MULTIPATH FAULT TOLERANT ROUTING PROTOCOL IN MANET

V. Jayalakshmi[1] and Dr. R. Rameshkumar[2]

[1]Department of Computer Applications, Sudharsan Engineering College, Tamilnadu

jayasekar1996@yahoo.co.in

[2]Principal, Lalgudi Cooperative Polytechnic College, Lalgudi, Tamilnadu

rramesh1968@gmail.com

ABSTRACT

Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired backbone network and it the makes the routing a crucial issue to the design of the MANET. Multiple path routing protocols are shown to be performance-effective alternatives over single-path routing for ad hoc networks and it represents a promising routing method for wireless mobile ad hoc networks. Multi-path routing achieves load balancing and is more resilient to route failures..In this paper we propose an energy efficient multipath fault tolerant routing protocol to improve the reliability of data routing in Mobile ad hoc networks. The proposed RFTA is a multi objective routing protocol that meets diverse application requirements by considering the changing conditions of the network. The efficiency of the proposed protocol has been evaluated on different scenarios and there has been a noticeable improvement in the packet delivery ratio and also in the reduction of end-to-end delay comparing to SMR,SMS and MDSR.

KEYWORDS

MANET, Multipath routing,SMR, SMS and MDSR

1. INTRODUCTION

Wireless local area networks based on the 802.11a, b, g and n standards became one of the most ubiquitous ways of networking with mobile nodes. Most of these networks, however, are deployed in the configuration which can be called “wired everywhere, except the first hop”. If the goal of the user of the mobile computer is to connect to a website located halfway around the world, the best strategy is to escape as quickly as possible from the challenges of wireless domain and enter the reliability of fiber optic networks and time-tested networking protocols. In such networks, all the nodes connect to an access point which usually has a wired connection to the Internet. From the point of view of the network and higher layers, this first hop can be approximated as an Ethernet-type shared medium. In this scenario the nodes connected to the same wireless LAN communicate with each other only indirectly.

There are, however, many important applications where this model is not applicable. First, even if the goal is Internet access, the access point might not be able to cover all the relevant mobile nodes due to limitations in transmission range, cost or access rights considerations. Another case

DOI : 10.5121/ijans.2012.2103

is when Internet access is not desired (or is secondary importance), the main application being to communicate locally among a group of (potentially mobile) nodes.

These scenarios can be serviced only if we allow some (possibly all) routing hops to be performed in the wireless domain. Such networks can be set up in any location in an ad hoc manner, without the need of an existing wired infrastructure. These networks are known as ad hoc wireless networks [1], other proposed names being infrastructure less wireless networks, instant infrastructure [2] and mobile-mesh networking.

Mobile Ad Hoc Networks (MANETs) are collections of wireless mobile nodes, constructed dynamically without the use of any existing network infrastructure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed for one node to exchange data with another one across the network. MANETs are characterized by limited power resource, high mobility and limited bandwidth.

One of the major technological challenges of such networks is that they require new types of routing protocols. As opposed to the wired infrastructure, there are no dedicated router nodes: the task of routing needs to be performed by the user nodes, which can be mobile, unreliable and have limited energy and other resources.

Routing in MANETs can be accomplished through either single path or multiple paths. When using single-path routing protocols, the traffic is distributed through one route and is therefore less flexible than in multi-path routing protocols. It was shown that multi-path routing mechanism provides better throughput than single-path routing protocols [3], [4]. Although research on multi-path routing protocols has been covered quite thoroughly in wired networks, similar research for wireless networks is still in its infancy. Some multi-path routing protocols for MANETs have been proposed in [5], [6], [7], [8], [9].

The typical problems encountered in designing single path protocols for a mobile wireless environment also arise in designing multipath protocols. Mobility makes it difficult or impossible to maintain a global view of the network. Mobility also has implications in terms of caching policies. If cached information at intermediate nodes is frequently out of date, caching can degrade routing performance because detecting inaccurate routing. Information is not instantaneous. In addition to the dynamic topology, unreliable and range limited wireless transmission makes resiliency a requirement rather than an enhancement in a routing solution. Since mobile transmitters are likely to be battery powered, routing protocols need to minimize the communication for coordinating network nodes. At the protocol level, the design of multipath routing [9] needs to consider failure models, characteristics of redundant routes, coordinating nodes to construct routes, mechanisms for locating mobile destination and intermediate forwarding nodes, and failure recovery.

