Middle-East Journal of Scientific Research 24 (4): 1194-1206, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.04.23259

Qualitative Analysis on Ad hoc Routing Protocols

[1]P. Dharanyadevi, [2]K. Rajakumari and [3]K. Venkatalakshmi

[1]Department of Information Technology, Anna University Villupuram Campus, Villupuram, India
[2]Department of Information Technology, Anna University, Regional Centre, Coimbatore, India
[3]Department of Electronics and Communication Engineering, Anna University Tindivanam Campus, Tindivanam, India

Abstract: Ad hoc networks are deemed as a novel class of wireless networks. Ad hoc network is an infrastructure less networks where the topology changes randomly due to the mobility of nodes which are connected by wireless links. This paper focuses on qualitative analysis on ad hoc routing techniques such as proactive, reactive and hybrid routing protocols in ad hoc wireless networks. The objective of routing is to find the viable path from source to destination for packet delivery. As in ad hoc networks the nodes have dreadfully high mobility there are oodles of challenges for routing the packets to their final destination which are addressed in the routing protocol. This paper sets the basis for the analysis of ad hoc routing protocols mechanism, its amenity and snag.

Key words: Ad hoc Networks · Infrastructure less · Wireless Networks · Routing Protocol · Proactive Routing protocols · Reactive Routing Protocols · Hybrid Routing Protocols · Qualitative Analysis · Amenity · Snag

INTRODUCTION

Wireless networks are an evolving, innovative technology that will consent users to access information and services electronically, irrespective of their topographical position. Wireless networks can be categorized into two types, infrastructure network and infrastructure less (ad hoc) networks. Infrastructure network entails of a network with fixed router and gateways. Indifference to infrastructure based networks, the nodes in ad hoc networks are mobile, no component is fixed and it can be connected dynamically in a random manner. All nodes of these networks act as routers and take part in the discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very useful in crisis search-and-rescue operations, meetings or resolutions in which people wish to swiftly share information and data acquisition processes in unreceptive terrain [1].

Wireless Ad hoc networks are pervasive, ubiquitous, infrastructure-free and without any centralized authority. Wireless ad hoc network; it is a decentralized network where each node is proficient to forward data packets between each intermediate node dynamically within the range.

Ad hoc Networks determine its next hop based on the network topology. Wireless Ad hoc networks are classified as Mobile Ad hoc NETwork (MANET), Wireless Mesh Network (WMN), Wireless Sensor Networks (WSN) and Vehicular Ad hoc NETworks (VANET). The petty challenges in the ad hoc network are medium access schemes, routing, transport layer protocol, Quality of Service, self-organizing, energy management, pricing scheme, scalability, addressing, service discovery, multicasting, security and so on. This poster focuses on routing in ad hoc networks. The responsibility of the routing protocols is to find the feasible paths to the destination from the source based on some criteria. While designing the routing protocols the challenges like host mobility, routing, shared broadcast channel, bandwidth constraint, hidden and exposed terminal problems, resource constraints and so forth need to be phizog [2].

Corresponding Author: P. Dharanyadevi, Department of Information Technology, Anna University Villupuram Campus, Villupuram, India.

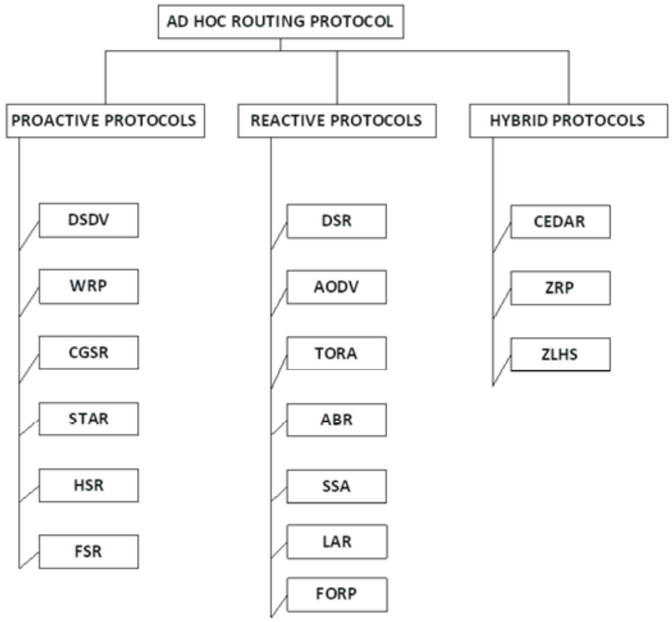

Fig. 1: Classification of Ad hoc Routing Protocols

The basic taxonomy of ad hoc routing protocols can be alienated into three classifications: table-driven, on-demand routing and hybrid routing protocols based on when and how the routes are exposed. The table driven routing protocols are reliable and up-to-date routing information to all nodes is maintained at each node, whereas in on-demand routing the routes are created only when desired by the source host [3]. Hybrid routing protocols have the best features of both table driven and on-demand routing protocol.

The paper is structured as follows: in section 2, we discuss the basic categories of ad hoc wireless routing protocols. In Section 3, we discuss the approaches, amenity and snag of existing popular proactive routing protocols. In section 4, the approaches, amenity and snag of the reactive or on-demand routing protocols are discussed. Section 5 constitutes the approaches, amenity and snag of the hybrid routing protocols. Finally the comparative analysis of the proactive, reactive and hybrid routing protocols are summarized.

Categories of AD HOC Routing Protocols: Fig. 1 depicts the classification of ad hoc protocols such as proactive routing protocols, reactive routing protocols and hybrid routing protocols.

Proactive Routing Protocols: This protocol is also called as table-driven routing protocol. When a source needs to send the packet to the destination, it uses the predefined routes in the routing table which are maintained by the nodes in the network. Thus, this protocol requires the continuous learning of the topological information that is exchanged among the nodes. Hence this protocol requires high bandwidth and power. This protocol has less time delay while finding the shortest path to the destination. The network organization of this protocol is flat/Hierarchical. This protocol has high control overhead and communication overhead [4].

