Issues in designing a Routing protocol for Ad-hoc wireless networks

1) **Mobility** :→ The network topology in an adhoc wireless network is highly dynamic due to the movement of nodes, hence an on-going session suffers frequent path breaks. Disruption occurs either due to the movement of the intermediate nodes in the path or due to the movement of end nodes. Such situations do not arise because of reliable links in the wired networks, and also ~~those~~ of wired n/ws find alternative path if the links break, & their convergence is very slow.

2) **Bandwidth Constraint** :→

Abundant bandwidth is available in wired networks due to the advent of fiber optics and due to the exploitation of the wavelength division multiplexing (WDM) technologies. But in wireless network, the radio bandwidth is limited, hence the data rates it can offer are much less than what a wired network can offer. This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.

3) **Error-Prone Shared Broadcast Radio channel**

The broadcast nature of the radio channel poses a unique challenge in adhoc wireless networks. The wireless links have time-varying characteristics in terms of link capacity and link-error probability. This requires that the adhoc wireless network routing protocol interacts with

Routing Protocols for Ad hoc Wireless Networks :-

With the increase in handy usage of Mobile computers necessitate the need to sharing of information between computers. So the users might need to perform administrative tasks and set up static, bi-directional links between the computers. If there exists no infrastructure and no administrative intervention required, then such an interconnection between mobile computers is called an Ad-Hoc network. In such an environment, it may be necessary for the mobile computers to take help of other computers in forwarding a packet to the destination due to limited range of each mobile host's wireless transmission. Mobile wireless networks can be classified into two types

1.) Infrastructured networks
   a) Networks with fixed and wired gateways
   b) Bridges for these networks are known as base stations
2) Infrastructureless mobile networks (Ad-hoc networks)
   a) No fixed routers
   b) All nodes can move and can be connected dynamically in an arbitrary manner
   c) Each node function as a router. It discovers and maintains routes to other nodes.

the MAC layer to find alternate routes through better quality links. Also, transmission in adhoc wireless networks results in collisions of data and control packets. Therefore, it is required that adhoc wireless network routing protocols find paths with less congestion.

4) Hidden and Exposed Terminal problems :-

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver. Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other. Solutions for this problem include (i) medium access collision avoidance (MACA)

(ii) Medium access collision avoidance for wireless (MACAW)

(iii) Floor acquisition multiple access (FAMA)

(iv) Dual busy tone multiple access (DBTMA)

5) Resource Constraints :-

Two essential and limited resources that form the major constraint for the nodes in an adhoc wireless network are battery life and processing power. Devices used in adhoc wireless n/ws in most cases requires portability, and hence they also have size and weight constraints along with the restrictions on power source.

6) Loop free Constraints :→ The Adhoc routing protocols must ~~decrease for loop free constraints~~ produce loop free routes.

Destination Sequenced Distance-Vector Routing Protocol (DSDV)

The DSDV routing protocol is one of the first protocols proposed for ad-hoc wireless networks. It is an enhanced version of the distributed Bellman-Ford algorithm, where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. It incorporates table updates with increasing sequence number tags to prevent loops, to counter the count-to-infinity problem, and for faster convergence.

Routes to all destinations are readily available at every node at all times. The tables are exchanged between neighbors at regular intervals or are forwarded if a node observes a significant change in network topology. The table updates are of two types (i) incremental updates
(ii) full dumps.

An incremental update takes a single network data packet unit (NDPU), while a full dump may take multiple NDPUs. Incremental updates are used when a node does not observe significant changes ~~significant or when an incremental update requires~~ in the local topology. A full dump is done either when the local topology changes significantly or whenan incremental update requires more than single NDPU.

Table updates are initiated by a destination with a new sequence number which is always greater than the previous one. The tables are forwarded to other nodes based on the best metric. Based on the sequence number of the table update, it may forward or reject the table.

The end node of the broken link initiates a table update message with the broken link's weight assigned to infinity (∞) and with a sequence number greater than the stored sequence number for that destination. A node always assigns an odd sequence number to the link break update to differentiate it from the even sequence number generated by the destination.

Advantages & Disadvantages

The availability of routes to all destinations at all times implies that much less delay is involved in the route setup process. The mechanism of incremental updates with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks with many fewer modifications. Also an up-to-date view of the network topology is available at all the nodes.