Considering the existing problems in both single-path stable routing and backup routing schemes, this paper proposes a robust fault tolerant multipath routing mechanism. This algorithm sets up the primary path and the corresponding local-backup paths based on contention-based mechanism. It has the following attractive advantages: (1) the route length of

this algorithm is approximately equal to that calculated by the shortest path algorithm; (2) the local-backup path remains available when the primary path fails (a prediction method is introduced to achieve this function); and (3) It greatly reduces the network overhead. For a network with N nodes, the number of route discovery packets for the proposed protocol is of order O(√N), while this number is of order O(N) for flooding and limited flooding.

The paper is organized in 5 sections. Section 2 gives the related work. Section 3 describes the proposed RFTA algorithm. Section 4 illustrates the performance evaluation with the other protocols. Section 5 presents conclusions at the end.

2. Related Work

Most of the multipath routing protocols originate from DSR [11] or AODV [12] protocols. These multipath routing protocols modify the route discovery and route maintenance mechanisms of DSR and AODV protocols to improve the performances of a network in terms of delay, reliability, overhead reduction, energy efficiency and network throughput. In order to have an understanding of the proposed multipath routing protocols it is necessary to know the basic mechanisms of the DSR and AODV protocols.

2.1. The DSR protocol

The DSR [11] protocol consists of two basic mechanisms: (1) route discovery and (2) route maintenance. Route discovery is the mechanism by which a source node discovers a route to a destination. When a source node wants to send a data packet, it first looks into the route cache to find a route. If a source cannot find a route in its route cache, the source initiates a route discovery mechanism by broadcasting a request packet to its neighbours. When a neighbour of a source receives a request packet, it first checks whether the request packet is intended for it or not. If a neighbour discovers that it is the destination, it sends a reply back to the source after copying the accumulated routing information contained in the route request packet into a route reply packet. If it is not the destination, it checks if there is any route available in the route cache for that destination. If this neighbouring node is neither a destination nor does it have a route in the route cache to that destination, it appends its address in the route request packet, and then it re-broadcasts a route request packet to its neighbours. This process continues until a route request packet reaches the destination node. Then the destination node replies all route requests. When a source node receives a route reply packet, it starts sending data packets using the route indicated in the reply packet. If multiple paths are discovered, it chooses a path that is the shortest one.
Route maintenance is the mechanism by which a node is able to detect any change in the network topology. When a node detects a broken link, for example, by using missing MAC layer acknowledgments, it removes the link from its route cache and sends a route error message to each node that has sent packets over that link.

2.2. The AODV protocol

The AODV protocol [10] is called a pure on-demand routing protocol because a mobile node does not have to maintain any routing information if it is not located in an active path. Like DSR, the AODV protocol also consists of a route discovery and a route maintenance mechanism. But the route request packet structure of the AODV protocol is different from that of the DSR protocol. To detect a fresh route from a stale route, each node maintains two counters called node sequence ID and broadcast ID. Each route request packet contains information about the destination sequence number and the source sequence number in addition to source address and destination address. The sequence numbers are used to indicate the freshness of a route. Each neighbour node either sends a reply to a source or re-broadcasts a request message to its neighbours depending on whether it is the destination or not. If a node is not the destination, it needs to keep track of a request packet to set up a reverse path as well as a forward path. When a destination replies back to a source, it uses the reverse path. Mobile nodes can determine whether a route is a current one or a stale one by comparing the destination sequence number in the route request packet with that of the sequence number stored in the route cache. If the route request sequence number is greater than the recorded one, it does not send a reply to the source. Instead, it re-broadcasts that request message. An intermediate node only replies from its route cache if the route request sequence number is less than or equal to the sequence number stored in the route cache. If a node does have a current route, it sends a reply using a unicast route reply packet. The reply packet travels along the reverse path, which was set up previously. When a reply packet travels back through the reverse path, each intermediate node sets up a forward pointer to the node from which it receives this reply. When a route reply packet reaches the source, the source starts sending data packets to the destination using the discovered path. If that source learns more routes later on, it updates its route cache accordingly.