Reactive Routing Protocols: This protocol is also called as on-demand routing protocol because it finds the path from the source to the destination whenever it is required. There is no need of maintaining any network topology information which in turn reduces path maintaining cost and results in low power and bandwidth requirement. The network organization of this protocol is flat. These protocols results in low control overhead and communication overhead, but the latency is high [5], Patent US 20050030921, “Routing protocol for ad hoc networks”.

Hybrid Routing Protocols: Hybrid routing protocols have the best features of both proactive and reactive routing protocols. Nodes within a certain distance from the node concerned, or within a particular geographic region, are said to be within the routing zone of the given node. For routing inside this zone, a table driven method is used. For nodes that are found outer this zone, an on-demand approach is used. The network organizations of this protocol are flat/hierarchical. Medium bandwidth and power is required. The control overhead and communication overhead are also medium for these protocols [6].

Proactive Rouitng Protocols

Destination Sequenced Distance-vector Routing Protocol (DSDV): DSDV is the proactive routing protocol which is proposed as the solution to prevent the looping problem and to count, the count-to-infinity problem which exists in the distributed Bellman-Ford algorithm or Routing Information Protocol (RIP). As DSDV is the table-driven routing protocol where each node maintains the routing information for all known destinations and it must be updated periodically if there is a change in the topology. The table updates are either Full Dump (carries the entire routing table and it is transmitted infrequently) or Incremental Update (carries only the information with regard to changes in routing tables and it is broadcasted frequently). The Routing Table (RT) entries are the sequence number which is originated from the destination resulted in the loop freeness, install time when the entry was made (used to delete stale entries from the table) and the next hop to reach the destination. In DSDV the routes to all destinations are readily available at every node all the times. If there is a change in the topology, then the RT which contains routing information is forwarded. Upon receiving this information the node performs the route selection process based on the following

If sequence $\_number_{new}$ > $sequence\_number_{previous}$
Then $sequence\_number_{new}$ is favorable rate
Else if $sequence\_number_{new}$ = $sequence\_number_{previous}$
Then the minimum cost path is the favored route

When a link failure is found in the network the weight of the broken link is assigned to infinity. This link is broken information is propagated to the entire network. The existence of the link is identified as:

If the link is present
    Then the sequence number is even
Else
    The sequence number is odd

When a node receives a message with infinity cost metric and the node has an item indicating a sequence number equal to or greater than the one announced. It initiates the new broadcast with that sequence number. This enables the node (the one which sent the initial broadcast message) to know an alternate path to the destination [7, 8].

Amenity: DSDV is simple routing protocol and it is uncomplicated to implement. It is an effective routing protocol because the routes to destination are already subsists in the source. Hence there is no latency while discovering the route. DSDV Routing Table is incorporated with the sequence number; hence the routing loop is prevented. DSDV does not maintain multiple routes instead it maintains only the best path.

Snag: Whenever there is a small change in the topology, the routing table should be updated regularly and the reconvergence of the network is happened at any time. Hence DSDV is not suitable for dynamic networks. It is only applicable to limited, small or medium sized networks. Because of the periodic updating of the routing table, the nodes consume power and small amount of bandwidth is required.

Wireless Routing Protocol (WRP): Wireless Routing Protocol (WRP) is the inherited version of a classic routing protocol called the distributed Bellman-Ford algorithm. Just like DSDV, in WRP the routes to destination are readily available and it maintains the up-to date view of the network. Each node in the network maintains the following tables.

Distance Table (DT): It contains the network view of the neighbors of a node.

Routing Table (RT): It gives the up-to-date view of the network for all destinations, shortest path, penultimate node, successor node and two flags.

Link Cost Table (LCT): It contains the cost of relaying messages through each link passed since the last successful update was received from that link. This is done to detect link breaks.

Message Retransmission List (MRL): Is an entity for each update message that is to be retransmitted and keeps a counter for each entity.

When an update message is received, a node updates its RT and reassesses the best path. It also performs the consistency check with its neighbors to eliminate loops and speed up the convergence. MRL maintains a list of which neighbors are yet to be acknowledged an update message. So they can be retransmitted if necessary. If there is no alteration in the RT, a node is essential to transmit a hello message to avow its connectivity [7].

Amenity: WRP has simple functionality. This protocol enables faster convergence and counts to the count-to-infinity problem. By storing the penalty nodes and successor nodes the loops are detected. By periodically transmitting the HELLO messages the nodes will keep track of the changes in the system. If any link failure is detected, then the reports are sent only to neighbors which indicate that the low number of updates are required.

Snag: As each node maintains four tables which involves complexity of maintenance of multiple tables demands a larger memory and greater processing power. WRP is not suitable for highly dynamic large networks. Because of high mobility the control overhead involved in updating table entries is almost the same as that of DSDV. The periodic usage of HELLO messages consumes power and bandwidth. There is a limited effective data transmission in small networks.

Cluster- Head Gateway Switch Routing Protocol (CGSR): Cluster-head Gateway Switch Routing protocol (CGSR) is a proactive routing protocol. The nodes in the network are organized into a group called cluster. In cluster the special node that is having the capability to be reached by the other Cluster Head (CH) is elected dynamically as the CH of this cluster by Least Cluster Change (LCC) algorithm. Except this CH all other nodes are said to be a Cluster Member (CM). The CM communicates through the CH. The nodes which are the members of both clusters is said to be Gateway. Gateways have the capability to simultaneously communicate over two different interfaces. So that there are no gateway conflicts. Thus CGSR uses hierarchical network topology whereas other routing protocols uses flat topologies. Each node in the network maintains two tables. They are Cluster Member Table (CMT) and Routing Table (RT). CMT has target CH for each node in the network, whereas the RT has the next hop towards the destination. When a node has packets to transmit to the destination, then Cluster (hierarchical) routing protocol is invoked. The node gets token from its CH, destination CH and next hop from CMT and Rt. The route reconfiguration is necessary if there is a change in the Cluster Head and the stale entries in the Cluster Member Table and the Routing Table [8-12].

