Direction-Aware Routing Protocol for Mobile Ad Hoc Networks+

Wei-Her Chung, Sy-Yen Kuo, and Shih-I Chen***

Department of Electrical Engineering

National Taiwan University

Taipei, Taiwan

Abstract-Due to the development of wireless technology, people can now communicate while moving around. Wireless communication realizes people's dream to get rid of the constraint of wires. More and more applications based on wireless technology are designed and commercialized. Recently a type of mobile wireless network called " Mobile Ad Hoc Network" has attracted more and more attention. A mobile ad hoc network is a totally wire free network without any connection through access points to Internet. There is no centralized controlling center or infrastructure in a mobile ad hoc network. In such a network, mobile nodes are allowed to move around anywhere within a range and the topology which consists of mobile nodes changes frequently. The operation difficulty of a mobile ad hoc network is how a packet is to be routed. In this paper we propose a new and effective routing protocol named as "direction-aware routing protocol" for mobile ad hoc networks. Details of direction-aware routing algorithm will be described and we also present our simulation methodology and simulation results to show the performance advantage of our routing performance.

Keywords: Ad hoc, Direction-aware, routing, Mobile networks, Wireless, protocols

1 Introduction

An ad hoc network consists of mobile nodes without infrastructure and centralized controlling center. Mobile nodes can be laptop computers, notebooks, PDAs, and other devices. Each mobile node is supposed to be installed an antenna. Packets are transmitted through radio channel by the antenna between mobile nodes without the help of a transmission line. Besides, nodes are allowed to move around anywhere within an area of blurry size at any time. The border of the area within which mobile nodes are allowed to move around is blurry but around a certain range. Ad hoc networks are useful and can be easily applied in different scenarios. For example, in a conference venue, attendants may change their seats or walk around in the venue but they don't go outside the venue. The venue area is the so-called blurry area above. Each of the attendants takes a notebook or PDA and run the system in ad hoc mode. The attendants can communicate to one another by ad hoc network without any wire or infrastructure deployment. The communication among the attendants includes audio, video, electronic file etc. To take another example as in the military mission, a group of people are sent to a dicky place to perform the action. It's difficult to construct the communication infrastructure and the troops must move to different places all the time. Soldiers can use ad hoc network to talk to one another conveniently.

*Corresponding author, Email: sykuo@cc.ee.ntu.edu.tw

**Shih-I Chen is with Institute for Information Industry, Taiwan.

+Supported in part by the Development of Communication Software Core Technology project of Institute for Information Industry and sponsored by MOEA, Taiwan, R.O.C.

Recently, short-range wireless technology, such as IEEE802.11[6], is growing mature and coming to be commercialized. In the IEEE802.11 specification, it defines the physical and MAC layer of a short-range wireless communication standard. The radio transmission range in IEEE802.11 is about 200 to 300 meters. That means mobile nodes must be within that range to communicate to one another. The node which is outside the range loses the connectivity with other nodes. Routing algorithms in ad hoc networks can extend the geographical communication range without any change of the original physical and MAC layer. Our direction-aware routing algorithm is located at layer 3 in the communication protocol stack. The physical and MAC layers which are below our routing protocol can be IEEE802.11 or other wireless access specification.

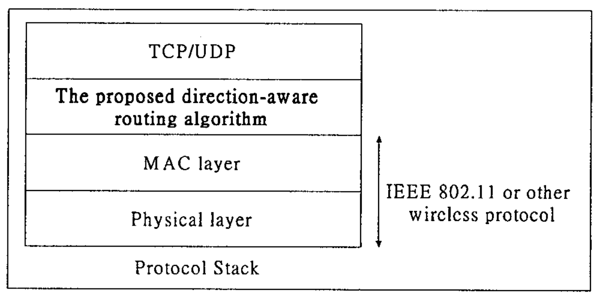

Fig.1. The proposed direction-aware routing algorithm in the protocol stack.