2.3. Multipath Routing Protocols

Reactive routing protocols like DSR and AODV do not scale well with the network size. The scalability problem arises from excessive routing overhead, high delay, unreliable data transfer and energy inefficiency. A reactive routing protocol generates a large number of overhead control messages in the network during the route discovery process. Excessive overhead packets cause contention and collision in the wireless medium and occupy a significant portion of useful bandwidth. Hence, the performance of a network is adversely affected. Discovering multiple paths by using fewer overhead control messages is one of the objectives of a multipath routing protocol. Another performance problem of a reactive routing protocol is high end-to-end packet delay. This delay arises from an inefficient path selection, unfair load distribution and high overhead. Improving the delay of a network is another objective of a multipath routing protocol. Unreliable data packet transfer is another problem of a reactive routing protocol. This problem occurs mainly from the node movements and also from the interference of the wireless medium. Multipath protocols have been proposed to ensure reliable packet transmission in the network. Energy inefficiency is another problem of a reactive routing protocol. Energy inefficient routing protocol incurs node failure in the network. Since a packet travels in a network in a multi-hop fashion, it is imperative to keep a mobile node operative as long as possible. protocols have been proposed to make a network energy efficient. Although a multipath routing protocol improves the performance of a network, it may not be a good choice in all cases. For example, a small network does not generate a large number of overhead packets. The interference level is also not high in such a small network. For that reason, a multipath routing protocol may not be a suitable choice for such a small network. There are cases when both a multipath routing protocol and a single path routing protocol need to be used depending on the network condition [12] and [13].

2.3.1. Split Multipath Routing Protocol

The main objective of SMR [14] is to reduce the frequency of route discovery processes and thereby reduce the control overhead in the network. The protocol uses a per packet allocation scheme to distribute a load into multiple paths. When a destination node receives route request packets from different paths, it chooses multiple disjoint routes and sends replies back to the source. The basic route discovery mechanism of the DSR protocol is used in the SMR protocol, but an intermediate node is not allowed to reply from its route cache if it has some routes available to that destination. To avoid overlapped multiple paths, the author introduces a different route request forwarding scheme. In this scheme, instead of dropping a duplicate request message, an intermediate node forwards this request packet in a different incoming link other than the link from which the first request was received and whose hop count is not larger than that of the first request message. When a destination node receives a route request message, it selects two paths that are maximally disjointed. Between these two routes, the first one is the shortest path. The shortest path is chosen to minimize the route discovery time because it is the earliest discovered route. After processing the first request, for the second path selection, a destination waits for a certain duration of time to receive more requests and learns all possible routes. After this it selects a route from one of the alternative paths, which is maximally disjointed with the shortest path. A maximally disjointed path is the path that has the least number of common nodes compared to the shortest path. If there is more than one maximally disjointed path is available, the shortest hop path is selected among them. Another major difference from DSR protocol is that an intermediate node does not need to maintain a route cache. For this reason, a node has a smaller cache. Although the SMR protocol uses less frequent route discovery mechanisms compared to the DSR protocol, one of the drawbacks of MSR is the redundant overhead packets. Since an intermediate node is not dropping a duplicate request message, the frequency of route discovery process need to be reduced to curb the overhead.

2.3.2 Multipath dynamic source routing (MDSR) protocol

A multipath extension of DSR protocol called multipath dynamic source routing (MDSR) [15] protocol has been proposed. MDSR protocol reduces the flooding problem of DSR protocol. One major disadvantage of DSR protocol is the query flooding that is used to discover new source route. Such query flooding generates a large number of overhead packets. These overhead packets occupy a substantial portion of the bandwidth of a network. It is an intelligent multipath protocol can reduce the frequency of query flooding. In DSR protocol, a destination node replies to every received request packet. But in MDSR protocol, a destination replies only to a selected set of request messages. After receiving all requests, a destination replies back only to those route requests that are link-disjointed from the primary source route (i.e., the shortest path route). A destination node keeps record of the shortest path and based on the shortest path information, it figures out which route request it should reply to. A source keeps all the routes in the cache. If the shortest route is broken, it uses an alternative route, which is the shortest among the remaining routes in the cache. If this route is also broken, it uses another alternative route. This process of choosing alternative paths continues until all paths are used. If all routes in a cache are broken, a source initiates another route discovery. Fig 1 illustrates the idea of MDSR protocol. In this figure, the primary route is depicted by the link sequence L_1–L_2– – –L_k. Each node in the primary route n_i has an alternative path Pi to the destination. The source S uses the primary route for transmitting data packets to a destination node D until it breaks. Let us assume that the link Li is broken, in this scenario, the node n_i responds to the situation by replacing the unused portion of the route L_i– L_k in the data packet header by an alternative route P_i. This will continue until a link in path P_i breaks. If a link on P_i breaks, it will cause an error packet transmitted backward up to node n_i-1, which will quench the error packet and switch data packets to its own alternative route P_i-1 by modifying the source route in the packet header as before. Thus, when a route breaks, an intermediate node makes alternative routing decisions to replace broken links. This process continues until a source gets an error packet and has no alternative route to fall back. Simulation results show that although the route discovery frequency is reduced, an alternative path is usually longer and hence the delay per packet increases. In addition to this delay increase, there may be only a few intermediate nodes that have alternative paths to a destination and this can trigger frequent route discoveries and eventually increase overhead.