Amenity: This protocol is trouble-free in working. As CGSR is a hierarchical routing scheme, there is a partial coordination between nodes by electing cluster-heads. Hence enhanced bandwidth utilization is achievable. As the routing is performed only over the cluster heads, the size of the distance vector table is reduced. In addition to the advantages, the routing performance is also improved by routing packets through CH and gateways.

Snag: As CGSR uses the clustering technique, it spends more time in selecting the cluster head and gateways. Hence it consumes more power. The cluster-head node performs more computation and also has more communication overload than other nodes. The regular changes in the cluster head result in various path breaks. The reliability of the network may also be pretentious due to distinct points of failure of these critical nodes. If CDMA/TDMA is used by the mobile node, then it takes some time to get permission to send packets. Due to the high mobility of the nodes, the system results in instability.

Source –Tree Adaptive Routing Protocol (STAR): Source –Tree Adaptive Routing Protocol (STAR) is the hierarchical table driven routing protocol. In STAR the LORA (Least Overhead Routing Approach) is used. The concept is that, instead of finding the shortest path, LORA concentrates on finding a feasible path with less control overhead. The idea is that each node maintains the source tree, a tree which is connecting the nodes to all destinations that are known to the nodes. Then, using this own source tree and the source tree information reported by its neighbors, a partial topology graph for the node is formed. Whenever there is a link failure or any other significant changes is found in the partial topology graph, then the changes are communicated and the source tree is updated [13]. The updating is done when one of the following events occurs

- Unreachable destination
- New destination
- The possibility of permanent routing table
- Cost of paths exceeding a given threshold

Amenity: STAR protocol works well for static or slow moving nodes because of their low mobility patterns. Hence, in this case the frequency of updates is minimized which results in very low communication overhead. In addition to these the use of the LORA approach in this routing protocol reduces the average control overhead. STAR protocol can also be used to support Quality of Service.

Snag: STAR protocol requires the link layer, which is free from hidden terminal interference in order to transmit the local broadcast message. If the routing table has any invalid information, then it results in the various side effects on the protocol performance. Moreover, this protocol does not work well for high mobility patterns, fast moving nodes and for scalable networks.

Hierarchical State Routing (HSR): Hierarchical State Routing (HSR) uses the hierarchical network topology. Here the nodes are grouped into a cluster in a logical way. Cluster Heads (CHs) are arranged hierarchically where the lower level CH becomes the member of the next higher level. The cluster formed at the higher level is said to be the Supercluster. If a node wants to communicate with a node outside of their cluster, it should ask the CH to forward their packet to the next level, until the CH of the other node is in the same cluster. The packet then travels down to the destination nodes. But HSR does not specify how the cluster is formed [12, 13].

Amenity: The hierarchy information's are used to reduce the routing table size. Hence this protocol has less control overhead.

Snag: HSR has a disadvantage that the information exchange process concerned with all the levels of the hierarchy and the leader election process in every cluster makes it quite difficult for ad hoc networks.

Fisheye State Routing (FSR): Fisheye State Routing Protocol (FSR) is a flat routing scheme. It is an improvement of GSR. FSR uses the "Fisheye technology". That is the information through the focal length is visibly caught while the information outside the focal length is vague. The scope of FSR is to maintain the nodes immediate neighbourhood of the destination and its path quality information and in addition to that it requires reduced the amount of details. The routing protocol performs the following tasks.

- Neighbor Discovery (responsible for establishing and monitoring neighbor relationships)
- Information Dissemination (responsible for disseminating the Link State Packets (LSP), which contains neighbor link information to other nodes in the network)
- Route computation (responsible for computing routes to each destination using them information of the LSPs)
- Nodes stores the link state for every destination in the network
- Nodes periodically broadcast update messages to its neighbors
- Update corresponds to closer nodes propagate more frequently

Amenity: FSR is uncomplicated because it maintains updated shortest routes. In FSR each node maintains the topology map, thus there is no need of disseminating the topology information. As the update packets are exchanged among the neighbors, the bandwidth consumed is reduced.

Snag: The disadvantages of FSR are processing overhead and the storage complexity. FSR doesn't provide security compared to other protocols. It has limited scalability. As the mobility surges, the routes to distant destination become less accurate.

Table 1 illustrates the comparison of proactive routing protocols with the metrics such as construction, route computation, route maintenance, source routing, number of required tables, warehoused information, utilizing sequence numbers, utilize hello messages, apprise information, apprise period, apprise destination, technique, critical nodes and routing metric.

On-Demand Routing Protocols

Dynamic Source Routing Protocol (DSR): Dynamic Source Routing (DSR) is a self-maintaining on-demand routing protocol for wireless networks which can perform with cellular telephone systems and mobile networks with up to about 200 nodes. A DSR network can configure and organize itself independently of oversight by human administrators. Each node in the network maintains Route Cache where multiple routes to the destination are stored. DSR operates through two important mechanisms which operates entirely on-demand. They are;

Route Discovery: Source (S) node wishes to forward a packet to the destination (D) node, then the route to the destination is attained.

Route Maintenance: When S is using a discovered route to D, S may identify that the route is broken. In such cases S may use an alternate route to D (if it is known), or start another Route Discovery phase.

