Asian Journal of Information Technology 6 (11): 1117-1124, 2007
ISSN: 1682-3915

Path Selection Based Route Finding Protocol in Mobile Ad Hoc Network

Nusrat Nowsheen and Mosaddek Hossain Kamal
Department of Computer Science and Engineering, University of Dhaka, Dhaka-1000, Bangladesh

Abstract: Mobile Ad Hoc Network (MANET) is an autonomous system of functionally equivalent mobile nodes, which must be able to communicate while moving, without any kind of wired infrastructure. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. To this end, mobile nodes must cooperate to provide the routing service. Routing in mobile environment is challenging due to the constraints existing on the resources (transmission bandwidth CPU time and battery power) and the required ability of the protocol to effectively track topological changes. Limited bandwidth and a high degree of mobility require that routing protocols for ad hoc networks be robust, simple and energy conserving. Efficient, dynamic routing is also one of the key challenges in this network. In recent past, this problem has been addressed by several research efforts, resulting in a large body of literature. Each node participating in the network acts both as host and a router and must therefore be willing to forward packets for other nodes. For this purpose, a number of routing protocols like Dynamic Source Routing (DSR) Protocol, Ad Hoc On-Demand Distance Vector (AODV) Routing, Destination Sequenced Distance Vector (DSDV) and Temporally Ordered Routing Algorithm (TORA) have been implemented. This study presents a new on demand protocol for routing in ad hoc networks that selects a route of smallest hop count and consisting of nodes in a non-existing path. Our protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. The path selection method used in this protocol always prefers to a route with more non-forwarding nodes and provides the solution to cope with network mobility by selecting route efficiently. Our route finding protocol provides loop free routes even while able to repair broken links. Because the protocol does not require global periodic routing advertisements the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that require such advertisements. Nevertheless, we can still maintain most of the advantages of basic Distance vector routing mechanisms. Our algorithm scales to large populations of mobile nodes wishing to form ad-hoc networks. We also point out future research issues in the context of individual routing approaches as well as from the overall system perspective.

Key words: Ad-hoc networking, broadcasting, distance vector routing, link state routing, Mobile Ad-hoc Network (MANET)

INTRODUCTION

Developing support for routing is one of the most significant challenges in ad hoc networks and is critical for the basic network operations. Certain unique combinations of characteristics make routing in ad hoc networks interesting. First, nodes in an ad hoc network are allowed to move in an uncontrolled manner. Such node mobility results in a highly dynamic network with rapid topological changes causing frequent route failures. A good routing protocol for this network environment has to dynamically adapt to the changing network topology (Royer and Toh, 1996; Tanebaum, 1996). Second, the underlying wireless channel provides much lower and more variable bandwidth than wired networks. The wireless channel working as a shared medium makes available bandwidth per node even lower. So routing protocols should be bandwidth-efficient by expending a minimal overhead for computing routes so that much of the remaining bandwidth is available for the actual data communication. Third, nodes run on batteries which have limited energy supply. In order for nodes to stay and

Corresponding Author: Nusrat Nowsheen, Department of Computer Science and Engineering, University of Dhaka, Dhaka-1000, Bangladesh

communicate for longer periods, it is desirable that a routing protocol be energy-efficient as well. This also provides another reason why overheads must be kept low (http://www.cis.ohio-state.edu/-jain/cis788-9/adhoc_ routing/indexhtml, Lee and Kim, 2000). Thus, routing protocols must meet the conflicting goals of dynamic adaptation and low overhead to deliver good overall performance. Therefore, routing protocols, for network without infrastructures, have to be developed. These protocols determine how messages can be forwarded, from a source node to a destination node which is out of the range of the former, using other mobile nodes of the network.

