I. J. Computer Network and Information Security, 2013, 12, 68-79
Published Online October 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.12.09

Survey of Current Multipath Routing Protocols for Mobile AD Hoc Networks

P.Periyasamy
Department of Computer Science and Applications, Sree Saraswathi Thyagaraja College, Pollachi - 642 107, Tamil Nadu, India.
pereee@yahoo.com

Dr.E.Karthikeyan
Department of Computer Science, Government Arts College, Udumalpet - 642 126, Tamil Nadu, India.
e_karthi@yahoo.com

***Abstract* —** A Mobile Ad hoc NETwork (MANET) is a wireless communication network with minimum physical infrastructure with diverse communication applications. Mobility and Multihopping are the main characteristics of MANET. Multipath routing protocols establish multiple routes between nodes. The construction of multiple routes should be done with minimum overhead and bandwidth consumption. The purpose of this article is to analyze the characteristics and functionality of various multipath routing protocols and to do the performance comparison between these multipath routing protocols to choose the best among them to use in large networks.

***Index Terms* —** MANET, route failure, load balancing, mobility, multihop, multipath, routing protocols

I. Introduction

A MANET is a collection of mobile nodes by wireless links forming a dynamic topology without much physical network infrastructure such as routers, servers, access points or cables or centralized administration. Each mobile node is acting as a router as well as a node. The issues involved in MANET [1,29] are: (i) unpredictable link properties expose packet collision and signal propagation, (ii) node mobility creates dynamic topology, (iii) limited battery life of mobile devices, (iv) hidden and exposed terminal problems occur when signals of two nodes are colliding with each other. (v) route maintenance is very difficult because of changing behavior of the communication medium, and (vi) insecurity is the most important issue of MANET.

Multipath routing protocols are needed to send communication from source to destination by having backup routes. During end-to-end communication, if a primary route fails, the backup routes are used for efficient delivery of messages at their destination. The ad hoc multipath routing protocols can be classified into three major groups based on the routing strategy as shown in Fig.1.

The rest of this paper is organized as follows: In section II, the characteristics and functionality of various proactive multipath routing protocols are analysed; in section III the characteristics and functionality of various reactive multipath routing protocols are analysed; in section IV the characteristics and functionality of various hybrid multipath routing protocols are analysed and finally in section V the conclusion is given.

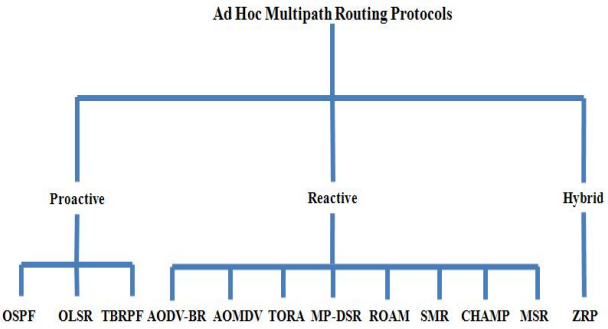

Figure.1. Classification of Multipath Routing Protocols for Mobile Ad Hoc Networks

II. Proactive Multipath Routing Protocols

In proactive/table-driven multipath routing protocols, each node maintains up-to-date routing information to each and every node in the network. The routing information is stored in a number of different tables. These tables are periodically updated when the network topology changes in order to maintain a consistent network view. The way of detecting and updating routing information is kept in a routing table and the number of routing tables differ from each of these protocols. This section describes the characteristics and functionality of the existing proactive multipath routing protocols.

A. Open Shortest Path First (OSPF)

The two primary characteristics of OSPF [3] is an open protocol, which means its specification is in the public domain and it is a protocol based on the *shortest path first* (SPF) algorithm, which in turn is termed as *Dijkstra's* algorithm. Unlike other protocols which use distance-vector or Bellman-Ford technology, OSPF uses link-state

or SPF-based technology in order to build and calculate the shortest path to all well-known destinations. The link-state database is formed in the network by flooding the individual *link-state advertisements* (LSAs) which describes small pieces of the routing domain. The routers in OSPF have identical link-state databases, which are synchronized through a reliable flooding algorithm. The link-state database is used for each router to build a routing table by calculating a shortest-path tree, rooted at the router itself.

In OSPF, the existence of several equal-cost routes to a destination, the traffic is distributed equally among them. These multiple routes need not to be node-disjoints or even link-disjoints. Each node listens its neighbours via HELLO messages. These messages are not only used for acquiring neighbours, but also used to keep-alive packets

The properties [30] of OSPF are: (i) working based on Shortest-Path First (SPF or Dijkstra's algorithm), (ii) link-state protocol, (iii) common link-state database formed by individual Link-State Advertisements (LSAs), (iv) each node computes a shortest-path tree from the link-state database, (v) each node periodically sends out a LSA and (vi) multiple paths from source to destination are possible.

B. Optimized Link State Routing (OLSR)

The OLSR [4,5,6] protocol is an optimization of a pure link state protocol by compacting the size of the control packets that contain link-state information and reducing the number of transmissions needed to flood those control packets to the entire network. The multipoint relaying technique is used to flood its control messages in an efficient and economic way. The main aim of multipoint relays is to minimize the flooding of broadcast packets in the network by reducing the number of retransmissions in the same region. In OLSR, each node selects a set of 1-hop neighbour nodes, called the multipoint relays (MPRs) of that node, which retransmits its packets.The neighbours of any node N do not retransmit the broadcast packets received from node N if they are not in the MPR set whereas they can read and process packets. Each node maintains a set of neighbours for retransmission of packets called MPR Selectors.

All the neighbour nodes (radio range) within two hops away from N must be covered by the MPRs of N. These two-hop neighbourhood of N must have bi-directional links with the MPRs of N. The selection of MPR around a node N is shown in Fig.2.

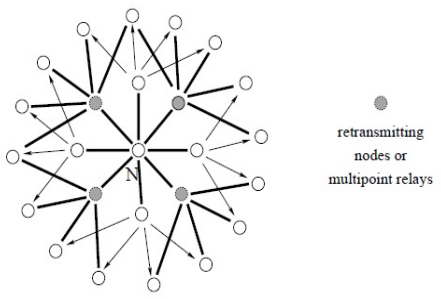

Figure.2. Selection of MPR around node N.

Each node N periodically broadcasts HELLO messages to its one-hop neighbours for selecting the MPRs. Each HELLO message is having a list of neighbours that are connected to N via bidirectional links and it also have the list of neighbours that are heard by N but are not connected via bidirectional links. On receiving the HELLO message, each node can learn the link-state information of all neighbours up to two hops.