2 The Direction-Aware Routing Protocol

2.1 Overview of direction-aware routing protocol

There have been several ad hoc network routing algorithms proposed in the past few years, such as Dynamic Source Routing(DSR)[1], Ad-hoc On-Demand Distance Vector algorithm(AODV)[4], Destination-Sequenced Distance-Vector Routing (DSDV)[7], etc. In a mobile ad hoc network which is a highly distributed system, each mobile node has quite limited information about other nodes and the whole network. When an ad hoc network

0-7803-7547-5/02/$17.00 ©2002 IEEE

initially starts to operate, each mobile node even knows nothing of the network. Several mechanisms were designed for a mobile node to discover and maintain enough information to route packets in the algorithms proposed in the past few years. These mechanisms include broadcasting route discovery, periodic broadcasting, routing table maintenance, TTL(time to live) to expire route entry etc. When an ad hoc network starts to operate or a new node just joins a pre-existing ad hoc network, there exist nodes that have no information about the network and other nodes. The nodes that do not have enough information to route packets must broadcast route discovery packets. And the nodes which receive a broadcast packet either process the packet and re-broadcast it or reply to the packet. The mechanism which uses broadcast to discover routing information is called flooding. Flooding was often used to discover a useful path in ad hoc networks in the papers of the past few years. Obviously flooding would consume large amount of bandwidth.

2.2 Operation of Direction-Aware Routing Protocol

A mobile node in a mobile ad hoc network is called MN(Mobile Node). The number of nodes in an ad hoc network can be from 10 to 10000. Multiple simultaneous connections are allowed in an ad hoc network. Each node has its own unique ID in an ad hoc network. The node from which packets are originated is called the source node. The node to which packets are destined is called the destination node. A node may play the roles of source nodes and destination nodes simultaneously in different node-to-node connection. A path is a list of nodes' IDs by which packets can be routed from the source node to the destination node. The list is usually a series of concatenated IDs. When a source node needs to transfer packets to a certain destination node, the source node issues a path discovery packet. The packet is issued through MAC layer broadcast. All of the nodes in the issuer's radio transmission range can receive the packet. The path discovery packet contains the following fields:

Source Node ID

Destination Node ID

Sequence Number

Hop Count

Stale Route List

The Source Node ID is the ID of the node which needs to discover the path and issues the path discover packet. The destination Node ID means the ID of the destination node to which the source node wants to transfer packets. Each node must have its own counter and must record its own Sequence Number. Each time a node issues a path discovery packet it increments its own counter and sets the number of the counter as the Sequence Number of the path discovery packet. Number space of the counter must be large enough such that the same number wouldn't appear more than once in the same node during the operation period of the ad hoc network. That means different path discovery packets issued from the same node definitely have different Sequence Number. Each node maintains a table named History Table to record lately received packets. Every time, a path discovery packet is received by a mobile node, the mobile node records the pair (Source Node ID, Sequence Number) as an entry in its own History Table and sets up an expiration time for the entry. When the expiration time is up, the timeout entry in the History Table is silently dropped. The expiration time setup can prevent the History Table from growing too large and help the mobile nodes to save memory space. By checking the pair (Source Node ID, Sequence Number) in the History Table, all the nodes can judge if a path discovery packet has been received and processed previously. If the path discovery packet has been received and processed by a certain node, the node knows this truth by (Source Node ID, Sequence Number) pair and drops that path discovery packet silently. Thus the problem of looping is avoided.

When an intermediate node MNk receives a path discovery packet and the packet is not a repeated packet, this node attaches its ID MNk at the end of the packet, processes the Hop Count of the packet, and then uses MAC layer broadcast to send that packet out. Before the packet is sent out by the intermediate node, the intermediate node checks if its ID is in the packet's Stale Route List. If the intermediate node's own ID is in the Stale Route List, the intermediate node sets the Hop Count to a pre-defined " Life Depth ". If the intermediate node's ID isn't in the Stale Route List of the packet, the intermediate node decrements the Hop Count of the packet and sends the packet out by MAC layer broadcast.

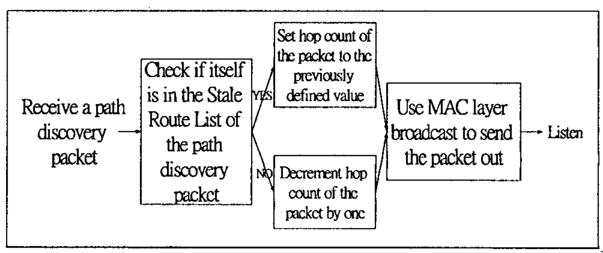

Fig.2. Intermediate node state diagram in forwarding path discovery packets.

