A Survey of Unicast Routing Protocols in Mobile Ad Hoc Networks

Anuradha Banerjee

Assistant Professor, Dept. Of Computer Applications, Kalyani Govt. Engg College

DOI: https://doi.org/10.51244/IJRSI.2026.1303000148

Received: 10 March 2026; Accepted: 16 March 2026; Published: 09 April 2026

ABSTRACT

A mobile ad hoc network is a collection of mobile nodes that do not require any infrastructure for communication. The nodes co-operatively maintain network connectivity. These kinds of networks are very useful in emergency applications like battlefield communication, disaster recovery, traffic management etc. There exists an abstract electronic circle around each node within which the nodes can directly send information. This circle is called radio-circle and communication with the nodes residing within the radio-circle of a node is called single-hop communication. Radius of the radio-circle is called radio-range. The collection of nodes n_j that reside within the radio-circle of one particular ode n_i at time t, is called the set of downlink neighbours of n_i at that time t. Similarly, the collection of nodes n_j that contain n_i within their radio-circle at time t, is called the set of uplink neighbours of n_i at time t. For a communication session, if the destination resides within the radio-circle of the source then it is a single hop communication. On the other hand, if the destination is not within the radio-range of the source then a multi-hop steady path needs to be established. In this multi-hop path, several nodes act as bridge or routers that forward the packet of the source. Building such a multi-hop path from source to destination is very difficult due to random node dynamics in ad hoc networks. Design of routing protocols for ad hoc networks is very difficult due to inherent dynamism and frequent topology change. A huge number of research articles on unicast, multicast, broadcast and geocast protocols are available in the literature of ad hoc networks. Some of them are power-aware. Similarly, several clustering mechanisms as well as selfish and malicious activity detection and prevention techniques have evolved. In this paper a survey of unicast routing protocols in ad hoc networks is presented.

Keywords: Ad hoc networks, broadcast, communication protocols, multicast, survey, unicast.

SURVEY OF UNICAST ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS

Unicast routing protocols for ad hoc networks belonging to different routing philosophies are available in the literature. A proactive routing protocol determines the routes between any two nodes irrespective of the necessity of such routes. On the other hand, reactive routing protocols discover the routes on-demand i.e. only when required. Some protocols consider the nodes as peers (flat topology) while the others consider a hierarchy among nodes and only the nodes at same hierarchy are treated as peers. Routing protocols which are sensitive to the available battery power at the nodes and the energy required to transmit a packet, have also been reported in literature. Some routing protocols discover and maintain multiple paths for a given pair of nodes. The motivation and usage of those multiple paths depend on the underlying protocols.

The survey is organized as follows. Sections 2 and 3 are devoted to considering proactive and reactive routing protocols respectively. Details about zone based routing protocols appear in section 4. Sections 5 and 6 illustrate the cluster-based routing protocols and core-node based routing protocols, respectively. Power-aware protocols and link stability based routing protocols appear in sections 7 and 8 respectively. Fuzzy controlled protocols are studied in chapter 9 whereas section 10 concludes the paper.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

TYPICAL PROACTIVE ROUTING PROTOCOLS

Among the proactive routing protocols, the following are state-of-the-art.

Wireless Routing Protocol (WRP)

The wireless routing protocol (WRP) [1] is a proactive routing protocol that uses distributed Bellman-Ford Distance Vector routing algorithm. In WRP, each node maintains a distance table, routing table, a link-cost table and message-transmission list. An entry in the routing table contains the distance to a destination node in terms of number of hops, the predecessor and successor along the paths to the destination and a tag to identify its state, i.e. whether it is a simple path (single/ multi-hop path without loops), a loop or an invalid one. Storing predecessor and successor in the routing table helps to detect routing loops. A mobile node creates an entry for each neighbour in the link cost table. The entry contains the cost of link connecting the neighbour and the number of timeouts since the last error-free message was received from that neighbour.

In WRP, mobile nodes exchange routing tables with their neighbours using update messages. The update messages can be sent either periodically or whenever link state changes happen. Even if there is no change in the routing table since last update, a node is required to send a HELLO message to ensure its connectivity. Receiver of a HELLO message acknowledges with ACK message. In WRP, a node checks the consistency of its neighbours after detecting any link change. A consistency check helps to eliminate loops and speed up convergence. One important shortcoming of WRP is that it needs large memory storage to store routes to all nodes in the network proactively. It has limited scalability and is not suitable for large networks. The path with minimum number of hops is chosen as optimal.

Destination-sequenced distance vector (DSDV) routing protocol

The destination-sequenced distance vector (DSDV) [2] is a proactive unicast routing protocol which is also based on distributed Bellman-Ford Distance Vector routing algorithm. In routing tables of DSDV, an entry stores the next hop towards the destination, the cost for the routing path to it, the cost for the routing path and a destination sequence number generated by the destination itself. Sequence numbers are used in DSDV to distinguish fresh routes from stale ones and to avoid formation of loops.

The route-updates of DSDV can be either time-driven or event-driven. Every node periodically transmits updates including its routing information to its immediate neighbours. When a significant change occurs from the last update, a node can transmit its changed routing table in an event-triggered style. Moreover, DSDV has two ways of sending routing table updates. One is “full dump” update type where the full routing table is included inside the update. It could span many packets. The other way is termed as “incremental update” where only the entries that have undergone changes since last update, are transmitted. Additionally, an incremental update generally fits in one packet. Choice of the optimal path is similar to that in WRP.

Fisheye State Routing (FSR) protocol

Fisheye state routing (FSR) utilizes a function similar to fish eye. The eyes of fishes catch the nearby pixels with high detail and the detail decreases as their distance from the focal point increases. Similar to fish eyes, FSR maintains the accurate distance and path quality information about the immediate neighbouring nodes and progressively reduces detail as the distance increases. In FSR, nodes exchange link state information only with neighbouring nodes to up-to-date topology information. Link state updates are exchanged periodically in FSR and each node maintains a full topology map of the network. Link state updates corresponding to the nodes within a smaller scope are propagated with higher frequency.

FSR exhibits a better scalability concerning the network size compared to other link state protocols because it does not strive for keeping all nodes in the network on same knowledge level. Instead the accuracy of topology information is inversely proportional to the distance. This reduces the traffic overhead caused by exchanging link state information because this information is exchanged more frequently with nearby nodes than with the nodes far away. In FSR, the shortest path is elected for communication.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

Distance Routing Effect Algorithm for Mobility (DREAM)

DREAM [4] is a proactive, multi-path, location-aware routing protocol. DREAM makes use of the so called distance effect to regulate the frequency of topological updates. According to the distance effect, the greater the distance between two nodes, the lower is their relative mobility. DREAM also makes use of the mobility rate of nodes to regulate the frequency of location updates. According to the distance effect, the greater the distance between two nodes, the lower is their relative mobility. DREAM also makes use of the mobility rate of nodes to regulate the frequency of location updates; the faster a node moves, the higher is the frequency of location updates from that node. A node records the locations of all its peer nodes in a location table. Using this location information, a node forwards the data packet to a set of neighbours that lie in the direction of the destination. If no such neighbours could be selected, then the data packet is dropped. The destination responds with an ACK when it receives the data packet. The shortest path is selected as optimal.

TYPICAL REACTIVE ROUTING PROTOCOLS

The following reactive routing protocols are mention-worthy.

Dynamic source routing (DSR)

The Dynamic Source Routing (DSR) [5] is a reactive unicast routing protocol that utilizes source routing algorithm. In source routing algorithm, each data packet contains complete routing information to reach its dissemination. Additionally, in DSR each node uses caching technology to maintain route information it has learnt.

