should not rise unnecessarily. Longer routes require more packet transmissions and thereby reduce network capacity. This effect has to be traded off against the benefit of a possibly reduced routing overhead due to fewer route failures [Gerharz *et al.*, 2003].

To remove the bias against longer routes, the following procedure is considered to compare route metrics. Denote RFC_1 and RFC_2 the metric obtained for two routes R_1

and R_2, if N_1 and N_2 are the number of hops in the respective routes. Then the following condition was used to decide. If R_1 is better than R_2, than

$$\frac{RFC_1}{N_1} < \frac{RFC_2}{N_2}. \tag{8}$$

So, in order to quantify and compare the dynamic nature of routes, we use the following:

- The route whose *RFC* evaluates to zero, features nodes that are moving with zero relative speed. Such a route would out-live any route with a greater value of *RFC*.
- The shortest route is not necessarily the best route. By employing a comparison strategy that normalizes the *RFC* by hop-length, we allow discovery of longer, but more stable, routes.

3.3. *Route fragility protocol*

The route fragility protocol proceeds in two phases:

- First, on receiving a Route Request (*RREQ*) packet, each node on the route computes the extent by which the "link" to its previous hop is contracting or expanding. The extent of expansion or contraction is captured by a function of the received power samples. Assuming a free-space path loss model, the received powers of two successive packets are examined. If the nodes are moving apart the second power measurement is lesser, if they are moving closer the second power measurement is greater. Using Eqs. (3) or (4) to calculate *CEM* or *CCM* according to expansion or contraction. The result is then added to one of two counters in *RREQ* (one for expansion and the other for contraction), as in Eq. (7).
- Second, the destination collects multiple *RREQs* and employs Eq. (8) (function of the number of hops and the value of *RFC*) for the routes represented by each *RREQ* to arrive at the best route, and replies to it.

3.4. *Route fragility coefficient evaluation*

In this section, the protocol proposed in [Tickoo, Raghunath & Kalyanaraman, 2003] for route selection in mobile *ad hoc* network is presented. This protocol provides a new metric — calculated in a distributed manner — that measures the fragility of a route (*RFC*); it is used to quantify the dynamic nature of a route and allow the routing protocol to choose the more static and long-lasting routes; without requiring any global positioning information, clock synchronization or periodic beacon packets. This metric (*RFC*) is calculated by accumulating the link fragility coefficients (*LFC*) of the links composing it.

The NS-2 simulation was used to prove the enhancing of route selection using *RFC*. The objectives of the experiments were two-fold: (a) To verify the relation of RFC with route longevity and the resultant gains in throughput, and (b) to examine the gains in terms of reduced route over-head. The simulation consisted of wireless nodes moving in an area of 1000 m × 500 m according the 'random waypoint' model. The nodes move with velocities that are chosen randomly. Varying velocities, varying network size (number of sources) and varying transmission rates are used.

The throughput's results show the percentage of packets delivered successfully; it has been found that *RFC* consistently out-performs original protocols, across various network sizes. Further at higher speeds ($\geq 20\,\text{m/s}$) and moderate network size (30 to 40 nodes), the gains with *RFC* are higher, indicating the fact that stable and less dynamic routes are being exploited. This can be viewed as a cause of higher variance in node velocities. With higher variance, the spread in relative velocities is higher, implying the existence of more routes which are dynamic.

Simulation results prove that using *RFC* leads to very smaller number of route errors generated. There are multiple reasons for this gain. First, as noted earlier *RFC* chooses routes that last longer and hence reduces the number of route errors. Second, with higher mobility, the original protocols cache has many of stale routes leading to increased route errors. Thus the gain in terms of reduced route errors increases with higher node speeds.

An important benefit of long-lasting routes is the reduced control overhead in terms of lesser route discovery iterations. Since route selection based on *RFC* leads to a choice of routes that are more durable, we would expect to see a reduction in the number of routing packets sent for every data packet transmitted.

