Journal of Computer Science 4 (3): 172-180, 2008
ISSN 1549-3636

A New Distance Based Route Maintenance Strategy for Dynamic Source Routing Protocol

[1]Muhammad Farhan Sjaugi, [1]Mohamed Othman and [2]Mohd. Fadlee A. Rasid
[1]Department of Communication System and Network,
Faculty of Computer Science and Information Technology
[2]Department of Computer and Communication Systems Engineering,
Faculty of Engineering
University Putra Malaysia, Serdang 43400, Selangor D.E., Malaysia

Abstract: Although DSR can respond a route quickly, it yields a long delay when a route is rebuilt. This is because when source node receives RERR packet, it will try to find alternative routes from the route cache. If alternative routes are not available, the source node, then, will enter route discovery phase to find new routes. We introduced a new route maintenance strategy by utilizing location information, called the DISTANCE (DIstance baSed rouTe maintenANCE) algorithm. The DISTANCE algorithm works by adding another node (called bridge node) into the source list to prevent the link from failure. From the simulation result, the DISTANCE algorithm improved the performance of DSR in terms of packet sending ratio, delay and routing overhead.

Key words: Route maintenance, routing protocol, mobile ad hoc network, dynamic source routing protocols

INTRODUCTION

Earlier, the idea of mobile computers and ad hoc networks was not on the mind of anyone. All specifications and implementations for the computer networks during that time were designed for wired systems. This is a big challenge for computer engineer since these two systems have different characteristics. Wireless network means dynamic topology, dynamic structure and no infrastructure, while wired network is the opposite. Most of wired network design and implementation must be modified or redesigned in order to operate in the mobile wireless network. Basically mobile wireless network has the same standard layers of structure, with modifications and functionality that differ from the earlier networks because of the absence of infrastructure.

There are currently two variations of mobile wireless networks. The first is known as infrastructured network. The bridges for these networks are known as base stations. A mobile unit within these networks connects to and communicates with, the nearest base station that is within its communication radius. As the mobile unit travels out of range of one base station into the range of another, a "handoff" occurs from the old base station to the new, allowing the mobile to be able to continue communication seamlessly throughout the network. Typical applications of this type of network include office wireless local area networks (WLANs).

The second type of mobile wireless network is the mobile adhoc network or MANET. Unlike infrastructured network, this type of network needs no base station. Mobile nodes communicate to each other by either directly or through intermediate nodes. Adhoc network becomes popular since it can be applied in many situations, such as emergency search-and-rescue operations, classroom, meetings or conference and many more.

To facilitate communication within the network, a routing protocol is used to discover routes between nodes. Building a MANET routing protocol is not an easy job, since efficiency and correctness becomes the main concern. Some approach had been proposed to make routing protocol becomes efficient and correct. Routing protocols in MANET, generally, can be categorized as table-driven and on-demand. In table-driven (also called proactive protocol), like in most routing protocol for wired network, each node is required to maintain routing table keep updated whether there is or not a request for routes. The examples of

Corresponding Author: Mohamed Othman, Department of Communication System and Network, Faculty of Computer Science and Information Technology, University Putra Malaysia, Serdang 43400, Selangor D.E., Malaysia

table-driven routing protocol are DSDV[10], WRP[7] and CGSR[3]. In on-demand (also called as reactive protocol), each node seeks for routes only when there is need to do so. This category also called as reactive protocol. The examples of on-demand routing protocol are DSR[5,6], PAR[12], DBR^{2}P[11] and DSR-ARM[8,2].

In some regular situation, some links in the route may fail. In this situation, any packets that travel through these routes will be lost or dropped. In some cases any packets may still reach its destination, but with some delay. This delay is very expensive and leads to undesired effect, especially in real time networks and the networks with QoS, where the packet delay and packet delivery is the main concern.

We organized this article as follows. First, we discussed about some related work in route maintenance in MANET routing protocol, particularly focusing DSR routing protocol on how mobile nodes can detect route failure and how does the response of mobile nodes when route failure is detected or failure. Second, we introduced our proposed model for detecting and responding to route failure. These will be our main contributions. Finally we presented the result based on simulation and evaluated the performance.