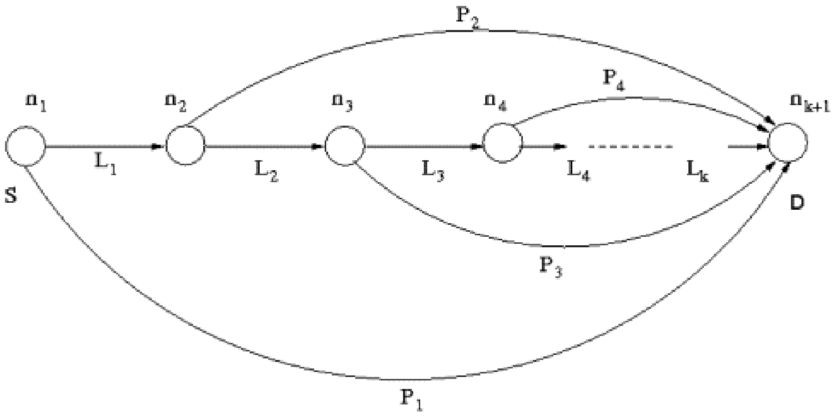
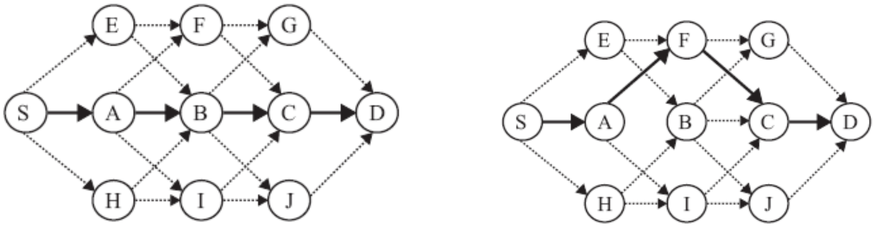


Fig. 1.

2.3.3. Shortest Multipath Source (SMS)

SMS routing protocol is proposed based on DSR. It builds multiple partial-disjoint paths from source S to destination D in order to avoid the overhead of additional route discoveries and to quick recovery in case of route breaks. Improved performance in terms of Fraction of packets delivered, end-to-end delay and routing overheads is obtained. SMS earns multiple partial-disjoint paths that will bypass at least one intermediate node on the primary path that is shown in Fig. 2-a.Consider the case of traffic flowing between nodes Sand D using link A-B as a segment of the path. In case of a link failure between A and B, the source node will search for an alternate route that does not contain node B that is shown in Fig. 2-b. An alternative route between source S and destination D is (S, A, F, C, D)



(a)

(b)

Fig. 2 (a) Partial Disjoint Multiple Paths (b) Select the alternate path

3. Proposed Protocol : RFTA

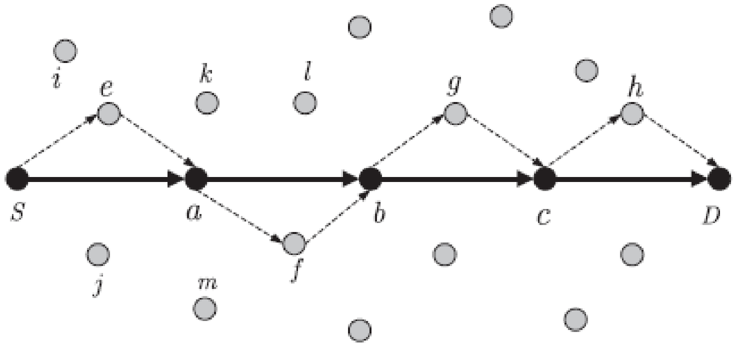
This part provides a detailed description of the proposed protocol. Each node gets the position information of its neighbour nodes by periodically broadcasting one-hop HELLO beacons, which include node ID and position information (unlike in other velocity-aided routing protocols, the

HELLO beacons in the RFTA protocol do not contain node velocity information and therefore have a lower overhead). All nodes maintain a neighbour table, which stores the ID and position of each neighbour. The data structures maintained by the routing node are as follows:

- Primary path table: stores primary path information for a destination node.
- Backup path table: stores local-backup path information for the links in the primary path.
- Data cache: stores the latest several data packets that have recently been forwarded.
- RREQ_Seen table : each node should save the RREQ messages it receives from other nodes and has an additional field in RREQ_Seen table of each node, called Neighbour_Count (N_C) which will be used to count the number of active neighbours identified after sending the RREQ message