There are two major phases in DSR, (i) the route discovery phase and (ii) the route maintenance phase. When a source node needs to send a packet, it first consults its route cache. If the required route is available, the source node includes the routing information inside the data packet before sending it. Otherwise, the source node initiates a route discovery operation by broadcasting route request packets. A route request packet contains addresses of both the source and the destination and a unique number to identify the request. Receiving a route request packet, a node checks its route cache. If the node doesn't have routing information for the requested destination, it appends its own address to the route record field of the route request packet. Then, the request packet is forwarded to its neighbours. To limit the communication overhead of route request packets, a node processes route request packets that both it has not seen before and its address is not presented in the route record field. If the route request packet reaches the destination or an intermediate node has routing information to the destination, a route reply packet is generated. When the route reply packet is generated by the destination, it comprises addresses of nodes that have been traversed by the route request packet. Otherwise, the route reply packet comprises the addresses of nodes the route request packet has traversed concatenated with the route in the intermediate node's route cache.

After being created, either by the destination or by an intermediate node, a route reply packet needs a route back to the source. There are three possibilities to get a backward route. The first one is that the node already has a route to the source. The second possibility is that the network has symmetric (bi-directional) links. The route reply packet is sent using the collected routing information in the route record field, but in a reverse order as shown in Figure 1. In the last case, there exists asymmetric (uni-directional) links and a new route discovery procedure is initiated to the source. The discovered route is piggybacked in the route request packet.

In DSR, when the data link layer detects a link disconnection, a ROUTE_ERROR packet is sent back to the source. After encountering the ROUTE_ERROR packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the ROUTE_ERROR packet is transmitted to the source. DSR has increased traffic overhead by containing complete routing information into each data packet, which degrades its routing performance.

Ad hoc on-demand distance vector routing (AODV)

The Ad Hoc On-demand Distance Vector Routing (AODV) protocol [6] is a reactive unicast routing protocol for mobile ad hoc networks. As a reactive routing protocol, AODV only needs to maintain the routing

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

information about the active paths. In AODV, routing information is maintained in routing tables of the nodes. Every mobile node keeps a next-hop routing table, which contains the destinations to which it currently has a route. A routing table entry expires if it has not been used or reactivated for a pre-specified expiration time. Moreover, AODV adopts the destination sequence number technique used by DSDV in an on-demand manner.

In AODV, when a source node wants to send packets to the destination but no route is available, it initiates a route discovery operation. In the route discovery operation, the source broadcasts route request (RREQ) packets. An RREQ includes addresses of the source and the destination, the broadcast ID, which is used as its identifier, the last seen sequence number of the destination as well as the sequence number of the source node. Sequence numbers are important to ensure loop-free and up-to-date routes. To reduce the flooding overhead, a node discards RREQs that it has seen before and the expanding ring search algorithm is used in route discovery operation. The RREQ starts with a small TTL (Time-To-Live) value. If the destination is not found, the TTL is increased in following RREQs.

In AODV, each node maintains a cache to keep track of RREQs it has received. The cache also stores the path back to each RREQ originator. When the destination or a node that has a route to the destination receives the RREQ, it checks the destination sequence numbers it currently knows and the one specified in the RREQ. To guarantee the freshness of the routing information, a route reply (RREP) packet is created and forwarded back to the source only if the destination sequence number is greater than or equal to the one specified in RREQ. AODV uses only symmetric links and a RREP follows the reverse path of the respective RREP. Upon receiving the RREP packet, each intermediate node along the route updates its next-hop table entries with respect to the destination node. The redundant RREP packets or RREP packets with lower destination sequence number will be dropped.

In AODV, a node uses HELLO messages to notify its existence to its neighbours. Therefore, the link status to the next hop in an active route can be monitored. When a node discovers a link disconnection, it broadcasts a route error (RERR) packet to its neighbours, which in turn propagates the RERR packet towards nodes whose routes may be affected by the disconnected link. Then, the affected source can re-initiate a route discovery operation if the route is still needed.

Temporary ordered routing algorithm (TORA)

The Temporally Ordered Routing Algorithm (TORA) [7] is a reactive routing algorithm based on the concept of link reversal. TORA improves the partial link reversal method by detecting partitions and stopping non-productive link reversals. TORA can be used for highly dynamic mobile ad hoc networks.

In TORA, the network topology is regarded as a directed graph. A Directed Acyclic Graph (DAG) is accomplished for the network by assigning each node n_i a height metric h_i. A link directional from n_i to n_j means $h_i > h_j$. In TORA, the height of a node is defined as a quintuple, which includes (i) the logical time of a link failure, (ii) the unique ID of the node that defines the new reference level, (iii) a reflection indicator bit, (iv) a propagation ordering parameter and (v) an unique ID of the node. The first three elements collectively represent the reference level. The last two values define an offset with respect to the reference level. Like water flowing, a packet goes from upstream to downstream according the height difference between nodes. DAG provides TORA the capability that many nodes can send packets to a given destination and guarantees that all routes are loop-free.

TORA has three basic operations: route creation, route maintenance and route erasure. A route creation operation starts with setting the height (propagation ordering parameter in the quintuple) of the destination to 0 and heights of all other nodes to NULL (i.e., undefined). The source broadcasts a QRY (query) packet containing the destination's ID. A node with a non-NULL height responds by broadcasting a UPD (update) packet containing the height of its own. On receiving a UPD packet, a node sets its height to one more than that of the UPD generator. A node with higher height is considered as upstream and the node with lower height is considered as downstream. In this way, a directed acyclic graph is constructed from the source to the destination and multiple paths route may exist.

The DAG in TORA may be disconnected because of node mobility. So, route maintenance operation is an

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

important part of TORA. TORA has the unique feature that control messages are localized into a small set of nodes near the occurrence of topology changes. After a node loses its last downstream link, it generates a new reference level and broadcasts the reference to its neighbours. Therefore, links are reversed to reflect the topology change and adapt to the new reference level. The erase operation in TORA floods CLR (clear) packets through the network and erase invalid routes.

Location aided routing (LAR) protocol

The operation of LAR [8] is similar to that of DSR, except that the flooding of control packets is limited only towards the direction in which the destination node is expected to be located. In this context, the source node defines the expected zone and requested zone for a route-request. The expected zone is centred in the vicinity of the destination and is calculated purely based on the last known location, current time and average speed of the destination. The request zone is larger than the expected zone and is preferred to be as small as possible to reduce the magnitude of the redundant broadcast. The route with the shortest hop is elected for communication.

Light weight mobile routing (LMR) protocol

Like TORA, the LMR [9] protocol is based on the concept of link reversal. The main difference between LMR and TORA is their reaction to link and route failures. LMR's reaction to link failure is more pessimistic as it uses as erase and build mechanism, while TORA is more optimistic, reverses links to destination oriented directed acyclic graph (DAG) of the neck. LMR requires two passes to re-establish and converge to an alternate route, if one exists. When an alternative path exists, TORA requires only a single path to detect it. On the other hand, LMR can erase invalid routes and detect partition in a single pass; TORA requires three passes to do the same. Hence, LMR is better for sparse topologies where network partitions are more frequent whereas TORA is more suitable for dense networks. LMR is also designed to reduce control message propagation in the presence of highly dynamic mobile networking environment.

Most forward with fixed radius (MFR)

MFR [10] minimizes the umber of hops from source to destination by letting a node to always transmit to the neighbour with largest forward progress. Progress is the distance between the transmitting and receiving node projected on the line joining the transmitter and the final destination. If the progress is positive, a neighbour is said to be in the direction from transmitter to the destination. Similarly, if the progress is negative, a neighbour is said to be in the backward direction. MFR elects the path with minimum number of hops.

ZONE BASED HIERARCHICAL ROUTING PROTOCOLS

The following zone based hierarchical routing protocols are note-worthy.

