Route Maintenance using Link State Prediction for Dense Mobile Ad hoc Networks

Sharmila Sankar[1], V. Sankaranarayanan[2]
[1]Department of Computer Science and Engineering
B S A Crescent Engineering College
Chennai, India
sharmilasankar@yahoo.com

[2]Director (University Project)
B S A Crescent Engineering College
Chennai, India
sankarammu@yahoo.com

Journal of Digital Information Management

ABSTRACT: *An ad hoc network is a multi-hop wireless network formed by a collection of mobile nodes without the intervention of fixed infrastructure. Limited bandwidth and a high degree of mobility require that routing protocols for ad hoc networks be robust and simple. In mobile ad hoc networks (MANETs), node mobility causes network topologies to change dynamically over time, which complicates the important tasks such as route discovery and maintenance. Most of the routing algorithms usually focus on how to discover a stable route, but rarely considers the adaptability of constructed route to the change of node's motion. This paper proposes a new ad hoc route maintenance protocol called Route Maintenance using Link State Prediction (RM-LSP). RM-LSP utilizes node locality to enhance resilience against mobility and hence the throughput. RM-LSP reduces the overhead of route failure recovery in source end and attempts to improve route efficiency and network throughput. Our simulation results show that RM-LSP delivers packets efficiently while substantially reducing control overhead in various environments. Simulation study of the algorithm proves it to offer significant benefits in dense scenarios.*

Categories and Subject Descriptors
C.2.1 [Network Architecture and Design]: Wireless communication;
C.2.2 [Network Protocols Routing]: Protocols

General Terms: Mobile ad hoc networks, MANET routing protocols, Network links

Keywords: RM-LSP, Handoff, RCPI, Promiscuous mode

Received: 18 January 2011, Revised 12 March 2011, Accepted 30 April 2011

1. Introduction

A MANET is a dynamic wireless network with or without fixed infrastructure. Nodes may move freely and organize themselves arbitrarily; thus the network's wireless topology may change rapidly and unpredictably. Each node may communicate directly with any node within transmission range. Communication beyond that range is achieved by using intermediate nodes to relay messages hop by hop. Such a route may include multiple hops, and therefore, the resulting network may or may not be a multi-hop network. MANETs do not depend on centralized administration, rather each node acts as an independent router and typically also as an application node, generating and receiving application data. As such, network management is distributed across the nodes. MANET routing protocols can be classified into two main categories: proactive routing protocols and reactive routing protocols. Proactive routing protocols attempt to maintain routing information for every pair of network nodes by actively propagating route updates. Reactive protocols establish a route to a destination only when needed [1]. The source node initiates a route discovery process when the route is required, and once a route has been established it is maintained until either the destination becomes inaccessible or until the route is no longer used. Both categories of MANET routing protocols assume the existence of a full (possibly, multi-hop) route from source to destination at the time of sending, and if one is not available routing fails. This assumption makes MANET routing protocols unsuitable for environments where disconnections are frequent and potentially long-term.

Many stability-oriented routing protocols had been proposed for enhancing the stability and the continuity of the data transmission, which makes efforts to decrease the impact of node's motion to routes. The basic idea of the stability-oriented routing protocol is that the route is established with a series of adjacent nodes which can communicate as much time as they can with each other[2] [3]. Two essential components of the stability-oriented routing protocol are the evaluation of the stability and the maintenance of route, the former is characteristic of the stability-oriented routing protocol which is the basic of establishing stable route, and the latter is common in routing protocols, which is used to ensure that there are available routes for data transmission after the current used route is down. There are some issues about the two afore mentioned essential components of the stability-oriented routing still should be considered. Firstly, the periodic message exchange is used by some stability evaluation methods to obtain necessary information about the neighborhood of nodes. However, an appropriate exchange interval is hard to set. When the interval is long and node mobility is high, the route exchanges cannot reflect topology changes; when the interval is short, the routing overhead will consume too much network capacity. Furthermore, this periodic exchange, which involves all nodes in whole network, can be a large consumption of network resources and increase the opportunity of collision.