The pre-defined "Life Depth" mechanism plays an important role in our direction-aware routing protocol. The Stale Route List also means a lot in discovering a newly useful path. When two mobile nodes are communicating to each other, the path is composed of intermediate mobile nodes. The intermediate nodes play the role of routers. The intermediate nodes forward packets for the source node and the destination node. When one or several of the intermediate nodes on the path move out of radio transmission range to its neighbor nodes on the path, the path is broken. Upon or not far from the time at which the path is broken, the nodes on the originally active path are still around the area between the source node and the destination node. That is to say, maybe a certain direct node-to-node connection of the original active path fails. But the nodes on the original active path have not gone very far. There are high probability that one or more useful paths from the source node to the destination node exist close to the nodes of the original active path. The Hop Count field of a packet can be viewed as the "life" of that packet. When the Hop Count of the packet is decremented to zero, the packet is dropped by the mobile node which processes the packet. That means the packet "died". Based on the intuition that it's quite possible that there exist useful paths close to the nodes of the original active path, the path discovery packet's life must be strengthened by setting the packet's Hop Count field to a pre-defined "Life Depth " when the path discovery packet meets the nodes on the original active path. Path discovery packets of other directions which are not pointing to destination node will gradually be dropped and unnecessary bandwidth consumption can be avoided.

When the destination node receives the path discovery packet, the destination node checks the Destination Node ID field of the packet and knows it itself is the destination node to be searched. The destination node removes the header of the packet and gets the tail part of the packet. The tail part of the packet is an ID list which consists of the nodes who are on the new path from the source node to the destination node. That ID list is the path found. The destination node uses routing layer unicast to reply a path reply packet to the source node along the path gotten from the path discovery packet.

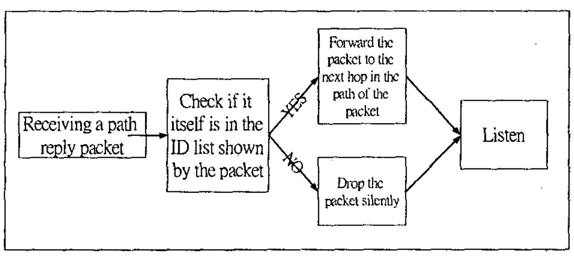

Fig.3. Intermediate node state diagram in forwarding path reply packets.

Now an example is used to demonstrate the Direction-Aware Routing Protocol(DARP) in details. The following Fig.4(a)(b)(c)(d)(e)(f) are time sequences of the path recovery processes. These graphs illustrate the condition of link breakage, DARP path discovery, and path reply in the order of the time. In this example, pre-defined Life Depth is 2. Each node has its own ID as in the graphs. Node A plays the role of the source node and node D plays the role of the destination node. The path discovery packet is abbreviated as PDP and the path reply packet is abbreviated as PRP. The path is described in words by a series of ID's concatenation.

In Fig.4(a), the temporary active path is A-B-C-E-D.

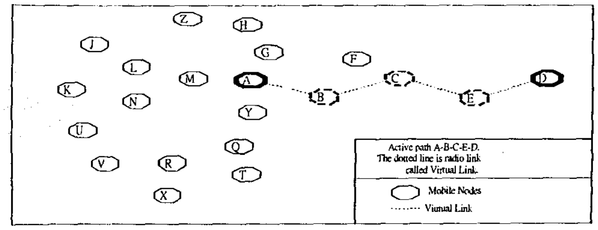

Fig.4(a). Active path A-B-C-E-D.

In Fig.4(b), Node B moves and A-B link is broken. Of course, the other nodes are moving too, but Node B should be especially noticed. Node B causes the breakage of the active path.