The updates due to broken links lead to a heavy control overhead during high mobility. Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth. This leads to excessive control overhead because of limited bandwidth. In order to obtain information about a particular node, a node has to wait for a table update message initiated by the same destination. This delay could result in stale routing information at nodes

Cluster-Head Gateway Switch Routing Protocol (CGSR)

CGSR uses a hierarchical network topology which is different from other table driven routing approaches that uses flat topologies. CGSR organises nodes into clusters (group of nodes) with coordination among the members of each cluster entrusted to a special node named cluster-head. This cluster head is elected dynamically by employing a least cluster change (LCC) algorithm. According to this algorithm, a node ceases to be a cluster-head only if it comes under the range of another cluster-head, where the tie is broken either using the lowest ID or highest connectivity algorithms. Clustering helps in ~~re~~using improving frequency reuse, ~~by~~ as cluster heads can operate on different spreading codes on a CDMA system. Inside a cluster, the cluster-head can coordinate the channel access based on a token-based polling protocol. All member nodes of a cluster can be reached by a cluster head within a single hop.

~~assuring existing the cluster head to provide improved~~

A token-based scheduling (assigning access token to the nodes in a cluster) is used within a cluster for sharing bandwidth. CGSR assumes that all communication passes through cluster-head. Communication between clusters takes place through the common member nodes that are members of both the clusters called as gateways. A gateway is expected to be able to listen to multiple spreading codes that are currently in operation in the clusters in which the node exists as a member.

A gateway conflict is said to occur when a cluster-head issues a token to a gateway over a spreading code while gateway is tuned to another code. ~~to another code~~. So gateways should be capable of simultaneously communicating over the two interfaces can avoid geteway conficts.

The routing protocol used in CGSR is an extension of DSDV. Every member node maintains a routing table containing the destination cluster-head for every node in the network. Every node also maintains a routing table which keeps the list of next-hop nodes for reaching to every destination cluster. The cluster (hierarchical) routing protocol is used here. In this protocol, when a node with packets to be transmitted to a destination gets the token from its cluster-head, it obtains the destination cluster-head and the next-hop node from the cluster member table and the routing table respectively. A path from any node a to any node b will be similar to $a - C_1 - G_1 - C_2 - G_2 - \cdots - C_i - G_j \cdots G_n - b$, where G_i and C_j are the i^{th} gateway and the j^{th} cluster-head, respectively, in the path. Route configuration is necessitated by mainly two factors: firstly, the change in cluster-head and secondly, the stale enteries in the cluster member table and routing table

Advantages and Disadvantages

Better Bandwidth utilization is possible due to partial coordination between nodes by electing cluster-heads. It is easy to implement priority scheduling schemes with token scheduling and gateway code scheduling.

The main disadvantage of CGSR are increase in path length and instability in the system at high mobility when the rate of change of cluster heads is high. In order to avoid gateway conflicts, more resources (such as additional interfaces) are required. The Power consumption at the cluster-head node is also a matter of concern. This could lead to frequent changes in the cluster head, which may result in multiple path breaks.

Dynamic Source Routing :- (DSR)

DSR is an On-demand protocol designed to restrict the bandwidth consumed by control packets, eliminated by table-driven approach. DSR is a beacon-less and hence does not require periodic hello packets (beacon) transmission, which are used by a node to inform its presence to the neighbours.

The basic approach of this protocol is to establish the route by flooding Route Request packets in the network. The destination node on receiving a Route Request packet, responds by sending a Route Reply packet back to source, which carries the route traversed by the Route Request packets received.

When a source node has data packets to be sent to the destination, firstly it initiates the Route Request packets, which are flooded throughout the network. Each node on receiving Route Request packet, rebroadcasts the packets to its neighbors if it has not forwarded already or if the node is not the destination node, provided the packet's time to live (TTL) counter has not exceeded. Each Route Request carries a sequence number generated by the source node and the path it has traversed. The packet is forwarded by intermidiate nodes only if it is not a duplicate Route Request to prevent loop formations and to avoid multiple transmissions of the same Route request. A destination node, after receiving the first Route Request packet, replies to the source node through the reverse path the Route Request packet has traversed. This protocol uses a route cache that stores all possible information extracted from the source route contained in the data packet. Nodes can also learn about neighboring route

traversed by data packets if operated in the promiscuous mo
(the mode of operation in which a node can receive the
packets that are neither broadcast nor addressed to itself
During route construction if an intermediate node
receiving a Route Request has a route to the destination
in its route cache, then it replies to the source node
by sending Route Reply with entire route information.

Optimizations

DSR uses route caches which are populated with
routes that can be extracted from the information contain
in data packets that get forwarded. This helps intermediate
nodes to reply to source, the route to destination.

By operating in promiscuous mode, an intermediat
node learns about route breaks, and thus update the route
cache. During network partitions, the affected nodes initiate
Route Request packets. An exponential backoff algorithm
is used to avoid frequent Route Request flooding in the
network when the destination is in another disjoint set.
DSR also allows piggy-backing of a data packet on
the Route Request so that the data packet can be sent
along with the Route Request.

