International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 31(September, 2015), PP. 239-244

TREE BASED ROUTING MECHANISM FOR MANET

Pradnya Kinge[#1], Dr. Lata Ragha[#2]
[1] ME Computes Engineering Student, Second Year,
Terna Engineering College, Nerul, Navi Mumbai, India
pradnya.kinge@gmail.com
[2] Prof & HOD, Computer Department
Terna Engineering College, Nerul, Navi Mumbai, India
lata.ragha@gmail.com

***Abstract*: Mobile Ad Hoc Networks (MANETs) are widely used in emergency scenarios, disaster management, battlefield communication where no infrastructure is present. Innovating routing in MANET is crucial for unleashing the full potential of such networks. Due to lack of lightweight proactive routing scheme with strong routing capability, opportunistic data forwarding has not been widely used in MANET. We propose the new lightweight proactive routing based on concept of tree structure that will reduce communication overhead and provide nodes with more network structure information than distance vector (DV) based protocols [e.g. Destination Sequenced Distance Vector (DSDV)], Link State (LS) based protocols [e.g. Optimized Link State Routing (OLSR)] and reactive source routing [e.g. Dynamic Source Routing (DSR)]. The proposed technique provides every node with a Breadth First Spanning Tree (BFST) of the entire network rooted at itself. To reduce overhead, instead of broadcasting the entire network tree structure, it broadcast only the differential update message of the tree structure.**

Keywords: mobile ad hoc network, routing, tree structure

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ad-hoc network topologies which allow people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g. disaster recovery environments.

The advantages such as flexibility, mobility, resilience and independence of fixed infrastructure, elicited immediate interest among military police and rescue agencies in the use of such network under disorganized or hostile environments. Today because of the emergence of Real Time applications and the widespread use of wireless and mobile devices, mobile ad hoc networks are receiving attention due to many potential military and civilian applications, rescue operations [1].

Mobile nodes are autonomous units that are capable of roaming independently. Typical mobile ad hoc wireless node are laptops, PDAs, Packet PCs, Cellular Phones, Internet Mobile Phones, Palmtops or any other mobile wireless devices. A mobile ad hoc network is an adaptive, self-configurable, self-organizing, infrastructure-less multi-hop wireless network with unpredictable dynamic topologies [2]. By adaptive, self-configurable and self-organizing, we mean that an ad hoc network can be formed, merged together or partitioned into separated networks on the fly depending on the networking needs [3].

In addition some networks (e.g. mobile military networks of highways networks) may be relatively large (e.g. tens or hundreds of nodes per routing area), although the need for scalability is not unique to MANETs. However, owing to the preceding characteristics, the mechanisms required to achieve scalability likely are more complicated. Actually, most of the existing protocols break down for large networks. The challenges in this area include end-to-end data transfer, link access control, scalability, security and providing support for real-time multimedia streaming. In network layer, many routing protocols with different objectives for various applications have been proposed. Considering the special properties of MANET, a multi-hop routing protocol expects properties like protocol should support opportunistic data forwarding, it should be loop free, its routing overhead should be less, bandwidth consumption should be minimum, it should be event driven as well as timer driven, it should support high scalability, etc., though all of these might not be possible to incorporate in a single solution.

In this paper, the literature survey of some protocols like DSDV, OLSR, DSR, AODV are done in section II, the problem definition is given in section III, our proposed technique to for solution to problem definition is explained in section IV and we conclude in section V.

II. LITERATURE SURVEY

A. Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

DSDV [4] is proactive routing protocol which is modification of conventional Bellman–Ford routing algorithm. DSDV is based on Routing Information Protocol [RIP] used in parts of internet. Therefore DSDV only use bidirectional links and it is one of the earlier ad hoc routing protocol developed.

In this protocol, every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. This makes it better in terms of routing path adaptation. On the other hand, it increases traffic overhead as it broadcasts routing information even if there is no change in network topology. DSDV also maintains routing paths which are never used. This protocol was motivated for use of data exchange along changing and arbitrary paths of interconnection which may not be close to any base station.