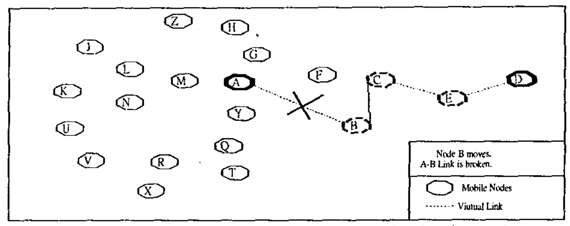

Fig.4(b). The active path A-B-C-E-D is broken due to the movement of Node B.

In Fig.4(c), Node A notices the link is broken and broadcasts a PDP with Hop Count = 2 (pre-defined Life Depth). The PDP's Stale Route List is set as the previously active path A-B-C-E-D and the PDP is concatenated with Node A's ID to be PDP-A. All the neighbor nodes(Node F, G, M, Y) within Node A's radio transmission range will receive PDP-A.

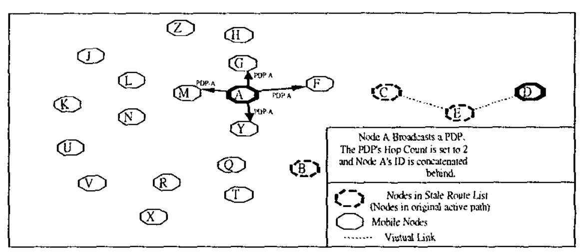

Fig.4(c). Node A broadcasts direction-aware path discovery packets.

In Fig.4(d), Node F, G, M, Y decrement the PDP's Hop Count by one respectively, concatenate their own ID to their individual PDP and broadcast the PDPs. At this step, Node H, L, N, Q, C receive the PDP.

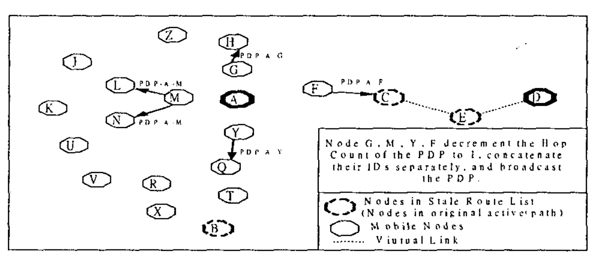

Fig.4(d). The intermediate nodes(Node F, H, M, Y) keep forwarding the packets after decrementing the PDP's Hop Count.

In Fig.4(e), Node H, L, N, Q decrement the PDP's Hop Count by one and find that the Hop Count of the PDP is zero. So according to the protocol, Node H, L, N, Q should drop the PDPs silently. At the same time, Node C finds itself in the Stale Route List of the PDP and should let the Hop Count of the PDP be 2(pre-defined Life Depth) according to the DARP. So Node C sets the Hop Count to 2 and broadcasts the PDP. Node E receives the PDP. After that, Node E also sets the Hop Count to 2 and broadcasts the PDP. Finally node D receives the PDP.

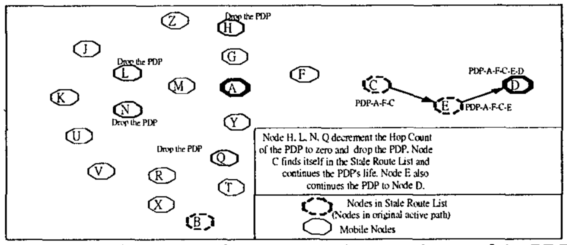

Fig.4(e). Node H, L, N, Q decrement the Hop Count of the PDP to zero and drop the PDPs silently. Node C and E are in the Stale Route List and set the Hop Count of the PDP to 2. Node C and Node E keep forwarding the PDP. Finally the PDP reaches the destination Node D.

In Fig.4(f), Node D checks the tail concatenation of the PDP and gets the path A-F-C-E-D. Node D reverses the derived path to D-E-C-F-A and sends a PRP concatenated with A-F-C-E-D back to Node A along the path D-E-C-F-A. Node A knows the new useful path A-F-C-E-D and then starts to communicate with Node D.