Zone Routing Protocol (ZRP)

The zone routing protocol (ZRP) [11] is a hybrid routing protocol for mobile ad hoc networks. The hybrid protocols are proposed to reduce the control overhead of proactive routing approaches and decrease the latency caused by route search operations in reactive routing approaches. In ZRP, the network is divided into routing zones according to distances between mobile nodes. Given a hop distance *d* and a node N, all nodes within at most *d* hop distance from N belong to the routing zone of N. Peripheral nodes of N are N's neighbouring nodes in its routing zone which are exactly *d* hops away from N.

In ZRP, different routing approaches are exploited for inter-zone and intra-zone packets. The proactive routing approach, i.e., the Intra-zone Routing protocol (IARP), is used inside routing zones and the reactive Inter-zone Routing Protocol (IERP) is used between routing zones, respectively. The IARP maintains link state information for nodes within specified distance *d*. Therefore, if the source and destination nodes are in the same routing zone, a route can be available immediately. Most of the existing proactive routing schemes can be used as the IARP for ZRP. The IERP reactively initiates a route discovery when the source node and the destination are residing in different zones. The route discovery in IERP is similar to DSR with the exception that route requests are propagated via peripheral nodes.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

Hybrid ad hoc routing protocol (HARP)

The Hybrid Ad hoc Routing Protocol (HARP) [12] is a hybrid routing scheme, which exploits a two-level zone based hierarchical network structure. Different routing approaches are utilized in two levels, for intra-zone routing and inter-zone routing, respectively. In HARP, nodes periodically exchange topology messages with their neighbours. A forest is constructed from the network topology in a distributed way. Each tree of the forest forms a zone. Therefore, the network is divided into a number of non-overlapping dynamic zones.

A mobile node keeps routing information for all other nodes in the same zone. The nodes belonging to different zones but are within the direct transmission range are defined as gateway nodes. Gateway nodes have the responsibility of forwarding packets to the neighbouring zones. In addition to routing information for nodes in the local zone, each node also maintains those of the neighbouring zones.

As in ZRP, the intra-zone routing of HARP relies on an existing proactive scheme and a reactive scheme is used for inter-zone communication. Depending on whether the forwarding and the destination node are inside the same zone, the respective routing scheme will be applied.

Zone based hierarchical link state routing (ZHLS)

The Zone-based Hierarchical Link State routing (ZHLS) [13] is a hybrid routing protocol. In ZHLS, mobile nodes are assumed to know their physical locations with assistance from a locating system like GPS. The network is divided into non-overlapping zones based on geographical information.

ZHLS uses a hierarchical addressing scheme that contains zone ID and node ID. A node determines its zone ID according to its location and the pre-defined zone map is well known to all nodes in the network. It is assumed that a virtual link connects two zones if there exists at least one physical link between the zones. A two-level network topology structure is defined in ZHLS, the node level topology and the zone level topology. Respectively, there are two kinds of link state updates, the node level LSP (Link State Packet) and the zone level LSP. A node level LSP contains the node IDs of its neighbours in the same zone and the zone IDs of all other zones. A node periodically broadcast its node level LSP to all other nodes in the same zone. Therefore, through periodic node level LSP exchanges, all nodes in a zone keep identical node level link state information. In ZHLS, gateway nodes broadcast the zone LSP throughout the network whenever a virtual link is broken or created. Consequently, every node knows the current zone level topology of the network.

Before sending packets, a source firstly checks its intra-zone routing table. If the destination is in the same zone as the source, the routing information is already there. Otherwise, the source sends a location request to all other zones through gateway nodes. After a gateway node of the zone, in which the destination node resides, receives the location request, it replies with a location response containing the zone ID of the destination. The zone ID and the node ID of the destination node will be specified in the header of the data packets originated from the source. During the packet forwarding procedure, intermediate nodes except nodes in the destination zone will use inter-zone routing table, and when the packet arrives the destination zone, an intra-zone routing table will be used.

CLUSTER BASED ROUTING PROTOCOLS

The following cluster based routing protocols are mentioned here.

Cluster-head gateway switch routing (CGSR)

The Clusterhead Gateway Switch Routing (CGSR) [14] is a hierarchical routing protocol. The cluster structure improves performance of the routing protocol because it provides effective membership and traffic management. Besides routing information collection, updation and distribution, cluster construction and clusterhead selection algorithms are important components of cluster based routing protocols.

CGSR uses similar proactive routing mechanism as DSDV. Using CGSR, mobile nodes are aggregated into clusters and a cluster-head is elected for each cluster. Gateway nodes are responsible for communication between two or more clusterheads. Nodes maintain a cluster member table that maps each node to its respective

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

cluster-head. A node broadcasts its cluster member table periodically. After receiving broadcasts from other nodes, a node uses the DSDV algorithm to update its cluster member table. In addition, each node maintains a routing table that determines the next hop to reach other clusters.

In a dynamic network, cluster based schemes suffer from performance degradation due to the frequent elections of a clusterhead. To improve the performance of CGSR, a Least Cluster Change (LCC) algorithm is proposed. Only when changes of network topology cause two clusterheads merging into one or a node being out of the coverage of all current clusters, LCC is initiated to change current state of clusters.

Hierarchical state routing (HSR)

The Hierarchical State Routing (HSR) [15] is a multi-level cluster-based hierarchical routing protocol. In HSR, mobile nodes are grouped into clusters and a clusterhead is elected for each cluster. The clusterheads of low level clusters again organize themselves into upper level clusters, and so on. Inside a cluster, nodes broadcast their link state information to all others. The clusterhead summarizes link state information of its cluster and sends the information to its neighbouring clusterheads via gateway nodes. Nodes in upper level hierarchical clusters flood the network topology information obtained by them to the nodes in the lower level clusters.

In HSR, a hierarchical address is assigned to every node. The hierarchical address reflects the network topology and provides enough information for packet deliveries in the network. Mobile nodes are also partitioned into logical subnetworks corresponding to different user groups. Each node also has a logical address in the form of <subnet, host>. For each subnetwork, there is a location management server (LMS) which records the logical addresses of all nodes in the subnetwork. LMSs advertise their hierarchical addresses to the top level of hierarchical clusters. The routing information, which contains hierarchical addresses of LMSs, is sent down to all LMSs too. If a source node only knows the logical address of the destination node, before sending a packet, the source node first checks its LMS and tries to find the hierarchical address of the destination's LMS. Then the source sends the packet to the LMS of the destination, and the destination's LMS forwards the packet to the destination. Once the source becomes aware of the hierarchical address of the destination, it sends packets directly to the destination without consulting LMSs.

In HSR, logical addresses reflect the group property of mobile nodes and hierarchical addresses reflect their physical locations. Combining these addressing schemes may improve adaptability of the routing algorithm.

Cluster-based routing protocol (CBRP)

In the Cluster Based Routing Protocol (CBRP) [16], nodes are divided into clusters and the clustering algorithm is performed when a node joins the network. Before joining, a node is in the "undecided" state. The "undecided" node initiates the joining operation by setting a timer and broadcasts a Hello message. If a clusterhead receives the Hello message, it replies with a triggered Hello message. Receiving the triggered Hello message, the "undecided" node changes its state to "member" state. If the "undecided" node has bi-directional links to some neighbours but does not receive a message from a clusterhead before the local timer generates a timeout, it makes itself a clusterhead. Otherwise, the node remains in "undecided" mode and repeats the joining operation later. In CBRP, every node maintains a neighbour table in which it stores the information about link states (uni-directional or bi-directional) and the state of its neighbours. In addition to the information of all members in its cluster, a clusterhead keeps information of its neighbouring clusters, which includes the clusterheads of neighbouring clusters and gateway nodes connecting it to neighbouring clusters.