Table 1: Comparison of Proactive Routing Protocols

	DSDV	WRP	CGSR	STAR	FSR
Construction	Flat	Flat	Hierarchy	Hierarchy	Flat
Route Computation	Proactive/ distributed	Proactive/ distributed	Proactive/ Distributed	Proactive	Proactive
Route Maintenance	Single	Single	Single	Single	Single
Source Routing	No source routing	No source routing	No source routing	No source routing	No source routing
Number Of Required Tables	Two	Four	Two	One	Three
Warehoused Information	Distance vector	Distance table, link cost table, message and retransmission list.	Distance vector and cluster member table.	Link information.	Distance vector and path quality information.
Utilizing Sequence Numbers	Yes	Yes	Yes	Yes	Yes
Utilize Hello Messages	Yes	Yes	No	Yes	No
Apprise Information	Distance vector	Distance vector	Distance vector and cluster member table.	New destination counting loops and path cost if threshold exceeds.	Link state information
Apprise Period	Hybrid	Hybrid	Periodic	Hybrid	Hybrid
Apprise Destination	Neighbour	Neighbour	Neighbour and cluster head.	Neighbour	Neighbour
Technique	Broadcast	Broadcast	Broadcast	Broadcast	Unicast
Critical Nodes	No	No	Yes(cluster head)	No	No
Routing Metric	Shortest path	Shortest path	Shortest path	Shortest path	Based on the scope of FSR.

Consider if Source node (S) wants to forward a packet to a Destination node (D), there are two cases. The first case is explained as follows

If the route from S to D is present in the Route Cache

Then

S will add the sequence of hops to D in the header of the packets. Then S will send the packet to the first node in the sequence

If the route from S to D is not found in the Route Cache

Then

S initiates Route Discovery Protocol

The second case that when a source has packets to be sent to the destination the Route request (RREQ) packet is initiated and it is flooded throughout the network. The node which is receiving this RREQ packet, checks whether it has already forwarded and the Time To Live (TTL) counter has been exceeded. If not, then RREQ packets rebroadcasting continues till the destination is reached. Then the destination replies the source via the reverse path that the RREQ traversed. RREQ packet is stamped with the unique ID assigned by the initiator.

Amenity: As DSR is an energy efficient Routing Protocol, it does not require the periodic flooding of table update messages. Hence the bandwidth consumed is reduced. In addition to that, the routes are discovered by the Route Discovery Process whenever it is required. As each node maintains a route cache to remember routes that it has learned about. If the routes are found in the cache, then it is retrieved easily. Hence the control overhead is reduced. The route cache maintains multiple paths from source node to the destination node. If any one of the route to the destination is broken, then alternate route is chosen from Route Cache. It does not require symmetric links, Patent US 084956, titled “A Routing Protocol for General Mobile Ad Hoc Networks”.

Snag: As DSR is the Source Routing Protocol, there is a substantial amount of routing overhead and this overhead increase if the length of the path increases. If any broken link is found, then it should not be repaired locally by the route maintenance mechanism. There is also a possibility for stale entries in the Route Cache which is maintained by each node. So that inconsistencies are resulted during the route reconstruction phase. When compared to the Table driven Routing Protocol, there is a higher delay in the connection setup. DSR works well in the environment, having low mobility nodes and static nodes. But if the mobility grows, then the performance lowers swiftly.

Ad Hocon-Demand Distance Vector Routing Protocol (AODV): An Ad Hoc On-Demand Distance Vector (AODV) is also a reactive routing protocol which supports unicasting and multicasting within a uniform network. The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV is consequently deliberated as an on-demand algorithm and does not build any additional traffic for communication along the links. AODV makes use of sequence numbers to guarantee route freshness. This protocol is self-starting and loop-free as well scaling too many mobile nodes. AODV is same as DSR except the way of maintaining route information. If a node has packets to transmit to the destination, then the messages like RREQ and RREP are used. Source searches its Route Table for a route to destination. If no route, then the RREQ message is initiated with the following components

- IP addresses of Source and Destination
- Current sequence number of Source and the last known sequence number of destinations
- Broadcast ID from source. This broadcast ID is incremented each time when Source sends a RREQ message.

The node which is receiving RREQ checks in the Route Table whether this RREQ is processed. If not, then RREQ is processed and the reverse route is setup and it is entered in the route table for a source. This entity contains the IP address and current sequence number of source, number of hops to source and the address of the neighbour from whom the node got the RREQ. The entries in the Route Table have lifetime associated with it. If the route entity iis not used within its specified lifetime then it is considered to be stale entry and it is deleted [14-28].

Amenity: In AODV the routes are recognized whenever it is needed and the new route to the destination is found by using the destination sequence numbers. This is the main advantage of this protocol. In addition to this AODV does not require any central management as it is a flat routing protocol. Moreover AODV is loop free and it has less delay for connection setup. This protocol supports both unicast and multicast routing.

Snag: If the sequence number of the source is hoary then the unreliable routes are led by the intermediate nodes. And also if the intermediate nodes do not have the latest destination sequence number, thereby having fusty entries. The control overhead is heavy when there is multiple Route Reply packets are sent as a response to a single Route Request packet. If the scalability of the network grows, then several performance metrics decreases. Because of periodic beaconing the bandwidth is consumed unnecessarily. In addition, if the node's mobility increases, then the routing overhead also increases.

Temporally Oredered Routing Algorithm (TORA): The Temporally Ordered Routing Algorithm (TORA) is a source-initiated routing algorithm which is very adaptive, effective and scalable routing algorithm. By using TORA various routes have been discovered between the source and destination. When a link fails, then the control messages are only proliferated around the point of failure, but the other protocols are in need to re-initiate a route discovery process. TORA would be able to cover it up around the fact of failure. This feature allows TORA to scale up to the greater networks, but has higher overhead for smaller networks. The protocol has three basic tasks, Route creation, Route maintenance and Route erasure.

Route Creation: The route creation method renovates an undirected network into a DAG rooted at the destination by assigning directions to the links.

Route Maintenance: In case of link failures with some nodes may lose all the paths to destinations. In order to reorient the network itself in a state where each node has a path to the destination, some of the links are reversed by the persistence of route maintenance.