Secondly, the parameter for evaluation and the stability evaluation method itself determine the accuracy of the stability evaluated. Thirdly, the stability-oriented routing algorithm usually adopts reactive manner, which has a general routing cycle: route discovery; route maintenance and route rediscovery. Although the stable routes for data transmission are established in route discovery process, it should alert the change of the stability of routes which is caused by node's motion during the transmission of data, since it turns to impact the route rediscovery process.

Route rediscovery usually occurs when a routing algorithm fails to maintain a valid route for an ongoing traffic flow. The flow is interrupted while a new route is found, which leads to unacceptable traffic delivery gaps for real-time applications. To enable the mobile ad hoc network to carry as many applications as traditional networks do, the stability-oriented routing algorithm needs to provide continuous valid routes for ongoing flows in high-mobility scenarios. Finally, the routing overhead should be adaptive, so that the amount of routing overhead is consistent with the topology and traffic demands In order to limit the network overhead efficiently and adaptively, keep track of the varying topology and provide continuous and valid routes for the stable data delivery, a mobility-adaptive routing algorithm RM-LSP is proposed.

A route in Ad-hoc network may suffer from route break due to host migration, signal interference or power outages. Thus, most of the previous research [4-6] performed a route reconstruction process at the occurrence of route disconnection. Traditional route maintenance works only after an active path fails. The cost of detecting a failure is higher compared to typical packet latencies. Thus, when a path breaks down, packets experience large delays before failure is detected and a new path is established. The reconstruction process establishes another route by flooding messages from source to destination, which causes not only heavy traffic but also long delays for route recovery. In contrast to previous works, the route maintenance protocol proposed in this paper determines an active node that is predicted to cause a weak connection in the future. By monitoring the signal strength of neighboring hosts, two end hosts of a weak link (or unreliable link) will perform an local route repair to recover the weak link before the route is broken. The local route repair is automatically performed by the end host/s of the weak link thus involving small set of message exchanges and fast reconstruction of route with no flooding overhead of route reconstruction.

2. Related Work

Several routing protocols have been suggested to solve the link failure problem and support reliable data transmission [7-10]. Based on the AODV routing protocol, Sung-Ju Lee and Mario Gerla proposed a backup routing protocol called AODV-BR [7]. In AODV-BR, the backup routes are made by overhearing a RREP message. If any node is aware of a link failure because of node movement, packet collision and limited battery during the data transmission, it broadcasts the data to find a backup node. Despite offering a more stable connection than AODV, AODV-BR ignores the network environment. To establish the backup nodes, the network should be very dense. In that case, there are many collisions at the node that is in original route and receives the data from failed link. Moreover the route recovery might increase the hop count of the route and then enlarge the end-to-end delays.

In AODV-ABR which is proposed by Wei Kuang Lai, Sheng-Yu Hsiao and Yuh-Chung Lin, the establishment of backup routes takes advantage of overhearing RREP packets with hop count to the destination [8]. When any node detects a link failure, AODV-ABR starts a three way handshake. AODV-ABR considers hop count of route and competition of multiple backup nodes. However the control message overhead is large.

Many studies that sought to improve the data packet delivery ratio have been done, but these works leave a considerable number of routing overhead messages. Our approach in this paper is different from the previous schemes. The proposed method avoids the construction of backup routes by overhearing, thus reducing the energy depletion caused in nodes when operating in promiscuous mode. Section 3 describes a detailed scheme to improve the data packet delivery ratio while reducing the number of routing overhead messages by finding an one-hop neighbor of the main route nodes to handoff, when a link failure is likely to occur. The proposed method basically exploits the node density in the network.