A source node may get multiple replies of destination
intermediate nodes maintaing cache. The source node
selects the latest and the best route. Each data packet carries
the complete path to the destination.

When an intermediate node in the path moves away,
causing a wireless link to break, a RouteError message is
generated from the node adjacent to the broken link to
inform the source node. The source node reinitiates the route
establishment procedure. The route cache entries at all the
effected nodes are removed. If a link breaks due to the
movements of edge nodes (source or destination), the source
node again initiates the route discovery process.

Advantages & Disadvantages of DSR

This protocol uses a reactive approach which eliminates the need to periodically flood the n/w with table update messages. The route is established only when it is required and hence the need to find route to all other nodes in the network is eliminated. The route cache information helps in reducing overheads

The disadvantage of this protocol is that the route maintenance mechanism does not locally repair the broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is also drawback. The performance degrades with increasing mobility.

Ad Hoc On-demand Distance-Vector Routing protocol (AODV)

AODV uses on-demand approach for finding routes. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and 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 stores the next-hop information corresponding to each flow for data packet transmission. 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 than the last DestSeqNum stored at the Node.

The Route Request 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. When an intermediate node receives a RouteRequest, it either forwards it or prepares the RouteReply if it has a valid route to the destination by comparing the sequence number. If a RouteRequest is received multiple times, which is indicated by the BcastID-SrcID pair, the duplicate copies are discarded. Every intermediate node, while forwarding a RouteReply, enters the previous node address and its BcastID. A timer is used to delete this entry in case a RouteReply is not received before the timer expires. 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.

All intermediate nodes receiving a RouteReply update their route tables with the latest destination sequence number. They also update the routing information if it leads to a shorter path between source and destination.

AODV does not repair a broken path locally. When a link breaks, which is determined by observing the periodical beacons or through link level acknowledgements, the end nodes (i.e. source and destination nodes) are notified. When a source node learns about the path break, it reestablishes the route to the destination if required by the higher layers. If a path break is detected at an intermediate node, the node informs the end nodes by sending an unsolicited RouteReply with the hop count set as ∞.

Advantages and Disadvantages

The main advantage of this protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destinations. The connection setup delay is less

One of the disadvantages 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. Also multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead. Periodic beaconing also leads to unnecessary bandwidth consumption.

Location-Aided Routing :→ (LAR)

LAR utilizes the location information for improving the efficiency of routing by reducing the control overhead. It uses global positioning system (GPS) for obtaining the geographical position. LAR designates two geographical regions for selective forwarding of control packets

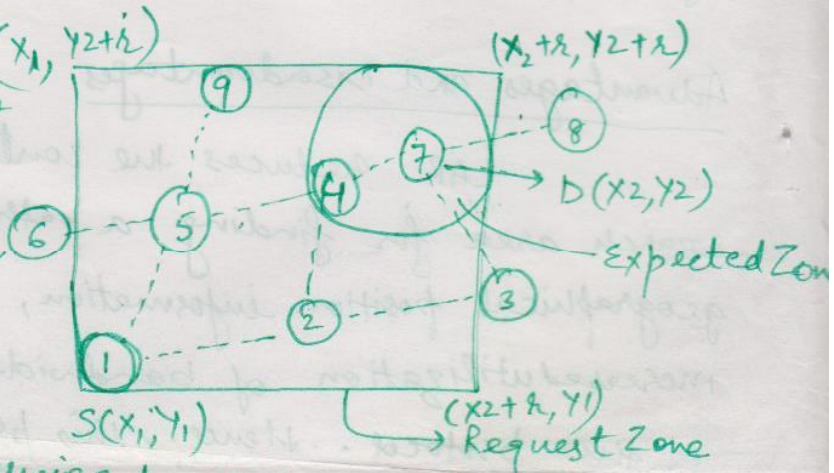
(i) Expected Zone
(ii) Request Zone

The ExpectedZone is a region in which the destination node is expected to be present, given information regarding its location in the past and its mobility information. If past information is not available, then the entire network area is considered to be the ExpectedZone of the destination.

The RequestZone is a geographical region within which the path-finding control packets are permitted to be propagated. This area is determined by the sender of a data & are forwarded by nodes present in RequestZone. other nodes outside RequestZone discard the control packets. When the first attempt for obtaining a path to a destination using the initial RequestZone fails, additional area is included for forwarding the packets. Flooding here is restricted to a small geographical region. The nodes decide to forward or discard the control packets based on two algorithms, namely

(i) LAR1
(ii) LAR2

In the LAR1 algorithm, the source node (say S) explicitly specifies the RequestZone in the RouteRequest Packet. The Request Zone is the smallest rectangle that includes the source node (S) and the ExpectedZone, the sides of which are parallel to X and Y axes, when the node S is outside the expected zone. When the node S is within the ExpectedZone, then the RequestZone is reduced to the ExpectedZone itself.