As an example, if routing tables at each node viz., Node A, Node B and Node C. If node B increases Sequence number from 100 to 102, node B broadcasts routing information to its neighbor viz., node A and node C including destination sequence numbers. DSDV protocol responds to topology changes immediately. The topology change can consists of new routes, broken links or metric change. DSDV uses full and incremental updates. Full update means sending all information from own routing table and incremental update is sent only for those entries that has changed which will make it fit into one single packet.

Advantages and Limitations: DSDV guarantees loop-free paths and the count to infinity problem is reduced in DSDV. Extra traffic can be avoided with incremental updates instead of full dump updates. For path finding, DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, amount of space in routing table is reduced. As with advantages of DSDV there are some limitations as well like firstly it is difficult to maintain the routing table's advertisement for larger networks. Each and every host in network should maintain routing table for advertising. But it is not feasible to large networks as it consume bandwidth. Secondly it is difficult to determine a time delay for the advertisements of routes. Thirdly the update packets are broadcast throughout the network so every node in the network knows how to reach every other node. As the number of nodes in the network grows, the size of the routing tables and the bandwidth required to update them also grows. Also it is difficult to deal with high node mobility rates. Also it maintains routes which are never used and it doesn't support multi path routing. It is unstable until update packet propagate throughout the network.

B. Optimized Link State Routing Protocol (OLSR)

Optimized link state routing is a proactive protocol in which, each node intermittently broadcasts its routing table, allowing each node to build an inclusive view of the network topology [5]. The Multipoint Relays (MPR) is the key idea behind the OLSR protocol to reduce the information exchange overhead. Instead of pure flooding the OLSR uses MPR to reduce the number of the host which broadcasts the information throughout the network. The MPR is a host's one hop neighbor which may forward its messages. The MPR set of host is kept small in order for the protocol to be efficient. In OLSR only the MPRs can forward the data throughout the network.

In OLSR protocol, each router discovers its neighbors and measures the link cost to each of them. Each node maintains a view of the network topology with a cost for each link and periodically distributes the link-state information to all other routers called as flooding. It finally computes the shortest path to every other router.

Flooding is accomplished through hop-by-hop dissemination where the originating node transmits the link state of its outgoing links to its neighboring nodes called as ‘link state advertisement’ (LSA). The neighboring nodes, in turn, forward this link state information to their neighbors, and so on. This way, after some time, all nodes in the network find out the link state information of various links. The LSA contains Source Node, Link ID, and Link Cost. LSA needs basic information like Source Node, Link Id and Link Cost. But this information can’t resolve timings, so time stamping needs to be added and it is typically done with sequence number. However, sequence number comes from a finite-bit space; so aging is added for safeguard and the new LSA format contains Source Node, Link Id, Link Cost, Sequence Number, and Age.

Advantages and Limitations: OLSR sent messages periodically and its delivery need not be sequential. It has less end-to-end delay for packet transfer but on other hand it needs more time to re-discover a broken link and needs more processing power when discovering the alternate route.

C. Dynamic Source Routing (DSR)

DSR allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination [6]. In this protocol, the mobile nodes are required to maintain route caches or the known routes. The route cache is updated when any new route is known for a particular entry in the route cache. Routing in DSR is done using two phases: route discovery and route maintenance. When a source node wants to send a packet to a destination, it first consults its route cache to determine whether it already knows about any route to the destination or not. If already there is an entry for that destination, the source uses that to send the packet. If not, it initiates a route request broadcast.

For a network topology, if a Node S wants to send a packet to Node D but does not know the route to reach Node D. To find route to reach Node D, Node S initiates a route discovery process where source Node S floods the network with Route Request (RREQ) packet. Each node appends its own network identifier while forwarding route request RREQ packet. Neighbor node receives packet RREQ from its two neighbors, thus the potential for collision.

Two nodes may broadcast RREQ to Node D. But since, the two nodes are hidden from each other, their transmissions may collide. Node D will not forward RREQ, because Node D is the intended target of the route discovery process. In DSR, destination Node D on receiving the first RREQ, sends a Route Reply (RREP) by the route obtained by reversing the route appended by received RREQ. RREP includes route from Node S to Node D on which RREQ was received by Node D.

Node S on receiving RREP, caches the route included in the RREP. When node S sends a data packet to Node D, the entire route is included in the packet header, hence, the name is Source Routing Protocol. In DSR, intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded. In DSR, packet size grows with route length as the entire path is stored in packet header.