Routing protocols developed for wired networks are inadequate here as they not only assume mostly fixed topology but also have high overheads. These Protocols generally use either distance vector or link state routing algorithms, both of which require periodic routing advertisement to be broadcast by each router. In distance vector routing (Hedrick, 1988; John *et al*., 1977; Gursharan *et al*., 1990; Paul, 1990; Xeros Corporation, 1981) each router broadcasts to each of its neighbor routers the distance to all hosts and each router computes the shortest path to each host based on the information advertised by each of its neighbors. In link state routing (ISO, 1990; John *et al*., 1980; Moy, 1991) each router instead broadcasts to all other routers in the network its view of the status of each of its adjacent network links and each router then computes the shortest distance to each host based on the complete picture of the network formed from the most recent link information from all routers. In addition to its use in wired networks, the basic distance vector algorithm has also been adapted for routing in wireless ad hoc networks, essentially treating each mobile host as a router (John and Janet, 1987; Charles and Pravin, 1994; Nachum and Jil, 1987). This has lead to several routing proposals specifically targeted for ad hoc networks. While some of these proposals are optimized variants of protocols originally designed for wired networks, the rest adopt new paradigms such as on-demand routing, where routes are maintained reactively only when needed e.g., AODV (Perkins, 2000; Perkins *et al*., 2000), DSR (Johnson *et al*., 2001; Johnson and Maltz, 1996) etc. This is in contrast with the traditional, proactive Internet-based protocols. Other new paradigms also have emerged-for example, exploiting location information from routing and energy-efficient routing, etc.

This study describes the design of a routing protocol for ad-hoc network that instead selects a route which looks more efficient at the moment of communication. It provides solution to cope with the dynamic nature of mobile nodes. When a host needs a route to another host it dynamically determines one based on cached information and on the results of route discovery protocol. The protocol described here always prefers a route of smallest hop count and more non-forwarding nodes. Forwarding nodes are those are busy in transferring packets to other nodes. So, it is preferable to select a route with few number of forwarding nodes and smallest hop count. The proposed dynamic routing protocol offers a number of potential advantages over conventional routing protocols such as distance vector in an ad hoc network. First, unlike conventional routing protocols, the proposed protocol uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead, particularly during periods when little or no significant host movement is taking place. Distance vector and link state routing, on the other hand, must continue to send advertisements even when nothing changes, so that other mobile hosts will continue to consider those routes or network links as valid. In addition, many of the links between routers seen by the routing algorithm may be redundant (John and Janet, 1987). Wired networks are usually explicitly configured to have only one (or a small number) of routers connecting any two networks, but there are no explicit links in an ad hoc network and all communication is by broadcast transmissions. The redundant paths in a wireless environment unnecessarily increase the size of routing updates that must be sent over the network and increase the CPU overhead required to process each update and to compute new routes.

The Destination Sequenced Distance Vector (DSDV) (Perkins and Bhahwat, 1994; Charles and Pravin, 1994) algorithm has been proposed as a variant of the distance vector routing method by which mobile nodes cooperate to form an ad-hoc network. DSDV is effective for creating ad-hoc networks for small populations of mobile nodes. But it is a fairly brute force approach because it depends for its correct operation on the periodic advertisement and global dissemination of connectivity information. DSDV also requires each mobile node to maintain a complete list of routes one for each destination within the ad-hoc network. Keeping a complete routing table does reduce route acquisition latency before transmission of the first packet to a destination. It is however, possible to design a system whereby routes are created on-demand e.g. (Johnson and Maltz, 1996). Such systems must take steps to limit the time used for route acquisition otherwise users of the ad-hoc nodes might experience unacceptably long waits before transmitting urgent information. The advantage here is that a smoothly functioning ad-hoc system with on-demand routes could largely eliminate the need for periodic broadcast of route advertisements. With the goals of minimizing broadcasts and transmission latency when new routes are needed, we designed a protocol to improve upon the performance characteristics of DSDV in the creation and maintenance of ad-hoc networks. Although AODV, an on-demand protocol recovers the problems of periodic broadcast and complete routing table management (Perkins and Royer, 1999). In AODV (Perkins, 2000; Perkins *et al.*, 2000; Charles, 1998) when a route discovery is requested the node which is able to reply to this request always reply to the first request. It receives and replies to the request without considering any efficiency of this route. Route repair is done locally by the node that encounters the link failure. In our path selection protocol during route discovery the reply is made based on the route that looks best at that moment in terms of route efficiency and robustness. All the nodes in half of the way from destination take part in repairing the route locally.