Every intermediate node that receives the Route Request packet verifies the RequestZone information contained in the packet and forward it further, if the node is within the RequestZone; otherwise packet is discarded. As an option, the current speed of movement can be included in the RouteReply packet is used by the source node for future route establishment procedures.

In LAR2 algorithm, the source node S includes the distance between itself and the destination node D along with (X, Y) coordinates of the destination node D in the RouteRequest packet instead of the explicit information about the Expected Region. When an intermediate node receives this RouteRequest packet, it computes the distance to the node D. If this distance is less than the distance from S to node D + δ, where δ is a parameter of the algorithm decided based on the error in location estimation & mobility, then the Route Request packet is forwarded. Otherwise, the RouteRequest is discarded. The distance between the forwarding node and D is updated in the RouteRequest packet for further relaying.

Once the RouteRequest reaches destination, it originates a RouteReply packet back to the source node, containing the path through which future data packets are to be propagated. In order to compensate for the location error (due to the inaccuracy of GPS information or due to changes in the mobility of the nodes), a larger Request zone that can accommodate the amount of error that occured is considered.

Advantages and Disadvantages

LAR reduces the control overhead by limiting the search area for finding a path. The efficient use of the geographical position information, reduced control overhead, and increased utilization of bandwidth are the major advantages of this protocol. Hence, this protocol cannot be used in situations where there is no sources of location information like GPS and it will also increase the cost of overall system due to GPS supporting equipments situated at the mobile nodes.

Global State Routing (GSR)

GSR is based on the link-state philosophy where each node in the network maintains the knowledge of the full network topology. The increase in the popularity of link state protocols over distance vector schemes was primarily due to their ability to converge quickly and avoid routing loops. However, with the bandwidth constrained links in the adhoc network, the flooding technique used by traditional link state schemes would be far too resource intensive. GSR avoids the flooding by periodically exchanging its link-state table with its neighbours only.

Global State Routing (GSR) is almost the same as DSDV, because it has the idea of link state routing but it makes a progress by decreasing the flooding of routing messages. In this algorithm, each node maintains a neighbour list, a topology table, a next hop table and a distance table.

•The neighbour list of a node includes the list of its neighbours (all nodes that can be heard by it).

• The link state information for each destination is maintained in the topology table together with the timestamp of the information.

• The next hop table includes the next hop to which the packets for each destination must be dispatched.

• The distance table contains the shortest distance to each destination node.

Information Dissemination

The key difference between our GSR and traditional LS is the way routing information is disseminated. In LS, link state packets are generated and flooded into the network whenever a node detects topology changes. GSR doesn't flood the link state packets. Instead, nodes in GSR maintain the link state table based on the up to date information received from neighboring nodes, and periodically exchange it with their local neighbors only. Information is disseminated as the link state with larger sequence numbers replaces the one with smaller sequence numbers. In this respect, it is similar to DBF (or more precisely, the DSDV [4]) where the value of distances is replaced according to the time stamp of sequence.

Fish Eye State Routing Algorithm (FSR)

The FSR protocol is a generalization of GSR protocol. FSR uses Fish Eye Technique to reduce information required to represent graphical data, to reduce routing overhead. The basic principle behind this technique is the property of a fish eye that can capture pixel information with greater accuracy near its eye's focal point. This accuracy decreases with an increase in the distance from the centre of focal point. The protocol uses the same data structure as GSR and its periodic route updates also only go as far as a node's neighbours.

⇒ The topology information exchange takes place periodically rather than be driven by an event. This is because instability of wireless links may cause excessive control overhead when event driven updates are employed. FSR defines routing scope which is the set of nodes that are reachable in a specific number of hops.

Example :- The scope of a node at two hops is the set of nodes that can be reached in two hops. The routing overhead is significantly reduced by adopting different frequencies of updates for nodes belonging to different scope. Entries for nodes with the smaller scope are propagated to neighbours with

the highest frequency while the remaining entries are broadcast at lower rate. This strategy ensures that topology changes for nodes near a node are propagated quickly, while there are latencies in transmitting information on the state of connections with nodes that are far away. This should not be seen as a disadvantage since, although inaccurate information is initially used for distant nodes, the packet is still accurately routed because the level of accuracy increases as the packet approaches the destination node.

Advantages

The notion of multilevel scopes employed by FSR significantly reduces the bandwidth consumed by (Link state) LS update packets. Hence FSR is suitable for large and highly mobile ad-hoc wireless networks.

The choice of number of hops associated with each scope level has a significant influence on the performance of the protocol at different mobility values and hence must be carefully choosen.