4. Node Fragility Coefficient

In *Ad hoc* networks, any node can be a forwarding station for any station connections, so any movement of a node can break many connections. Note that routes usually consist of more than one hop, i.e. passes over more than two nodes, so node stability is a very important factor.

As clear from the previous section, the link fragility coefficient considers the movement of a node in one end of the link with respect to the node in the other end, regardless of the movement of the other nodes surrounding any one of them. In this paper, we suggest estimating a node fragility coefficient; this coefficient will consider the movement of a node with respect to all other nodes surrounding it, i.e. its stability in its original position.

This section is divided into two subsections; the first one explains how the node fragility is estimated. In the second one the protocol routing based on node fragility metric is illustrated.

4.1. *Node fragility estimation*

To estimate the node stability, we must consider the movement from its original position with respect to all nodes around it, not only one node.

Note that estimation of the speed done in Sec. 3.1 considers essentially the nodes (not links) movement, so the derived equations in the previous section hold. Then, the individual link fragility coefficient metric from [Beongku & Papavassiliou, 2002] is used to obtain a more efficient metric to estimate the route stability; this is the Node Fragility Coefficient (*NFC*) metric.

Let L denotes the set of links connected to node m at a moment, the node fragility NFC_m is the sum of the *LFC* of all links connected to m. It is calculated as follows:

$$NFC_m = \sum_{i \in L} LFC_i; \tag{9}$$

where L is the set of links connecting m to all nodes in its range.

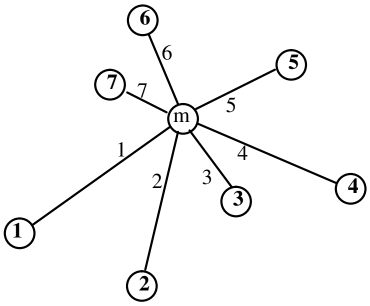


Fig. 4.

LFC of any link i — with one end node m — is calculated using equations in Sec. 3, as follows:

*Over a number of time periods, do the following:

- Node m receives power level from the other end node of link i.
  - ○ If it is smaller than that received the last time period, use Eq. (3) to calculate *CEM*.
  - ○ If it is greater than that received the last time period, use Eq. (4) to calculate *CCM*.
- Use Eq. (7) to accumulate the calculated value in the previous step to obtain LFC_i.

NFC for any node m is calculated by accumulating the link fragility coefficient for all links connecting it directly to any other nodes (Eq. (9)). For example in Fig. 4;

$$NFC_m = LFC_1 + LFC_2 + LFC_3 + LFC_4 + LFC_5 + LFC_6 + LFC_7.$$

A detailed example; explaining how to calculate *LFC* and *RFC*; is given in the Appendix.

Of course, node fragility of node m (NFC_m) can change at any moment because of:

- Change of any *LFC* value of any of the connecting links at this moment.
- Some links do no more existing (their other end nodes are out of the transmission range of node m).
- New links are added (their other end nodes enter the transmission range of node m).

4.2. *Routing protocol based on node fragility coefficient*

Known that every node sends “HELLO” packet every time period (ΔT), the node fragility protocol proceeds as follows:

- Any node has a packet to send, issues a Route Request (*RREQ*) packet propagating in all directions. It also sets an *NFC* counter and a hop counter — in the *RREQ* — to zero.
- On receiving a Route Request (*RREQ*) packet, any intermediate node i do the following:
  - ○ Uses the successive power levels received each ΔT to calculate *LFC*s of all links connecting it to all nodes in its transmission range.
  - ○ Uses Eq. (9) to compute its NFC_i.

  - ○ Accumulates its NFC_i to the NFC counter in the $RREQ$, and increment the hop counter in the $RREQ$ by 1.
  - ○ Finally propagates the $RREQ$ packet in all directions (except the one it comes from).
- The destination collects multiple $RREQ$s and employs equation similar to that in (8) but for NFCs (function of the number of hops and the value of NFC) to choose the $RREQ$ representing the best route and replies to it.