PATH SELECTION BASED ROUTE FINDING PROTOCOL

Our basic proposal can be called a pure on-demand route finding system because nodes that do not lie on active path neither maintain any routing information not participate in any periodic routing table exchanges. When a node wants to communicate with any other node it does a route discovery to form a route to the destination. Each mobile node becomes aware of other neighbor nodes on the way of its route to maintain the communication active. The routing tables of the nodes are maintained to optimize response time to local movements and provide quick response time for requests for establishment of new route. The dields of an entry of routing table is shown in Table 1.

Path discovery: The path discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its routing table. Every node maintains two separate information:

- Source node sequence number
- Request broadcast id

Generating rout reguest: The source node initiates path discovery by broadcasting a Route Request (RR) packet to its neighbors. The range of dissemination of such RR is indicated by the TTL in the IP header. The information contained in RR packet is shown in Table 2.

Table 1: The dields of an entry of routing table

Destination IP Address
Destination Sequence Number
Valid Destination Sequence Number Flag
Other State and Routing Flags (e.g., valid, invalid, repairable),
Hop Count (number of hops needed to reach destination)
Next Hop
List of Precursors
Lifetime (expiration or deletion time of the route)

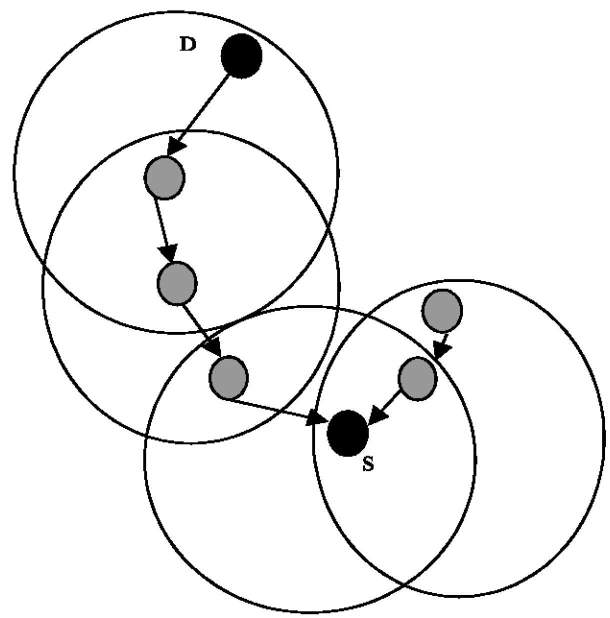

Fig. 1: Reverse path

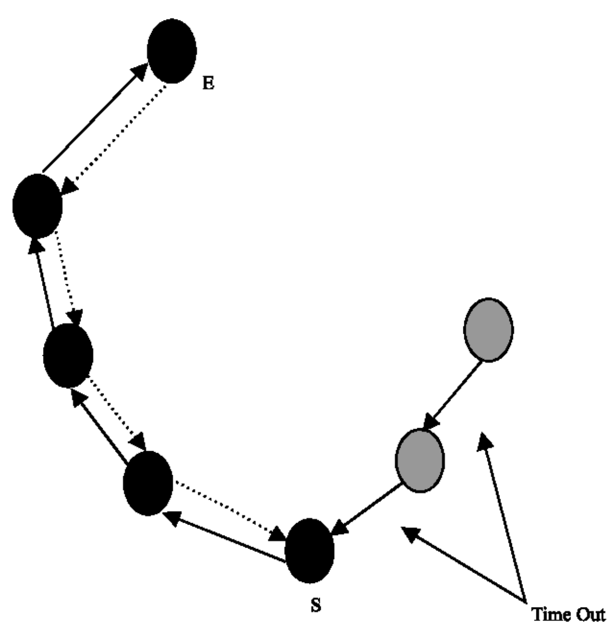

Fig. 2: Forward path

Table 2: The information contained in RR packet

Message fields	Description
Type	Type of message
Source(originator) address	The IP address of the originator of route discovery
Source Sequence Number	Current sequence number to be used in the route entry pointing towards the originator
Request Broadcast Id	A sequence number uniquely identifies a request from a particular source
Destination sequence number	Latest sequence number originator has for the destination
Hop Count	Number of hops from source to the node handling route request
Forward Count (FC)	Node receiving route request increments this count if it exists in any route
Non-Forwarding Count (NC)	Node receiving route request increments this count if it doesn't exist in any route
Destination Route	Inform the intermediate node to notify the destination about reverse route
US	Unknown sequence number