If a source node wants to send a packet without having any active route, it floods route request to clusterhead of its own and all neighbouring clusters. If a clusterhead receives a request it has seen before, it discards the request. Otherwise, the clusterhead checks if the destination of the request is in its cluster. If the destination is in the same cluster, the clusterhead sends the request to the destination, or it floods the request to its neighbouring clusterheads. Source routing is used during the route search procedure and only the addresses of clusterheads on the route are recorded. The destination sends a reply including the route information recorded in the request if it successfully receives a route request. If the source doesn't receive a reply in the specified time period, it starts an exponentially back-off algorithm and sends the request later.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

The shortening route is proposed in CBRP for performance optimization. Because CBRP uses a source routing scheme, a node gets all information about the route when receiving a packet. To reduce the hop number and adapt to network topology changes, nodes exploit route shortening to choose the most distant neighbouring node in a route as next hop.

Another optimization method exploited by CBRP is local repair. Whenever a node has a packet to forward and the next hop is not reachable, it checks the routing information contained in the packet. If the next hop or the hop after next hop in the route is reachable through one of its neighbours, the packet is forwarded through the new route.

CORE NODE BASED ROUTING PROTOCOLS

The following core node based routing protocols are discussed in brief.

Landmark ad hoc routing (LANMAR)

In the Fisheye State Routing protocol (FSR), every node in the network needs to maintain whole network topology information. This definitely limits its scalability. The Landmark Ad hoc Routing (LANMAR) [17] is proposed as a modification of FSR and aims to gain better scalability. In contrast to FSR, LANMAR belongs to the non-uniform routing category of mobile ad hoc networks. In LANMAR, mobile nodes are divided into predefined logical subnets according to their mobility patterns, i.e., all nodes in a subnet are prone to move as a group. A landmark node is pre-specified for every logical subset to keep track of the subnet.

Using LANMAR, every mobile node has a hierarchical address that includes its subnet identifier. A node maintains the topology information of its neighbours and all landmark nodes, which represent logical subnets. Similar to FSR, neighbouring nodes in LANMAR periodically exchange topology information and the distance vector of landmark nodes. When a source sends packets to the destination inside its neighbouring scope (i.e., the source and the destination belong to the same subnet), desired routing information can be found from the routing table of the source. Otherwise, the subnet identified in the destination node’s address will be searched. Then, according to the distance vector, the packets will be routed towards the landmark node of the logical subset.

Compared to FSR, LANMAR is more efficient because the need to exchange topology information is reduced substantially. However, LANMAR assumes that nodes are grouped into subsets according to their movement patterns and the membership of each subnet remains unchanged during the lifetime of the network. Naturally it is only suitable for specific application scenarios.

Core-extraction distributed ad hoc routing (CEDAR)

The Core-Extraction Distributed Ad Hoc Routing (CEDAR) [18] is a non-uniform routing protocol. In CEDAR, a subset of nodes in the network is identified as the "core". Core is determined according to a distributed algorithm and the number of core nodes is kept to be small. To select core nodes, neighbouring nodes periodically exchange link state messages.

Every mobile node in the network must be adjacent to at least one core node and picks this core node as its dominator. The algorithm guarantees that there is a core node at most 3 hops away from another core node. Every core node determines paths to nearby core node using localized broadcasts. The link state information is propagated only among core nodes. The propagation distance of a link state through the network is a function of its stability and bandwidth. Only the state of stable links with high bandwidth is propagated far away and the link state information includes dominators of link endpoints. Hence, in CEDAR, a core node not only knows the state of local links but also the state of stable and high bandwidth links far away.

When a source node wants to send packets to its destination, it informs its dominator core node. Then the dominator of the source finds a route in the core network to the dominator of the destination. This is done by means of a DSR-like route discovery process among core nodes. Then, core nodes involved in the previous

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

step build a route from the source to the destination. Locally available link state information is used according to the QoS requirement such like bandwidth. It is not necessary for the route to include core nodes.

Optimized link state routing (OLSR)

The optimized link state routing protocol (OLSR) [19] is a proactive non-uniform Link State routing approach. In the original Link State algorithm, each node propagates its link state information to all other nodes in the network. OLSR reduces the overhead and only fewer nodes re-broadcast link state information.

In OLSR, every node transmits its neighbour list using periodical beacons. So, all nodes can know their 2-hop neighbours. Like in CEDAR, OLSR uses an extraction algorithm for multipoint relay (MPR) selection. The multipoint relay set of a node N is the minimal (or near minimal) set of N's one-hop neighbours so that each of N's two-hop neighbours has at least one of N's multipoint relays as its one-hop neighbour. In OLSR, each node selects its MPR independently and only the knowledge of its two-hop neighbours is needed.

When a node broadcasts a message, all of its neighbours will receive the message. Only the MPRs, which have not seen the message before, rebroadcast the message. Therefore, the overhead for message flooding can be greatly reduced.

Using OLSR, each node periodically floods the link state information of its MPR set through the network. The frequency of link state updates is adjusted according to whether a change of the MPR set has been detected. If the MPR set has undergone change, the period of link state exchange is set to a minimum value. If the MPR set remains stable, the period is increased until it reaches a refresh interval value. Each node obtains network topology information and constructs its routing table through link state messages. Routes used in OLSR only include multipoint relays as intermediate nodes.

POWER AWARE ROUTING PROTOCOLS

The following power sensitive routing protocols are referred here.

Maximum residual packet capacity (MRPC) routing

Given the battery power level at all nodes, the MRPC algorithm [20] selects the path that maximizes the total number of packets that may be ideally transmitted. Such a path should sustain for a long time. Otherwise it is most likely not to transmit more packets. Hence, MRPC could be put under the category of stability based routing. Let the battery power of a node n_i at a certain time instant be B_i. Let $E_{i,j}$ be the transmission energy required by node n_i to transmit a packet over link (n_i, n_j) to node n_j. Let r be a route between the source n_s and destination n_d and it includes the link (n_i, n_j). Assuming all other flows sharing the path *r* do not transmit any further traffic, the maximum number of packets node n_i can forward over the link (n_i, n_j) to node n_j is defined as the node-link metric $C_{i,j} = B_i / E_{i,j}$. The maximum lifetime of the route r is determined by the weakest intermediate node i.e. the one with the least $C_{i,j}$ value. $Life_r = Min\{C_{i,j}\}$ where the link (n_i, n_j) $\in$ r. If Q is the set of all available n_s-n_d routes, the MRPC protocol selects the route k $\in$ Q so that $Life_k = Max\{ Life_r \mid r \in Q\}$.

Minimum battery cost routing (MBCR)

MBCR [21] aims for a route with the maximum remaining battery capacity. Let the battery power of a node n_i at a certain time instant be B_i. The battery cost function f(i) at that node is given by, $f(i) = 1 / B_i$. The battery cost C_r of a route r between the source n_s and destination n_d consisting of l nodes is given by,

$$C_r = \sum_{i=0}^{l-1} f(i)$$

If Q is the set of all available n_s-n_d routes, the MBCR protocol selects the route k $\in$ Q so that $C_k = Min\{ C_r \mid r \in Q\}$.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

Min-Max battery cost routing (MMBCR)

MMBCR [22] assigns the battery power of a route to the minimum residual battery power of a node (bottleneck node) along the route. The desired route is then the route with the maximum battery power. If there is a tie, MMBCR chooses the route with the shortest hop count. When all nodes in the network have almost identical residual battery power, MMBCR would result in frequent route changes. This is because the algorithm is sensitive to even slight changes in the residual battery power of the nodes and path selection often has to be done using the secondary criteria of hop count. When nodes have fairly different residual battery power, MMBCR would result in less frequent route changes. This is because MMBCR chooses nodes that have a larger residual battery power and these nodes are more likely to survive for a longer time in comparison to nodes that have a lesser residual battery power.