In DSR optimization, each node caches a new route it learns by any means. When node S finds route to node D, an intermediate node may also learn a route when it overhears Data, thus these stale caches may increase the overheads.

Advantages and Limitations: DSR Eliminates need to periodically flooding the network with table update messages. As the route information is passed through intermediate nodes, they also utilize the cache information efficiently to reduce the control overhead. But on another hand, the performance of the protocol degrades in highly mobile environment. Also its connection setup delay is higher than the table driven protocols. And the route maintenance mechanism does not locally repair the broken links in network.

D. Ad Hoc On-Demand Distance Vector Routing (AODV)

AODV is reactive protocol and is basically an improvement of DSDV [7]. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps for establishing a reverse path.

Ad hoc on-demand distance vector routing protocol in MANET allows mobile nodes to respond quickly to link breakages and changes in network topology. When link breaks, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the broken link.

Destination Sequence Numbers are used in packet headers to recognizing latest packets. This destination sequence number is generated by destination for any route information it sends to its requesting nodes. If node has two or more choices for routes to a destination, then a requesting node always selects the one with greatest sequence number.

There are four types of messages used in AODV. These are given below:

1. *Route Request (RREQ):* When a route to new destination is needed, the node uses a broadcast RREQ to find the route to destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a “fresh enough” route to the destination

2. *Route Reply (RREP):* The route is made available by unicasting a RREP back to the source of the RREQ. Since each node receiving the request caches a route back to the source of the request, the RREP can be unicast back from the destination to the source.

3. *Route Error (RERR):* Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates which destinations are now unreachable due to the loss of the link.

4. *Hello Messages: H*ello messages are RREP messages with TTL = 1. This message is used for broadcasting connectivity information. A node should use Hello messages only if it is part of an active route.

Advantages and limitations: As AODV is reactive in nature, it can handle highly dynamic behavior of MANET. And also it can be used for unicasting n multicasting. At the same time periodic beaconing messages leads to unnecessary bandwidth consumption in network. As the protocol is reactive, calculated route stays correct only for the demand situation but later intermediate routes can carry stale entries.

III. THE PROBLEM DEFINITION

MANET is required nowadays in many application areas and the most important factor needed is its scalability with efficient performance in terms of its throughput with less end to end delay, and routing overhead. If we use distance vector (DV) protocols, then its data size grows with increase in topology i.e. number of nodes as nodes need to maintain latest updated information. AODV, DSDV and other DV based routing algorithms were not designed for source routing. Hence, they are not suitable for opportunistic data forwarding because every nodes in these protocols only knows the next hop to reach a given destination but not the complete path. OLSR and other link state (LS) based protocols can support source routing but their overhead is fairly high over load sensitive MANET. DSR and its derivations have long bootstrap delay and are therefore not efficacious for frequent data exchange, particularly when there is large number of data sources [8]. Thus we need a strong efficient proactive routing protocol to support scalability issues with high throughput and less overhead. We propose a new tree based efficient proactive routing protocol to address above issues.

IV. THE PROPOSED MECHANISM

The proposed system can be used to facilitate opportunistic data forwarding in MANET, where, a node maintains a Breadth First Search Spanning Tree (BFST) of the network rooted at it. This information will be periodically exchanged in all neighboring nodes for updated network topology information. This technique allows a node to have full details of path to all other existing nodes in the network, though the communication cost is linear to total number of nodes in the network. This allows supporting both source routing mechanism and conventional IP forwarding mechanism.

The protocol is based upon Path Finding Algorithm (PFA) [9] and WRP. PFA is based on DV and improves the mechanism by incorporating the predecessor of destination in routing update. WRP is used to build framework of PFA for each node to use a tree to achieve loop-free routing.

To make our algorithm more suitable for MANET, we adopt combined route update strategy that takes advantage of both "event-driven" and "timer-driven" approaches where nodes would hold their broadcast after receiving a route update for a period of time. If more updates have been received in this window, all updates are consolidated before triggering one broadcast. The period of the update cycle is an important parameter in this algorithm. First, we interleave full dump and differential updates to strike the balance between efficient and robust network operation. Second, we package affected links into forests to avoid duplicating nodes in the tree structure. Finally, for reducing more size of differential update messages, every node will try to alter minimum of the routing tree which maintained as the network change structure.