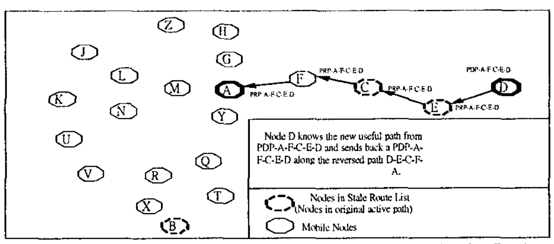

Fig.4(f) Node D uses routing layer unicast to reply the Path Reply Packet(PRP). The PRP is forwarded to Node A by the aid of the intermediate nodes(Node E, C, F).

In this example of Fig.4(a)(b)(c)(d)(e)(f), we can see the DARP's intuition that the PDPs with setting of pre-defined Life Depth would die away soon without the aid of the nodes in the Stale Route List. Because of this, the PDPs will not spread out to the whole network. For example in these graphs, Node Z, J, K, U, V, R, X, T(the periphery nodes) are not affected by any packets. And in fact these periphery nodes are not helpful at the routing process from Node A to Node D so they shouldn't be affected at best. With the aid of the previously active nodes(in Stale Route List), only the nodes located at the area between Node A and Node D would be asked to forward the PDPs and PRPs. Through DARP mechanism the PDPs and PRPs are confined locally. This example demonstrates a condition with only 21 nodes and a single link. If we consider a larger network with much more nodes and much more links, the benefit of DARP would be more obvious. Thus DARP will have better scalability.

The source node has to set up a timer when the path discovery packet is sent out. If the timer is timed out and the source node hasn't received the corresponding path reply packet, this path discovery process is considered failed. If the value of Life Depth is well evaluated and properly set up, the useful path can usually be found. If the failure happens, the source node uses flooding instead to search for the useful path.

3 Simulation results

In the simulation environment, we set up (1). 50 mobile nodes in a square of 1000(meters)X1000(meters) and (2). 100 mobile nodes in a square of 1500(meters)X1500(meters). Each mobile node has the radio transmission range of 250 meters. We choose 250 meters because it's assumed to be 200 to 300 meters in the IEEE802.11 specification. One round of simulation is set up as: (1) All mobile nodes have the same speed in the same round. Different rounds can have different speed. The speeds are respectively 10, 20, and 30 m/s. (2) All nodes are moving straight along their directions. Different nodes have different directions. Initially each node's direction is uniformly randomized from 0 to 360 degree. Every 3 seconds each node changes its direction randomly from 0 to 360 degree. When one node bumps into the border of the 1000X1000 square, the node will be reflected back and continue moving. (3) Each round is simulated for 2.5 hours (9000 seconds). (4) We randomly select two nodes, one as the source node and the other one as the destination node. We keep the single connection between the source node and the destination node from the beginning to the end of the round(9000 seconds).

We use "Average number of path finding messages per node per second" as the performance metric. Routing protocols use packets such as path discovery packets and path reply packets to accomplish the job of finding the path. The more the path finding messages, the more bandwidth is consumed and normal payload messages will have less throughput. "Average number of path finding messages per node per second" means how many times one node is bothered by the path finding messages per second. The speeds of simulation 30 m/s, 20m/s, 10 m/s are analogous to different vehicular speeds. And in our simulation the nodes are non-stop moving for 9000 seconds. In real world, the nodes' moving patterns wouldn't be so severe and the overhead would be lower. Of course when the nodes represent devices carried by human beings, the overhead would be even lower.

We collect all of the path finding messages in the round and compute its average shown below.

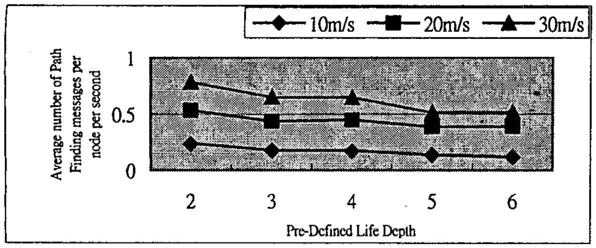

Fig.5. Average number of path finding messages per node per second vs. Pre-defined life depth (The speeds are respectively 10, 20, 30 m/s). 50 nodes in 1000(m)X1000(m) square.