The MPRs are selected via the information contained in a neighbour table. Each node is broadcasting the specific control messages called Topology Control (TC) messages. Each TC messages originating from a node N has the list of MPRs of N with a sequential number and is forwarded only by the MPRs of the network. Each node maintains a topology table which is constructed from the information obtained from the TC messages for representing the topology of the network. Each node also maintains a routing table in which each entry in the routing table corresponds to an optimal route, in terms of the number of hops, to a particular destination. Each entry is having a destination address, next-hop address, and the number of hops to the destination. The routing table is constructed based on the information available in the neighbour table and the topology table. Each route is a sequence of hops through the multipoint relays from every source to destination.

The properties [30] of OLSR are: (i) optimization of pure link-state protocol, (ii) neighbours are discovered via HELLO messages containing all neighbours and link-states, (iii) routes are created from MPRs (intermediate nodes are all MPR nodes), (iv) MPRs are 1-hop neighbours via a bi-directional link covering all 2-hop neighbours, (v) multiple routes to destination are possible, and (vi) no complete routes known at the source (only next hops).

C. Topology Broadcast Based on Reverse Path Forwarding (TBRPF)

TBRPF [7,8,9] is a link-state based routing protocol, which uses the concept of reverse-path forwarding to broadcast link-state updates in the reverse direction along with the spanning tree formed by minimum-hop paths from all nodes to the source. Unlike a pure link-state routing algorithm, TBRPF requires only the non-leaf nodes in the broadcast tree to forward update packets. Hence the TBRPF generates less update traffic than pure link-state routing algorithms. The use of minimum-hop tree makes the broadcast tree more stable than a shortest-path tree and also has less communication cost to maintain the tree. In TBRPF, each node maintains a list of its one-hop neighbours and a topology table. In the topology table, each entry for a link contains the most recent cost and sequence number associated with that link. With this information each node can compute a source tree in order to provide shortest paths to all reachable remote nodes. For every node src $\neq$ i, node i keeps the record of: (1) a parent p_i(src) which is the neighbour of node i and the next hop on the minimum-hop path from node i to node src, (2) a list of children $children_i$(src) which are the neighbours of i, and (3) the sequence number sn_i(src) of the most recent link-state update

originating from node src. The parents p_i(src) are forming a minimum-hop spanning tree directed towards src for all i ≠ src. Node src is broadcasting the update message in the reverse direction along its spanning tree to other nodes. When the update message is received from p_i(src), a node i accepts that message, modifies its topology table and forwards that message to every node in $children_i$(src). Moreover, the updated message had a larger sequence number than the corresponding entry in its topology table. When a node i detects the changing of that parent for node src, it sends a CANCEL PARENT message, which contains the identity of src, to the reachable current parent. It also sends a NEW PARENT message, which contains the identity of src and sn_i(src), to the newly computed parent.

On receiving this message, the new parent finds out all the link-state information from its topology table that originated from src and direct it to i. When a node i is detecting any change in its neighbourhood, for example, appearance of a new node or loss of connectivity with an existing neighbour, it is updating the link cost and the sequence number field for the corresponding link in its topology table. Then the node i also sends the corresponding link-state message to all its neighbours of $children_i$(i). The node recomputes its list of parents when it causes change in a neighbour to become inaccessible. Each node of the network has (1) a topology table, which contains all link-states stored at the node, (2) a list of neighbour nodes and (3) for each node, a parent (next node on the minimum-hop path to the source), a list of children and the sequence number of the most recent link-state update.

The properties [30] of TBRPF are: (i) with the use of a minimum-hop spanning tree, broadcast link-state is updated, (ii) minimum-hop spanning tree is rooted at the update of the source, (iii) minimum-hop tree is maintained with info received from the tree itself, (iv)each node is provided with full topology information, and (v) multiple paths to destinations are possible.

D. Summary of proactive multipath routing

Among the flat routed global routing the OLSR may scale well. The scallability in OLSR is achieved by reducing the number of rebroadcasting through the MPR mechanism. The MPR is used to elect only a number of neighbouring nodes for rebroadcasting the message. Since the hierarchical routed global routing is scaling well than the flat routed global routing, the OSPF is the best for the internet community. Due to the dynamic changes in the mobility management, the unnecessary control packets are transmitted in OSPF. The performance comparison of various proactive multipath routing protocols [2] are illustrated in Table 1. Note that the performance metrics represent the worst case scenario of each routing protocol.

Table 1: Comparison of various proactive multipath routing protocols

Proactive Protocol	WCC	WTC	RS	Number of tables	Frequency of updates	Critical Nodes	HM	Advantages	Disadvantages
OLSR	O(N)	O(D)	F	3 (Routing, neighbour and topology tables)	Periodic	No	Yes	MPR and Contention Reduces Control Overhead	2-hop neighbour knowledge required
OSPF	O(N)	O(D)	H	1 (Routing table is constructed from link-state database)	Periodic by sending LSAs	No	Yes	Optimization of pure link-state routing protocol	Only best for Internet community.
TBRPF	O(N)	O(D)	F	1 Table, 4 lists	Periodic and differential	Yes, Parent node	Yes	Low WCC when comparing with pure link-state routing	Overheads increase with the changing of node mobility and network size

WCC: Worst Case Communication Complexity, i.e., number of messages needed to perform an update operation in worst case; WTC: Worst Case Time complexity, i.e. number of steps involved to perform an update operation in worst case; RS: Routing Structure; F: Flat; H: Hierarchical; HM: HELLO Messages; N: Number of nodes in the network; D: Diameter of the network.

III. REACTIVE MULTIPATH ROUTING PROTOCOLS

Reactive or on-demand multipath routing protocols are reducing the overheads in proactive multipath protocols by maintaining the information for active routes only. This means that the routes are determined and maintained whenever nodes need to send data to a particular destination. Route discovery happens by flooding a route request packets through the network. When a node with a route to the destination (or the destination itself) is reached, it sends a route reply packet back to the source node using link reversal if the route request has travelled through bi-directional links or by piggy-backing the route via flooding. The two categories of reactive multipath protocols based on routing strategy [2] are **(i) source routing and (ii) hop-by-hop routing.**

In ***source routing*** [2, 10, 11], the complete source to destination address is carried by each data packet. The intermediate nodes then forward these packets based on the information kept in the header of each packet. It means that the intermediate nodes need not to maintain up-to-date routing information for each active route in order to forward the packet towards their destination. Moreover, these nodes need not to maintain the neighbour connectivity through periodic beaconing messages. The major drawback of the source routing protocols is that they do not perform well in large networks due to two main reasons: (i) the probability of route failure is directly proportional to the growth of the intermediate nodes in each route. This can be seen

as $p(f) = l.n$, where is $p(f)$ the probability of route failure, l is the probability of a link failure and n is the number of intermediate nodes in a route and then it can be seen as $n \to \infty$, then $p(f) \to \infty$, (ii) the amount of overhead carried in each header of each data packet depends upon the number of intermediate nodes in each route. These protocols may not scale well in large networks with significant levels of multihoping and high levels of mobility.