Minimum transmission power routing (MTPR)

MTPR [23] considers the energy consumed per hop (n_i, n_j) from node n_i to node n_j as the link metric. The total transmission power P_r of a route r between the source n_s and destination n_d consisting of l nodes is given by,

$P_r = \sum_{i=0}^{l-1} P(n_i, n_{i+1})$ where $P(n_i, n_{i+1})$ is the power that n_i spends in transmitting a packet to n_{i+1} in route r; $n_0 = n_s$, $n_l = n_d$ and for all i, $n_i \in r$. If Q is the set of all available n_s-n_d routes, the MBCR protocol selects the route $k \in Q$ such that $P_k = \text{Min}\{ P_r \mid r \in Q\}$

LINK STABILITY BASED ROUTING PROTOCOLS

The following link stability based routing protocols are state-of-the-art.

Associativity based routing (ABR)

The overhead of routing protocols for mobile ad hoc networks mainly comes from the dynamic changes of network topology. Some protocols have been proposed aiming to provide routing paths with longevity to reduce the maintenance overhead. The Associativity Based Routing (ABR) protocol [25] uses the degree of association stability as routing metric and tries to find routes that are expected to last longer time.

In ABR, periodic beacons are exchanged between neighbouring nodes. Every node keeps an associativity table, in which it records the connection stability between the node and its neighbours over time and space. When receiving a beacon, nodes increase the associativity tick with respect to the sender. Therefore, the link with higher associativity tick is more stable than the one with lower associativity tick. When a neighbouring node moves out, the corresponding associativity tick is reset.

There are three phases in ABR, namely, **route discovery, route reconstruction** (RRC) and **route deletion**. When a routing path is needed, the source floods a Broadcast Query (BQ) to initiate the route discovery operation. On receiving a BQ, a node checks if the same message has been seen before. If yes, it discards the BQ. Otherwise, it appends its address and its association ticks inside the BQ packet and broadcasts the BQ. When a subsequent node receives the BQ from its upstream node, it erases the associativity tick entries of its upstream node except the one concerning itself. So, when a BQ arrives at the destination, it contains the addresses of the intermediate nodes and the associativity ticks about all the links along the route. The destination selects the best route according to the longevity of all possible routing paths. The route with the shortest hop number will be chosen if there are multiple paths with the same degree of association stability. Then, the destination sends a reply packet that contains routing information of the selected path back to the source. When an intermediate node forwards the reply packet, it marks its route as valid, therefore, no duplicated data packet will be sent to the destination.

The **route reconstruction** (RRC) phase may consist of operations like partial route discovery, invalid route erasure, valid route update and new route discovery. If the movement of the source causes a RRC, a new route

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

discovery procedure will be initiated and the source sends a route notification (RN) message to erase the route entries concerning the out-of-date route. When the destination moves, its immediate upstream node erases the routing entry associating with the destination. Then, a localized query (LQ) is sent by the immediate upstream node to test if the destination is still reachable. The hop number from the node to the destination is included in the LQ. If the destination receives the LQ, it selects the best partial route and replies. Otherwise, the next upstream node will repeat the same operation, and an RN message is sent to the next upstream node to erase the invalid route and a LQ is sent to the destination. If the operation has backtracked more than halfway to the source and the destination still cannot be reachable, the source initiates a new BQ process instead of the localized query.

In ABR, a source node initiates the **route deletion** (RD) operation by broadcasting a RD message when a route is no longer needed. After receiving the RD message, all nodes along the route delete the respective route entries.

Signal stability based adaptive routing (SSR) protocol

The Signal Stability-based adaptive Routing protocol (SSR) [26] is a reactive routing protocol for mobile ad hoc networks. In SSR, the twin routing metrics are signal strength and location stability. SSR has two components: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP). All packets received are processed by DRP to update routing information before being passed to SRP. DRP maintains the Signal Stability Table (SST) and Routing Table (RT).

In SSR, nodes periodically exchange beacons with their neighbours. So, each node knows the signal strength from all its neighbouring nodes and stores this information in its SST. When a packet arrives, the SRP checks whether the host node is the destination. If yes, it passes the packet to the high layer. Otherwise, it consults the RT to find a route to the destination. If there is no route available for the destination, it initiates a route-search operation.

Route-request packets are forwarded only through the strong channels. The destination responds to the first arriving route-request packet with a route-reply message which includes the reversed route to the initiator of route-request packets. The DRPs of the nodes along the path update their RTs accordingly. In this way, the routing paths in SSR have the strongest signal stability because the route-request packets being forwarded over weak channels have been dropped at intermediate nodes.

Sometimes, it is impossible to compose a route merely by strong links and the source will time out before receiving a route-reply. To find a route, a field of route-request header is set to indicate that links over weak channel are also acceptable.

A route maintenance operation will be initiated whenever an intermediate node detects a link failure. The intermediate node sends an error message informing the source which channel has failed. Then, the source replies with an erase message to notify all nodes of the broken link. A new route-search procedure is initiated if a route to the destination is still needed.

Flow oriented routing protocol (FORP)

FORP [27] is a stable path routing protocol that utilizes the mobility and location information of the nodes to approximately predict the expiration time of a wireless link (LET). During the route-request (RREQ) flooding process, before broadcasting the RREQ to the neighbourhood, a node records the LET of the link from which the RREQ message was received. The destination receives RREQs through several paths. The Route Expiration Time (RET) of a path is the minimum of the LET values of all the constituent wireless links on the path. The destination selects the route with the maximum value of the RET and the route-reply (RREP) is sent on the selected route. FORP falls under the category of stability-based routing.

Node velocity based stable path (NVSP) routing protocol

NVSP [28] is the only beaconless stable path routing protocol that has been proposed for ad hoc networks. NVSP is an on-demand routing protocol that uses the RREQ-RREP cycle to discover routes whenever

required. During the propagation of the RREQ messages, every forwarding node includes its current node velocity information in the RREQs. The bottleneck velocity of a path is the maximum of the velocity of an intermediate node on the path. The destination chooses the path with the smallest bottleneck velocity and sends a RREP packet on the chosen path. The end-to-end delay and the energy consumed per data packet incurred by NVSP are significantly lower than that of FORP and are lower or equal to that incurred for DSR.

FUZZY LOGIC BASED ROUTING PROTOCOLS

Fuzzy routing protocol

This routing scheme [99] for ad hoc networks applies fuzzy logic to differentiated resource allocation, considering traffic importance and network state. Messages are routed over zero or more maximally disjoint paths to the destination. Important packets are forwarded redundantly over multiple disjoint paths for increased reliability, while less important traffic are suppressed at the source.

Multi-metric routing decisions for ad hoc networks using fuzzy logic

The multi-metric based routing scheme (MMR) [100] is mainly based on the DSR [5] protocol. Among all the routes discovered in DSR, only some are stored in route cache depending upon their performance with respect to link strength, energy available at link vertices and number of hops in a path. Nodes periodically transmit beacons as a means of identifying themselves. These beacons are counted and used as a measure of connectivity, nodes with a high beacon count are considered to be stable and as such can be used to route packets through.

CONCLUSION

The detailed survey about ad hoc networks unicast protocols, presents illustrative discussion about proactive, reactive, energy efficient, core based etc. protocols generating a clear picture of research works performed in that domain so far. This will help the researchers in extracting the scope for further exploration and research.