RELATED WORKS

Route Maintenance: In MANET, each mobile node may communicate with other nodes either directly or through some intermediate or relay nodes. Before mobile nodes send packets to the destination node, first those mobile nodes need to establish routes to reach its destination node. Once the route is established, those mobile nodes can start sending data packets to the destination nodes. In regular situation, some links in the route may fail. Therefore, any packets that travel through these routes will be lost or dropped. In some cases the data packets may still reach its destination, but with some delay. This delay is very expensive and leads to undesired effect, especially in real time networks and the networks with QoS, where the packet delay and packet delivery is the main concern.

Most of the routing protocols for MANET have mechanism to handle this situation. This mechanism is called route maintenance. Route maintenance play important role in ad hoc networks by reducing or eliminating the broken link in order to prevent interruption in the services that the network can offer. Each routing protocol has its own specification to route maintenance, but there is some similarity from one protocol to another protocol.

DSR Route Maintenance: Dynamic Source Routing (DSR) [5,6], which is an on-demand routing protocol, becomes the most popular source routing protocol for MANET. Each mobile node is required to maintain route caches that contain the source routes of which the mobile is aware. How DSR search for some routes from source node to destination node are as follows; first source node will start to "flood" the network with route request (RREQ) packets (assumed source node does not have any route to reach destination node before).Intermediate nodes, then will check whether it is by itself the destination node or not. If this node is not the destination node, then this node will add itself into the route list in the RREQ packet header and then forward this packet into its neighbor. If this node is the destination node, then this node will send route reply (RREP) packet to the originator of this RREQ packet (i.e. source node), including the route list to reach this particular node, which was gathered from RREQ packet header. How the RREP packets travel to reach source node is just simply by following the route list. Once this packet reach the source node, then the source node will start sending data packets to the destination node. Entries in the route cache are continually updated as new routes are learned. Intermediate nodes, then will do passive learning by storing some information from the route list (inside RREP packet header) into their route caches for future routing purposes. All of this process is called Route Discovery.

In case of link/route failure, the intermediate nodes, which detect link/route failure, will send route error (RERR) packet to the source node. When source node receives RERR packet, it will try to find alternative routes from its route cache. If alternative routes are not available, source node, then, will enter route discovery phase to find new routes. Although DSR can respond a route quickly, unfortunately it yields a long delay when a route is rebuilt. Finding a route in wireless network require considerable resources, such as time, bandwidth and power because it relies on broadcasting.

Some of the previous works for solving route maintenance problem in DSR, includes Dynamic Backup Route Routing Protocol (DBR^{2}P) [11] and Anticipate Route Maintenance (ARM) [8, 2].

In [11], Wang and Chao proposed Dynamic Backup Route Routing Protocol (DBR^{2}P). DBR^{2}P enhance DSR by adding route backup in case of a link/route failure. DBR^{2}P “armed” intermediate nodes with alternative/backup path to reach destination node. DBR^{2}P includes three phases, route discovery, backup node setup and route maintenance. When a destination node receives route request messages (in DBR^{2}P it is called RD-request), it will build backup setup packet

(BS-Packet). BS-Packet contains backup routes to reach the destination node. A node (including the source node) which has more than one possible route to a destination node is called backup node. BS-Packet is sent by destination node to the backup nodes. When the backup nodes receive BS-Packet, they will store the routes to their local cache. In case of route/link failure, the detector will try to replace the routes with backup routes, taken from the backup cache. This replacement is done on the spot. If that node does not have backup routes, it will send route error packet to their upstream. Then, the upstream nodes will check whether they have backup routes or not, if a backup node is available they will replace the routes and continue sending the data packets, otherwise a route error packet is sent to the upstream.

Park and Van Voorst[8] proposed Anticipated Route Maintenance (ARM). ARM is a distributed algorithm that anticipates route failure and performs preventative route maintenance using location information to increase a route lifespan by expanding the routes. The term route lifespan refers to the amount of time the route can function without failing. ARM determines the position when a node becomes unsafe by calculating the Time-to-Failure (TTF). If TTF is less than or equals to some pre-defined value (T), then the link is called unsafe. ARM itself depends on another MANET routing protocol to perform route discovery or searching path. ARM can be embedded into any reactive routing protocol. The combination of DSR and ARM can be seen in[2]. Unfortunately, calculating TTF value needs a complex calculation, because each node needs to know their next-hop position, as well as the velocity and the angle of the movement. This means that each node have to plan their movement precisely before informing the other nodes of its current location and plans to move somewhere.

