International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 539-543

A CROSS LAYER DESIGN FOR ROUTE MAINTENANCE IN DENSE MANETS

Sharmila Sankar[1] & V. Sankaranarayanan[2]

Ad hoc networks are deployed in situations where no base station is available and a network has to be built impromptu. Since there is no wired backbone, each host is a router and a packet forwarder. Each node may be mobile, and topology changes frequently and unpredictably. Routing protocol development has received much attention because mobility management and efficient bandwidth and power usage are critical in ad hoc networks. The primary concerns in ad hoc networks are bandwidth limitations and unpredictable topology changes. Thus, efficient utilization of routing packets and immediate recovery of route breaks are critical in ad hoc routing protocols. The available route maintenance methods for MANETs work well only for networks with certain limited assumptions of number of nodes, density of nodes and mobility. In this paper, we introduce a mobility prediction based algorithm for route maintenance scheme for MANETs, which works well under a wide range of network topologies, nodes-density, and nodes-mobility. Simulation study of the algorithm proves it to offer significant benefits in dense scenarios.

Keywords: Handoff, Cross layer, RCPI, Promiscuous Mode

1. Introduction

The natural ability of MANET host to self configure and roam makes the topology change frequently. One of the critical challenges in the design of MANET is the development of efficient routing protocols that can provide high-quality communications among mobile hosts. Current routing protocols in MANET can be classified as proactive (table driven) and reactive (on-demand) [1]. The reactive protocols, like DSR [2] and Ad hoc On-demand Distance Vector (AODV) [3], comprise three separate parts: route discovery, data forwarding and route maintenance. In route discovery phase the source node shall broadcast a RREQ (route request) packet to all its neighbors. The RREQ may be replied through a RREP (route reply) packet by some intermediate nodes, if they have cached one path towards this destination node. Otherwise, the RREQ will be forwarded in a broadcasting mode until the destination node receives it and reacts with a RREP packet. Since there may be several RREP packets, representing different path choices, the source node shall select one from all those candidates according to a certain rule, for example, hop count in DSR [2]. Routing maintenance is to find an alternative path for a broken one. It is triggered only after a certain routing path breaks. An error packet is transmitted back to the sender, reporting this route break. On receiving this packet, the source node shall check its local cache for an alternative path towards the same destination. If there is no such path in cache, another route discovery has to be done to build a new routing path.

[1]Department of Computer Science and Engineering, B S Abdur Rahman University
[2]Director (University Project), B S Abdur Rahman University, Chennai, India
E-mail: [1]sharmilasankar@yahoo.com, [2]sanakarammu@yahoo.com

A route in Ad-hoc networks may suffer from route break due to host migration, signal interference or power outages. Thus, most of the previous research [4][5][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 recovering. 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 exchange and fast reconstruction of route with no flooding overhead of route reconstruction.

2. Prediction Based Route Maintenance For Dense MANETs

2.1 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 interval 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 routi ng 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 are called backs to the network layer sent by the MAC layer, explicitly declaring a transmission error indicating that a packet could not be forwarded to its next hop node[7]. 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.

2.2 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 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, therefore the probability of locating a bridge node is high.

2.3 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.

Table 1
Link Stability Prediction Table

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

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 sent HLP packet. The neighbor list received from the neighbor node along the path, is scanned to detected 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.

2.4 Case Study

From Fig.1 suppose B is the source 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 router 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 itself is intact and the link with C is getting weaker.