3.1. Route discovery

Each node has a unique IP address or ID. Let S and D denote the source and the destination, respectively. Route discovery is started before transmitting a data packet if S cannot find a route to D. In this paper, GPSR is adopted to forward RREQ instead of data packets. GPSR is a kind of classical geographic information routing protocol. In GPSR, a packet is normally routed in greedy forwarding manner, and the route switches to perimeter forwarding when reaching a void [16]. Greedy forwarding uses the positions of neighbour nodes and a packet's destination to make packet forwarding decisions. Specifically, if a node knows its neighbours' positions, the locally optimal choice of the next hop is the neighbour that is geographically [19] closest to the packet's destination. In this, each RREQ packet has the same structure, including the ID and position of the destination, the ID, position and velocity of the current node Ni, and the link lifetime calculated by Ni (the RREQ sent by S does not include the link lifetime, so the initial value of the link lifetime in the RREQ is set as 0).



Primary path ⟶ Local-backup path - - - ▶

Fig 3

3.1.1. Primary path discovery procedure

Node Ni (including S, S = N1) unicasts the RREQ to D by using GPSR. Here, we use a modified MAC scheme for the RREQ forwarding. During the RREQ delivery procedure, the RREQ's

MAC address is always the broadcast address (e.g., if the IEEE 802.11 MAC [17] is used, then the MAC address of RREQ is always -1). When node Ni's neighbours receive this RREQ, all of them send it to the routing layer. In other words, although the RREQ is unicasted to the destination at the routing layer, it is a broadcast frame at the MAC layer. Because the RREQ is a broadcast frame at the MAC layer, when Ni transmits a RREQ, all Ni's neighbours
can receive this RREQ.

Let us denote an arbitrary node in Nei(Ni) by $\mathbf{N}_{\mathbf{i}}^{\mathbf{j}}$. Having received this RREQ, $\mathbf{N}_{\mathbf{i}}^{\mathbf{j}}$ adds the corresponding information to its RREQ table. If $\mathbf{N}_{\mathbf{i}}^{\mathbf{j}} \neq N_{i+1}$ and $\mathbf{N}_{\mathbf{i}}^{\mathbf{j}} \neq N_{i-1}$, then $\mathbf{N}_{\mathbf{i}}^{\mathbf{j}}$ starts local-backup path discovery and then discards the RREQ. If $\mathbf{N}_{\mathbf{i}}^{\mathbf{j}} = N_{i+1}$, then $\mathbf{N}_{\mathbf{i}}^{\mathbf{j}}$ calculates LET(N_i, N_{i+1}) and then adds the reverse path to the primary path table. Then, N_{i+1}checks whether it itself is the destination. If not, N_{i+1}adds LET(N_i, N_{i+1}) as well as its velocity and position information to the RREQ packet and then sends it to the MAC layer.

When the RREQ is received by D, a RREP is sent back through the reverse path (the RREP is unicasted in the MAC layer as well as in the routing layer). Upon receiving the RREP, S and the intermediate nodes set up a primary path to D according to the RREP, and then S can transmit data packets to D with this route.

3.2.2 Local-backup path discovery

Because the two neighbours obtain each other's motion values, such as position, velocity, and transmission range, the duration of a link between these nodes can be determined based on their positions and velocities of movement [18]. The link expiration time is mentioned by Su et al. [17].

We take Fig. 3 as an example for the route discovery. When S is about to send data to D and no route for D is available, then route discovery is started. S selects the node nearest to D (here node a is selected) from its neighbour table as the next hop and sends RREQ (by RREQS, we denote the RREQ packet sent by S) to it. Here, the link (S, a) of primary path is established. Nodes a, e, i, and j may receive this RREQ simultaneously. When a receives RREQS, it records

RREQS in its RREQ table and updates the corresponding fields of RREQ (RREQS) with its ID, position, velocity, and LET(S, a). Then, node a selects b as its next hop and sends RREQa to b (RREQa denotes the RREQ that has been updated by a). When e, i, and j receive RREQS, they add it to their respective RREQ tables. When e and j receive the same RREQa, they calculate PET(S, e, a) and PET(S, j, a), respectively