5. Numerical Results

This section is divided into three subsections. The first one describes the network model used. The second illustrates the performance parameters used to evaluate the proposed node fragility metric. Simulation results comparing routing protocols aiming to use stable routes based on using RFC and NFC metric are illustrated in the third subsection.

5.1. *Network model*

As shown in Fig. 5, a mobile *ad hoc* network is represented by a graph consisting of a set of nodes together with a set of edges. At any time instant, an edge exists between two nodes if and only if one node can successfully transmit to the other node (they are in each other's range). In this case, we say that the link from node to node is up. Otherwise, the link is down or has failed. Of course, the topology of a mobile *ad hoc* network changes continuously.

Since it is very difficult to estimate how users will move when these *ad hoc* networks are deployed, it is good to give the routing protocols as hard time as possible for the movement models, so the following assumptions must hold for each node:

- The node's initial location must be random, so its coordinates are created randomly.
- The node's motion must be random, so the distance it covers and the direction of its movement are created random.

Also for each packet, source, destination and arrival time are created randomly.

5.2. *Performance parameters*

The following six parameters are used to compare the routing protocols using Route fragility Coefficient (RFC) and Node Fragility Coefficient (NFC) metrics to estimate route stability:

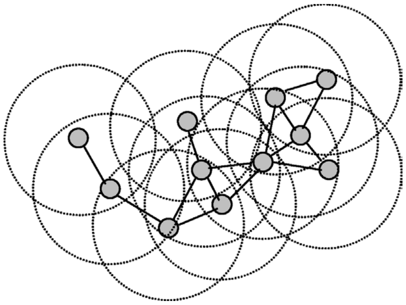


Fig. 5. *Ad hoc* network model.

1. *Throughput*

Assuming available channels, throughput represents the average number of packets delivered per second.

$$Throughput = \frac{Total\ number\ of\ packets\ delivered}{Time\ needed\ to\ deliver\ these\ packets\ in\ seconds}.$$

2. *Average packet's delay*

This parameter calculates the average time between the source starts sending the packet and the destination receives it.

$$Average\ packet\text{'}s\ delay = \frac{\sum_{\forall\, delivered\ packets} (Arrival\ time_{at\ destination} - Sent\ time_{at\ source})}{Total\ number\ of\ delivered\ packets}.$$

3. *Average number of hops*

This parameter calculates the average number of hops/route for all delivered packets.

$$\begin{aligned} &Average\ number\ of\ hops \\ &\quad = \frac{\sum_{\forall\, delivered\ packets} (Number\ of\ hops\ in\ the\ route\ traversed\ by\ the\ packet)}{Total\ number\ of\ delivered\ packets}. \end{aligned}$$

4. *Average packet's power*

The energy consumption corresponding to each transmission can be formulated as: $E_1(r) = k_1 r^w + k_2$ where r is the radio transmission range, w is the path loss exponent, k_1 is determined by the characteristic of the transmitter and the channel, and k_2 is the transceiver energy consumption that is not related to r.

If E_r is the energy consumption of receiving, decoding, and processing data packets at the receiver. As a result of the above formulation, the single-transmission consumed energy is fixed for a given r and is given by $E_1(r) + E_r$. Quantities k_1, $k_2 + E_r$ and w are assumed to be 6.6319×10^{-5}, 1.476×10^{-2} and 2 respectively [Deng *et al.*, 2004].

$$\begin{aligned} &Average\ packet\text{'}s\ power\ consumed \\ &\quad = \frac{\sum_{\forall\ delivered\ packets} (Power\ consumed\ to\ deliverer\ the\ packet)}{Total\ number\ of\ delivered\ packets}. \end{aligned}$$

5. *Percentage of route change*

This parameter is used to calculate the percentage of route changes needed in case of link failure in an established route.

$$Percentage\ of\ route\ changes\ = \frac{Number\ of\ route\ changes}{Total\ number\ of\ routes} * 100.$$

