ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS: A LITERATURE REVIEW

Najiya A, Fameela K.A, and Asst. Professor Reshma V.K
Department of Computer Science
Nehru College of Engineering and Research Centre,Pampady, Kerala.

Abstract— **A mobile ad hoc network (MANET) is a self configuring infrastructure less network of mobile devices connected by wireless. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other nodes frequently. The routing overhead associated with route discovery is very high which leads to poor packet delivery ratio and a high delay. This paper presents a comprehensive summary of recent work related to the routing protocols in MANETs and how they are used for reducing the routing overhead in the field of mobile nodes.**

Keywords— Proactive protocols; heterogenous MANET; broadcast storm problem; overhead;

I. Introduction

Each node in MANETs may act either as an end user node or a router. To manage the communication in the mobile ad hoc networks many routing protocols have been proposed. The routing protocols react differently to the network conditions. The node heterogeneity significantly affects the performance of the routing protocols. MANETs are useful in places that have no communications infrastructure or when that infrastructure is severely damaged. Typical applications are emergency rescue operations, disaster relief efforts, low enforcement and military operations. Y.C. Tseng et al., [1], proposed that extreme amounts of broadcast traffic constitute a broadcast storm. Sufficient network resources are consumed by the broadcast storm so as to render the network unable to transport normal traffic. A packet that induces such a storm is known as a Chernobyl packet. In a mobile ad hoc network , route request (RREQ) packets are usually broadcast to discover new routes. These RREQ packets may cause broadcast storms and compete over the channel with data packets. One approach to alleviate the broadcast storm problem is to inhibit some hosts from rebroadcasting to reduce the redundancy, and thus contention and collision. A straight-forward approach to perform broadcast is by flooding. On receiving a broadcast message for the first time, a host has the obligation to rebroadcast the message. Clearly, this costs n transmissions in a network. Due to this, problems such as redundant rebroadcasts, contention and collisions would occur.

Redundant rebroadcasts means when a mobile host decides to rebroadcast a broadcast message to its neighbours, all its neighbours already have the message. Contention means after a mobile host broadcasts a message, if many of its neighbours decide to rebroadcast the message, these transmissions (which are all from nearby hosts) may severely contend with each other. Collision means because of the absence of any collision detection mechanism, collisions are more likely to occur and cause more damage.

II. PROBLEM DEFINITION

Mobility brings fundamental challenges to the design of protocol for mobile ad hoc networks. Due to the movement of nodes, the routing protocols have to cope with frequent topology evolutions and ensure quick response and adaptation to topology changes. The proactive protocols provide fast response to topology change by continuously monitoring the changes in topology and disseminating that information all over the network. The overhead of routing is very high in proactive protocols. It will lead to increase in delay and less packet delivery ratio. In the worst case, it will lead to the broadcast problem and the whole network is congested.

Broadcasting is an effective mechanism for route discovery, but the routing overhead associated with the broadcasting can be quite large, especially in high dynamic networks. The rebroadcast is very costly and consumes too much network resource. The broadcasting incurs large routing overhead and causes many problems such as redundant retransmissions, contentions, and collisions. Therefore the redundant rebroadcast increases the packet collision which leads to a decrease in the packet delivery ratio and increases the average end-to-end delay.

III. DIFFERENT APPROACHES IN ROUTING

A. Ad Hoc On Demand Distance Vector Routing

C. Perkins et al., [2], proposed that an ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Ad hoc On Demand Distance Vector Routing (AODV) is a novel algorithm for the operation of such ad hoc networks. Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

The AODV Routing Protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the Route Request (RREQ) packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single Route Request. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater or equal than the last DestSeqNum stored at the node with smaller hop count.

A RouteRequest carries the source identifier (SrcID), the destination identifier (DestID), the source sequence number (SrcSeqNum), the destination sequence number (DestSeqNum), the broadcast identifier (BcastID), and the time to live (TTL) field. DestSeqNum indicates the freshness of the route that is accepted by the source. When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet. If a RouteRequest is received multiple times, which is indicated by the BcastID-SrcID pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RouteReply packets to the source. Every intermediate node, while forwarding a RouteRequest, enters the previous node address and it's BcastID. A timer is used to delete this entry in case a RouteReply is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets. When a node receives a RouteReply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination. One disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also, multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead. Another disadvantage of AODV is unnecessary bandwidth consumption due to periodic beaconing. AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

B. Dynamic Source Routing

D. Johnson et al., [3], proposed a Dynamic Source Routing (DSR) protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

The mentioned protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbours of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding RouteRequest packets in the network. The destination node, on receiving a RouteRequest packet, responds by sending a RouteReply packet back to the source, which carries the route traversed by the RouteRequest packet received.

Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a RouteRequest packet. The RouteRequest is flooded throughout the network. Each node, upon receiving a RouteRequest packet, rebroadcasts the packet to its neighbours if it has not forwarded it already, provided that the node is not the destination node and that the packet's time to live (TTL) counter has not been exceeded. Each RouteRequest carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a RouteRequest packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate RouteRequest. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same RouteRequest by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase. A destination node, after receiving the first RouteRequest packet, replies to the source node through the reverse path the RouteRequest packet had traversed. Nodes can also learn about the neighbouring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself). This route cache is also used during the route construction phase.