MATERIAL AND METHODS

The key of improvement in our research is that the performance of DSR can be achieved only by preventing a link from failure. There are some advantages by using this approach, first MANET devices can save its resources (i.e., energy consumption) while not performing full route discovery procedure which is costly. Another advantage is some performance objectives such as high data throughput, minimum transmission delay and high ratio of data transmission can be achieved by using this approach. As the response to solve route maintenance problems in DSR, we developed a new route maintenance strategy that utilized geographical location information. We call it as DISTANCE (DIstance baSed rouTe maintenANCE). Based on location information, the DISTANCE algorithm tries to prevent the link from failure.

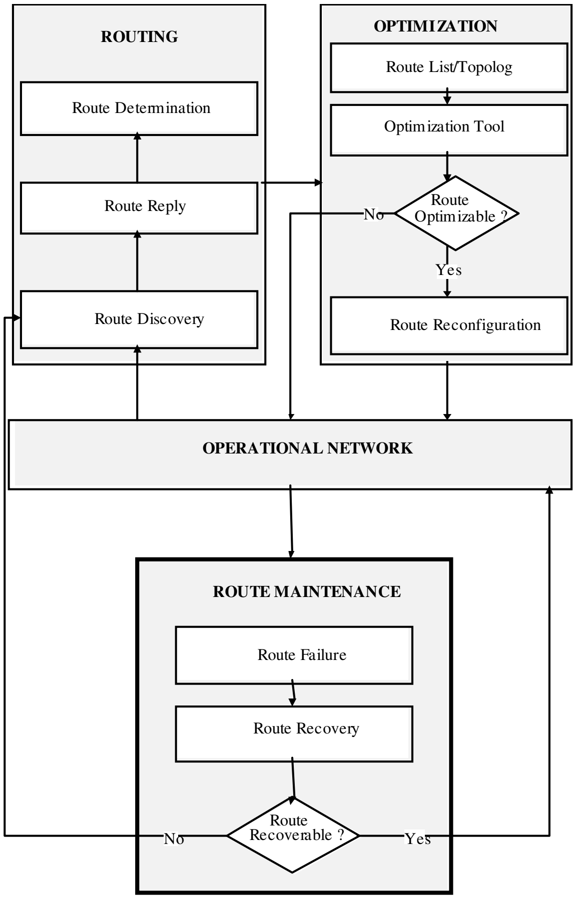

Fig. 1: The DSR routing protocol framework

The DISTANCE algorithm is developed on top of the DSR routing protocol framework. Figure 1 shows how the DSR routing protocol framework looks alike. It consists of three main stages: routing, optimization and route maintenance. Routing stage has responsible to determine possible route from the source node to the destination node. It is possible that more than one route are available to reach the destination node. In this case, optimization stage will take place to optimize which route is the best route. Once the route is established, those route needs to be maintained. In case of route failure, route maintenance stage will try to recover (or even replace) the current route. This process is handled by route maintenance stage. We focused our work to route maintenance stage. A proactive link failure prevention module is added into the route maintenance stage to provide unsafe link detection and prevention.