REFERENCES

1. Murthy, S. and J.J. Garcia-Luna-Aceves, An Efficient Routing Protocol for Wireless Networks, ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97
2. C. E. Perkins and P. Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers, ACM Computer Communication Review, Vol. 24, No.4, (ACM SIGCOMM'94) Oct. 1994, pp. 234 - 244
3. G. Pei, M. Gerla and T.-W. Chen, Fisheye State Routing in Mobile Ad Hoc Networks. In Proceedings of the 2000 ICDCS Workshops, Taipei, Taiwan, Apr. 2000, pp. D71-D78
4. S. Basagni, I. Chlamtac, V. Syrotiuk and B. WoodWard, A Distance Routing Effect Algorithm for Mobility (DREAM). Proc. 4th MOBICOM, 1998
5. D. Johnson, D. A. Maltz, Dynamic source routing in ad hoc wireless networks, in Mobile Computing (T. Imielinski and H. Korth, eds.), Kluwer Acad. Publ., 1996
6. C.E. Perkins and E.M. Royer. Ad hoc on demand Distance Vector routing, mobile computing systems and applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, 1999, pp.90 - 100
7. V. Park, and S. Corson, Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification IETF Internet draft, 1997
8. Y. B. Ko and N. H. Vaidya. Location Aid Routing (LAR) in mobile ad hoc networks. In Proc. ACM/IEEE MOBICOM, Oct. 1998
9. M. S. Corson and A. Ephremides, A Distributed Algorithm for Mobile Wireless Networks, Wireless Networks, Vol. 1, pp. 61 – 81, 1995.
10. T-C. Hou and V. O. K. Li, "Transmission Range Control in Multi-hop Packet Radio Networks," *IEEE Transactions on Communications*, Vol. 34, No. 1, pp. 38 – 44, Jan. 1986
11. Z. J. Haas and M.R Pearlman, The Zone Routing Protocol (ZRP) for ad hoc networks. IETF Internet draft, August 1998

12. Navid Nikaein, Christian Bonnet and Neda Nikaein, HARP - Hybrid Ad Hoc Routing Protocol, in proceeding of IST 2001: International Symposium on Telecommunications, Iran/Tehran 2001
13. M. Joa-Ng and I-Tai Lu, A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks, IEEE on Selected Areas in Communications, vol. 17, no. 8, pp. 1415 1425, 1999
14. C. C. Chiang, T. C. Tsai, W. Liu and M. Gerla, Routing in clustered multihop, mobile wireless networks with fading channel, The Next Millennium, The IEEE SICON, 1997
15. A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, Scalable routing strategies for ad hoc wireless networks. IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, August 1999, pp. 1369-1379
16. Mingliang Jiang, Jinyang Li and Y. C. Tay. Cluster Based Routing Protocol (CBRP), Internet draft,draft-ietf- manet-cbrp-spec-01.txt
17. G. Pei, M. Gerla, and X. Hong, LANMAR: Landmark routing for large scale wireless ad hoc networks with group mobility. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), pp. 11-18, 2000
18. P. Sinha, R. Sivakumar and V. Bharghaven, CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm. IEEE INFOCOM, March 1999
19. P. Jacquet, P. Muhlethaler, and A. Qayyum, Optimized Link State Routing Protocol, IETF MANET, Internet draft 1998
20. A. Misra and S. Banerjee, MRPC: Maximizing Network Lifetime for Reliable Routing in Wireless Environments, Proceedings of WCNC, 2002
21. C.-K. Toh, "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks," IEEE Communications Magazine, June 2001
22. Murthy, S. and J.J. Garcia-Luna-Aceves, An Efficient Routing Protocol for Wireless Networks, ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97
23. Natarajan Meghanathan, Survey and taxonomy of unicast routing protocols for mobile ad hoc networks, International journal of applications of graph theory in wireless ad hoc and sensor networks, vol 1 no. 1, Dec 2009
24. N. Meghanathan, "Energy Consumption Analysis of the Stable Path and Minimum Hop Path Routing Strategies for Mobile Ad hoc Networks," International Journal of Computer Science and Network Security, Vol. 7, No. 10, pp. 30 – 39, October 2007
25. C.-K. Toh, Associativity Based Routing For Ad Hoc Mobile Networks . Wireless Personal Communications Journal, Special Issue on Mobile Networking and Computing Systems, pp. 103-139, March 1997
26. R. Dube et al., Signal stability based adaptive routing for ad hoc mobile networks, IEEE Pers. Comm., February 1997, pp. 36-45
27. W. Su, S-J. Lee and M. Gerla, Mobility Prediction and Routing in Ad hoc Wireless Networks, *International* Journal of Network Management, Vol. 11, No. 1, pp. 3-30, 2001
28. N. Meghanathan, A Beaconless Node Velocity-based Stable Path Routing Protocol for Mobile Ad hoc Networks, Proceedings of the IEEE Sarnoff Symposium Conference, Princeton, NJ, March 30- April 1, 2009
29. M. Liu, R. Talpade, A. McAuley, and E. Bommaiah, AMRoute: Ad-hoc multicast routing protocol. Technical Report, CSHCN T. R. 99-1, University of Maryland.
30. Murthy S., J.J. Garcia-Luna-Aceves, An efficient routing protocol for wireless networks, ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-197
31. C.W. Wu, Y.C. Tay, AMRIS: a multicast protocol for ad hoc wireless networks. Proceedings IEEE MILCOM'99, Atlantic City, Nov. 1999
32. S.J. Lee, M. Gerla, C.C. Chiang, On Demand Multicast Routing Protocol. Proceedings of IEEE WCNC'99, New Orleans, pages 1298-1302, Sept 1999
33. P. Dhammika, K. Minseok, R-ODMRP: Resilient On-demand Multicast Routing Protocol, 21st International Conference on Advanced Information Networking and Applications Workshop, vol.2, pp.85-92, 2007
34. Y. Soon, P. joon Sang and G. Mario, E-ODMRP: Enhanced ODMRP with Motion Adaptive Refreash, Journal of Parallel Distribution Computering, vol. 68, pp. 1044-1053