The DSR protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. The routing overhead is directly proportional to the path length.

C. Gossip Based Approach

Z. Hass et al., [4], proposed the gossiping-based approach, in which each node forwards a message with some probability, to reduce the overhead of the routing protocols. Gossiping exhibits bimodal behavior in sufficiently large networks. In some executions, the gossip dies out quickly and hardly any node gets the message. In the remaining executions, a substantial fraction of the nodes gets the message. The fraction of executions in which most nodes get the message depends on the gossiping probability and the topology of the network. For large networks, the simple gossiping protocol uses up to 35% fewer messages than flooding, with improved performance. Gossiping can also be combined with various optimizations of flooding to yield further benefits. Simulations show that adding gossiping to AODV results in significant performance improvement, even in networks as small as 150 nodes.

In gossiping, it is assumed that any node in the network can send a message to any other node, either because there is a direct link to that node or a route to that node is known. Gossiping proceeds by choosing some set of nodes at random to which to gossip. In an ad hoc network, if a message is transmitted by anode, due to the nature of radio communications, the message is usually received by the entire nodes one hop away from the sender. Because of the fact that wireless resources are expensive, it makes sense to take advantage of this physical-layer broadcasting feature of the radio transmission. In the gossiping protocol, the probability can be controlled with which the physical-layer broadcast is sent. A source sends the route request with probability 1. When a node first receives a route request, with probability p it broadcasts the request to its neighbours and with probability $1 - p$ it discards the request; if the node receives the same route request again, it is discarded. Thus, a node broadcasts a given route request at most once.

The gossip approach has a slight problem with initial conditions. If the source has relatively few neighbours, there is a chance that none of them will gossip, and the gossip will die. To make sure this does not happen, we gossip with probability 1 for the first k hops before continuing to gossip with probability p. The performance clearly depends on the choice of p and k. The real problem with gossiping is that, if we gossip with too low a probability, the message may "die out" in a certain fraction of the executions. Measures can be taken to prevent this (for example, having successors of nodes with low degree gossip with a higher probability) but, unfortunately, there is no way for a node to know if a message is dying out.

The bimodal distribution observed in the use of gossiping can be viewed as a significant advantage. Once a route is found, acknowledgments are propagated back to the source along the route, so the source knows the route. If a route is not found within a certain timeout period, there are two possibilities: either there is no route at all, or the protocol did not detect it. Our focus is on networks that are sufficiently well connected that there typically is a route. However, when using a gossiping protocol, there is always a possibility that a route will not be found even if it exists. Despite the various optimizations, with flooding-based routing, many routing messages are propagated unnecessarily. Gossiping can reduce control traffic up to 35% when compared to flooding. This protocol is simple and easy to incorporate into existing protocols. When adding gossiping to AODV, simulations show significant performance improvements in all the performance metrics, even in networks as small as 150 nodes. Moreover, simulation with AODV has shown, gossiping can provide significant advantages even in small networks. Gossiping is also quite robust and able to tolerate fault.

D. Dynamic Probabilistic Route Discovery (DPR)

Abdulai *et al.,* [5], proposed a Dynamic Probabilistic Route Discovery (DPR) scheme based on neighbour coverage. In this approach, each node determines the forwarding probability according to the number of its neighbours and the set of neighbours which are covered by the previous broadcast. The DPR scheme prioritizes the routing operation at each node with respect to different network parameters such as the number of duplicated packets, and local and global network density. The performance of the proposed scheme DPR has been examined in MANETs, in terms of a number of important metrics such as RREQ rebroadcast number and RREQ collision number. High mobility nodes often have frequent link breakages. This potentially leads to re-discovery of same routes. The main aim is to set up the most stable routes to avoid any possible link breakage. These schemes also enhance the overall network performance by suppressing the broadcast storm problem, which occurs during the route discovery process A proper rebroadcast probability and timer are set The DPR scheme only considers the coverage ratio by the previous node, and it does not consider the neighbours receiving the duplicate RREQ packet. Thus, there is a room of further optimization and extension for the DPR protocol.

E. Neighbour Coverage Based Probabilistic Rebroadcast

Xin Ming Zhang and et al., [6], suggested that the initial motivation of the system is to optimize broadcasting. For optimization of broadcasting in route discovery, many methods have been introduced. These methods have their own advantages as well as disadvantages. But to optimize the rebroadcast in a more efficient manner a new system is used here by combining the advantages of neighbour coverage based method and probabilistic methods. The main objectives of the Neighbour Coverage Based Probabilistic Rebroadcast based on neighbour coverage area is to optimize the number of redundant retransmissions, to increase the routing performance and to reduce the routing overhead.