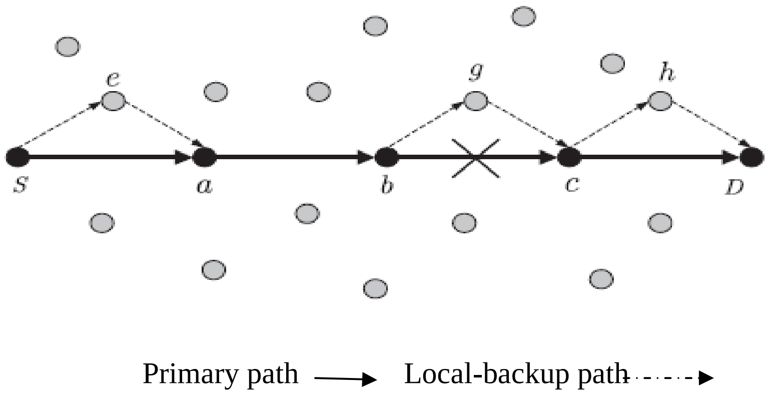


Fig 4. Illustration of Route Maintanence

3.2 Route maintenance

The different possible situations in route maintenance are as follows:

- There is a local-backup path between Ni and Ni+1: If link (Ni, Ni+1) in the primary path fails, then data packets continue to be transported through the corresponding local-backup path
- There is no local-backup path between Ni and Ni+1, but there is between Ni and Ni+2 data goes through the localbackup path to Ni+2 when neither the primary pathnor local-backup path to Ni+1 is available.
- There is no local-backup path from N_i to N_{i+1} or N_{i+2}: to reduce the packet loss rate, a new backup route setup procedure is started when the lifetime of link (N_i, N_{i+1}) is less than Remainder_Rate _ LET(N_i, N_{i+1}). This is a prediction scheme. Ni obtains LET(N_i, N_{i+1}) and the Remainder_Rate _ LET(N_i, N_{i+1}) in the route establishment procedure and uses them to predict how soon the link will break. In simulations, the protocol parameter Remainder_Rate is set to 0.2.
- Neither the primary path nor the local-backup path is available: RERR is sent back to the source, which then initiates a new route discovery process. For example, as shown in Fig. 4, when link (b, c) fails, the local-backup path (b, g, c) is used. When the data packets reach c, the primary path is used again if it is available,

4. Performance Evaluation Results

4.1. Simulation Environments

The simulation environment is ns2[20]. The network includes 50 mobile host nodes which are placed in 1000X1000 meter flat area in random and the number of source nodes was 30 of 50 hosts. Each node has a radio propagation range of 250 m and channel capacity was 2Mbps . The IEEE 802.11 Distribution Coordination Function (DCF) is used as Medium Access Control (MAC).A traffic generator was random constant bit rate (cbr) . The size of data payload was 512 bytes. The random waypoint model was used as a mobility model. Sending rate of packets was set to 3 packets per second and the simulation was run in 30 seconds as a pause time. The maximum and minimum speed was varied between 0 and 10 *m/s* .

Three important metrics are evaluated:

- *Throughput*: measured as the ratio of the number of data packets delivered to the number of data packets sent by the source.
- *End-to-end delay*: measured as the average end-to-end latency of data packets.
- *Routing loads*: measured in terms of the total number of routing packets transmitted per data packet delivered at the destination. Each broadcast transmissions was count as one single transmission.

4.1.1 Simulation Scenarios

We ran experiments with two different base settings. In the first setting, 100 nodes are randomly placed inside an area of 1000 x 1000 m^2. For the second setting, then number of nodes and the size of the simulation area are varied, while keeping the average node density constant

4.2. Simulation Results

In the first scenario, to evaluate capability of the protocols for different node mobility, we change node mobility by varying the maximum speed. The number of nodes and pause time was fixed at 100 nodes and 1 second, respectively.

Figures 3 and 4 show the evolution of the packet delivery ratio and average delay for increasing node speed (from 10 to 50 m/s) in a random waypoint model

Throughput of the four protocols is shown in Fig. 5. In moderately loaded networks, the loss of RREP packets results in the failure of the route discovery process. In on demand protocols the source uses an exponential back-off algorithm to limit the rate at which new route discoveries are initiated. Since the back-off time is large compared to send buffer capacity, application packets within the back-off time may be dropped due to buffer overflow. But with this proposed RFTA algorithm uses local-backup paths which prolongs the route lifetimes shows higher Throughput than the other protocols.