6. *Percentage of undelivered packets*

As a medium access control protocol, to deliver a packet from any node i to another node j, a request to send (*RTS*) packet is sent from node i to node j. In case of agreement (available channel), node j sends a clear to send (*CTS*) packet to i, so node i sends the packet

[Toh, 2002]. An undelivered packet is the one whose source receives a CTS packet, so it sends the packet, but the destination has been out of the source range before the packet reaches it.

$$Percentage\ of\ undelivered\ packets\ = \frac{Number\ of\ undelivered\ packets}{Total\ number\ of\ packets} * 100.$$

5.3. *Results*

In recent years many routing algorithms for *ad hoc* networks have been proposed. The algorithms are most often compared using simulation.

This section shows the simulation results obtained to compare routing protocols using *RFC* and *NFC* to estimate route stability. Simulation was built using C++ language. The used model consists of 30 nodes randomly distributed over a 200 × 200 meters area. Any sender node may reach a node 25 meters away. Every 500 msec (1/2 minute), nodes' position are changed randomly (distance and direction) but with maximum speed.

Known that network creation and movement and also packets' information; are created randomly. However, in order to obtain correct results, we must use the same information (nodes' initial and all next locations and also packets' information) for the two routing protocols. So the network creation and movement and also packet creation programs; are separated from the routing protocols' program.

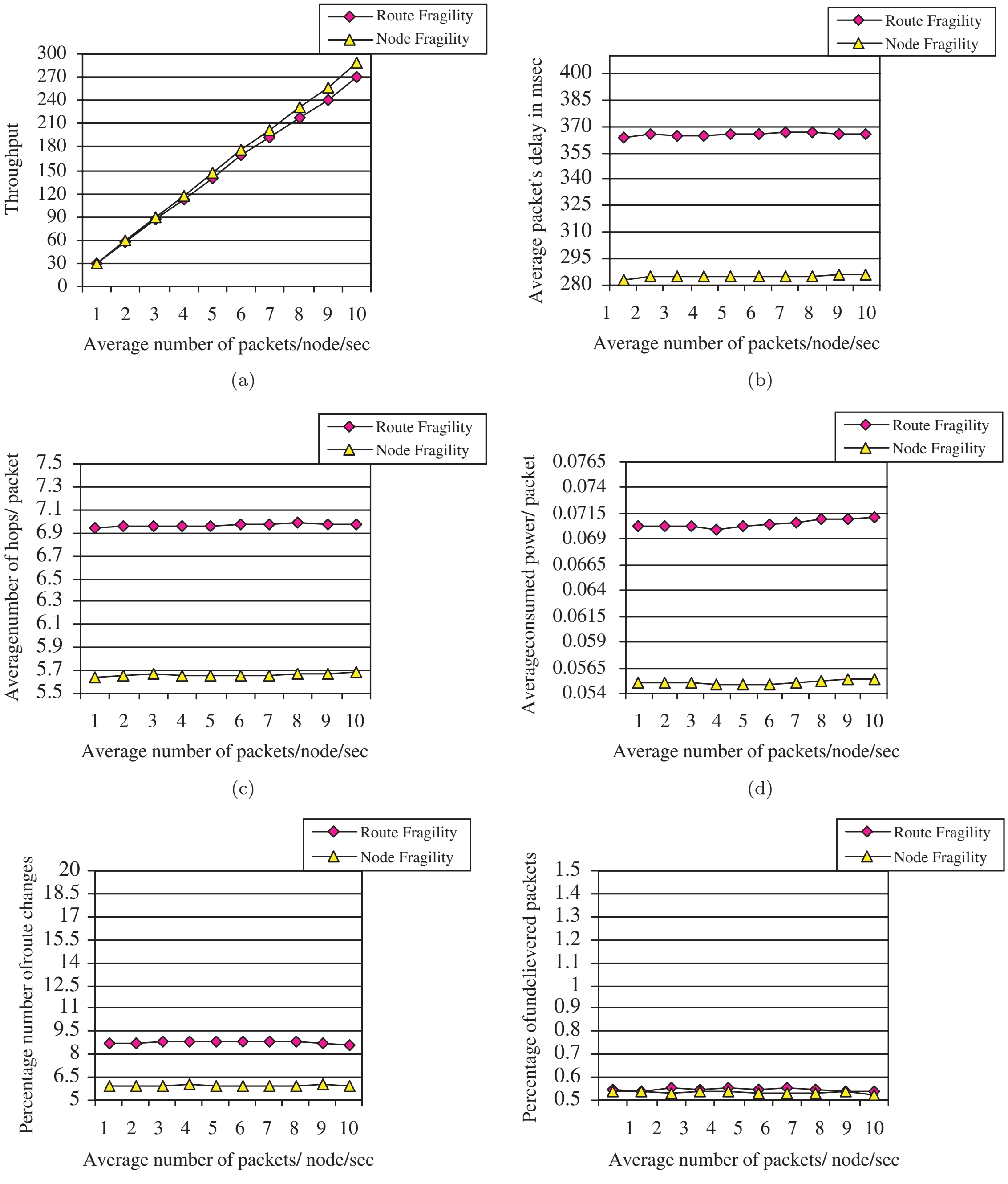
For a 30 minutes simulation time (1800 sec), comparisons are done using data rate varying from 1 to 10 packets/node/second. Three maximum speeds are used; 10, 15 and 20 m/sec. Of course with increasing speed, the probability of node movement far from its position increases, this leads to increasing the probability of route break for any packet trying to reach this node. So: (1) The need of route change increases, (2) the route's length traversed by the packet (number of hops) increases, (3) the packet end to end delay increases, (4) the consumed power by the packet increases, (5) also the number of undelivered packet may increase.