An uncovered neighbour set is defined first and using this novel rebroadcast delay is calculated. The rebroadcast delay is to determine the forwarding order. The node which has more common neighbours with the previous node has the lower delay. If this node rebroadcasts a packet, then more common neighbours will know this fact. Therefore the rebroadcast delay enables the information that the nodes have transmitted the packet spread to more neighbours. Also we are proposing a rebroadcast probability. It considers the information about uncovered neighbours, connectivity metric and local node density to calculate the rebroadcast probability. The rebroadcast probability is composed of additional coverage ratio, which is the ratio of the number of nodes that should be covered by a single broadcast to the total number of neighbours; and the connectivity factor, which reflects the relationship of network connectivity and the number of neighbours of a given node.
The rebroadcast delay is defined with the following reasons: Firstly, the delay time is used to determine the node transmission order. To sufficiently exploit the neighbour coverage knowledge, it should be disseminated as quickly as possible. The objective of this rebroadcast delay is not to rebroadcast the RREQ packet to more nodes, but to disseminate the neighbour coverage knowledge more quickly. After determining the rebroadcast delay, the node can set its own timer.

The node which has a larger rebroadcast delay may listen to RREQ packets from the nodes which have lower one. For example, if node ni receives a duplicate RREQ packet from its neighbour nj , it knows that how many its neighbours have been covered by the RREQ packet from nj. Thus, node ni could further adjust its UCN set according to the neighbour list in the RREQ packet from nj . When the timer of the rebroadcast delay of node ni expires, the node obtains the final UCN set. The nodes belonging to the final UCN set are the nodes that need to receive and process the RREQ packet. The additional coverage ratio indicates the ratio of the number of nodes that are additionally covered by this rebroadcast to the total number of neighbours of node ni. The nodes that are additionally covered need to receive and process the RREQ packet. As additional coverage ratio becomes bigger, more nodes will be covered by this rebroadcast, and more nodes need to receive and process the RREQ packet, and, thus, the rebroadcast probability should be set to be higher. If each node connects to more than 5.1774 log n of its nearest neighbours, then the probability of the network being connected is approaching 1 as n increases, where n is the number of nodes in the network. Then we can use 5.1774 log n as the connectivity metric of the network. The ratio of the number of nodes that need to receive the RREQ packet to the total number of neighbours of node ni is assumed to be connectivity factor.

IV. CONCLUSION

High mobility of nodes in MANETs leads to the routing overhead in the route discovery. Several approaches are used for reducing the routing overhead in such networks. They have their own advantages and disadvantages. In this paper a survey of different routing protocol approaches are depicted.

REFERENCES

[1] S.Y. Ni, Y.C. Tseng, Y.S. Chen, and J.P. Sheu, “The Broadcast Storm Problem in a Mobile Ad Hoc Network,” Proc.ACM/IEEE MobiCom,pp, 151-162.
[2] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On-Demand Distance Vector (AODV) Routing,” *IETF RFC 3561,2003.*

[3] D. Johnson, Y. Hu, and D. Maltz, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) for IPV4,IETF RFC 4278,vol. 15,pp.153-181,2007.

[4] Z. Haas, J. Y. Halpem, and L. Li, "Gossip-Based Ad Hoc Routing," Proc.IEEE INFOCOM,vol.21,pp.1707-1716.

[5] J.D. Abdulai, M. Ould-Khaoua, L.M. Mackenzie, and A. Mohammed,"Neighbour Coverage: A Dynamic Probabilistic Route Discovery for Mobile Ad Hoc Networks," Proc. Int'l Symp.Performance Evaluation of Computer and Telecomm. Systems (SPECTS'08), pp. 165-172, 2008.

[6] Xin Ming Zhang, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, "A Neighbour Coverage Based Probabilistic Rebrodcast for Reducing Routing Overhead in MANETs," Proc.IEEE Transactions On Mobile Computing,Vol.12 MARCH 2013

[7] X. Wu, H.R. Sadjadpour, and J.J. Garcia-Luna-Aceves, "Routing Overhead as a Function of Node Mobility : Modeling Framework and Implications on Proactive Routing," Proc. IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS '07), pp. 1-9, 2007.

[8] B. Williams and T. Camp, "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks," Proc. ACM MobiHoc, pp. 194-205, 2002.

[9] J. Kim, Q. Zhang, and D.P. Agrawal, "Probabilistic Broadcasting Based on Coverage Area and Neighbor Confirmation in Mobile Ad Hoc Networks," Proc. IEEE GlobeCom, 2004.

[10] Abdulai J.D, M.Ould-Khaoua, and L.M .Mackenzie, "Improving Probabilistic Route Discovery in Mobile Ad Hoc Networks," Proc. of IEEE Conference on Local Computer Networks, pp. 739-746, 2007.

[11] Peng S and X. Lu,"On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks," Proc. Of ACM MobiHoc'00, pp. 129-130, 2000.

[12] Chen J, Y. Z. Lee, H. Zhou, M. Gerla, and Y. Shu, "Robust Ad Hoc Routing for Lossy Wireless Environment," Proc. of MILCOM'06, pp. 1-7, 2006 .