35. J. Garcia-Luna-Aceves and E.L. Madruga, The Core-Assisted Mesh Protocol. The IEEE Journal on Selected Area in Communication, vol.17, no.8, Aug. 1999, pp1380-1394.
36. E. M. Royer and C. E. Perkins, Multicast operation of the Ad-hoc On-demand Distance Vector routing protocol. Proceedings of ACM/IEEE MOBICOM'99, Seattle, pages 207-218, August 1999
37. S. Zahoor Ul Huq et. Al, EMMR: A Multicast Routing Protocol for Mobile Ad Hoc Networks, International Journal of Computer Science and Network Security, vol. 9, no. 4 April 2009
38. A. B. Manouer et. Al., OPHMR: an optimized polymorphic hybrid multicast routing protocol for MANETs, IEEE Transaction on Mobile Computing, vol. 6, no. 5, pp. 503-514, 2007
39. Zeyad M. Alfawaer et. Al., A Novel Multicast Routing Protocol For Ad Hoc Networks, American Journal of Applied Sciences, vol. 4, no. 5, pp. 333-338, 2007
40. C. Gui and P. Mohapatra, "Efficient Overlay Multicast for Mobile Ad Hoc Networks," In the Proceedings of IEEE WCNC'03, New Orleans, March 2003
41. Ravindra Vaishampayan and J.J. Garcia-Luna-Aceves, Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks, In the Proceeding of first Internation Conference on Mobile Ad hoc and Sensor Systems (MASS), 2004, Florida, USA.
42. S. K. Das, B. S. Manoj, and C. S. R. Murthy, "A Dynamic Core Based Multicast Routing Protocol for Ad Hoc Wireless Networks," in ACM MobiHoc, June 2002
43. Seungjoon Lee and Chongkwon Kim,"Neighbour supporting ad hoc multicast routing protocol ", In the Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing, Boston, Massachusetts, USA, 2000
44. J.G. Jetcheva and D.B. Johnson, "Adaptive demand-driven multicast routing in multi-hop wireless ad hoc network," Second Symposium on Mobile Ad Hoc Networking and Computing, pp.33–44, 2001
45. P. Sinha et. Al, MCEDAR: Multicast Core Extraction Distributed Ad Hoc Routing, In proceedings of IEEE WCNC 1999, pp. 1313 – 1317
46. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.61.9906
47. A. Sabari, K. Duraiswamy, Ant-based Adaptive Multicast Routing protocol (AAMRP) for ad Hoc networks, International Journal of Computer Science and Network Security, vol. 6, no. 2, 2009
48. www.ece.rutgers.edu/~pompili/paper/MED04-**PPMA**.pdf
49. B. Williams, D.P. Mehta, T. Camp and W. Navidi, "Predictive models to rebroadcast in mobile ad hoc networks", IEEE Transaction on Mobile Computing, vol. 3, no. 3, September 2004
50. W. Chen, W. Sun, Z. Zhang, Y. Qin, "A lifetime aware broadcast protocol in ad hoc networks", In Proceedings of International Conference on Wireless, Mobile and Sensor Networks 2007, pp. 620-623
51. V. Drabkin, R. Friedman, M. Segal, "Efficient Byzantine Broadcast in Wireless Ad Hoc Network", In Proceedings of International Conference on Dependable Systems and Networks 2005, pp. 160-169
52. D. Michael, "Intelligent Broadcasting in Mobile Ad Hoc Networks: Three Classes of Adaptive Protocols", Eurasip Journal on Wireless Communications and Network, vol. 2007, Article id 10216, doi: 10.1155/2007/10216
53. F. Foroosan, K. Tepe, A high performance cluster based broadcasting algorithm for wireless ad hoc networks based on a novel gateway selection approach" , International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Canada, 2005, pp. 65-70
54. P. Kyasanur, R. Chaudhury, I. Gupta, "Smart Gossip: An adaptive gossip-based broadcasting service for sensor networks", IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2006, Canada
55. L. Tan, X. Zhan, J. Lie, F. Zhao, "A novel tree-based broadcast algorithm for wireless ad hoc networks", International Journal on Wireless and Mobile Computing, vol. 1, no. 2, 2006, pp. 156-162
56. A. Rahman, E. Hoque, F. Rahman, S.K. Kundu, "Enhanced Partial Dominant Pruning (EPDP) based broadcasting in ad hoc networks", Journal of Networks, vol. 4 no. 9, Nov 2009, pp. 895-905
57. J. Cartigny, F. Ingelrest, D. Simplot, I. Stojmenovis, "Localized LMST and RNG based minimum energy broadcast protocols in ad hoc networks", Ad Hoc Networks 2005, pp. 1-16
58. W. Lou, J. Wu, "Double Covered Broadcast (DCB): A Simple Reliable Broadcast Algorithm in Ad Hoc Networks", http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.58.2687, 2004
59. N. Karthikeyan, V. Palanisamy, K. Duraiswamy, "Optimum density based model for probabilistic flooding protocol in mobile ad hoc networks", European Journal of Scientific Research, vol. 39 no. 4, 2010, pp. 577-588

60. J. Lipman, P. Boustead and J. Chicharo, "Reliable optimistic flooding in ad hoc networks", IEEE 6th Symposium on Emerging Technologies on Mobile and Wireless Communication, China, May 31-June 2, 2004
61. www.citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.9481
62. G. wang, D. Lu, W. Jia and J. Chao, "Reliable gossip based broadcast protocol in mobile ad hoc networks", Lecture Notes in Computer Science 2005, Volume 3794/2005, 207-218, DOI: 10.1007/11599463_21
63. Y.C. Hu, A Perrig and D.B. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, Dept. of Computer Science, Rice University, Technical Report: TR01-384, Dec. 2001
64. A. Perrig, R. Canetti, D. Tygar and D. Song, The TESLA Broadcast Authentication Protocol, Cryptobytes, vol. 5 no. 2, RSA Laboratories, 2002
65. F. Kargl, A Klenk, S. Schlott and M. Weber, Advanced Detection of Selfish and Malicious Nodes in Ad Hoc Networks, 1st European Workshop on Security in Ad Hoc and Sensor Networks (ESAS 2004), Germany
66. Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields. A Secure Routing Protocol for Ad Hoc Networks In Proceedings of the 10th Conference on Network Protocols (ICNP), November 2002
67. M. G. Zapata, Secure Ad Hoc On-demand Distance Vector (SAODV) Routing, INTERNET-DRAFT, August 2002
68. S. Yi, P. Naldurg, and R. Kravets Security-Aware Ad hoc Routing for Wireless Networks The Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001
69. Panagiotis Papadimitratos and Zygmunt J. Haas Secure Routing for Mobile Ad hoc Networks SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002
70. Pietro Michiardi, Refik Molva Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks in Communication and Multimedia Security Conference, 2002
71. Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-hoc NeTworks In Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, June 2002
72. Sergio Marti and T. J. Giuli and Kevin Lai and Mary Baker. Mitigating routing misbehaviour in mobile ad hoc networks. Mobile Computing and Networking (2000).
73. L. Buttyan and J. P. Hubaux, Enforcing service availability in mobile ad-hoc WANs, in IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, August 2000
74. L. Buttyan and J. P. Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks, ACM Journal for Mobile Networks (MONET) special issue on Mobile Ad Hoc Networks, summer 2002
75. S. Zhong, Y. Yang and J. Chen, Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad Hoc Networks, In proceedings of IEEE INFOCOM 2003
76. M. Kargar, M. Ghodsi, Truthful and Secure Routing in Ad Hoc Networks with Malicious and Selfish Nodes, International Journal of Security and its Applications, vol. 3 no. 1 January 2009, pp. 117-129
77. A. Rajaram, Dr. S. Palaniswami, Malicious Node Detection System for Mobile Ad Hoc Networks, International Journal of Computer Science and Information Technologies, vol. 1, no. 2, 2010, pp. 77-85
78. S. Dhanalakshmi, Dr. M. Rajaram, A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANETS, International Journal of Computer Science and Network Security, vol. 8, no. 10, October 2008
79. M.R. Babu, S. Selvan, An Energy Efficient Secure Authenticated Routing Protocol for Mobile Ad Hoc Networks, American Journal of Scientific Research, Issue 4 (2010), pp. 12-22
80. S. Gupta, C. Kumar, A Novel Routing Strategy For Ad Hoc Network With Selfish Nodes, Journal of Telecommunications, vol. 3, issue 2, July 2010
81. M.T. Rafaei, V. Srivastava, L. De Silva, M. Eltoweissy, A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks, in Proceedings of 2nd IEEE International Conference on Mobile and Ubiquitous Systems, Networking and Services (MobiQuitous 2005)
82. Seung-Chul M. Woo and Suresh Singh, Scalable Routing Protocol for ad hoc networks, Wireless Networks, vol. 7 no. 5, pp. 513-529