3. Route Maintenance using Link State Prediction for Dense MANETs

3.1 Route Failure Detection

Routing failure can be defined as unusable routes as a result from failures of some links in the route list. There are some factors that a link failure occurs, including node mobility, environment conditions, node failure (i.e., lack of energy power support) and hard medium contention. Ad hoc network routing protocol may detect failed link using hello messages, feedback provided to the protocol by the MAC layer and passive acknowledgements. Hello messages can be used to determine link existence. This method is quite simple, originated from the assumption that by receiving a hello message, link availability is signified. Hello messages are transmitted at regular intervals of time. Failing to receive hello message three successive times from a neighbor is interpreted as a sign that the link to the given neighbor is failed. One of the routing protocols that implement this technique is AODV. The disadvantage of this method is that it needs additional control message (aside the other routing control message packets) to detect link availability, which subsequently increase the routing overhead and decrease the routing efficiency as well.

Another method that can be used to detect link failure is by using MAC layer feedback. MAC layer feedback to the network layer, explicitly declaring a transmission error indicating that a packet could not be forwarded to its next hop node [12] is used to detect the link break. This method gives the routing protocol to take a quick response to link failure. Passive acknowledgement also can be used to detect link failure. When a packet is transmitted to the next hop on the route, the node, which is transmitting the packet continues to listen to the channel and overhears whether the next hop forwards the packet further along the path. If it does not hear the forwarding of the packet for some period of time, it draws a conclusion that the link is failed.

3.2 Route Failure Prevention

In the proposed method each intermediate node on an active route detects a danger of a link break based on the strength of the received radio. The received power at the time of receiving packets is given by the MAC layer parameter, Received Channel Power Indicator (RCPI). When the received power at the time of receiving the data packets is less than the threshold and has decreased as compared with the previous received power, the node initiates the local (self) recovery. Once a link is detected unsafe, the current active node will send a local help (HLP) packet to its neighbors along the path for finding a bridge node to the next hop. Density is the key factor to find a bridge node for local self recovery. When the number of neighbor nodes around each intermediate node increases and the density rises, the probability of locating a bridge node is high.

3.3 Link Stability Prediction

When an intermediate node moves towards the downstream node, the strength of the received radio fades gradually and the strength of the transmitted radio will increase gradually. The strength of the transmitted radio signal is obtained as all the nodes are in promiscuous mode. Vice versa is also true. If an intermediate node moves away from both its neighbors, then

the strength of both the received and transmitted radio fades gradually. The following link stability prediction table (LSPT) has been constructed considering increase in signal strength as 1 and decrease as 0.

Cases	Received Radio	Transmitted Radio	Stability of Successor Link	Stability of Predecessor Link
1	0	0	Weak	Weak
2	0	1	Strong	Weak
3	1	0	Weak	Strong
4	1	1	Strong	Strong

Table 1. Link stability prediction table

Every intermediate node in the active path compares the strength of the received and transmitted radio with that of the values recorded in the routing table during the previous communication, to verify the stability of its successor and predecessor links. If a link is detected to be weak by a node, the node transmits a HLP packet to the respective nodes. Upon the reception of HLP packet, the upstream or/and the downstream node transmits their neighbor list to the node that has sent HLP packet. The neighbor list received from the neighboring node along the path, is scanned to detect a new neighbor which could act as bridge node between the upstream/downstream node and the current node. Due to the high node density in the dense networks, the probability of finding a bridge node is very high.

3.4 Case Study

From fig.1 suppose B is at the source end and D is the destination. The path from S to D is S – A – B – C – D (this is determined during route discovery/construction phase) each node will receive the RCPI value of the packet that arrives and the packet that is overheard from its successor neighbor, from the MAC layer. This received signal strength is compared with that of the stored value in the routing table. Node B compares the received RCPI values with the threshold RCPI. If the received RCPI is lesser than the threshold, then node B initiates the route handoff, in order to prevent the link break that might occur due to the movement of the nodes. Now node B decides on involving its neighbors in the handoff by comparing the received RCPI values with that of the values stored in its routing table. For example if the value stored in the successor link field of the routing table of node B is -85dbm and the new value returned by MAC on overhearing is -95dbm, then, the node B and its successor neighbor C are moving away from each other. B determines that the link between A and it is intact and the link with C is getting weaker.