The pair <source address, request broadcast id> uniquely identifies a RR. Request Broadcast Id is incremented whenever the source issues a new RR. Each neighbor either satisfies the RR by sending a route reply RP back to the source from its routing table or re-broadcasts the RR to its own neighbors after increasing the hop count. A node may receive multiple copies of the same route broadcast packet from various neighbors. When an intermediate node receives a RR and is not able to reply from its route cache and if it has already received a RR with the same request broadcast id and source address; it drops the redundant RR and does not rebroadcast it. Otherwise, it broadcasts the RR. Destination sequence number is used to indicate how fresh a route to the destination must be before it can be accepted by the source. As the RR travels from source to destinations, it automatically sets up the reverse path from all nodes back to source as illustrated in Fig. 1. Route Reply (RP). If an originator node expects a bidirectional communication with the destination node, any generation of RP by intermediate node for delivery of a route to the source node also notifies the destination about a route back to the source node. A special flag (DR) in Route Request (RR) packet is set and the intermediate node sends a Route reply (RP) to the destination. A node should not originate RR messages more than a certain limit. After sending a RR the source waits for a reply from the destination of the message or any intermediate node that has a route in its route cache to reply such request. If a route is not discovered within a certain time the node may try to discover the route by broadcasting another RR up to a maximum limit. Each new attempt must increment the Request Broadcast Id. Figure 2 represents the forward path setup as the RP travels from destination to source.

Processing and forwarding route request: When a node receives a route request packet, it first creates a reverse route to the previous hop. It then checks whether it has a route to the destination in its route cache. If the node has a route for the destination in its route cache, it then checks to determine whether it has already received a RR with the same <Source address and Request Broadcast Id>. If received then the node compares last two requests to select a best path from source to this node. If not received then it delays slightly before replying from its cache. It waits for another request to select a best route. If the node does not have any valid route to the destination; it then checks to determine whether it has received RR with the same <Source address and Request Broadcast Id>. If such a request has been received, the node silently discards the newly received request. In this case the node does not make any delay. Each time a node receives a new request, it first increments the hop count value in the request by one and then the node searches for a route to the source. If no route is found then the node creates a route using the source sequence number from the RR packet. The reverse route is needed if the node receives a Route Reply back to source.

The information contained in RR packet

Packet field	Description
Destination IP address	IP address of the destination for which a route is supplied
Destination Sequence Number	Destination sequence number associated to the route
Source IP address	The IP address of the node originated the RR.
Hop Count	Number of hops from source to destination
Lifetime	Time for which nodes receiving route reply consider the route to be valid

Generating route reply: A node generates a Route Reply if it is a destination, or it has an active route to the destination and the destination sequence number in the route table entry is greater than or equal to the destination sequence number of the RR packet. The information contained in RR packet is shown in Table 3.

When a node (intermediate or destination) receives a non-duplicate route request packet and is ready to generate a Route Reply (RP) the node does not reply the request immediately. It waits for a delay period:

d = $H * (h-1+r)$; Where,
r = Random Number between 0 and 1
H = mall constant introduced per hop

to receive another request with <Same Broadcast Id and Source IP Address>. A receiver receives many route discovery packets. When a receiver receives a non-Table 3.

duplicate route discovery packet, it stores the information of the packet header into request cache and delays sending reply for a short time. It computes the weighted path length (hc + (1-a) * NC + a * FC);

Where,
hc = Hop Count of request packet,
FC = No of forwarding nodes,
NC = No of non-forwarding nodes and $0.5 < a <= 1$ is the relative weight.

If it receives another request by this delay time then the node computes the weighted path length of the new one and compares it with the previous one. If the new path is better (shorter weight length) than the currently best path then the receiver replaces the request cache with the information of new path. It sends the reply packet using the information of best path stored in the request cache after pre-determined time elapsed since the non-duplicate route discovery reception (Fig. 3).

The node replies to the request selected as best path. When generating a Route Reply (RP), a node copies the Destination IP address and Source sequence number from the RR into the corresponding fields in RP packet. The Route Reply is forwarded back toward the node which originated the Route request message As the RP passes along the way from destination to source each node that receives this packet must set the forwarding flag in its route entry to one.