Route Erasure: If a network is partitioned, the route erasure mechanism removes all paths in partitions which do not contain the destination.

Each node has a quintuple associated with it,

- Logical time of a link failure
- The exclusive ID of the node that demarcated the novel reference level
- A reflection indicator bit
- A propagation ordering parameter
- The unique ID of the node

When a node wants to send a message to a destination, it broadcasts the QUERY packet to all neighbours within its broadcast range. If the destination or the node having the route information to the destination is not found, then the rebroadcasting of QUERY packet continues by propagating the UPDATE packets which are having the height information.

Amenity: An on-demand routing protocol creates a DAG only when there is a necessity. Multiple paths are created from source to destination, so that failures of nodes can be resolved quickly. Hence it is reliable in nature. This protocol is good in dense networks.

Snag: This protocol has grave control overhead. The local reconfiguration of paths results in non-optimal routes. It is not scalable by any means. There is a possibility for fluctuations to arise, especially when several sets of coordinating nodes are simultaneously discovering partitions, erasing routes and constructing new routes based on each other. Though such fluctuations are short-term and route merging will eventually arise, it poses real threat to employ TORA at its completion.

Associativity-based Routing Protocol (ABR): Associativity-Based Routing Protocol (ABR) is an on-demand routing protocol, which considers the stability of a link called the degree of association with stability. This degree of the association is measured by the number of beacons received from the other end of the link. The higher the degree of a link's stability, lower the mobility of the node at the link's other end [9, 12]. ABR works under three phases. They are Route Discovery, Route Reconstruction and Route Deletion.

Route Discovery: Each node broadcasts a query message (BQ message just to sound different) in order to find a destination. In addition to the address, the associativity ticks with respect to their neighbours are appended. The receiving node chooses the best one. Thus, at the target, multiple routes are available. It chooses the one that is best in terms of associativity ticks. If there is a tie, then the shortest path is chosen.then the destination generates the REPLY message and sends to the source. The intermediate nodes that forward this message mark the corresponding routes as valid. Thus, only one route at a given time is considered.

Route Maintenance: This phase is similar to DSR except for associative. This phase comprises both the Route Reconstruction phase and the Route Deletion phase. At the point of failure in the system while routing, the intermediate nodes will try and rediscover route. If any link failure is found, then the route is recovered partially. During this phase if any routes are found no longer valid, then they would be erased.

Amenity: In ABR fixes the link failure locally, hence there is no need to start a novel path-finding-process by the source when a cracked link seems. This protocol tries to find stable routes which results in lower overhead in some scenarios. Partial recovery may be faster in some cases.

Snag: It is imprecise if the overhead incurred in maintaining stability information is higher than the actual gains. Partial recovery may lead to longer and less stable routes. And also while repairing the route there will be a high delay when broadcasting the local query.

Signal Stability Based Adaptive Routing (SSA): Signal Stability based Adaptive Routing (SSA) is a reactive routing protocol which is different from other reactive routing protocols. This protocol works based on the signal strength parameter.

Principle of SSA: This protocol selects the routes by comparing the signal strength of the nodes and also based on the stability of the node's location. The route having the stronger connectivity is chosen as the favourite route for transmitting the packets from source node to the target node.

SSA has two cooperative protocols are;

- The Dynamic Routing Protocol (DRP)
- The Static Routing Protocol (SRP)

The Dynamic Routing Protocol (DRP): The responsibility of the DRP is that it maintains the Signal Stability Table (SST) and also the Routing Table (RT). SST stores the neighbouring node's signal strength which is got by means of periodic beaconing. DRP processes the received packet, updates the tables and passes the received packet to the static routing protocol.

The Static Routing Protocol (SRP): This protocol forwards the packet up to the transport layer if it is the receiver. If the received node is not the destination, then it looks up the routing table. If an entry is found in the table, then it forwards the packet to the appropriate next-hop, otherwise it initiates a Route Search process.

The Route Search: The Route Search process begins by propagating the Route requests throughout the network. The next hop which is receiving the Route Request should receive over the "strong channels" and also they have not yet been processed previously. The destination choses the query message which is arrived first. DRP sends the route-reply to the source by reversing the route.

Amenity: DRP results in more stable routes since signal strength indicates stability. This protocol performs well when there are adequate numbers of strong routes. There is no overhead incurred in dissemination of tables. The packet processing overhead is low.

Snag: The time over which the signal strength is averaged out might be an issue of the DRP. If any link failure is detected, then the source needs to initiate the route discovery process. The broken links can be only detected, but they cannot be repaired. Bandwidth is consumed considerably due the flooding of the RREQ messages which consequences in the delay of the route discovery process.

Location–Aided Rouitng (LAR): Location-Aided Routing Protocol (LAR) is also a reactive approach for routing, which uses the location information for routing mechanism. The location information is obtained using GPS (Global Positioning System). LAR forwards the packet towards the destination instead of forwarding it indiscretly [7, 19]. LAR is an improvement to the flooding algorithm and this protocol uses two zones, namely Expected Zone and Request Zone. These zones are explained as follows.

Expected Zone: If a source node knows that a target was at position L at some time t0, it has some notion of where the destination might be at a later time t1. If the average speed of the D is v, then S might expect that D is within a circle of radius v (t1-t0) which is centred at L. However, note that this is only an estimate. If the actual speed was higher, the node might be outside the circle. This circular region is called the "expected zone".

Request Zone: Source node defines what is known as a request zone. If the node belongs to the request zone, then the request is forwarded otherwise not. Typically, the Expected Zone would be included in the Request Zone. The nodes which are around the Expected Zone are also included in the Request Zone. Source node might not belong to the expected zone. If other nodes do not belong to the Expected Zone then it needs to forward the request towards the Expected Zone. In the initial request zone, if the destination is not found (because no route exists entirely within the request zone), then an expanded request zone may be defined. In an extreme case, the expanded request zone might be just doing flooding. There is a trade-off between latency and message overhead.