In ***hop-by-hop routing*** (also called ***point-to-point routing***) [2, 12], only the destination address and the next hop address are carried by each data packet. Moreover, each intermediate node in the path to the destination uses its routing table in order to forward each data packet towards their destination. The main advantage of this strategy is that the routes are adaptable to the dynamically changing environment of MANETs, since each node can update its routing table upon receiving the fresh topology information and hence forward the data packets over fresh and better routes. The fresh routes require fewer route recalculations during data transmission. The main disadvantage of this strategy is that each intermediate node must store and maintain routing information for each active route and each node may require being aware of their surrounding neighbours through the use of beaconing messages. A numerous reactive routing protocols have been proposed to increase the performance of reactive routing. This section describes the characteristics and functionality of existing reactive multipath routing protocols.

A. Ad hoc On-demand Distance Vector – Backup Routing (AODV-BR)

The AODV-BR [15] protocol uses the same AODV's [25] RREQ (route request) propagation process. When a source needs to initiate a data session to a destination and there is no route to that destination in its route cache, it searches a route by flooding a RREQ packet. Each of these RREQ packets has a unique identifier in order to detect and drop duplicate packets by the nodes. When an intermediate node is receiving a non-duplicate RREQ, it records the previous hop and the source node information in its routing table (i.e., backward learning) and then broadcasts the packet or sends back a RREP (route reply) packet to the source when a route to the destination is known. On receiving the first RREQ or subsequent RREQs that traversed from a better route (fresher or shorter route) than the previously replied route, the destination node sends a RREP through that selected route.

The slight modification (for the consideration of the broadcast nature of wireless communications) in the AODV's RREP phase establishes the mesh and multipaths without transmitting any extra control message.When a node that is not part of the selected route overhears a RREP packet not directed to itself transmitted by the sending neighbour (on the primary route), it records that the sending neighbour as the next hop to the destination in its alternate route table. In this way, a node may receive numerous RREPs for the same route when it is within the radio propagation range of more than one intermediate node of the primary route. Therefore, it chooses the best route among them and inserts it to the alternate route table. When the source of the route is receiving the RREP packet, the primary route between the source and the destination has been established for the instant use. Nodes that have an entry to the destination in their alternate route table are forming the mesh. The primary and alternate routes together is forming a mesh which is similar to a fish bone as shown in Fig.3.

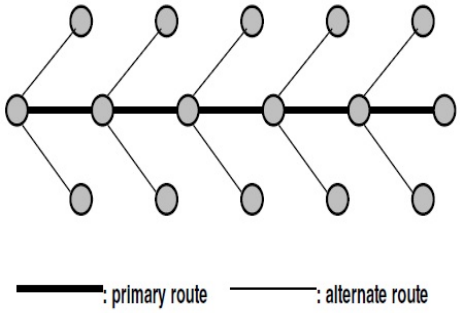

Figure. 3. Multiple routes forming a fish bone structure.

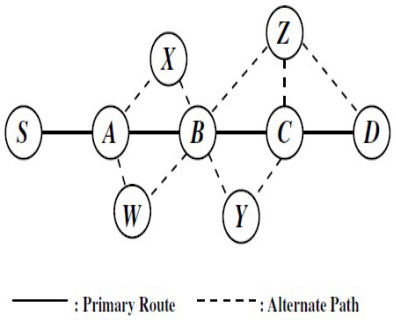

Figure. 4. An alternate path with the same path length as the primary route.

For example, the node Z forwords the packet from B directly to the destination D without sending it through node C if the link between nodes B and C fails. Hence the packet is delivered through the path <S-A-B-Z-D> has the same hop length as the primary route <S-A-B-C-D> as shown in Fig.4.

The properties [30] of AODV-BR are: (i) the extension of AODV, (ii) flood RREQs with unique IDs hence the duplicates are discarded, (iii) each node maintains backup route(s) in its alternative route table, (iv) Distance vector protocol so only destination, next hop and number of hops known, (v) alternative route (backup) route(s) used when primary fails, (vi) multiple complete routes are not available, (vii) Alternative route(s) determined in RREP phase by overhearing RREPs to other nodes, and (viii) a source does not know complete route(s) information.

B. Ad hoc On-demand Multipath Distance Vector routing (AOMDV)

AOMDV [16] is the extension of AODV [25] so as to eliminate the occurrence of frequent link failures and route breaks in highly dynamic ad hoc networks. It adds some extra fields in routing tables and control packets,

and follows the two rules during a route discovery phase in order to compute loop-free and link-disjoint multiple routes between source and destination. These rules are (i) a route update rule establishes and maintains multiple loop-free paths at each node, and (ii) a distributed protocol finds link-disjoint paths. Link failures may occur because of node mobility, node failures, congestion in traffic, packet collisions, and so on.

There is no any common link among the multiple routes between a source and destination pair in the link-disjoint routes. To achieve loop-freedom, every node maintains a variable called the advertised hop count. The advertised hop count is added in each RREQ or RREP and in addition to the routing table has the usual fields that are used for AODV. The advertised hop count field of a node is set to the length of the longest available path to the destination expressed in terms of the number of hops if it initiates a RREQ or RREP with a particular destination sequence number and it remains unchanged till the associated destination sequence number is changed.

The loop-freedom rule says that if a node receives a RREQ (RREP) for a particular destination with a destination sequence number: (a) it should update its routing information with the information obtained from the received RREQ (RREP) if the destination sequence number is higher than the one stored in its routing table; (b) it can re-send the received RREQ (RREP) when the advertised hop count in the RREQ (RREP) is greater than the corresponding value in its routing table and if the destination sequence number is equal to the one stored in its routing table; and (c) it can update its routing table with the information contained in the received RREQ (RREP) when the advertised hop count in the RREQ (RREP) is less than the corresponding value in its routing table if the destination sequence number is equal to the one stored in its routing table.

For link-disjointness, each node maintains a route list in its routing table for a particular destination and its route list contains the next hop, last hop, and hop count information for the destination. The next hop represents a downstream neighbour through which the destination can be reached. The last hop refers to the node immediately preceding the destination. The hop count is used to measure the distance from the node to the destination through the associated next and last hops. The link-disjointness among all the paths can be achieved if a node can ensure that those paths to a destination from itself differ in their next and last hops. Using this observation, AOMDV ensures link-disjointness among multiple routes for the same source and destination pair and also adds a last hop field in each RREQ and RREP.