Route reply generation by destination: If the generating node is destination itself it sets the destination sequence number to the maximum of its current sequence number and the destination sequence number in the RR packet.

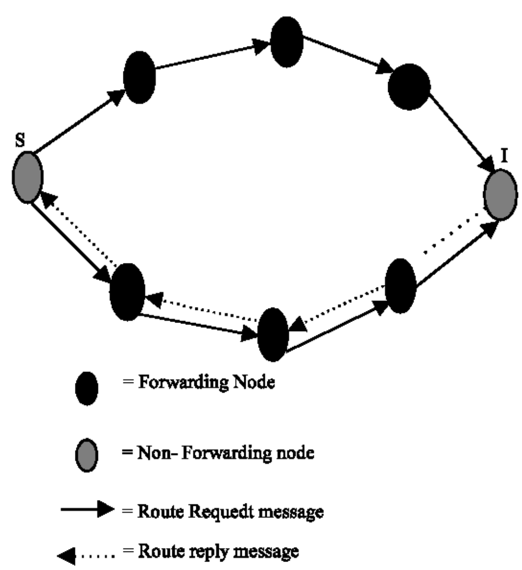

Fig. 3: Path with more non forwarding nodes

The destination node places its destination sequence number into the destination sequence number field of the Reply packet and it also sets the hop count field to zero. Destination node sets the lifetime field of RP.

Route reply generation by an intermediate node: If the node generating the RP is not the destination node, but instead is an intermediate hop along the path from the originator to the destination, it copies its known sequence number for the destination into the Destination Sequence Number field in the Reply message. The intermediate node updates the forward route entry by placing the last hop node (from which it received the RR) into the precursor list for the forward route entry -- i.e., the entry for the Destination IP Address. The intermediate node also updates its route table entry for the node originating the RR by placing the next hop towards the destination in the precursor list for the reverse route entry -- i.e., the entry for the Originator IP Address field of the RR. The intermediate node places its distance in hops from the destination (indicated by the hop count in the routing table) into the hop count field in the RP. The Lifetime field of the RREP is calculated by subtracting the current time from the expiration time in its route table entry.

Receiving and forwarding route replies: When a node receives a RP message, it searches for a route to the previous hop. If needed, a route is created for the previous hop, the node then increments the hop count value in the RP by one. Then the forward route for this destination is created if it does not already exist. Otherwise, the node compares the Destination Sequence Number in the message with its own stored destination sequence number for the Destination IP Address in the RP message. Upon comparison, the existing entry is updated only in the following circumstances:

- The sequence number in the routing table is marked as invalid in route table entry.
- The Destination Sequence Number in the RP is greater than the node's copy of the destination sequence no.
- The sequence numbers are the same and the new Hop Count is smaller than the hop count in route table entry.

If the route table entry to the destination is created or updated, then the route is marked as valid, the next hop in the route entry is assigned to be the node from which the RP is received, the hop count is set to the value of the new hop count, The expiry time is set to the current time plus the value of the Lifetime in the RP message and the destination sequence number is the Destination Sequence Number in the RP message. The current node can subsequently use this route to forward data packets to

Table 4: The information contained in RR packet

Packet fields	Description
Type	Type of message
N	No delete flag; set when a node has performed a local repair of a route upstream node should not delete the route
Destcount	The number of unreachable destinations included in the message; must be at least 1
Unreachable destination IP address	IP address of the destination that has become unreachable due to a link break
Unreachable destination sequence number	The sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field
Additional Unreachable destination IP address	IP address of the additional destination that has become unreachable due to a link break.
Additional Unreachable destination sequence number	The sequence number in the route table entry for the additional destination listed in the previous Unreachable Destination IP Address field

the destination. If the current node is not the node indicated by the Originator IP Address in the RP message and a forward route has been created or updated described above, the node consults its route table entry for the originating node to determine the next hop for the RP packet and then forwards the RP towards the originator using the information in that route table entry. When any node transmits a RP, the precursor list for the corresponding destination node is updated by adding to it the next hop node to which the RP is forwarded. Finally, the precursor list for the next hop towards the destination is updated to contain the next hop towards the source.