3.5 Routing Handoff

Routing handoff is a proactive approach of dealing with route breaks. In routing handoff, each node makes use of its neighbor

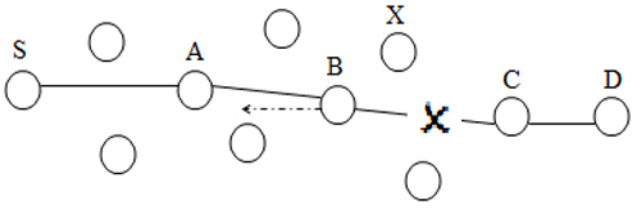

Figure 1. Path from S to D with B moving towards A

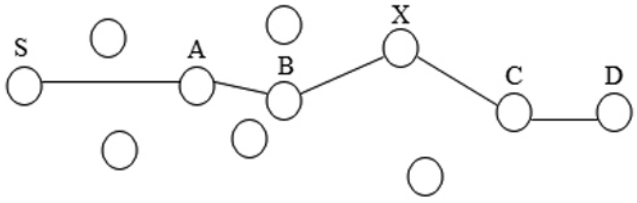

Figure 2. Path from S to D after fixing up link likely to be broken between B & C

list (nblist). The central idea of routing handoff is to find a node in the neighborhood to take the task of routing the packets routed through a link that is about to break.

When a movement of the intermediate node may cause a link to break, from the above example (section 2.4) the node B sends HLP packet to C. HLP is a single hop packet. The neighbor node C, which receives the HLP packet, responds to B by sending its nblist to B. B on receiving the nblist of C, compares its nblist with that of the received nblist. If it could find a neighbor node in common as shown in figure 2, then the common neighbor node (node X in figure 2) is added as the new intermediate node between B and C, thus expanding the path length by 1 hop. In the case of dense network, the number of neighbors of each node in the network is typically higher and hence the probability of finding a node to patch up the link likely to be broken is high. When a node is moving away, from its predecessor and successor neighbor nodes (case 1 in LSPT), it hands off the routing information to a new common neighbor of the successor and predecessor nodes along the communication path.

The algorithm followed by each node in the network to perform routing handoff is outlined below. Here Received Packet, refers to data/ routing/ Hello/ help (HLP) packets. Hello messages are used to discover neighbors and maintain the information table. For each node in the network:

```
Begin
.
.
if ( power of Received Data Packet <= threshold power)
{
      Create HLP packet;
      Send HLP packet to successor and/or predecessor checking the LSPT;
}
if (received packet == HLP)
{
      Send handoff reply with nblist;
}
if (Received Packet == HLP reply)
{
      Find a new common neighbor;
      Update routing table;
}
}
End
```

4. Simulation Parameters and Performance Evaluation Metrics

The comparative performance of AODV and proposed protocol is studied in different simulation scenarios based on the selected performance parameters.

4.1 Simulation Environment

The object oriented, event driven OMNET++ has been used as the simulation tool. The source destination pairs are spread randomly over the network. Each data point represents the average of 25 runs. The parameters for simulation are illustrated in Table 2.

Parameters	Value
Simulation Environment	OmNet++
Simulation time	500 seconds
Simulation Area	750mX750m
Mobility model	Random way point
Traffic Type	CBR
Packet Size	512 bytes
Transmission Range	250 m
Link Capacity	2 Mbps
Receive Sensitivity	-95.0 db

Table 2. Simulation Parameters

4.2 Performance evaluation Metrics

To analyze the performance of the proposed prediction based route maintenance for dense MANETs, two metrics have been studied. The performance parameters/metrics considered are the average end-to-end delay and Packet delivery ratio.

1. Packet Delivery Ratio: The ratio between the number of packets received by the destination and the number of CBR packets originated by the source.
2. Average End-to-end Delay: Average of total time to deliver packet from source to destination.
3. Normalized Control Packet Overhead: Normalized routing overhead is the number of routing packets transmitted per data packet which is delivered at the destination.