In AOMDV, all copies of an RREQ are examined for the potential alternate reverse paths during route discovery. On receiving an RREQ, an intermediate node creates a reverse path if the RREQ satisfies the rules for loop-freedom and link-disjointness. Moreover, it checks if it has one or more valid next hop entries for the destination. The intermediate node generates an RREP and sends it back to the source along the reverse path if such an entry is found. Otherwise, it rebroadcasts the RREQ. The destination follows the same rules for creating reverse paths if it receives RREQ copies. Unike the intermediate nodes, it generates an RREP for every copy of RREQ that arrives via a loop-free path, for increasing the possibility of finding more disjoint routes.

The properties [30] of AOMDV are: (i) extension of AODV, (ii) RREQs from different neighbours of the source are accepted at intermediate nodes, (iii) multiple link-disjoint (node-disjoint) routes are created, (iv) maximum hopcount to each destination ("advertised hopcount") is used for avoiding loops, (v) multiple routes are established in single route discovery process, (vi) nodes maintain next-hop information for destinations (may have multiple next-hops), (vii) a source does not know complete route(s) information, and (vii) the occurrence of frequent link failures and route breaks in a highly dynamic ad hoc networks are eliminated.

C.Temporally-Ordered Routing Algorithm (TORA)

TORA [17] is a highly adaptive, distributed routing protocol based on the Light-weight Mobile Routing (LMR) protocol, which uses similar link reversal, route repair and the query/reply procedure (to create a DAGs) as in LMR in order to provide multiple loop-free paths for a source and destination pair. The two main advantages of TORA are (1) the far-reaching control messages to a set of neighbouring nodes are reduced even if the topology change has been occurred and (2) also provides multicasting support even this is not incorporated into its basic operation. This protocol has the three basic functions such as route creation, route maintenance and route erasure.

A directed a-cyclic graph (DAG) is created based on a "height" metric, in order to establish and maintain routes. The height of a node is defined by the parameters such as a reference level and a delta with respect to the reference level, which differs per destination and also one DAG per destination. The height of the destination is always zero, where as the heights of other intermediate nodes increase by 1 towards the source node via increasing the delta value.In TORA, the new routes are created using query (QRY) and update (UPD) packets. Each node initiates a route by broadcasting a QRY to its neighbours. The QRY is re-broadcasted through the network as long as it reaches the destination or a node has a route to the destination. When a node is the destination or a route to the destination is replied via UPD packets back to the source, which contains its height with respect to the destination. On receiving UPD, each node sets its own height which is greater than the height sent by the neighbour as shown in Fig.5(a).

From Fig.5(b), a node generates a new reference level based on the propagation of the reference level, by neighbours effective co-ordination and structured reaction, if it loses its last downstream link. Then node erases the invalid routes to the destination by flooding a clear (CLR) packet throughout the network. Therefore, the links are reversed in order to adopt the new reference level by changing the direction of links if a node has no downstream links. Since the "height" metric depends on

the logical time of a link failure (time-dependent), all nodes are having a common clock. TORA's metric is a quintuple which consists : (1) the logical time of the link failure, (2) the unique ID of the node defining the new reference level, (3) a reflection indicator bit, (4) a propagation ordering parameter and (5) the unique ID of the node. The first three elements represent the reference level. The internodal co-ordination of TORA can be quite instable due to link failures. The link failures can be avoided by the route erasure and link reversal procedures.

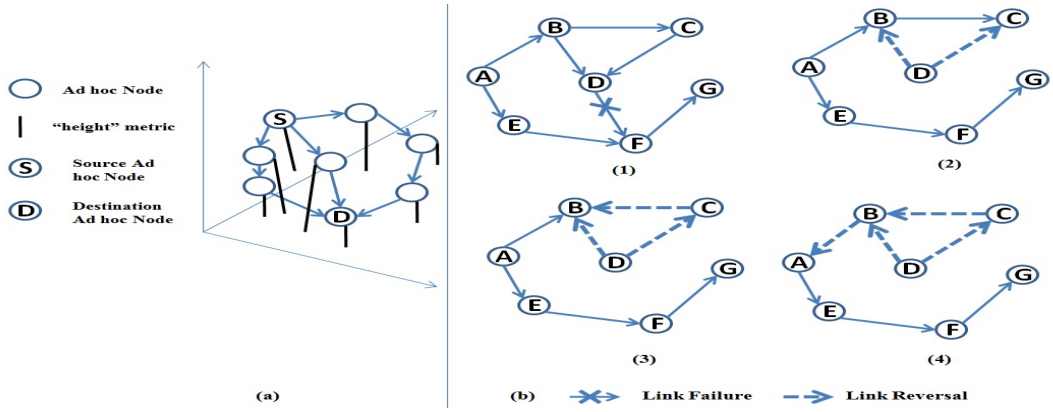

Figure. 5. (a) Route creation and (b) Route Maintenance in TORA.

The properties [30] of TORA are:(i) the routes are created using DAG, (ii) QRY are sent and replied with UPD to create DAG(s), (iii) a DAG is formed using height metrics, (iv) the link failures get new reference levels (heights) and links are reversed to notify the source, (v) all nodes need to have a common clock, (vi) provides multiple routes to destination, (vii) there may not be optimum routes between a source and destination may pair, and (viii) a source does not know complete route(s) information.

D. MultiPath Dynamic Source Routing (MP-DSR)

MP-DSR [18] is a QoS-aware multipath source routing protocol, based on Dynamic Source Routing protocol (DSR), which creates and selects routes based on a newly defined QoS metric, *end-to-end reliability*. This protocol computes a set of routes in order to satisfy a minimum *end-to-end reliability* requirement. In MP-DSR, multiple node-disjoint paths for data transmission are discovered for the specific end-to-end reliability requirement. The probability of having a successful transmission between two nodes in the network within the specific period is called end-to-end reliability. Unlike DSR [27,28], the MP-DSR provides a minimum end-to-end requirement based on the determination of the number of paths needed (m_0) and the lowest path reliability (Π_{lower}) requirement by every path for route discovery. The relationship between m_0 and Π_{lower} is that there are fewer paths between a source and a destination (m_0 is low), more reliable paths are required (Π_{lower} is higher) to ensure the end-to-end reliability. The Π_{lower} is computed using $\prod_{lower} = 1 - \sqrt[m_0]{1 - P_u}$, where $P_u = P(t)$ is the required end-to-end reliability and $P(t)$ is the resulting end-to-end reliability. The link availability of m_0 neighbours is greater than Π_{lower} used to determine m_0. To keep the data and RREQ traffic at a minimum end-to-end reliability requirement, this protocol starts the route discovery process by setting m_0 to 1 and incrementing it by 1 every time as long as the neighbours did not satisfy Π_{lower}. This means that the procedure is stopped if the required end-to-end reliability is met. More reliable paths are preferred from the fewer paths between a source and destination pair if Π_{lower} is higher and then the source sends m_0 and RREQs, each of which contains Π_{lower}, the path traversed, the corresponding path reliability, etc.