Figures 6, 7 and 8 show the comparison results using the three maximum speeds used 10, 20 and 30 m/sec. From these figures, it is clear that using Node Fragility Coefficient (*NFC*) metric to estimate route stability leads to much better results than using Route Fragility Coefficient (*RFC*) metric. It leads to:

- Slightly more throughput, especially with increasing the data rate (in '*a*' figures).
- Much less end to end delay (average packet delay in '*b*' figures).
- Much less route length (average number of hops/packet in '*c*' figures).
- Much less consumed power (average consumed power/packet in '*d*' figures).
- Much less needs for route changes (percentage number of route changes in '*e*' figures).
- Less undelivered packets (percentage number of undelivered packets in '*f*' figures).

6. Conclusion and Future Works

The Route Fragility Coefficient (*RFC*) metric was proposed in [Tickoo *et al.*, 2003] to choose stable routes for mobile *Ad hoc* networks. In this paper, another metric based on individual link fragility is proposed; the Node Fragility Coefficient (*NFC*) metric, this metric is also used to choose stable routes for mobile *Ad hoc* networks. Using simulation programs, we

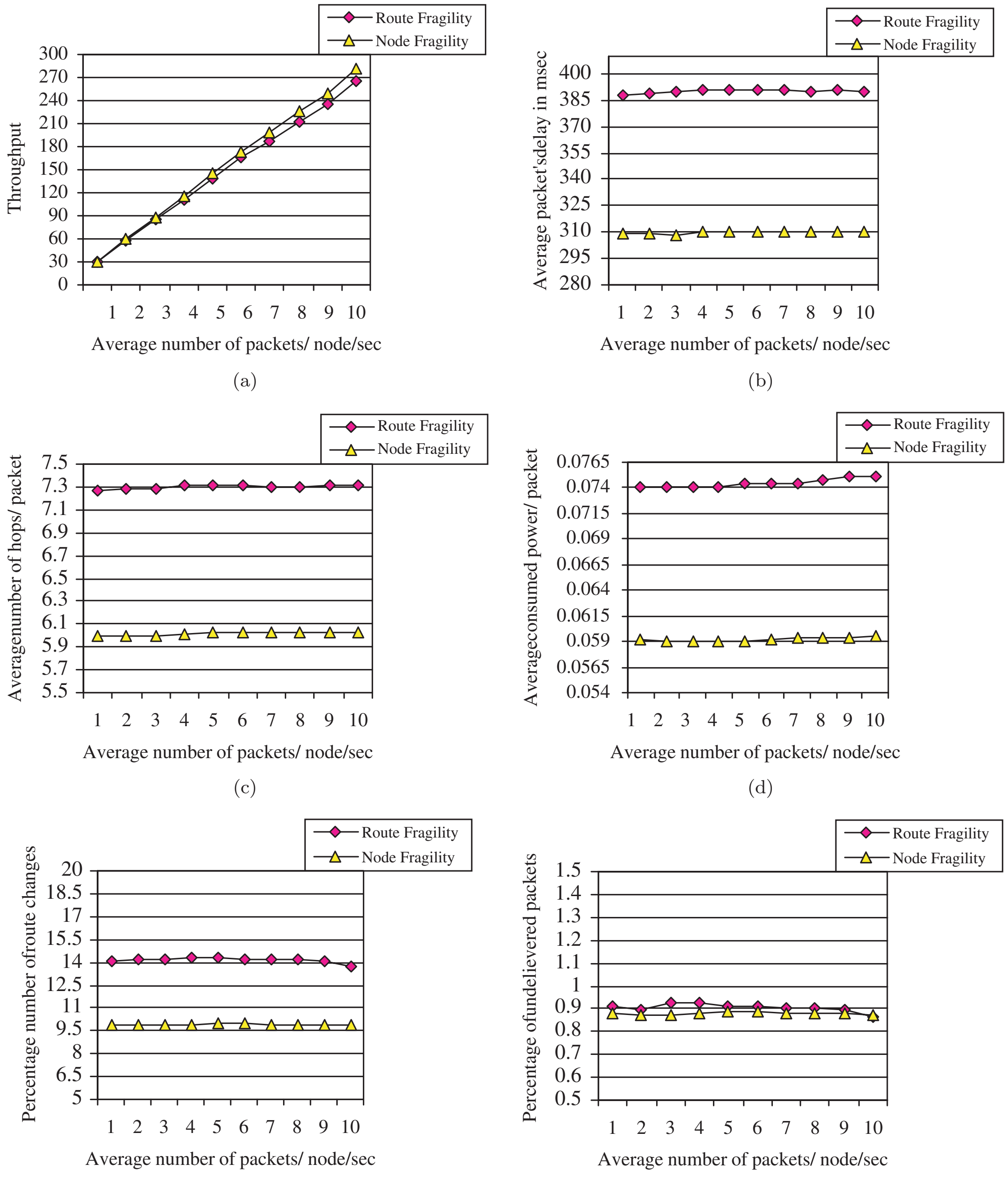


(a) (b)

(c) (d)

(e) (f)

Fig. 6. Results using speed = 10 m/sec.