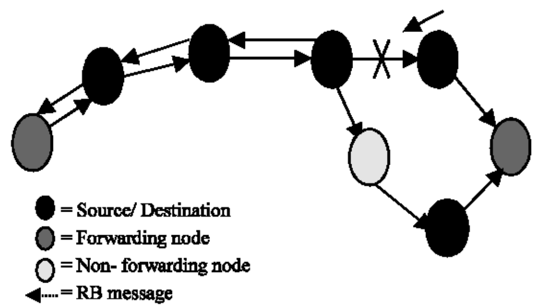

Fig. 4: Local repair of link failure

Path maintenance: Nodes that do not exist in an active route do not affect the routing if they move. If the source node moves during an active session it can reinitiate the route discovery procedure to establish a new route to the destination. If the destination or any other intermediate node moves a special message is sent to the affected source nodes.

Handling link failure: A node may offer connectivity information by broadcasting local connect messages. A node should only use connect messages if it is part of an active route. A node may determine connectivity by listening for packets from its set of neighbors. When a link failure occurs, a route break message is generated and sent to all the precursors. The information contained in RR packet is shown in Table 4.

A node initiates processing for a RB message in three situations: If it detects a link break for the next hop of an active route in its routing table while transmitting data (and route repair, if attempted, was unsuccessful, or) If it gets a data packet destined to a node for which it does not have an active route and is not repairing (if using local repair), or) If it receives a RB from a neighbor for one or more active routes. For case a, the node first makes a list of unreachable destinations consisting of the unreachable neighbor and any additional destinations in the local routing table that use the unreachable neighbor as the next hop. For case b, there is only one unreachable destination, which is the destination of the data packet that cannot be delivered. For case c, the list should consist of those destinations in the RB for which there exists a corresponding entry in the local routing table that has the transmitter of the received RB as the next hop.

Maintaining local connectivity (local repair): When a link break in an active route occurs, the node upstream of that break may choose to repair the link locally. To repair the link break, the node increments the sequence number for the destination and then broadcasts a RR for that destination. During local repair data packets should be buffered. If, at the end of the discovery period, the repairing node has not received a RP (or other control message creating or updating the route) for that destination, it proceeds by transmitting a RB message to all the precursors for that destination. The precursors that use this node as the next hope towards the destination will try to recover the route locally.

This local repair process continues until the RB message passes half of the way from destination to source. On the other hand, if the node receives one or more RP (or other control message creating or updating the route to the desired destination) during the discovery period, it first compares the hop count of the new route with the value in the hop count field of the invalid route table entry for that destination. If the hop count of the newly determined route to the destination is greater than the hop count of the previously known route the node should issue a RB message for the destination (Fig. 4), with the N bit set. Then it proceeds as the RP proceeds towards the source updating its route table entry for that destination. The source may initiate route discovery if it needs fresh route to the destination.

FUTURE WORK

Mobile Ad-Hoc networking has gained an important part of the interest of researchers and become very popular for the past few years, due to its potential and possibilities. The nodes in MANETs operate both as hosts as well as routers. The nodes are mobile and so the creation of routing paths is affected by the addition and deletion of nodes. The topology of the network may change rapidly and unexpectedly. Different specification of ad-hoc routing protocols have been to IETF MANET working group. There are further improvements that could be subjected to future research.

Speed, location and direction: The protocol can be extended by adding speed, position and direction information of mobile nodes in the route discovery packet so that these features also play an important role in route selection. Adding these criteria in route selection may perform better in high mobility.

Reducing control message overhead: High range of control message overhead slows down data transmission in ad-hoc networks. Transfer of many control messages is a threat in high mobility. Research work is going on to show whether it is feasible to send a large number of small control messages that are costly than that of fewer number of long control messages.

Security: Security in Ad-hoc network is a very important issue and is being considered in various research works. Routing protocols are prime targets of impersonating attacks. These attacks can upset the whole idea of data transmission in ad-hoc networks. Ad-hoc network are formed without any centralized facility, so security can be controlled in distributed manner where several nodes can participate to provide security.

Multicast: Multicast as a basic tool for conferencing applications must be considered when designing routing algorithms for ad-hoc networks. Nodes in the network that are members of the same multicast group together with the nodes used as routers to connect group members form a network across which multicast data packets are relayed.