On receiving RREQ message, each node checks whether the message meets the path reliability requirement. If so that node updates RREQ message and forwards multiple copies of this message based on the number of neighbours that can receive this RREQ without failing the path reliability, and bounding with m_0 to restrict the message to be forwarded across the network. The destination selects node-disjoint paths and replies RREP messages back to source along with these disjoint paths when it receives the RREQ messages. The source node starts data transmission via the routes from which it receives the RREPs.

The properties [30] of MP-DSR are: (i) extension of DSR, (ii) source routing, so that the packets contain complete path in their header, (iii) source has complete route information, (iv) QoS awareness: The probability of having a successful transmission between two nodes in the network within the specific period is called end-to-end reliability, (v) provides multiple node-disjoint routes between a source and a destination pair, (vi) an intermediate node compares the received RREQs with the required end-to-end reliability in order to determine whether they will be forwarded or discarded (vii) the destination sends RREPs back to the source along the node-disjoint paths which are meeting the end-to-end reliability in order to the source initiates the data transmission.

E. Routing on-demand acyclic multi-path (ROAM)

The ROAM [19] routing protocol is an extention of *diffusing update algorithm* (DUAL)[31] in order to provide on-demand routing. It uses internodal

coordination along directed acyclic subgraphs defined on the routers' distance to destination. This operation is called as a ''*diffusing computation*''. It also eliminates the search-to-infinity problem present in some of the on-demand routing protocols by stopping multiple flood searches if the required destination is no longer reachable. In ROAM, each router maintains entries in a route table to destinations by flowing data packets through them (i.e. the router is a node which completes/connects a router to the destination) to reduce the significant amount of storage space and bandwidth needed to maintain an up-to-date routing table. When the distance of a router to a destination changes by more than a defined threshold, the update messages to its neighbouring nodes are broadcasted. The benefit of increasing the network connectivity in highly dynamic networks is that it prevents nodes entering sleep mode to conserve power.

The properties [30] of ROAM are: (i) provides multiple loop-free paths to the destination, (ii) reduction in storage space and amount of band width, (iii) search-to-infinity problem is eliminated, and (iv) a router is sending update messages for active destinations if its distance to them does not increase within a given threshold.

F. Split Multipath Routing (SMR)

The SMR protocol [20] establishes multiple routes of maximally disjoint paths in order to minimize route recovery process and control message overhead. Node disjoint paths are maximally disjoint paths. This protocol minimizes the number of common nodes if there are no node-disjoint paths available. In SMR, the multiple routes are not necessarily equal in length but one of which has the shortest delay. If a source needs to initiate a data session to a destination it does it by flooding a RREQ packet across the network. Each RREQ packet contains the source ID and a sequence number which uniquely identify the packet. Several duplicate RREQ packets traverse through the network from different routes reach to the destination. The destination then selects multiple disjoint paths for sending RREP packets back to the source. This protocol uses source routing because the complete route information is in the header of the RREQ packets. In addition to that the intermediate nodes are not permitted to send RREPs eventhough they have route information to the destination. Nodes replied using their cache are difficult to find maximally disjoint multiple routes because the destination does not receive enough RREQs and will not know the information of routes formed from intermediate nodes cache. Instead of dropping the duplicate RREQs, the intermediate nodes only forward the RREQs through a different incoming link than the first received RREQ if its hop count is lesser than the hop count of the first received RREQ (known as a noval packet-forwarding approach).

The destination selects any two maximally disjoint routes and one of these routes with a shortest delay is taken by the first RREQ that the destination receives in the SMR protocol. This path is minimizing route acquisition latency needed by on-demand schemes. On receiving the first RREQ, the destination sends back a RREP to the source via this path and thus the RREP contains the entire path from which the intermediate nodes can forward the packet. The destination waits for a certain amount of time to receive more RREQs in order to determine all possible routes after the successful sending of the first RREP. Since the destination knows the route information from all possible routes, the maximally disjoint route to the already replied route can be determined. When more than one maximally disjoint routes are determined, the route with shortest hop distance is selected as the desired route. The path which is delivering the RREQ very faster is choosen first when the destination has more routes with same shortest hop distances and then the destination sends a second RREP to the source along path which is maximally disjoint to the first path.

The properties [30] of SMR are: (i) source routing because packets contain complete routes, (ii) source has complete route information (included in RREP), (iii) provides at least two paths which are maximally disjoint, (iv) Routes are selected by destination and one of them is the shortest-delay path, (v) RREQs contain the source ID and unique sequence number, (vi) intermediate nodes forward all duplicate RREQs which are traversed from a different incoming link, and (vii) destination first replies the fastest path (shortest-delay path) and then the maximally disjoint path after a while is replied.

G. CacHing And Multipath routing Protocol (CHAMP)

The CHAMP [21,22] uses co-operative data caching and shortest multipath routing for reducing the packet loss due to frequent route breakdowns and also to achieve energy-efficiency. Temporal locality in dropped packets are exploited using co-operative packet caching mechanism. Every node maintains a small buffer for caching packets which are passed through it. The upstream node with the pertinent data in its buffer and alternative route can retransmit the data if a downstream node encounters a forwarding error via the nodes having multiple routes to every active destination. The shortest multipath routes are selected based on minimizing delay and enabling a node to use any of the paths for data forwarding without severely disrupting the arrival order of packets at the destination. The intermediate nodes use the least used successor to the destination for spreading the data in a round robin way while forwarding the packets.

In CHAMP every node maintains a **route cache** for forwarding information and a **route request cache** for recently received and processed route requests. Each entry in the route cache has a destination identifier, the distance to the destination, the set of successor or next hop nodes for the destination, the time each successor node was last used and the number of times each successor node is used. Entries are deleted from the **route cache** if they have not been used for a period of particular time (RouteLifeTime). Each entry in the route request has a source identifier, identifier of node being searched, the sequence number, the minimum forward count, the set of nodes that forwarded the same request, and the status of the route request (i.e. Replied or

NotReplied). Moreover, each node maintains a send buffer for waiting packets or routes and a data cache for storing recently forwarded packets. When a node has no routes for the destination, it initiates a route discovery by flooding RREQ througout the network in order to establish a DAG rooted at the source by the destination. The destination sends back a RREP as soon as it receives a RREQ. The forwarding count is first initialized by 0 (source) and then increased by 1 for every retransmission. A minimum forwarding count value is used to establish multiple routes of equal length.