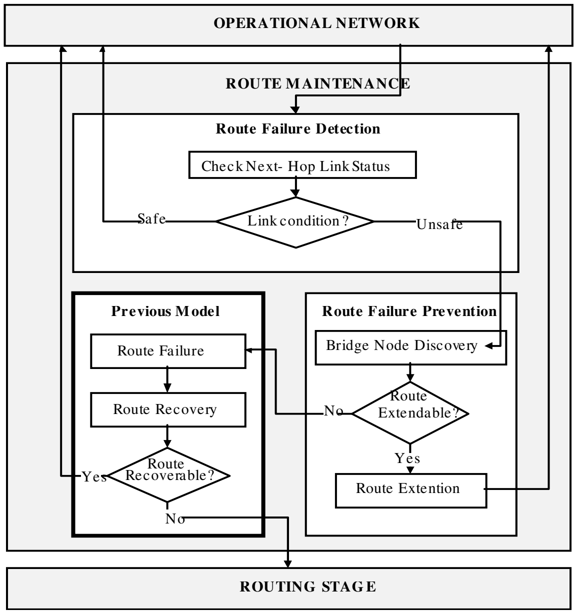

Fig. 2: The DISTANCE algorithm framework

Figure 2 shows how we modified the route maintenance stage. There are two main components in the modified route maintenance stage: route failure detection and route failure prevention. From Fig. 2, each node is required to check the link status to the next-hop. Any unsafe link will be detected here. If an unsafe link is detected here, the node will enter route expansion phase, which is finding a bridge node, otherwise just proceed with current route. We assumed that:

- Each node knows its current location (i.e., with Global Positioning System)
- All links are bi-directional and all nodes have the same transmission range (synchronous transmission range)
- Each node also maintains a location table that contains the positions of all its neighbors
- The routes are already established
- Route failure that is occurred by node disappearance (i.e., out of energy) is not considered

Basically there are two main procedures in the DISTANCE algorithm, in which, first we detect some unsafe link and then we expand the route by adding another node into the source list. In the DISTANCE algorithm, first the current active node will measure relative distance (RD) to the next-hop node from the source lists. The link is said unsafe if the RD is more than the threshold TH}. Once the link is detected unsafe, then the current active node will start to find a bridge node for bridging current link to next-hop node. If bridge node is found, expand the link, otherwise just proceed with the current link (the link cannot be expanded).

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[9]. 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 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. 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. One of the disadvantage of this technique is the network card must support promiscuous mode, which consumes a lot of energy. This is because the transmitting node needs to receive all the packets and decode it besides its own packets.

Today there is quite a lot of mobile device such as cell phone and PDA, which is equipped with Global Positioning System (GPS). This is because the production cost for the solution (i.e., receiver, chipset, etc.) is getting cheaper and the demand is getting higher. Most of the application of GPS is intended for guiding purpose such as road tracking. Besides using GPS to know current geographical location, GPS also can be used for routing purposes. Each node may know another nodes location by exchanging their current geographical location information. By knowing this information, the nodes may know the current network topology, so it can help to make routing decision.

The decision whether to add another node into the source list or not is based on the RD from current active node to the next hop node. A link is safe if RD is less than the TH; otherwise the link is said in unsafe state. We can say that RD is the cost for the link. Let A as the current active node, B as the next-hop from the route list. Assumed all nodes move in two dimensional planes, based on Cartesian coordinate. The RD can be formulated as:

$$\mathrm{RD(A,B)} = \sqrt{(\mathrm{Xa}-\mathrm{Xb})^2+(\mathrm{Ya}-\mathrm{Yb})^2} \qquad (1)$$

while TH can be defined as:

$$\mathrm{TH} = \mathrm{Transmission\,radius} * \omega \qquad (2)$$

where ω is a multiplier value, ranged between 0 and 1.

Based on the formula 1 above, each node will start to predict the condition of the link and try to prevent link failure if the link is detected unsafe.

Route Failure Prevention: Once a link is detected unsafe, the current active node will send a local broadcast packet (one-hop packet) to its neighbors for finding a bridge node to the next hop. If neighbor nodes have a link to the next hop, then these neighbor nodes will also calculate RD to both current active and the next hop node. If RD is more than TH (using the same formula to detect unsafe link) then this node will not propose itself to the current active node as a bridge node, otherwise it will propose itself as a bridge node to the current active node.