83. USCG Navigation Center GPS Page, January 2000, http://www.navcen.uscg.mil/gps/default.html
84. S.M. Das, H. Pucha, Y.C. Hu: Performance of Scalable location Services for Geographic Ad Hoc Routing, IEEE INFOCOM 2007
85. C.T. Cheng et. Al., SLALoM: A Scalable Location Management for Large Mobile Ad Hoc Networks, In Proceedings of Wireless Communications and Networking Conference 2005
86. Tetsuro Ueda et. Al., "ACR: An Adaptive Communication Aware Routing Through Maximally Zone-disjoint Shortest Paths In Ad Hoc Wireless Networks With Directional Antenna", Journal of Wireless Communications and Mobile Computing, 2007
87. http://pcl.cs.ucla.edu/projects/glomosim/
88. J.H. Chang, L. Tassiulus, Energy conserving routing in ad hoc networks, Proceedings of INFOCOM 2009, Tel Aviv, Israel
89. Basu P., Khan N. & Little T. (2001), A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks, in Proceedings of IEEE ICDC 2001, pp. 413-418, Arizona, USA
90. Basagni, S., Mastrogiovanni, M., Panconesi, A., & Petrioli, C. (2006). Localized Protocols for Ad Hoc Clustering and Backbone Formation: A Performance Comparison. IEEE Transactions on Parallel and Distributed Systems, 17(4), 292-306.
91. www.antd.nist.gov/wahn_goals.shtml
92. Chatterjee, M., Das, S. K., & Turgut, D. (2002). WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks. Cluster Computing, 5(2), 193-204.
93. J.Y. Yu & P.H.J. Chong (2005). A survey of Clustering Schemes for Mobile Ad Hoc Networks, IEEE Communications Survey and Tutorials, vol. 7 no. 1, 32-48
94. Sheu, P., & Wang, C. (2006). A Stable Clustering Algorithm Based on Battery Power for Mobile Ad Hoc Networks. Tamkang Journal of Science and Engineering, 9(3), 233-242
95. http://www.cs.ou.edu/~database/documents/Handbook-Chapter-08.pdf
96. S. Chinara & S.K. Rath (2009). TACA: A Topology Adaptive Clustering Algorithm for Mobile Ad Hoc Networks, Proceedings of ICWN 2009, Las Vegas
97. M. Tiwari et. Al (2010). A Bird Fly Inspired Clustering Based Routing Protocol For Mobile Ad Hoc Networks, International Journal of Computer Science and Network Security, vol. 10 no.3
98. http://dpse.eas.asu.edu/tdsm/papers/QShine07.pdf
99. http://wireless.nmsu.edu/wireless/papers/fuzzy.pdf
100. http://www.aws.cit.ie/personnel/papers/paper243.pdf
101. Anuradha Banerjee, Paramartha Dutta, Alternative Node Based Energy Depletion and Expected Residual Lifetime Balancing Method For Mobile Ad Hoc Networks, International Journal of Advanced Networking and Applications, vol. 5 no. 2, pp. 1886-1892, 2014
102. Anuradha Banerjee, Paramartha Dutta, Delay-efficient, Energy and Velocity-conscious Non-preemptive Scheduler for Mobile Ad Hoc Networks, International Journal of Advanced Networking and Applications, vol. 5 no. 4, pp. 2002-2010, 2014
103. Anuradha Banerjee, Cost Effective Route Discovery (CERD) For Mobile Ad Hoc Networks, International Journal of Advance Research in Science and Engineering, Vol. 04, Issue 01, march 2015
104. Anuradha Banerjee, FESA: Fuzzy-controlled Energy-efficient Selective Allocation and Reallocation of Tasks Among mobile Robots, International Journal of Advance Research in Science and Engineering, Vol. 04, Issue 01, march 2015
105. Anuradha Banerjee, Fuzzy-controlled Rebroadcasting Based on 2-hop Downlink Neighborhood Information (FR-2N) In Mobile Ad hoc Networks, International Journal of Applied Engineering Research (Scopus), vol. 10 no. 81, pp. 114-120 2015
106. Anuradha Banerjee, Paramartha Dutta, Cost-Effective routing Protocols Based on 2-hop Neighborhood Information (2NI) in Mobile Ad Hoc Networks, International Journal of Applied Networking and Applications, vol. 7 issue 3, pp. 2771-2778, 2015
107. Anuradha Banerjee, Paramartha Dutta Abu Sufian: "Fuzzy Controlled Scheduling on Real Time Data Packet (FSRP) in Mobile Ad-hoc Network", International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 5, pg- 507-5013, May-2016
108. A. Sufian, A. Banerjee, P. Dutta, "Survey of Various Real time and Non Real time Scheduling algorithms in Mobile Ad-hoc Networks" International Conference on Industry Interactive Innovations in Science, Engineering and Technology (I3SET-2K16), Proceedings published in Springer series of Lecture Notes in Networks and Systems (LNNS)

109. Abu Sufian, Anuradha Banerjee and Paramartha Dutta: "Fuzzy-controlled Scheduling of Route-Request Packets (FSRR) in Mobile Ad Hoc Networks", Indian Journal of Science and Technology, Vol 9(43), DOI: 10.17485/ijst/2016/v9i43/104384, November 2016
110. Anuradha Banerjee, Paramartha Dutta and Abu Sufian: "Fuzzy Route Switching for Energy Preservation (FEP) in Ad Hoc Networks", Indian Journal of Science and Technology, Vol 9(43), DOI: 10.17485/ijst/2016/v9i43/104383, November 2016
111. Anuradha Banerjee, Paramartha Dutta and Abu Sufian: "EMR-PL: Energy-efficient multipath routing based on link life prediction in ad hoc networks", Journal of Information and optimization Science (Taylor and Francis), vol. 39, issue 1, 2018
112. Anuradha Banerjee, Shirshadipta Chowdhury, "Expected Residual lifetime based Ad Hoc On-demand Multipath Routing Protocol (ERL-AOMDV) In Mobile Ad Hoc Networks", accepted for publication in International Journal of Information Technology (Springer), 2018
113. Anuradha Banerjee, D.M. Akbar Hussain, SD-EAR: Energy Aware Routing in Software Defined Networks, Applied Sciences (SCI Indexed, Impact factor: 1.627), Vol 8(7), 2018
114. Anuradha Banerjee, Paramartha Dutta, Abu Sufian, Movement Guided Management of Topology (MGMT) With Balanced Load In Mobile Ad Hoc Networks, accepted for publication in International Journal of Information Technology (Springer), 2018
115. Anuradha Banerjee, Paramartha Dutta, Abu Sufian, Fuzzy Controlled Energy Efficient Single Hop Clustering Scheme (FESC) In Mobile Ad Hoc Networks, accepted for publication in International Journal of Information Technology (Springer), 2018
116. Anuradha Banerjee, D.M. Akbar Hussain, "Experience Based Efficient Scheduling Algorithm (EXES) For Serving Requests in Cloud Using SDN Controller", Accepted in Journal of Intelligent and Fuzzy Systems (SCI Indexed, Impact Factor: 1.412), IOS Press, Netherlands, 2018
117. Sufian, A., Banerjee, A. & Dutta, P. "Energy and Velocity Based Tree Multicast Routing in Mobile Ad-Hoc Networks"Wireless Pers Commun (Springer, Impact Factor : 1.612) (2019). https://doi.org/10.1007/s11277-019-06378-y
118. A. Banerjee, A. Sufian, Smart-Green-Mult (SGM): overhear from topological kingpins in software defined wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing (SCI indexed, impact factor: 4.594), May 2020
119. Ghosh, S.; Mal, K. Energy-Efficient Routing in MANETs: A Review of Recent Advancements. Ad Hoc Netw. 2024, 132, 102682
120. Chen, J.; Zhang, Y.; Liu, W. Enhancing the Performance of AODV Protocol in Heterogeneous MANETs. Wirel. Netw. **2022**, 28, 2175–2190.
121. Zhao, J.; Wu, H. A Survey on Routing Protocols in Mobile Ad Hoc Networks: Challenges and Solutions. J. Netw. Comput. Appl. **2023**, 204, 103405.
122. Srilakshmi, U.; Veeraiah, N.; Alotaibi, Y.; Alghamdi, S.A.; Khalaf, O.I.; Subbayamma, B.V. An Improved Hybrid Secure Multipath Routing Protocol for MANET. IEEE Access **2021**, 9, 163043–163053