The properties [30] of CHAMP are: (i) non-disjoint multiple paths to destinations are established, (ii) source has no complete route(s), (iii) temporal caching is used to reduce packet losses, (iv) cached routes are used as backups, (v) selection of shortest multipath routes, and (vi) the traffic is distributed among multiple paths in a round-robin way.

H. Multipath Source Routing (MSR)

MSR [23,24] is an extension of the on-demand DSR [26,27] protocol, which consists a scheme to distribute load among multiple paths in a network. The route discovery process of DSR is also used in MSR but it generates multiple paths instead of only one path as in the DSR. When a source requires a route to a destination if it has no routes in the cache, it initiates a route discovery by flooding a RREQ packet for the entire network. The header of each RREQ contains a route record which records the sequence of hops that the packet passes through the intermediate nodes in the network. Moreover, each intermediate node appends its own address to the route record during route discovery. Once the destination receives the RREQ, a RREP reverses the route in the route record of the RREQ and traverses back via this route. Each route is stored in the cache with a unique index, so that it can easily pick multiple paths from there. The selection of disjoint paths are ensuring the independence between paths in MSR. The packet headers has complete routes during the route discovery process of MSR in order to eliminate the occurrence of looping, i.e., when a loop is detected in the route discovery of MSR, it will be immediately eliminated.

Table 2: Comparison of various reactive multipath routing protocols

Reactive Protocol	WCC [RD]	WCC [RM]	WTC [RD]	WTC [RM]	RS	MR	PB	Advantages	Disadvantages
AODV-BR	O(2N)	O(2N)	O(2D)	O(2D)	F	Yes	Yes*	Each node maintains backup route(s) in its alternative route table	Requires periodic HELLO messages
AOMDV	O(2N)	O(2N)	O(2D)	O(2D)	F	Yes	Yes*	Link-disjoint multi-path routing	Requires periodic HELLO messages
TORA	O(2N)	O(2A)	O(2D)	O(2D)	F	Yes	No	Localized route maintenance	Detect partitions falsely; Requires reliable and in-order delivery of route control packets; Temporary routing loops
MP-DSR	O(2N)	O(2N)	O(2D)	O(2D)	F	Yes	No	Intermediate nodes do not store route information; Can provide multiple paths	Stale caches and relay storm problems may arise in large and highly dynamic MANETs; Extra communication overhead due to source routing
ROAM	O(|E|)	$O(6G_A)$	O(D)	O(A)	F	Yes	No	Elimination of search-to-infinity problem.	Large control overhead in highly dynamic mobile environments
SMR	O(2N)	O(2N)	O(2D)	O(2D)	F	Yes	No	Intermediate nodes do not store route information; Can provide multiple paths	Stale caches and relay storm problems may arise in large and highly mobile MANETs; Additional communication overhead due to source routing
CHAMP	O(N+Y)	O(N+Y)	O(D+Z)	O(D+Z)	F	Yes	No	Packet losses are reduced using temporal caching; Traffic is distributed among multiple paths in round-robin manner	Requires Route cache for Packets Sending
MSR	O(2N)	O(2N)	O(2D)	O(2D)	F	Yes	Yes#	Multi-path routing and load balancing	Requires periodic probe packets in order to gather information

WCC: Worst Case Communication Complexity, i.e. number of messages needed to perform a route discover or an update operation in worst case; *WTC*: Worst Case Time complexity, i.e. number of steps involved to perform a route discovery or an update operation in worst case; *RD*: Route Discovery; *RM*: Route Maintenance; *RS*: Routing Structure; *F*: Flat; *H*: Hierarchical; *MR*: Multiple Routes; *PB*: Periodic Beacons; *N*: Number of nodes in the network; *D*: Diameter of the network; *A*: Number of affected nodes; *Z*: Diameter of the directed path where the RREP or RERR packet transits; Y: Total Number of nodes forming the directed path where the RREP or RERR packet transits; *: Beacons in terms of HELLO Messages; #: Sends periodic probe packets along active routes; G=maximum degree of the router; |E|=number of edges in the network.

Like DSR, the MSR uses source routing (i.e. routes are all calculated at the source), the intermediate nodes only forward the packet according to the route in the packet-header. In order to keep the information of each different route to a destination, a multiple-path table is used. For each route to the destination, the index of the path in the route cache, the destination ID, the delay (based on the estimated RTT) and the calculated load distribution weight of a route are all kept in the multiple-path table. The number of packets sent consecutively on a route is represented as the weight of a route and the load to be sent to the destination are distributed among multiple routes in order to achive load balancing.

The properties [30] of MSR are: (i) provides multiple paths from source(s) to destination(s), (ii) provides loop-free and disjoint paths, (iii) traffic load is distributed based on delay which means lower delay has more traffic), (iv) the source has complete route(s).

I. Summary of reactive multipath routing

Among the various reactive multipath routing protocols, the hop by hop routing protocols have significant impact on MANET than the source routing protocols. In hop by hop routing, the AODV-BR provides only back-up/alternate routes where as the AOMDV provides link and node disjoint multiple routes. Hence the AOMDV is the best in hop by hop routing. In source routing, the CHAMP is the best among MSR, SMR and ROAM because it reduces the packet losses using temporal caching and the balancing is achieved by distributing the traffic among multiple paths in a round robin manner. The performance comparison of various reactive multipath routing protocols [2] are illustrated in Table 2. Note that the performance metrics represent the worst case scenario for each routing protocol.

IV. HYBRID MULTIPATH ROUTING PROTOCOLS

The features of both proactive and reactive protocols are combined together to form a new generation of protocols called Hybrid multipath routing protocols. These protocols are used to increase scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads. This can be achieved by proactively maintaining routes to nearby nodes and determining routes to far away nodes using a route discovery strategy. Most of the hybrid protocols are zone-based, which means that the network is partitioned or seen as a number of zones by each node. Others are cluster-based, which means the nodes are grouped into trees or clusters. This section describes the widely used hybrid multipath routing protocol called Zone Routing Protocol (ZRP) and its performance comparison [2] is illustrated in Table 3. Note that the performance metrics represent the worst case scenario for each routing protocol.