After some time, the current active node will receive the proposed bridge nodes and then it will decide which of the proposed node to be chosen as a bridge node, based on:

$$\min\left\{\begin{matrix}\dfrac{\mathrm{RD(A,B_1)}+\mathrm{RD(B_1,C)}}{2}\\ \vdots\\ \dots,\dfrac{\mathrm{RD(A,B_n)}+\mathrm{RD(B_n,C)}}{}\end{matrix}\right\} \qquad (3)$$

1 Byte	1 Byte	2 Byte	4 Byte	8 Byte
Type	Length	Tequst ID	Next-hop IP address	Geographical information

Fig. 3: The neighbor request packet format

1 Byte	1 Byte	2 Byte	4 Byte	8 Byte
Type	Length	RD next-hop	Next-hop IP address	Geographical information

Fig. 4: The neighbor reply packet format

If neither neighbor nodes, which have RD less than TH, nor candidate nodes are available, DISTANCE will just let the link as is (no action will be taken, let normal DSR route maintenance works).

Location Information Updates: In general there are two types of geographical location information, relative and absolute location. In relative location, node location is marked based on regions or broadcast area, while in absolute location, each node will inform the current location precisely (by using coordinate numbers). We used piggybacked method, to exchanging location information between nodes, where each node will update its location to the other nodes by piggybacking its current absolute location into packet header of any packet. This is to reduce the number of packet control overhead. Figure 3 and 4 illustrate how we put the location information into the packet header.

Case Study: From Fig. 5, let say node A wants to send data packets to D. The route to reach D from A is A-B-C-D (this route is gotten from route discovery phase). Each node will measure RD to its next hop. For this example, let say the transmission range is 250 and the ω value is 0.50 so the TH is 125. At first the link condition is fine, all the RD value is less than TH. But, when node D move to D', the RD value from C to D' is changed to 150. This will make the RD value bigger than TH, so then the link becomes an unsafe link; the DISTANCE algorithm is triggered.

Node C will send a local broadcast packet to its neighbors (i.e., node E, F, G, H), asking whether there is any nodes that have a link to D’. From Fig. 6, node C managed to get two of its neighbors (E, F), which has a link to D’. Then these nodes (E, F) will calculate RD value from themselves to D’. We can say that a node which has a link to the destination node (in this case D’) as the candidate node. Once a candidate node finishes calculating RD value, then it will send a reply packet to inform A that it has a link to D'. Then C will choose the bridge node from the candidate nodes based on the smallest average RD value, in this case node E is chosen as the bridge node.

To complete the algorithm, node C will add node E into the source list to reach D'. Now the route from A to D' becomes A-B-C-E-D'. Figure 7 shows the current route after expansion.

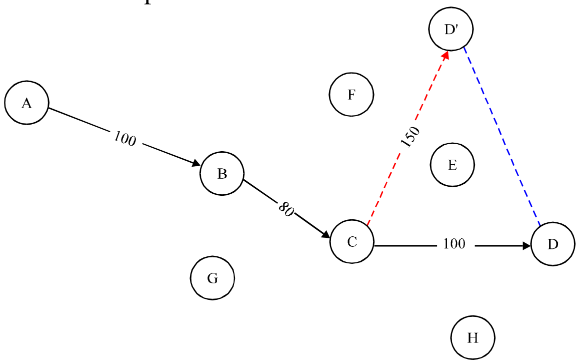

Fig. 5: Node D move to D', makes link from node C to D' becomes unsafe

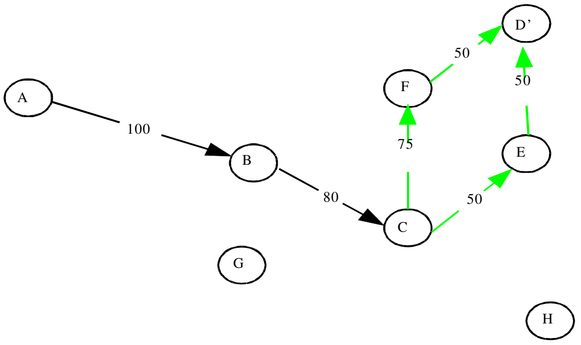

Fig. 6: Node C sends a local broadcast packet to find candidate nodes for bridging the link