Proposed Algorithms

The algorithm of proposed protocol is as given below:

Algorithm 1: Finding Neighbors to Construct BFST

Step 1: Initialize node v

Step 2: Find neighbors of v as N[v] to construct BFST i.e. star graph centered at v

Step 3: Exchange newly created BFST with neighbors

Step 4: Check more recent update from neighbor and update own BFST as T_u

Step 5: Construct Union Graph G_v such that,

$$G_v = S_v \cup (T_u - v)$$

Step 6: Send T_v (newly created BFST of G_v) in routing packet to broadcast neighbors of v

Algorithm 2: Neighborhood Trimming

Step 1: If routing update is not received from neighbor or if data transmission to node u is failed then

1. Update N[v] = N[v] – {u}
2. Construct union graph G_v such that,
   $$G_v = S_u \cup (T_w - v)$$
3. Construct BFST of T_v
4. Send updated T_v after set periodic time

Algorithm 3: Differential Update

Step 1: Make tree representation compact by using packet frame shown below:

Right Bit	Left Bit	IP Address

Step 2: Find difference of BFST (the nodes that have change parents) and broadcast it to Neighbors

Figure 1 shows tree topology of nodes. Node A is rooted at itself and connected to right child node E and left child B, Similarly node B and E has their own child nodes. So, according to Algorithm 3, this tree topology will be defined as A11B11E10C00D00F00.

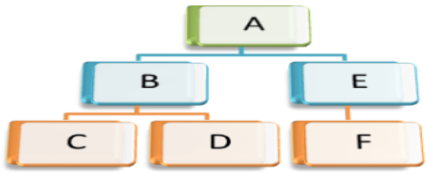

Figure 1

Implementation Details of Proposed Mechanism: The proposed mechanism can be implemented in NS2 network simulator. According to our proposed methodology, we are expecting to get similar or better data performance. We will measure the performance parameters with respect to different deployment scenarios as mentioned below in Table 1.

Parameters	**Values**
No. of Nodes	5, 10, 20, 30, 40, 50
Topology	Flat Grid Topology
Transmission Range	250m

Carrier Sensing Range	550m
Simulation Area	2000m * 2000m
Data Rate	1Mb/sec
Evaluation Parameters	Throughput, End-To-End Delay, Packet Drop Ratio, Control Overhead
Protocol Comparison	DSR, DSDV, OLSR

Table 1

V. CONCLUSION

In MANET, we need a strong routing protocol to support opportunistic data forwarding and improve scalability with better routing performance. We proposed a methodology by using tree structure which may provide more topology information than DVs with smaller overhead than LS routing protocols. The proposed mechanism can be made lightweight by using the tree structure for broadcasting topology information and try to improve its performance in terms of parameters like end-to-end delay, routing overhead, throughput over node density against different deployment scenarios.

References:

[1]S. A. Ade, P.A.Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks." July-December 2010, Volume 2, No.2, pp. 545-548.

[2]Cheng X, Ding M, Du D H, Jia X, "Virtual Backbone Construction in Multi-Hop Ad Hoc Wireless Networks," Wireless Comm. and Mobile Computing, vol. 6, pp.183-190, 2006.

[3]Swarnapriya, Vinodhini, Anthoniraj, Anand R.,"Autoconfiguration in mobile ad hoc networks", Innovations in Emerging Technologies (NCOIET), pp. 61-66, 2011

[4]C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers," *Comput. Commun. Rev.*, vol. 24, pp.

[5]T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626, Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[6]D. B. Johnson, Y.-C. Hu, and D. A. Maltz, "On The Dynamic Source Routing Protocol (DSR) for mobile ad hoc networks for IPv4," RFC 4728, Feb. 2007. [Online]:Available: http://www.ietf.org/rfc/rfc4728.txt

[7]C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt, 1991

[8]Zehua Wang, Cheng Li, Yuanzhu Chen, "PSR: Proactive Source Routing in Mobile Ad Hoc Networks", IEEE Globcom 2011

[9]S. Murthy, "Routing in packet-switched networks using path-finding algorithms," Ph.D. Dissertation, Computer Engineering, University of California, Santa Cruz, CA, USA, 1996