QoS: QoS is another important feature of routing protocols. AODV has been enhanced to provide basic QoS services namely delay and bandwidth assurances. We plan to investigate the efficacy of these additions in the near future.

CONCLUSION

Unlike routing protocols using distance vector or link state algorithms, our protocol uses on-demand source routing which adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. Our protocol always prefers a route with smaller hop-count as well as few number of forwarding nodes to provide route robustness and efficiency. We are currently working to expand our protocol features and simulate it in ns-2 simulator. We are trying to evaluate the protocol performance in different network environment and also to incorporate some additional optimizations and to quantify the effects of the individual optimizations on the behavior and performance of the protocol. We are also continuing to extend our protocol so that it can run in multicast environment. Although this study does not address the security concerns inherent in wireless networks or packet routing, we are currently examining these issues with respect to attacks on privacy and denial of service in the routing protocol.

REFERENCES

Charles E. Perkins and Pravin Bhagwat, 1994. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, In: Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, pp: 234-244.

Charles E. Perkins., 1998. Ad Hoc On Demand Distance Vector (AODV) Routing, Internet Draft, draft-ietf-manet-01.txt.

Gursharan S. Sidhu, Richard F. Andrews and Alan B. Oppenheimer, 1990. Inside Applied Talk. Addison Wesley, Reading, Massachusetts.

Hedrick, C., 1988. Routing Information Protocol. Internet Request for Comments RFC 1058.

International Standards Organization. Intermediate system to intermediate system intra-domain routing exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473). ISO DP 10589.

John Jubin and Janet D. Tornow. The DARPA packet radio network protocols. Proc. IEEE., 75: 21-32.

John M. McQuillan and David C. Walden, 1977. The ARPA network design decisions. Computer Networks, 1: 243-289.

John M. McQuillan, Ira Richer and Eric C. Rosen, 1980. The new routing algorithm for the ARPANET. IEEE. Trans. Commun. COM-28: 711-719.

Johnson, D. and D. Maltz, 1996. Dynamic Source Routing in Ad-hoc Wireless Networks. In: Computer Communications Review Proceedings of SIGCOMM.

Johnson, D.B., D.A. Maltz and J. Broch, 2001. DSR: The Dynamic Source Routing Protocols for Multi-Hop Wireless Ad Hoc Networks, Ad Hoc Networking, Addison Wesley, pp: 139-172.

Lee, S. and C. Kim, 2000. Neighbor Supporting Ad hoc Multicast Routing protocol, Proc. 1st ACM international symposium on Mobile ad hoc networking and computing, Boston, Massachusetts, Moy, J., 1991. OSPF version 2. Internet Request for Comments RFC 1247, pp: 37-44.

Nachum Shacham and Jil Westcott, 1987. Future directions in packet radio architectures and protocols. Proc. IEEE., 75: 83-99.

Perkins, C. and P. Bhahwat, 1994. Highly Dynamic Destination Sequenced Distance Vector Routing (Dsdv) for Mobile Computers, ACM SIGCOMM'94 Conference on Communications Architectures and Applications, London, UK.

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing, WMCSA: 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, USA., pp: 90-100.

Perkins, C.E., 2000. Ad hoc networking, Addison-Wesley.

Perkins, C.E., E.M. Royer and S. Das, 2000. Ad Hoc On Demand Distance Vector (AODV) Routing, IETF Internet Dtraft, March 2000, (Online). URL:http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-05.txt.

Routing Protocols for Ad Hoc Mobile Wireless Networks (Online).URL: http://www.cis.ohio-state.edu/~jain/cis788-99/adhoc_routing/indexhtml.

Royer, E.M. and C.K. Toh, 1999. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Commun. Mag., Vol. 6.

Tanenbaum, A.S., 1996. Computer Networks, 3rd Edn. Prentice Hall, Englewood Cliffs. 3rd Edn., 4: 263-264.

Turner, P., 1990. NetWare communications processes. NetWare Application Notes. Novell Res., pp: 25-81.

Xerox Corporation, 1981. Internet transport protocols. Xerox System Integration Standard 028112. Local repair of link failure.