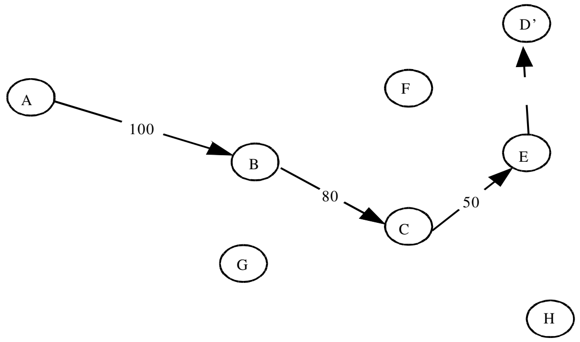

Fig. 7: New routes after expansion

Table 1: Simulation Parameter

Parameter	Value
Simulation time	500 seconds
Number of nodes	40 nodes
Area of simulation	1000×1000
Number of connections	10 connections
Data transmission	CBR, with 512 bytes packet size
Mobility	*RandomWaypoint*
Mobility speed	Max 10-50 mps with 10 mps incremental
Bandwidth for data transmission	2 Mbps
Medium access control model	IEEE 802.11

RESULTS AND DISCUSSION

We used JiST-SWANS[1] to simulate our proposed model. We ran JiST-SWANS on a PC with 3.8 GHz Dual-Core microprocessor with 2GB RAM. The summary of the simulation parameters used is described at Table 1. There are three performance metrics[4] that are used in this research:

- Average number of packet delivery ratio (APDR): Average number of received packets divides by number of sent packets.
- Average number of packet delivery time (APDT): Average number of time taken to deliver a packet from source node to destination node.
- Average number of routing overhead (ANRO): Average number of packets that are used for routing purposes.

To measure the performance of the proposed model, simulation based performance or analysis was conducted. The simulation are based on two scenarios, first based on varying mobility speed and second based on varying node density. The purpose of testing the model on varying mobility speed and node density is to see the impact of proposed route maintenance model to DSR as the mobility speed and node density are increased.

From Fig. 8, both DSR and DISTANCE have constant decreasing rate of APDR. Since in DSR route maintenance specification, a route must be re-established when this route is broken and it results in the decrease of packet sent/received ratio before a new route is established, it is clear that DISTANCE successfully increase the APDR. This is because the DISTANCE algorithm provides proactive method to prevent route failure, so it could reduce the number of route re-establishment. Moreover, Fig. 9 and 10 shows that the DISTANCE algorithm also successfully reduced the APDT and ANRO. This is because route re-establishment takes longer time than keeping the route still usable. During discovery of a bridge node,