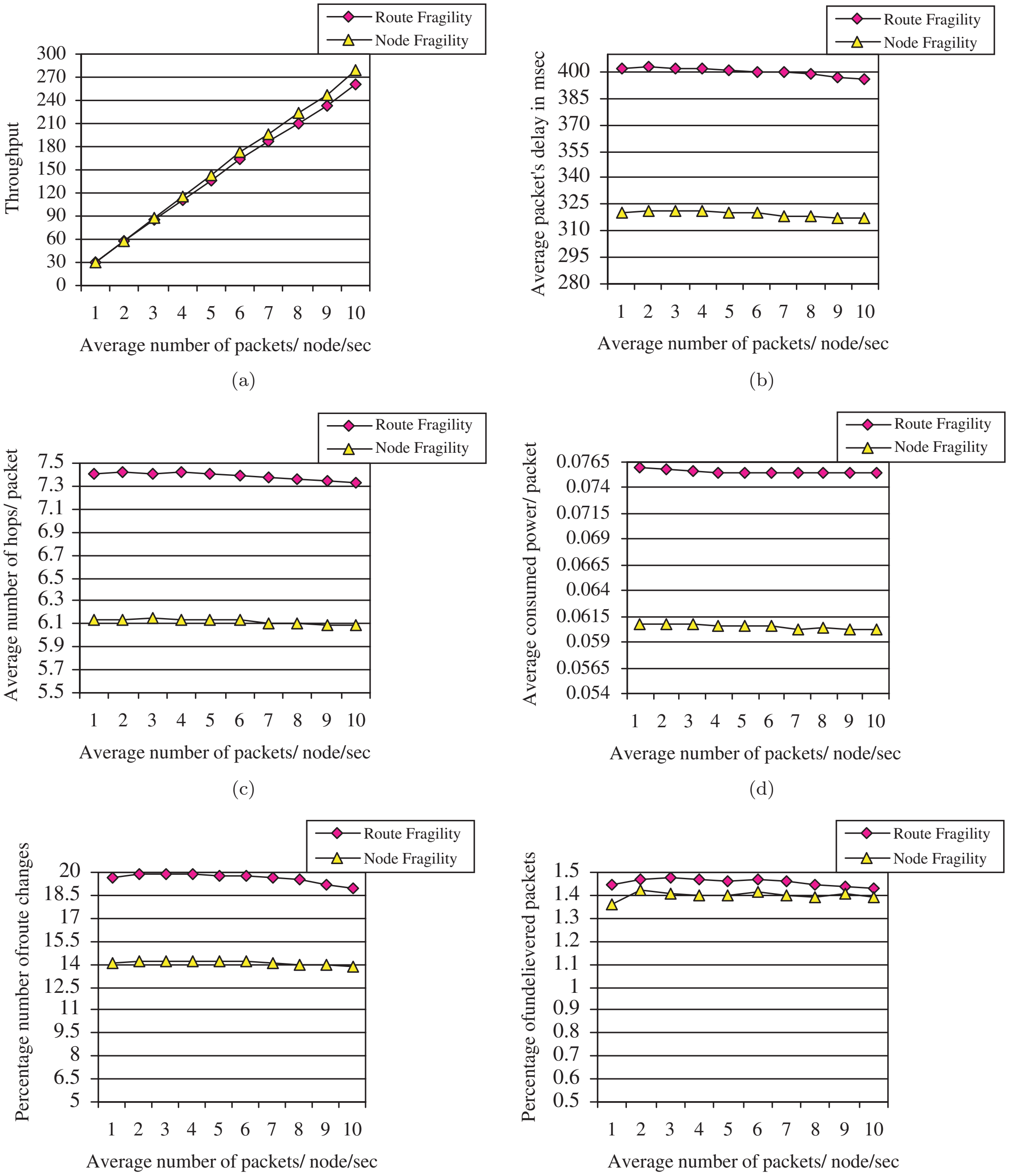


(a) (b)

(c) (d)

(e) (f)

Fig. 7. Results using speed = 15 m/sec.



(a) (b)

(c) (d)

(e) (f)

Fig. 8. Results using speed = 20 m/sec.

compare using these two metrics to choose the more stable routes for *Ad hoc* networks. It has been found that using the *NFC* metric to choose routes is much better than using *RFC* metric since it leads to better throughput, average packet's delay, average number of hops/packet, average consumed power/packet, percentage number of route changes and percentage number of undelivered packets.

Of course node fragility does not depend only on its stability in its position but also on the remaining power in its battery. So as a future work we will try to create a node fragility coefficient using both its stability and the remaining power in its battery. Also as future work, we may try to use *NFC* on choosing the core for multicast routing protocols.

Appendix

Consider a link L connecting node a to node b. Over time periods $t_1, t_2, t_3, \ldots, t_n$; if the length of L is equal to $d_1, d_2, d_3, \ldots, d_n$ and the power level the node a receives from node b is equal to $P_1, P_2, P_3, \ldots, P_n$ at these time periods respectively (note that $P_i \propto 1/d_i^2$).