Amenity: This protocol reduces the control overhead by limiting the search area for discovering a path. LAR efficiently exploits the geographical position information. In addition to this one of the major advantages of LAR is that it increases the utilization of bandwidth.

Snag: The main disadvantage of LAR is that every node is in need of location information. If we need to apply LAR then it depends heavily on the GPS availability infrastructure or similar sources of location information. Hence, this protocol cannot be used in situations where there is no access to such information. Moreover, prior and advance information about destination node may not readily available in source node.

Flow-Oriented Routing Protocol (FORP): The Flow-Oriented Routing Protocol (FORP) is the flat structured routing protocol in which the packets are delivered before the time bound exceeds and the packets should be delivered in an ordered way. If a node wants to transmit a packet and if there is no path means, then it is said to be route failure. As a result of this route failure, the packets are dropped. The "multihop handoff" mechanism is presented by the FORP. I.e. the nodes use the mobility information to regulate the route changes while reconstructing the alternate routes.

The nodes which are receiving this Flow-REQ message, attaches its ID and last link's LET before forwarding the Flow-REQ message to the next hop. For each route, using this list of routes travelled and each hops LET information. The target node picks the least LET value and computes the RET. There is an expectation that the GPS gives the same time reference to all nodes. After choosing the route the Flow-SETUP message is transmitted along the selected path to the source node. While forwarding the packets, the LETs are added continouly by the intermediate nodes. So that the target node follows the RET prediction. The Flow-HANDOFF message is propagated all through the network when the Tc is reached. Tc is the critical time and it is calculated by finding the difference between the expiration time of the route and the delay of the arrived packet in the same route. This critical time is determined by the destination and it can be expressed as Tc=RET-Td. When the Flow-HANDOFF messages are received by the source node, the new path based on their LETs and RETs [12, 13].

Amenity: FORP protocol reduces the path breaks. Proactive route reconfiguration mechanism is embraced here, well when the topology is extremely dynamic.

Snag: This protocol raises the control overhead because of requirements of time synchronization. The dependency on the GPS infrastructure affects the operability of this protocol in the environment where such infrastructure may not be obtainable.

Table 2: Comparison of On-Demand Routing Protocols

ON DEMAND	DSR	AODV	TORA	ABR	FORP
Organization	Flat	Flat	Flat	Flat	Flat
Source Routing	Yes	No	No	Yes	Yes
Warehoused Information	Routes to preferred destination.	Next hop for desired destination.	Neighbours height.	Neighbours associations.	Updates address
Apprise Period	Event driven	Event-driven	Event-driven	Event-driven/periodic	Event-driven
Apprise Destination source	Source Neighbor	Source	Neighbors	Neighbour/	
Technique broadcast	Unicast Broadcast	Unicast	Broadcast	Unicast/	
Complete Complexity	Medium	Medium	High	High	Medium
Loop-Free	Yes	Yes	Yes	Yes	Yes
Beaconing Desires	No	No	No	Yes	Yes
Overhead	Medium	Low	Medium	High	High
Route	Multiple	Single	Single	Single	Single
Route Maintenance	Route cache	Route table	Route table	Route table	Route table
Reconfiguration of Route	Erase route and report the source.	Erase route and acquaint the source.	Link reversal and route repair.	Localized broadcast query.	Broadcast query.
Route Metric	Shortest path	Shortest path and newest route.	Shortest	Strongest associatively.	First created route.
Sleep Mode	No	No	No	No	No
Scalability	Yes	Yes	Yes	Yes	Yes
Security	No	No	Yes	Yes	Yes
Time Complexity (Route Discovery And Route Maintenance)	O(2D) and O(2D)	O(2D) and O(2D)	O(2D) and O(2D)	O(D+P) and O(B+P)	O(D+P) and O(D+P)
Communication Complexity (Route Discovery And Route Maintenance)	O(2N) and O(2N)	O(2N) and O(2N)	O(2N) and O(2A)	O(N+R) and O(A+R)	O(N+R) and O(N+R)

Table 2 illustrates the comparison of on-demand routing protocols with respect to the organization, source routing, warehoused information, apprise period, apprise destination, technique, complete complexity, loop-free, beaconing desires, overhead, route, route maintenance, reconfiguration of route, route metric, sleep mode, scalability, security, time complexity (route discovery and route maintenance) and communication complexity (route discovery and route maintenance) .

where,

- D is the diameter of the network
- N is the number of nodes in the network
- A is the number of affected nodes
- B is the diameter of the affected area
- P is the diameter of the direct path of the RREP

Hybrid Routing Protocols

Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR): CEDAR, a dividing protocol divides the network into secure partitions. Each partition has the core node. This core node uses the reactive source routing protocol to compute the route from source node to target node. The path finding process can be done in two phases.

First Phase: It finds the core path from source to destination.

Second Phase: In this phase the mid core nodes identify in each iteration until the path to a destination with required bandwidth is found.

In the first phase, if the destination is not in the core node's local topology table, then the route request is initiated by a node. Then it is forwarded to the neighbouring core nodes. If the destination is not the member of that core node, then it performs further forwarding of route request until the destination. The core nodes having the destination as the member send replies to the source[14-28].

Key components of CEDAR are;

- Establishment of self organized routing setup and its maintenance, which is used to perform route computations.

- The sink states having high-bandwidth and the stable links are disseminated.
- At core nodes the route calculation is performed using available states.

If any broken path is identified, then it should be notified to the source. So that source stops transmission and establishes the route recombination process in order to avoid the dropping of packets.

Amenity: The main advantage of CEDAR is that it performs both routing and QOS path computation very efficiently with the help of core nodes. The CEDAR is very flexible while repairing the broken links. This protocol purposes more at robustness then optimality in calculating routes.