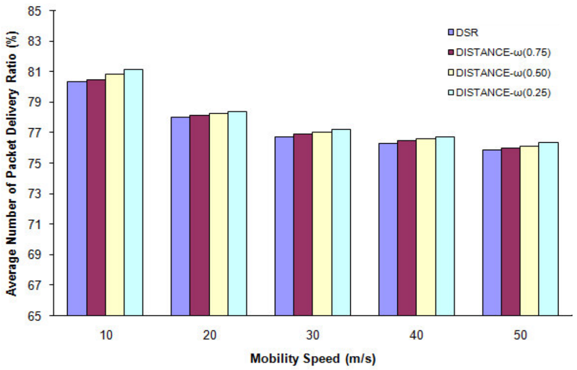

Fig. 8: APDR vs mobility speed

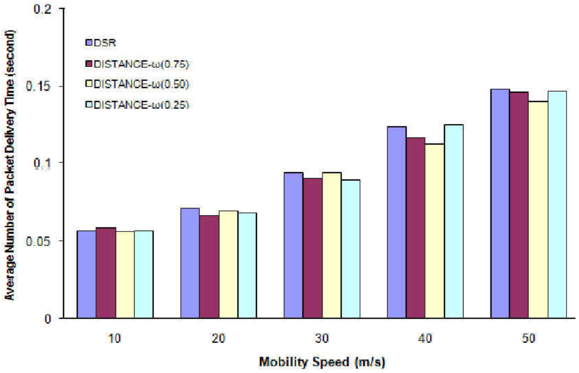

Fig. 9: APDT vs mobility speed

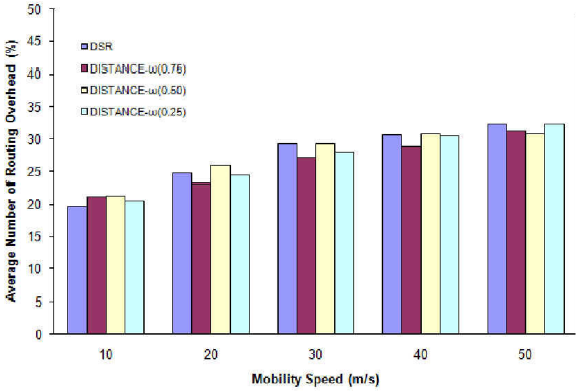

Fig. 10: ANRO vs mobility speed

current active node still can send and receive data packets. Once the link is detected unsafe and the route is successfully expanded, the current active node will use the new route to reach the next-hop node. Even though a bridge node is not found, current active node may still send and receive data packets until the route failure occurred.

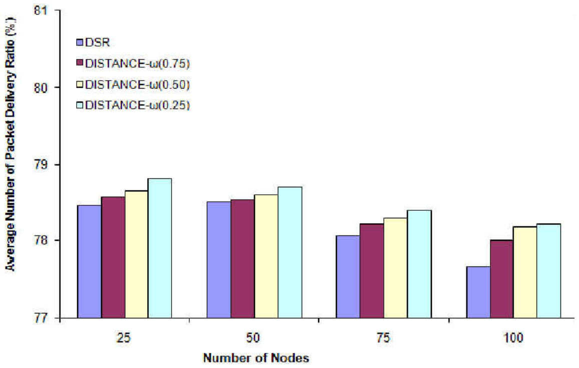

Fig. 11: APDR vs Number of Nodes

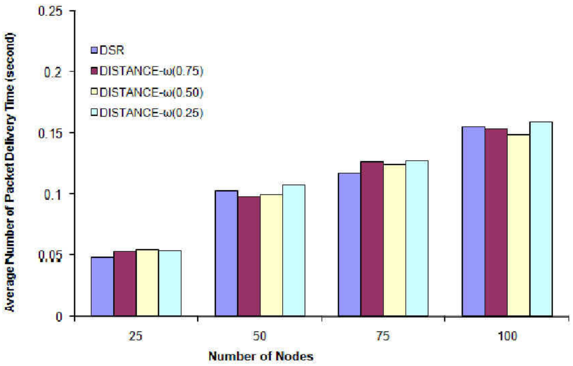

Fig. 12: APDT vs number of nodes

Another parameter captured during the experiment which gives different impact into the performance is ω. The ω value plays an important role in DISTANCE. By setting ω value close to 0, it makes the algorithm works more often and improves the performance of DSR more significantly, but the consequences are that the packet delay and routing overhead will be higher (even though in some situation based on simulation has shown result that are still lower than what legacy DSR route maintenance algorithm did). Setting ω value so close to 1 is also not recommended, since it will make the DISTANCE algorithm works less often. From simulation result, it is recommended that the value for ω is set between 0.5-0.75.

Referring to the result from Fig. 11, 12 and 13 it is clear that when the number of nodes is low (sparse topology), the performance of DSR is poor (low packet sent/received ratio, high packet losses) because there are less number of connections due to sparse nature of topology. As the number of nodes increased the performance becomes more or less constant but if the density is too large, more and more nodes try to access

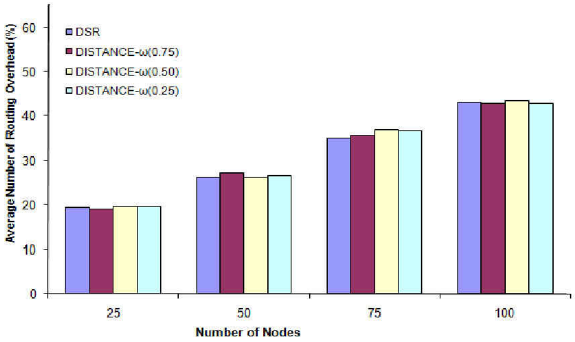

Fig. 13: ANRO vs number of nodes

the common medium, thus number of collisions increased thereby increasing the packet loss and decreasing the throughput as well. Node density also gives impact into the DISTANCE algorithm. Less dense means the probability of bridge nodes to be found is low, on the other hand the more dense the nodes are, the higher the probability will be but, since the DISTANCE algorithm only focuses on route maintenance; it also gives the same pattern with DSR if the node is getting higher density. From figures, it is also clear that the DISTANCE algorithm improved the performance of DSR in terms of APDR, APDT and ANRO.