Table 3: Comparison of hybrid multipath routing protocol

Hybrid Protocol	WCC [RD]	WCC [RM]	WTC [RD]	WTC [RM]	RS	MR	PB	Advantage Table 3: Comparison of hybrid multipath routing protocol s	Disadvantages
ZRP: interzone or intrazone	O(*N+r*) or O(*n*)	O(*N+r*) or O(*n*)	O(*2D*) or O(*d*)	O(*2D*) or O(*d*)	F	Yes	Yes*	Reduced communication Compared to pure proactive routing algorithms; Faster route discovery within a zone than any pure reactive routing protocol	For large values of routing zone it may behave like a pure reactive routing protocol; Overlapping Zones
WCC: Worst Case Communication Complexity, i.e. number of messages needed to perform a route discover or an update operation in worst case; WTC: Worst Case Time complexity, i.e. number of steps involved to perform a route discovery or an update operation in worst case; RD: Route Discovery; RM: Route Maintenance; RS: Routing Structure; F: Flat; H: Hierarchical; MR: Multiple Routes; PB: Periodic Beacons; N: Number of nodes in the network; D: Diameter of the network; *: Beacons in terms of HELLO Messages; n: Number of nodes in a zone, home region, cluster or tree; d: Diameter of a zone, home region or cluster or tree; r: Number of nodes in the route reply path.									

A. Zone Routing Protocol (ZRP)

The ZRP [12,13,14] combines the advantages of proactive and reactive protocols in a hybrid scheme. It acts as a proactive protocol in the neighbourhood of a node (IntrA-zone Routing Protocol, IARP) locally and a reactive protocol for routing between neighbourhoods (IntEr-zone Routing Protocol, IERP) globally. The local neighbourhoods are called zones, which are different for each node. Each node may be within multiple overlapping zones and each zone may be of a different size. The "size" of a zone is not determined by the geographical measurement but is determined by a radius of length ρ, where ρ is the number of hops to the perimeter of the zone.

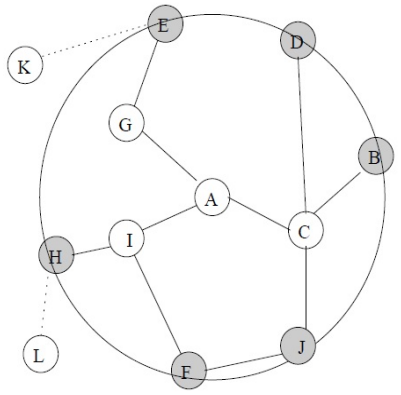

Figure. 6. Routing Zone of node A with $\rho = 2$

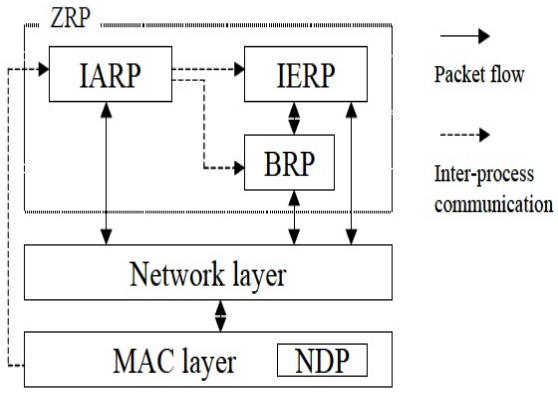

Figure. 7. ZRP architecture

The nodes of a zone are divided into the nodes whose minimum distance to the central node is exactly equal to the zone radius r called peripheral nodes and the nodes whose minimum distance is less than r are interior nodes called interior nodes. In Fig. 6, the nodes A–F are interior nodes, the nodes G–J are peripheral nodes and the nodes K and L are outside the routing zone. Note that the node H can be reached by two paths, one with length 2 and one with length 3 hops. The shortest path is less than or equal to the zone radius if the node is within the zone.

From Fig. 7, the IARP provides the topology information in the form of direct query request to the border of the zone is called as *border casting.* The Border cast Resolution Protocol (BRP) provides the delivery of bordercast packet. The route requests can be directed away from areas of the network which have been already covered through *query control* mechanisms. In ZRP, a Neighbour Discovery Protocol (NDP) provided by the Medium Access Control (MAC) layer is used to detect new neighbour nodes and link failures. The "HELLO" beacons are transmitted by NDP at regular intervals. The neighbour table is updated upon receiving a beacon. The Neighbours which has not been received beacon within a specified time, are removed from the table. The functionality of NDP must be provided by IARP if the MAC layer does not include a NDP.

Table 4: Overall Comparison of all multipath routing categories

Routing Class	Proactive	Reactive	Hybrid
Routing Structure	Both flat and hierarchical	Usually flat	Usually Hierarchical
Availability of Routes	Always available for reachable nodes	Determined when needed. Sometimes overheard routes are	Always available when the source and destination reside within the
		stored for a limited time (e.g. in MP-DSR).	same zone/cluster/tree.
Volume of control traffic	Usually high, reduction is attempted. E.g., OLSR, TBRPF	Usually lower than proactive routing.	Mostly, lower than proactive and reactive routing protocols
Storage requirements	Usually high	Depends on the number of routes kept or required. Usually lower than proactive protocols.	Usually lower than pure proactive and reactive routing protocols when the size of zones/ clusters/trees can be properly determined in large networks.
Delay for route discovery	Predetermined when the routes are small	Higher than proactive routing protocols	Similar to proactive routing protocols if source and destination are located within the same zone/ cluster/tree. Otherwise usually higher than proactive but lower than reactive.
Mobility support	Low to moderate mobility support. For hierarchical structured routing, Group mobility is usually required.	Can support higher mobility than proactive routing protocols.	Usually supports lower level of mobility than reactive routing protocols since routing structure is mostly hierarchical in this approach.
Scalability	Usually up to 100 nodes. OSPF and OLSR may scale higher.	Source routing protocol does not scale well, usually up to few hundred nodes. Hop by hop routing scales better than source routing.	1000 or more.

The two phases of reactive routing process are (1) the route request phase in which the source sends a route request packet to its peripheral nodes using BRP and (2) the route reply phase in which the receiver of a route request packet responds by sending a route reply back to the source if it knows the destination. Otherwise, it continues the process of bordercasting the packet. In this way, the route request is distributed throughout the network.When a node receives several copies of the same route request are considered as redundant and they are discarded.

The properties [30] of ZRP are: (i) hybrid protocol (combining the features of pro-active and re-active routing), (ii) no distinct protocol but framework, (iii) may or may not provide multiple paths (dependent of protocols used as IARP and IERP), (iv) neighbour

discovery through NDP, (v) locally pro-active and Inter-locally re-active, and (vi) framework which caters other protocols to function.

B. Summary of hybrid multipath routing

The hybrid multipath routing protocols are having higher scalability than the proactive or reactive multipath routing protocols because they attempt to minimize the number of rebroadcasting nodes by defining a structure. Other advantage of hybrid multipath routing protools is that they attempt to eliminate every single point of failure. The ZRP protocol is the best hybrid multipath routing which increases the scalability and provides stronger network connectivity in MANET.