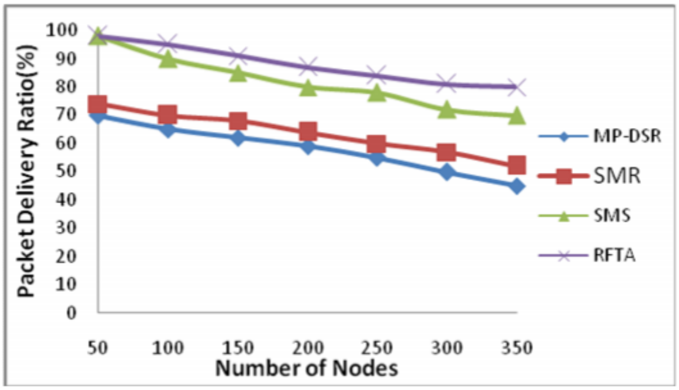


Fig. 5

The end-to-end delay of the four protocols is shown in Fig 6. SMR has the longest delay in mobile scenarios because it delivers data packets on routes longer than those of SMR. In addition, MP-DSR yields longer delays in reconstructing routes and the period of time the data packets are buffered at the source node during route recovery results in larger end-to-end delays.

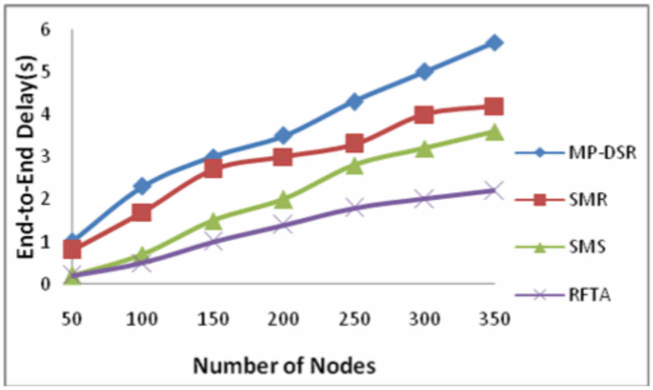


Fig .6

SMR uses the remaining valid route when one of the multiple routes is disconnected, and hence no route acquisition latency is required. The availability of shorter alternate routing paths in the former eliminates route discovery latency that contributes to the delay when an active route fails. When a congestion state occurs in a path, the source node can re-distribute incoming data packets to alternative routing paths, thereby reducing the queue waiting time of data packets.

The proposed algorithm routing outperforms the other protocols at lower mobility and node densities. SMS finds the shortest alternative routes in a single route discovery process, reducing delay and routing overheads incurred when recovering from route breaks. SMR overloads the network with control messages and data packets are dropped at full buffer of intermediate nodes. Routing load savings for M-DSR at higher nobilities and node densities came from a large saving on route requests.

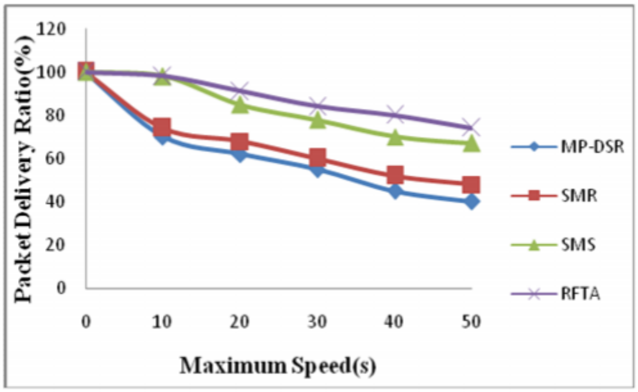


Fig 7

Fig 7 shows the PDRs of the 4 protocols with varying mobility speed. We observe that the PDR of the MP-DSR decreases quickly as the node velocity increases. On the contrary, RFTA has the highest PDR because it uses the local-backup paths when the primary path fails and repairs a broken route locally. Thus, an available route in RFTA usually lasts longer and more data packets can be delivered. As the node velocity increases, the PDR of the proposed protocol RFTA is still above 90%, which indicates that RFTA is stable and has a good tolerance of varying node velocity. When both the primary path and the local-backup path corresponding to the broken link fail, an RERR is sent back to the source to initiate a new route discovery process immediately to prevent further packet loss.

5 . CONCLUSIONS

Node mobility does not guarantee multimedia transmission in a network with a dynamic topology. This paper presents a fault tolerant routing protocol to improve route stability in mobile ad hoc networks. Route discovery for the primary path established in this proposed protocol approximately achieves the smallest hop count. Simultaneously, local-backup paths are constructed during the primary path discovery procedure according to the lifetime of each link. When a link in the primary path fails, the upstream node of the failed link in the primary path can continue the data delivery through the local-backup path. Compared with some representative existing stable and source -based routing protocols such as SMR, SMS, MDSR. The simulation results show that there has been a noticeable improvement in the packet delivery ratio and also in the reduction of end-to-end delay comparing to other protocols. The main direction of our future research is to consider other issues in RFTA such as routing overheads, QoS, security, and load balance.