CONCLUSION

DSR, which is an on-demand routing protocol, becomes the most popular source routing protocol for MANET. In case of link/route failure, the node, which detects link/route failure, will send RERR packet to source node. Although DSR can respond a route quickly, it yields a long delay when a route is rebuilt. This is because when source node receives RERR packet, it will try to find alternative routes from the route cache. If alternative routes are not available, source node, then, will enter route discovery phase to find new routes.

We proposed a new route maintenance strategy for DSR, called DISTANCE. From simulation results, we showed that the DISTANCE algorithm improves the functionality of DSR in terms of packet sending ratio and delay by preventing the links from failure.

The results conclude that in high node density environment the DISTANCE algorithm worked better since the probability of founding bridge node is higher. The issue that was captured during observation is that mobility gives more impact into the performance comparing with node density. As the mobility speed is increased, it is clear that the protocol performance deteriorate quite much, comparing to if the number of node is increased. Justification for this issue is that the WLAN (IEEE 802.11 standard) is not designed for high speed mobility, since the coverage area for wireless transmission is commonly a few hundred meters only. Wireless broadband such as WiMAX (IEEE 802.16 standard) might be more suitable for high mobility.

REFERENCES

1. Barr, R. SWANS – Scalable Wireless Network Simulator User Guide. 2004. http://jist.ece.cornell.edu/docs/040319-swans-user.pdf
2. Al-Shurman, M., Y. Seong-Moo and P. Seungjin, 2004. A performance simulation for route maintenance in wireless ad hoc. In ACM-SE 42: Proceedings of the 42nd Annual Southeast Regional Conference, pp: 25-30, ACM Press. 2004 doi: 10.1145/986537.986545
3. Liu, W., C. Chiang, H. Wu and M. Gerla, 1997. Routing in clustered multihop, mobile wireless networks. In IEEE SICON'97, pp: 197-211, April 1997. http://www.cs.ucla.edu/NRL/wireless/PAPER/Chiang_sicon97.ps.gz
4. Corson, S. and J. Macker, 1999. Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations, IETF RFC 2501. http://www.ietf.org/rfc/rfc2501.txt.
5. David, B.J., A.M. David and Hu Yih-Chun, 2004. The Dynamic Source Routing (DSR) Protocol for Mobile Ad Hoc Networks. IETF RFC 4728. http://www.ietf.org/internet-drafts/draft-etf-manet-dsr-10.txt, July 2004.
6. David, B.J. and A.M. David, 1996. Dynamic source routing in Ad hoc wireless networks. Mobile Comput., vol: 353. doi:10.1007/978-0-585-29603-6_5
7. Murthy, S. and J.J. Garcia-Luna-Aceves, 1996. An efficient routing protocol for wireless networks. Mobile Networks Applic., 1: 183-197. doi: 10.1007/BF01193336
8. Seungjin Park and B.V. Voorst, Anticipated route maintenance (arm) in location-aided mobile ad hoc networks. In Global Telecommunications Conference, 2001. Nov. 25-29, pp: 2809-2813, doi: 10.1109/GLOCOM.2001.965942
9. Charles E. Perkins and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, Feb. 25-26, pp: 90-100. doi:10.1145/313451.313538

10. Charles E. Perkins and Pravin Bhagwat, 1994. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In SIGCOMM '94: Proceedings of the Conference on Communications Architectures, Protocols and Applications, Aug. 31-Sep. 2, pp: 234-244, ACM Press. doi:10.1145/190314.190336
11. Ying-Hong Wang and Chih-Feng Chao, 2006. Dynamic backup routes routing protocol for mobile ad hoc networks. Inform. Sci., 176: 161-185. doi:10.1016/j.ins.2004.09.016
12. Zhang, B. and H.T. Mouftah, 2004. Position-aided on demand routing protocol for wireless adhoc networks. In Communications, IEEE International Conference on, June 20-24 pp: 3764-3768. doi: 10.1109/ICC.2004.1313245