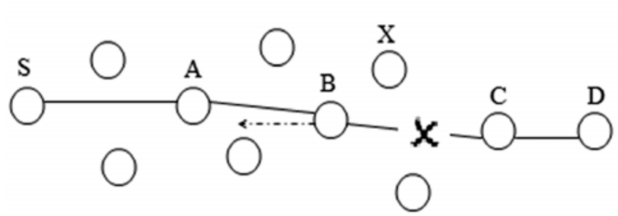

Fig. 1: Path from S to D with B Moving Towards A

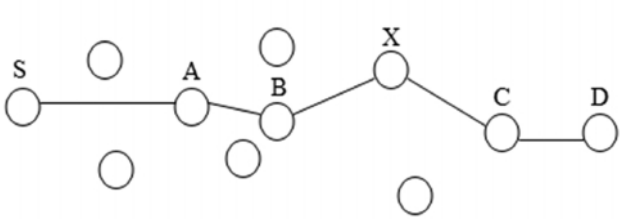

Fig. 2: Path from S to D After Fixing Up Link Likely to be Broken Between B & C

2.5 Routing Handoff

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

2.6 Algorithm

The algorithm followed by each node in the network to perform routing handoff is outlined below. Here Received Packet, refers to data, routing, Hello Message or 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
```

3. 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.

3.1 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 10 runs. The parameters for simulation are illustrated in Table 2.

Table 2
Simulation Parameters

Parameters	Value
Simulation Environment	OmNet++
Simulation time	500 seconds
Simulation Area	670mX670m
Mobility model	Random way point
Traffic Type	CBR
Packet Size	512 bytes
Transmission Range	250 m
Link Capacity	2 Mbps

3.2 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.

4. SIMULATION RESULTS AND ANALYSIS

4.1 Performance Evaluation Under Variable Node Density

The effect of node density is analyzed to test the behavior of the protocol for highly dense MANETs.

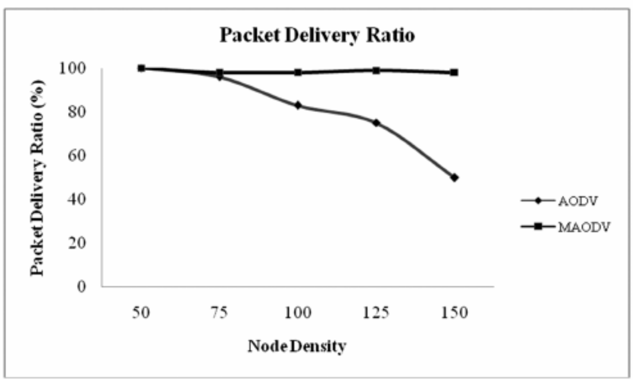

Fig. 3: Effect of Node Density on Packet Delivery Ratio

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 AODV and this causes the 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.

4.2. 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 [8][9]. 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 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 done in AODV is drastically reduced, which is obvious from Figure 4.

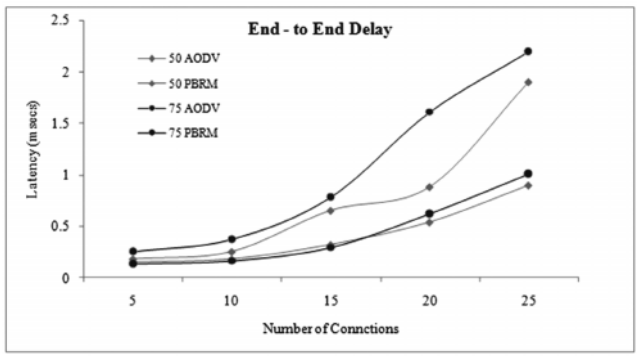

Fig.4: Latency for Various Traffic Loads

5. 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 Prediction Based Route Maintenance Protocol (PBRMP) 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 is close to 0 ms, as there is a high probability of finding a node to handoff. Since PBRMP 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. PBRMP 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 routing handoff becomes violated in certain conditions like very high mobile networks and sparse networks.

REFERENCES

[1] M. Abolhasan, T. Wysocki, E. Dutkiewicz, M. Abolhasan, "A Review of Routing Protocols for Mobile Ad hoc Networks, Ad hoc Networks", 2, pages:1-22, Jan 2004.

[2] D. B. Johnson, D. A. Maltz, Y. C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)", IETF draft-ietf-manetdsr- 10.txt, July 2004.

[3] C. E. Perkins, E. Belding-Royer, S. Das, "Ad hoc On Demand Distance Vector (AODV) Routing", IETF RFC3561, July 2003.

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

[5] Dong Shi, Xinming Zhang, Xuemei Gao, Wenbo Zhu, Fengfu Zou, "A Link Reliability-aware Route Maintenance Mechanism for Mobile Ad hoc Networks", Proceedings of the Sixth International Conference on Networking, IEEE 2007.

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

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

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

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