REFERENCES

[1] C. Perkins, Editor, Ad hoc Networking, Addison Wesley (2001).

[2] R. Bagrodia, M. Gerla, L. Kleinrock, J. Short, T. Tsai, A hierarchical simulation environment for mobile wireless networks, Technical report, Dept. of Computer Science, University of California at Los Angeles, 1996..

[3] Anurag , K, Manjunath D, Kuri J. Communication networking: an analytical approach. Los Altos, CA: Morgan Kaufmann Publishers; 2004. p. 715–6..

[4] D. Bertsekas and R. Gallager Data networks, (2nd ed.), Prentice-Hall, Englewood Cliffs, NJ (1992), p. 162–9.

[5] Cha M, Lee DK. Split-n-save multiplexing in wireless ad hoc routing In: Proceedings of the 24th annual joint conference of the IEEE computer and communications societies (INFOCOM), Miami, March 2005..

[6] Perkins CE, Royer EM, Marina MK. Performance comparison of two on-demand routing protocols for ad hoc networks. IEEE Personal Communications Magazine 2001:16–28 [special issue on Ad hoc Networking]..

[7] Dulman S, Wu J, Havinga P. An energy efficient multipath routing algorithm for wireless sensor networks. In: Proceedings of the 6th international symposium on autonomous decentralized systems with an emphasis on advanced distributed transportation systems, Pisa, Italy, April 2003..

[8] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, Highly-resilient, energy-efficient multipath routing in wireless sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review, 5 4 (2001), pp. 11–25.

[9] Taheri, N., Javan, D.: Reducing End-to-End Delay in Multipath Routing Algorithms for Mobile Ad-Hoc Networks. In: Zhang, H., Olariu, S., Cao, J., Johnson, D.B. (eds.) MSN 2007. LNCS, vol. 4864, pp. 715–724. Springer, Heidelberg (2007)obile

[10] C. E. Perkins and E. M. Royer, "The Ad hoc On-Demand Distance Vector Protocol," In C. E. Perkins, editor, Ad hoc Networking, pp. 173-219. Addison-Wesley, 2000.

[11] B. Johnson, D. A. Maltz. "Dynamic Source Routing in Ad-Hoc Wireless Networks," Mobile Computing, vol.353, pp. 153-81, 1996.

[12] Wang L, Zhang L, Shu Y. Dong multipath source routing in wireless ad hoc networks. In: Canadian conference on electrical and computer engineering, vol. 1, 2000, p. 479–83..

[13] Wei W, Zakhor A. Robust multipath source routing protocol (RMPSR) for video communication over wireless ad hoc networks. In: IEEE international conference on multimedia and expo, vol. 2, ICME 2004, p. 1379–82.

[14] Lee, S.j., Gerla, M.: Split Multipath Routing with Maximally Disjoint Paths in Ad-hoc Networks. In: Proceedings of IEEE International Conference on Communication (ICC), elsinki, Finland, pp. 3201–3205 (2001)

[15] Nasipuri A, Das SR. On-demand multipath routing for mobile ad hoc networks. In: Proceedings of the 8th international conference on computer communications and networks, Boston, October 1999, p. 64–70..

[16] Brad Karp, H.T. Kung, GPSR: Greedy perimeter stateless routing for wireless networks, August 2000, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 2000, pp. 243–254.

[17] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11-1997, IEEE Standards Dept., 1997

[18] [21] W. Su, S.-J. Lee, M. Gerla, Mobility prediction in wireless networks, in: Proc. of IEEE MILCOM 2000, Los Angeles, CA, vol. 1, October 2000, pp. 491–495.

[19] Charalampos Konstantopoulos, Damianos Gavalas, Grammati Pantziou, Clustering in mobile ad hoc networks through neighbourhood stability-based mobility prediction, Computer Networks 52 (9) (2008) 1797–1824.

[20] Network Simulator-2, http://www.isi.edu/nsnam/ns

Authors

V. Jayalakshmi is Assistant Professor in the Computer Applications Department of the Sudharsan Engineering College Pudukottai, India and has 12 years of experience in teaching and 5 years in research. She has received her MCA and MPhil degrees in Madras University and Bharathidasan University respectively. She is currently pursuing her Doctoral degree in Computer Science. Her area of interest is Network Security, Data mining and Mobile Adhoc Networks. She has published 6 papers in International and 4 papers in National.