Snag: Since the core nodes perform the routing calculation, the protocol performance is affected based on the core node movement. And also there should be significant control overhead while updating the core node information.

Zone Routing Protocol (ZRP): The Zone Routing Protocol (ZRP) provides a routing framework which is hybrid in nature, where every node maintains local routes within its zone in a pro-active method, while interzone communication is done in a reactive manner. Initially if source wants to send packets to the target node, then it should find the zone of the target whether it is interzone or intrazone. If target node is in intrazone the proactive protocol is used and the path to the target is obtained from the route table and delivers packets. If target is in interzone then reactive protocol is used by checking the zones successively, so that processing overhead is reduced [14, 20, 22].

Amenity: Since ZRP is a hybrid approach, the routing information packet floods in the network periodically, this result in the reduced control traffic. The bandwidth is reduced. This exhibits the best performance. ZRP is more appropriate than other protocols for large networks spanning diverse mobility patterns.

Snag: In ZRP there is a lack of query control. It inclines to produce greater control overhead than the proactive and reactive routing protocols. This is due to the reason overlapping between the routing zones are larger.

Zone-Based Hierarchical Link State Routing Protocol (ZHLS): ZHLS is also a hierarchical routing protocol which is hybrid in nature uses the node's location details, so that the non-overlapping zones are formed. The information about the topology inside a zone is maintained at every node in the zone and for areas, outer the zone, only the region connectivity data is maintained. ZHLS keeps the high level hierarchy for inter-zone routing packet forwarding and it is aided by the hierarchical address comprising of zone routing. Packet forwarding is aided by the reactive approach beyond the zone. A destination node's current location is identified by the zone ID of the zone in which it is present and is obtained by a route search mechanism. The inter-zone routing table is updated by executing the shortest path algorithm on the node-level topology of the zone. The node-level topology is obtained by using the intra-zone clustering mechanism, which is similar to the link state updates limited to the nodes present in the zone. Each node builds a one-hop topology by means of a link request and link response mechanism [11-13].

Amenity: As the hierarchical approach is used in ZHLS, there is considerable reduction in the storage requirements and also the overhead created by communication is also reduced. There is no overlapping of zones. And also the fact that there is no need of cluster head such that there is a reduction in traffic and single point failure. Because the topology information of the zones is disseminated to the nodes. This topology formed at the zone level is robust and it is resilient in case of path breaks.

Snag: If we want to create the zone level topology, then the geographical location is needed. But the geographical information is not offered in all the environments. This protocol does not work well for the applications where the network's geographic boundary is dynamic. Furthermore the overhead is deserved while creating and maintaining the zone level topology.

Table 3 illustrates the comparison of hybrid routing protocols with respect to the route computation, organization, route, source routing and warehoused information, apprise information, apprise period, apprise destination and technique.

Table 4 depicts the comparison of ad hoc routing protocols based on routing information such as its basic concept, protocols, benefits and drawbacks.

Table 3: Comparison of Hybrid Routing Protocols

Protocol	Route Computation	Organization	Route	Source Routing	Warehoused Information	Apprise Information	Apprise Period	Apprise Destination	Technique
CEDAR	Reactive/ Core BC Query	Hierarchy	Single	Yes	Core/ other nodes	Global/ local	Periodical/even driven	Neighbour/ core nodes	Core broadcast
ZRP	Proactive (intra)/ Reactive (inter)	Flat	Single/ Multiple	Yes	For inter zones	Local (within zone)	Periodical	Neighbor	Broadcast
ZHLS	Proactive / reactive	Hierarchy	Single	No	Local/ zone topology	Global	Periodical /even driven	Zone in all nodes	Broadcast

Table 4: Comparison of Ad Hoc Routing Protocols Based On Routing Information

Category	Basic Concept	Protocols	Benefits	Drawbacks
Proactive	Every node maintains the network topology information in the form of routing tables.	DSDV	Simple, fairly good overhead/storage, low latency in route discovery and guarantees loop free path.	Frequent updates are necessary if topology changes and lack of scalability.
		WRP	No loop formation and lower number of updates required.	Not scalable, significant overhead and messages may be large.
		CGSR	Better bandwidth utilization and easy to implement.	More power consumption, instability and path break due to frequent changes.
		STAR	Low communication overhead and reduced control overhead.	Some side effects on the performance.
Reactive	Do not maintain network topology information, they obtain necessary path whenever required by using a connection establishment process.	DSR	Reduced overhead and low route discovery cost.	Inefficiency, RREQ flooding, no energy saving, mess up routing and forwarding
		AODV	Establishes the route on-demand and less connection setup delay.	Leads to inconsistent routes, possibility for stale entries and heavy control overhead
		TORA	Creates DAG whenever required and good in dense networks.	Heavy control overhead and not scalable
		ABR	Faster and lower overhead.	Stability information is unclear and less stable routes.
		FORP	Reduces path breaks and adopted well for dynamic topology.	Increases control overhead and depends on GPS information which is not possible everywhere.
Hybrid	Combines the best features of reactive and proactive protocols. Geographic region is concerned. If nodes are within the zone proactive approach is used. If nodes are outside the zone reactive approach is used and vice versa in some cases.	CEDAR	Repair broken routes locally and computes the QOS path efficiently.	Movement of core nodes affects the performance and significant control overhead.
		ZRP	Reduces control overhead.	Overlapping of nodes occurs.
		ZHLS	Robust and requires storage requirements, reduces communication overhead.	Geographical information is required and additional overhead incurred.