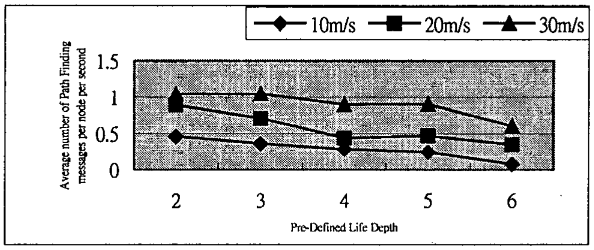

Fig.6. Average number of path finding messages per node per second vs. Pre-defined life depth (The speeds are respectively 10, 20, 30 m/s). 100 nodes in 1500(m)X1500(m) square.

In the following simulation environment, all of the conditions are the same as in the first simulation environment. We select the case of pre-defined "Life Depth" which is set to 3 in the Direction-Aware Routing Protocol to compare to Dynamic Source Routing(DSR). The results are shown as in the following graph.

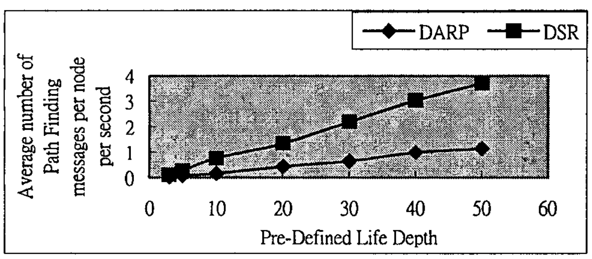

Fig.7. Comparison of DSR and DARP (The speeds are respectively 3, 5, 10, 20, 30, 40, 50 m/s). 50 nodes in 1000(m)X1000(m) square.

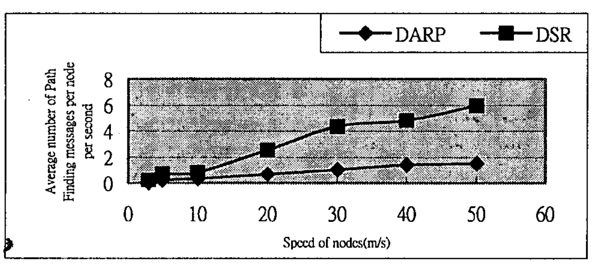

Fig.8. Comparison of DSR and DARP (The speeds are respectively 3, 5, 10, 20, 30, 40, 50 m/s). 100 nodes in 1500(m)X1500(m) square.

4 Conclusions

In this paper the direction-aware ad hoc network routing protocol is proposed. Much effort is put on the design of path discovery mechanism. An ad hoc network is a highly dynamic network and thus the probability of path failure is high. Nodes need to discover a new path very frequently. An efficient path discovery mechanism will be very helpful for ad hoc routing.

Because of the "Life Depth" mechanism designed, direction-aware routing protocol is aware of the direction of routing. Its path discovery packets can be directed from the source to the destination node. It's not like the flooding method which floods the whole network with one node's path discovery packets. Therefore, the direction-aware routing protocol is more efficient. And the simulation results show that the proposed direction-aware routing protocol has low overhead. When compared to Dynamic Source Routing, direction-aware routing protocol also has lower overhead. Because its path discovery is directional, direction-aware routing protocol is especially well suitable to large networks. We will continue to modify and improve its performance. We will also try to evaluate the performance of the direction-aware routing protocol in a much larger (50 to 500 nodes) network.

References

[1] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Eds.,Kluwer,1996, pp. 153-81.

[2] Broch, D. B. Johnson and D. A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," IETF Internet draft, draft-ietf-mannet-dsr-01.txt, Dec.1998.

[3] Elizabeth M.Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, April 1999.

[4] C. E. Perkins and E. M. Royer, "Ad Hoc On Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, IETF,Aug 1998.

[5] J. Broch, D. A. Maltz, D.B. Johnson, Y. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," in ACM/IEEE *Int. Conf. On Mobile Computing and Networking*, Oct1997, pp. 85-97.

[6] Brian P. Crow, Indra Widjaja, Jeong Geun Kim, Prescott T. Sakai, "IEEE 802.11 Wireless Local Area Networks," in IEEE Communications Magazine, September 1997.

[7] C.E. Perkins, P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," Proceedings of ACM SIGCOMM'94, London, UK (Aug-Sept 1994), 234-244.