5. Simulation Results and Analysis

5.1 Performance Evaluation under Variable Node Density

We defined the *normalized density* as the average number of nodes within the maximum transmission range of a given node. The density in these scenarios is a function of both the number of nodes in the simulation and the total area of the simulation topology. The effect of node density is analyzed to test the behavior of the protocol for highly dense MANETs. To analyze the Packet Delivery Ratio (PDR), we assume that each station sends the data at a rate of 15 packets/sec and the number of flows in the network as 5.

Packet delivery Ratio (PDR) (figure 3) is almost kept constant with node density in the proposed protocol, whereas in AODV the PDR drastically reduces with the increase in the node density. This is because with the increase in the node density, the number of data packet also increases. Route failure causes more packets to be dropped in high network load conditions in AODV. The latency in fixing the path break is very high in

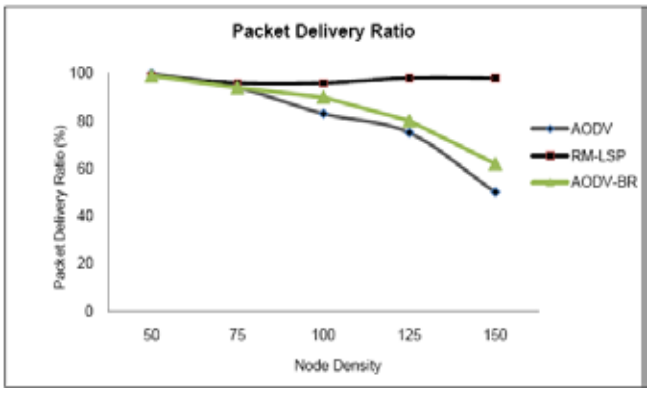

Figure 3. Effect of node density on Packet Delivery Ratio

AODV and this causes high packet drops. In the proposed protocol, the latency in fixing up the weak link is very less and it involves at most two control packets to be exchanged between nodes involved in path break. Moreover the proposed protocol tries to fix up the path that is likely to be broken. Hence the number of packets that are dropped due to path unavailability is zero in many cases.

Because RM-LSP attempts to use alternate path for data delivery even before the occurrence of route breaks, the protocol is able to deliver more packets to the destination than AODV. AODV simply drops data packets when routes are disconnected. AODV-BR also has some packet losses. Alternate paths may be broken as well as the primary route because of mobility, or be unavailable and not discovered during the route reply phase. Moreover, packets can be lost because of collisions and contention problems.

5.2. Performance Evaluation under Variable Traffic Load

The effect of varying traffic load for varying node densities is studied as it is very important for any routing protocol to deal with the situation when the network becomes heavily loaded. From figure 4 it can be seen that the average end-to-end delay rises with the increase packet rate and with the increase in node density in AODV. As traffic load increases, more packets populate the network and exceed the link capacity to transmit all packets at a time. So the buffers of the nodes become full much quickly and more packets need to wait in the queue for a longer time. This long waiting time increases the delay and also introduces packet drops, which in turn initiates the route discovery process in AODV. In the proposed protocol, load balancing is taken care of in the initial route discovery phase [12-13]. This decreases the congestion in the network and involves the nodes which are not participating in any of the active path. This decreases the early filling up of queue in heavy traffic conditions and hence the packet drops. Therefore the delay involved in the proposed method is much lesser than AODV in heavy traffic conditions. In high network densities the probability of finding a new node to handoff or bridge the path that is likely to be broken is very high and hence the problem is fixed locally. Hence the delay involved in finding a new path as compared with AODV is drastically reduced. It is obvious from figure 4 that with the increase in traffic flow (with a constant node density), the increase in the latency is very high in AODV and the latency involved in data transmission using the proposed method is reduced to 50% at higher traffic flows. Also in the proposed method with the increase in node density the average end-to-end delay is almost kept constant at a constant traffic flow where as in AODV the average end-to-end delay increases with the increase in traffic flow.