V. Conclusions

In this paper three categories of multipath routing protocols are discussed. Table 4 shows the overall comparison of all the three multipath routing categories. The routing in ad-hoc networks is much more difficult than in conventional networks because of its dynamic topology and unpredictability in wireless links. The proactive multipath routing maintains the network connectivity positively. The reactive multipath routing determines routes when needed. The hybrid multipath routing employs both proactive and reactive properties which maintain intra-zone information proactively and inter-zone information reactively. The study suggests that neither a single routing protocol nor a class of protocols is best suited for all scenarios of MANET.

References

[1] Elizabeth M. Royer, C-K Toh, “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”, IEEE Personal Communications, April 1999, pp.46-55.

[2] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz , “A review of routing protocols for mobile ad hoc networks”, Ad Hoc Networks, June 2003, pp.1-22.

[3] J. Moy, "Open Shortest Path First Version 2," RFC 2328, IETF, April 1998.

[4] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum and L. Viennot, “Optimized Link State Routing Protocol for Mobile Ad Hoc Networks”, IEEE INMIC, Pakistan 2001.

[5] P. Jacquet, P. Muhlethaler, and A. Qayyum, "Optimized Link State Routing Protocol", IETF Internet Draft, draft-ietf-manet-olsr-10.txt, June 2002.

[6] P. Jacquet and T. Clausen, "Optimized Link State Routing Protocol", IETF Internet Draft, draft-ietf-manet-olsr-11.txt, July 2003.

[7] Bellur and R. Ogier, “A Reliable, Efficient Topology Broadcast Protocol for Dynamic Networks”, Proceedings IEEE INFOCOM '99, p.178-186, March 1999.

[8] M. Lewis, F. Templin and R. Ogier, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)”, IETF Internet Draft, draft-ietf-manet-tbrpf-09.txt, June 2003.

[9] Bellur, et. al, “Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)”, IETF Internet Draft, draft-ietf-manet-tbrpf-08.txt, April 2003.

[10] D. Johnson, D. Maltz, J. Jetcheva, The dynamic source routing protocol for mobile ad hoc networks, Internet Draft, draft-ietf-manet- dsr-07.txt, work in progress, 2002.

[11] C. Toh, A novel distributed routing protocol to support ad-hoc mobile computing, in: IEEE 15th Annual International Phoenix Conf., 1996, pp. 480–486.

[12] J. Schaumann, “Analysis of the Zone Routing Protocol”, December 2002.

[13] Z. Haas and M. Pearlman, "The zone routing protocol (ZRP) for Ad Hoc networks", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[14] Z. Haas, “A New Routing Protocol for the Reconfigurable Wireless Networks”, Proceedings of IEEE ICUPC’97, San Diego, CA, pp. 562-566, October 1997.

[15] S. Lee and M. Gerla, "AODV-BR: Backup routing in ad hoc networks." Proceedings of IEEE WCNC 2000, Chicago, pages 1311-1316, September 2000.

[16] M. Marina and S. Das, “On-demand Multipath Distance Vector Routing in Ad Hoc Networks”, in Proceedings of the International Conference for Network Procotols (ICNP), Riverside, Nov. 2001.

[17] V. Park and M. Corson, ”A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks”, Proceedings of IEEE INFOCOM '97, April 1997.

[18] R. Leung, J. Liu, E. Poon, A. Chan and B. Li, “MP-DSR: A QoS-Aware Multi-Path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks”, In Proc. of the 26th IEEE Annual Conference on Local Computer Networks (LCN 2001), pp. 132-141, November, 2001.

[19] J. Raju and J. Garcia-Luna-Aceves, “A New Approach to On-demand Loop-Free Multipath Routing”, In Proc. Of the 8th Annual IEEE International. Conf. Computer Communications and Networks (ICCCN), Boston, MA, Oct 1999, pp. 522-527.

[20] S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks", Proceedings of the IEEE ICC, pp. 3201-3205, June 2001.

[21] Valera, W. Seah, and S. Rao, “Cooperative Packet Caching and Shortest Multipath Routing in Mobile Ad hoc Networks”, INFOCOM 2003, San Francisco, CA, USA, 2003.

[22] Valera, W. Seah and S. Rao, “CHAMP: A Highly-Resilient and Energy-Efficient Routing Protocol for Mobile Ad hoc Networks”, Proc. of Fourth IEEE

Conference on Mobile and Wireless Communications Networks (MWCN 2002), Sep 9 - 11, Stockholm, Sweden, 2002.
[23] L. Wang, Y. Shu, M. Dong, L. Zhang and O. Yang, "Adaptive Multipath Source Routing in Ad Hoc Networks", IEEE ICC 2001, Page(s): 867 -871 vol.3, June 2001.
[24] L. Wang, Y. Shu, Z. Zhao, L. Zhang and O. Yang, "Load Balancing of Multipath Source Routing in Ad Hoc Networks", Proceedings of IEEE ICC'02, April 2002.
[25] S. Das, C. Perkins and E. Royer, "Ad Hoc On Demand Distance Vector (AODV) Routing", IETF RFC3561, July 2003.
[26] D. Johnson, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Internet Draft, draft-ietf-manet-dsr-09.txt, April 2003.
[27] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Ad Hoc Networking, pp. 139-172, 2001.
[28] M. Pearlman, Z. Haas, P. Sholander and S. Tabrizi, "On the Impact of Alternate Path Routing for Load Balancing in Mobile Ad Hoc Networks", MobiHoc'2000, August 2000.
[29] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF WG Charter, http://www.ietf.org/html.charters/manet-charter.html, January 1999.
[30] "CACTUS Impulse Research project (Context-Aware Communication, Terminal and User)", A TU-Delft and TNO research project proposal for the Freeband Impulse Research Program in Telecommunications, July 2002.
[31] J. J. Garcia-Luna-Aceves. Loop-Free Routing Using Diffusing Computations. IEEE/ACM Transactions on Networking, 1(1):130–141, Feb 1993.

AUTHORS BIOGRAPHY

P.Periyasamy is working as an Assistant Professor in the Department of MCA, Sree Saraswathi Thyagaraja College, Pollachi, India. Interested in Mobile Ad hoc Networks Routing Protocols Design and Development.

Dr.E.Karthikeyan born in 1974 at Dharapuuram completed PG degree in the year 1996 and Ph.D from Gandhigram University, Dindigul, India in 2008. He is guiding students towards Ph.D. programme and his area of research is Network Security and Cryptography and Advanced Networking. He has published 12 papers in International Journals and more than 15 conferences National and International level. He has also published a book entitled "Text Book on C: Fundamentals, Data structures and Programming" by PHI. He delivered lectures and conducted workshops in various colleges. He is a life member of CSI, CRSI, IASCT etc. He is a Editor-in-Chief for an International Journal of Advanced Networking and Applications.