CONCLUSION

In this expose we discuss the foremost ad hoc wireless routing schemes, its amenity and snag. Ad hoc networks are classified based on its routing information update mechanism. In this paper, we discussed the different classes of protocol such as proactive, reactive and hybrid routing protocols in detail. The different classes of protocol share the common goal, such as reduce control packet overhead, maximize throughput, curtail routing overhead, reduce packet loss, minimize bandwidth utilization, increase the packet delivery ratio and minimize end-to-end delay. The main differentiating factor between the protocols is the ways of finding and/or maintaining the routes between source-destination pairs. By analyzing the existing routing protocols it is clear that the ad hoc networks are doable and economically feasible to the technological shifting archetype.

REFERENCES

1. Ahmad, A. Javed, S. Khan, R. Mahmood, A. Rahim, M. Sher and M. Shoaib, 2009. A Comparative study of Mobile and Vehicular Ad Hoc Networks, International Journal of Recent Trends in Engineering, 4: 195-197.
2. Manoj, B.S. and C. Siva Ram Murthy, 2004. Ad Hoc Wireless Networks architectures and protocols Pearson Education, New Delhi.
3. Ompal Gupta, Rajiv Chechi and Vikas Malik, 2012. Classification of Routing Protocols in Manet and their Pros and Cons:A Review, International Journal of Research in IT and Management, pp: 28-31.
4. Maqbool, Beigh Bilal and M.A. Peer, 2010. Classification of current routing protocols for ad hoc networks- A Review, International Journal of Computer Applications, 8: 26-32.

5. Gill Anju and Chander Diwaker, 2012. Comparative analysis of routing in MANET, International Journal of Advanced Research in Computer Science and Software Engineering, 7: 309-314.
6. Moltchanov Dmitri A., Routing Protocols for Ad Hoc Networks, hhtp://www.cs.tut.fi /kurssit/TLT-2616.
7. Girija, M., T. Guru Baskar, P. Manickam and Dr. D. Manimegalai, 2011. Performance Comparisons of Routing Protocols in Mobile Ad Hoc Networks, International Journal of Wireless and Mobile Networks, 1: 98-106.
8. Elizabeth Royer M. and Santa Barbara Chai-Keong TOH, 1999. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, IEEE Personal Communications.
9. Panda Ipsita, 2012. A Survey on Routing Protocols of MANETS by using QOS metrics, International Journal of Advanced Research in Computer Science and Software Engineering, 10: 120-129.
10. Boukerche Azzedine, 2001. A Performance Comparison of Routing Protocols for Ad Hoc Networks, This work was supported by UNT faculty Research Grant IEEE .
11. Bakht Humayun, 2011. Survey of Routing Protocols for Mobile Ad Hoc Network, International Journal of Information and Communication Technology Research, 6: 258-270.
12. Boukerche Azzedine, Begumhan Turgut, Damla Turgut, Z. Mohammed Ahmad, Nevin Aydin and Ladislace Boloni, 2013. Routing Protocols in ad hoc Networks: A Survey, Preprint submitted to Elsevier Science.
13. Eryk Dutkiewich, Mehran Abolhasan and Tadeusz Wysocki, 2004. A Review of Routing protocols for mobile ad hoc networks, Elsevier Ad Hoc, 2: 1-22.
14. Santhi, K. and I. Sumaiya Theseen, 2012. Performance Analysis of FSR, LAR and ZRP Routing Protocols in MANET, International Journal of Computer Applications, 4: 20-24.
15. Patil, V.P., 2012. Qualitative and Quantitative Performance Evaluation of Ad hoc on Demand Routing Protocol in Manet, IOSR journal of Electronics and Communication Engineering, 5: 34-42.
16. Huhtonen Aleksandr, 2004. Comparing AODV and OLSR Routing Protocols, HUT T-110.551 seminar on Internetworking.
17. Belding-Royer, E., S. Das and C. Perkins, 2003. Ad hoc On-Demand Distance Vector (AODV) Rouitng, RFC 3561, IETF networking group.
18. Cynthi Rais D., Kuang-yeb wang, Rohit Dube and K. Satish Tripathi, 1997. Signal Stability-Based Adaptive Routing (SSA) for Ad hoc Mobile Networks, IEEE Personal Communications.
19. Nitin H., Vaidya and Young-Bac Ko, Location-Aided Routing (LAR) in Mobile Ad hoc Networks, Research report is supported in part by Texas Advanced Technology Program Granti.
20. Bharghavan, V., P. Sinha and R. Sivakumar, 1999. CEDAR: A Core-Extraction Distributed Ad hoc Routing Algorithm, IEEE Journal on Selected areas in Communications.
21. Kilinkaridis Theofanis, Routing Protocols for Wireless Ad Hoc Networks Hybrid routing protocols, http://www.tcs.hut.fi/Studies/T-79.7001/2007SPR/kilinkaridis_paper_1_draft.pdf.
22. Beijar Nicklas, Zone Routing Protocol (ZRP), Networking Laboratory, Helsinki University of Technology, Finland.
23. Lin Chunhung Richard and Jain-Shing Liu, 1999. QOS routing in ad hoc wireless networks, IEEE Journal on selected areas in Communication, 8: 1426-1438.
24. Ganapathy and Jayakumar, 2007. Performance Comparison of Mobile ad hoc network routing protocol, International Journal of Computer Science and Network Security, 11: 77-84.
25. Yau and Po-wah, 2005. Routing protocol for ad hoc networks, U.S. Patent 20050030921, Oct 02,
26. Chan Sek Yuen Pat, R. Pillai and L. Zhou, 2002.A Routing Protocol For General Mobile Ad Hoc Networks, WIPO Patent 084956A1.
27. Balachandra Mamatha, K. V. Prema and Krishnamurthy Makkithaya, Enhancing the Efficiency of MANETs by Improving the On-demand Routing Protocols and QoSmetrics, Recent Advances in Communications and Networking Technology, DOI 10.2174/2211740711201020006.
28. How Cisco IT Simplified Network Growth with EIGRP, Cisco IT Case Study, May 2013. http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/enhanced-interior-gateway-routing-protocol-eigrp/EIGRP_Case_Study.pdf.