5.3 Normalized Control Packet Overhead

Figures 5 illustrates the normalized control overhead introduced in the network for 5 source-destination pairs. It can be seen that the proposed method produces significantly lower normalized control overheads than AODV and AODV-BR. The use of blind flooding and expanding ring search in AODV is the main culprit resulting in excessive overhead in dense networks or in scenarios where the number of hops between source and destination nodes is larger. The negative impact of the combined use of blind flooding and expanding ring search is evident from the excessive control packet overhead results shown in Figure 5. In AODV-BR the node that detected the link break also sends a ROUTE ERROR (RERR) packet to the source to initiate a route rediscovery. The reason for reconstructing a new route in AODV-BR instead of continuously using the alternate paths is to build a fresh and optimal route that reflects the current network situation and topology. This new route reconstruction accounts to the higher routing overheads compared with that of the proposed RM-LSP. Since many of the flow do not require new route reconstruction due to assumed lower mobility conditions, the normalized routing overhead in AODV-BR is lesser compared to that of AODV.

5.4 Throughput Analysis

It is clear that almost any reasonable routing metric will achieve similar performance when the network density is low because the number of available paths to choose from is limited. Figure 6 shows the average throughput with respect to the throughput of the AODV and RM-LSP combination. The average gain of RM-LSP represents the throughput increase achieved by our proposed method under the network density of 125 nodes. As expected, we see a clear increasing trend in average gain compared with that of AODV. The trend line of AODV in Figure 6 indicates that the average throughput decreases with the increase in the traffic

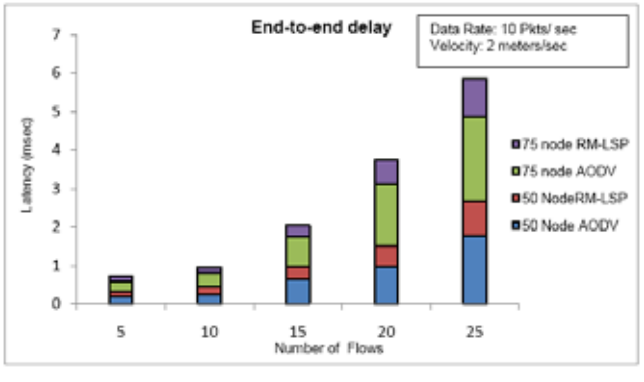

Figure 4. Latency for various traffic loads

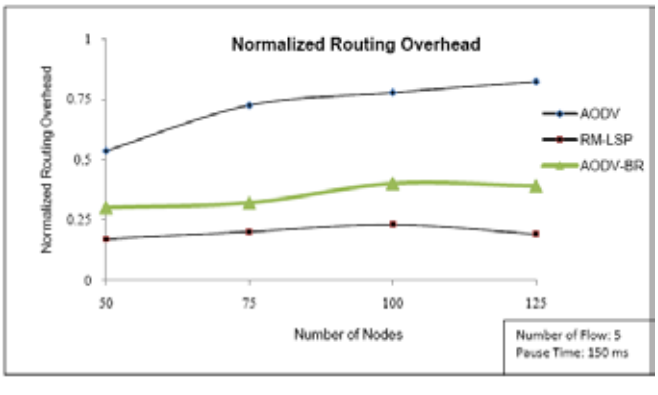

Figure 5. Control Overhead for 5 connections

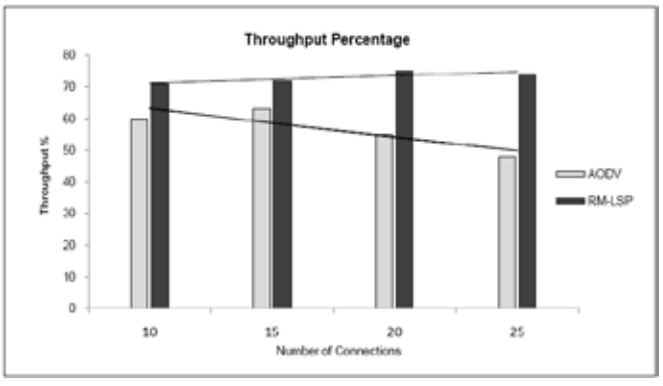

Figure 6. Throughput analysis for 125 nodes

flow/ load in the network. Even at the lowest traffic load, RM-LSP provides a modest 11% average increase in the throughput. At the highest simulated traffic load, we see a more substantial 26% average increase. The throughput should also be higher with even higher densities.