To calculate the link fragility coefficient for link L (LFC_L) perform the following:

- Set LFC_L to zero.
- Repeat the following $n-1$ time; for each two successive times periods t_i and t_{i+1}.
  - ♦ If $d_i < d_{i+1}$ ($P_i > P_{i+1}$); nodes a and b are moving apart, calculate;

$$\begin{aligned} CEM &= \frac{1}{(t_{i+1}-t_i)}\left(\frac{1}{\sqrt{P_{i+1}}} - \frac{1}{\sqrt{P_i}}\right), \\ LFC_L &= LFC_L + 2 \times CEM. \end{aligned} \tag{A.1}$$

  - ♦ If $d_i > d_{i+1}(P_i < P_{i+1})$; nodes a and b are moving closer, calculate;

$$\begin{aligned} CCM &= \frac{1}{(t_{i+1}-t_i)}\sqrt{\frac{1}{P_i} - \frac{1}{P_{i+1}}}, \\ LFC_L &= LFC_L + CCM. \end{aligned} \tag{A.2}$$

To calculate the node fragility coefficient for node n (NFC_n) perform the following:

- Calculate LFC_i for every link i connecting node n to any other node in its range.
- Calculate

$$NFC_n = \sum_{i \in L} LFC_i; \tag{A.3}$$

where L is the set of links connecting node n to all nodes in its range.

References

Agarwal, S., Ashish, A., Pal Singh, J. and Shorey, R. [2000] "Route-lifetime assessment based routing (RABR) protocol for mobile ad-hoc networks," *Proceeding of the 2000 IEEE International Conference on Communications.*

Agarwal, A. and Das, S. [2003] "Dead reckoning in mobile ad hoc networks," *Proceeding of the 2003 IEEE Wireless Communications and Networking Conference (WCNC 2003).*

Beongku, A. and Papavassiliou, S. [2002] "An entropy-based model for supporting and evaluating route stability in mobile ad-hoc wireless networks," *IEEE Communications Letters Magazine* **6**(8).

Deng, J., Han, Y., Po-Ning, C. and Varshney, P. [2004] "Optimum transmission range for wireless ad-hoc networks," *Proceeding of the 2004 IEEE Wireless Communications and Networking Conference (WCNC'04).*

Gerharz, M., De Waal, C., Martini, P. and James, P. [2003] "Strategies for finding stable paths in mobile wireless ad-hoc networks," 28th *Annual IEEE International Conference on Local Computer Networks.*

Geunhwi, L., Kwangwook, S., Seunghak, L., Yoon, H. and Joong Soo, M. [2002] "Link stability and route lifetime in ad-hoc wireless networks," *Proceedings of the 2002 IEEE International Conference on Parallel Processing Workshops (ICPPW'02).*

Kuladinithi, K., Görg, C. and Allee, O., *Mobile Ad Hoc Network*, http://www.comnets.uni-bremen.de/∼koo/manet-tutorial.pdf.

Mauve, M., Widmer, J. and Hartenstein, H. [2001] "A survey on position-based routing in mobile ad-hoc networks," *IEEE Network Magazine* **15**(6).

Perfkins, C. E. [2001] *Ad Hoc Networking* (Addison-Wesley).

Ramasubramanian, V., Haas, Z. and Gün Sirer, E. [2003] "SHARP: A hybrid adaptive routing protocol for mobile ad-hoc networks," *Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc).*

Sujeetv, *Mobility Predictions for Ad-Hoc Networks in a 3-Dimensional Space*, http://www2.cs.uh.edu/∼sujeetv/projects/Ad-Hoc/Report.PDF.

Tickoo, O., Raghunath, S. and Kalyanaraman, S. [2003] "Route fragility: A novel metric for route selection in mobile ad-hoc networks," *Proceeding of the 2003 IEEE International Conference on Network (ICON).*

Toh, C.-K. [2002] *Ad Hoc Mobile Wireless Networks: Protocols and Systems* (Prentice Hall).