6. Conclusion

The performance of reactive routing protocol is affected by routing overheads and delays in repairing broken routes. Routing overheads are the results of error broadcast followed by flooding in the route discovery phase. Delay in repairing routes is due to its inability to find an alternate route without reinitiating a route discovery phase. The proposed RM-LSP protocol performs better than traditional AODV during high density and high network load conditions. In most of the case, particularly in high density networks, the delay in fixing the weaker links or links likely to be broken is close to 0 ms, as there is a high probability of finding a node to handoff, whereas in AODV-BR there is drastic performance degradation in high density conditions due to contention. Since RM-LSP finds a bridge node and fixes the link likely to be broken due to the node mobility, the number of packets dropped is drastically reduced compared to AODV and AODV-BR. RM-LSP involves only the end nodes of the weak link to fix the link break problem (Local repair) and hence the network is not flooded with route error message, which decreases the performance of the network. The performance of RM-LSP becomes violated in certain conditions like very high mobile networks and sparse networks.

References

[1] Perkins, C.E., Royer, E.M., Das, S.R (2003). Ad hoc on-demand distance vector (AODV) routing, *IETF RFC 3561*.

[2] Ramasubramanian, Z.J., Haas, E.G., Sire, (2003). SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks, *In: Proceedings of 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*.

[3] Spohn, M., Garcia-Luna-Aceves, J.J. (2001). Neighborhood aware source routing, *In: Proceedings of 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*.

[4] Kang, Byung-Seok., Ko, In-Young (2010). Effective Route Maintenance and Restoration Schemes in Mobile Ad Hoc Networks, *Sensors*.

[5] Shi, Dong., Zhang, Xinming., Gao, Xuemei., Zhu, Wenbo., Zou, Fengfu (2007). A Link Reliability-aware Route Maintenance Mechanism for Mobile Ad hoc Networks, *In: Proceedings of the sixth International conference on Networking, IEEE 2007*.

[6] Liang Qin and Thomas Kunz, 2008. Adaptive MANET Routing: A Case Study, *ADHOC-NOW 2008, LNCS 5198, pp. 43–57, Springer-Verlag*.

[7] Lee, S.J., Gerla, M. AODV-BR: Backup routing in Ad Hoc networks, 2000. Proceedings of IEEE WCNC.

[8] Lai, Kuang., Wei, Hsiao, Sheng-Yu., Lin, Yuh-Chung (2007). Adaptive backup routing for ad-hoc networks, Computer Communications,

[9] Wang, Y.-H., Chuang, C.-C., Hsu, C.-P., Chung, C.M.(2003). Ad hoc ondemand routing protocol setup with backup routes. Proceedings of ITRE 2003, *In*: International Conference on Information Technology: Research and Education, p. 137–141.

[10] Ahmed, Izhar., Tepe, K. E., Singh, B. K. (2010). Reliable Coverage Area Based Link Expiration Time (LET) Routing Metric for Mobile Ad Hoc Networks, Ad Hoc Networks.

[11] Yao, Chang-hua, Wang, Cheng-gui, (2010). A Cross-Layer Synchronous Dynamic Token Protocol for Ad Hoc Networks, Proceedings of International Conference on Communications and Mobile Computing, IEEE.

[12] Sharmila Sankar, Sankaranarayanan, V (2010). Framework for Probabilistic Routing in Dense Ad hoc networks, *Recent Trends in Networks and Communications, CCIS, Springer-Verlag, 2010, V. 90, Part 2, 447-456*.

[13] Sharmila Sankar,.Sankaranarayanan, V (2010). A Low Overhead Reachability Guaranteed Dynamic Route Discovery Mechanism for Dense MANETs, *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) 1(3) 72 – 83*.