Murshedi, TA, Wang, X and Cheng, H

On-demand Multipath Routing Protocols for Mobile Ad-Hoc Networks: A Comparative Survey

On-demand Multipath Routing Protocols for Mobile Ad-hoc Networks: A Survey

Abstract
A Mobile Ad Hoc Network (MANET) is an infrastructure-less, self-organized and multi-hop network with a rapidly changing topology causing the wireless links to be broken at any time. Routing in such a network is challenging due to the mobility of its nodes and the challenge becomes more difficult when the network size increases. Due to the limited capacity of a multi-hop path and the high dynamics of wireless links, the single-path routing approach is unable to provide efficient high data rate transmission in MANETs. The multipath routing is the routing technique of using multiple alternative paths through a network. Furthermore, whenever a link failure is detected in a primary route, the source node can select the optimal route among multiple available routes. Therefore, the multipath routing approach is broadly utilized as one of the possible solutions to cope with the single-path limitation. It is widely known that multipath routing has the advantages such as improving transmission reliability, balancing load, avoiding congestion, reducing route inquiry frequency, and reducing routing overhead. Most of the multipath routing protocols are based on either Dynamic Source Routing (DSR) or Ad Hoc On-Demand Distance Vector (AODV). The objective of this paper is to provide a survey and compare sets of multipath routing protocols for mobile ad-hoc networks. This survey will motivate the design of new multipath routing protocols which overcome the weaknesses identified in this paper.

Keywords: Mobile ad-hoc networks, on-demand multipath routing, single path routing, dynamic source routing, ad hoc on-demand distance vector.

1. Introduction

In the last decades, mobile ad hoc networks (MANETs) have attracted amounts of attention. A mobile ad hoc network consists of a collection of wireless mobile nodes (or routers) dynamically forming a temporary network without using any existing infrastructure or centralized administration. The routers in MANETs are free to move and organize themselves; thus, the network topology changes rapidly and unpredictably. MANETs are characterized by multi-hop, mobility, large device heterogeneity, limited bandwidth, and limited battery energy supply. Due to these characteristics, a routing path connecting the source node with the destination node may be broken at any time, bringing a major challenge to the design of routing protocols in MANETs [1][2].

Routing is the process of searching and maintaining routes between the source node and the destination node in the network. A routing protocol is needed whenever a packet needs to be transmitted via a number of intermediate nodes. For MANETs, there are mainly two kinds of routing protocols, i.e., table-based protocols (also called proactive protocols) and on-demand protocols (also called reactive protocols). In table-based protocols, each node maintains a routing table which contain routes to all the other nodes in the network. Nodes must periodically exchange routing information to keep routing tables up-to-date. Therefore, routes between nodes are computed and stored, even when they are not needed. Table-based protocols will be impractical for large and highly dynamic networks.

Unlike table-based protocols, on-demand routing is a popular routing category for mobile ad hoc networks. It is a relatively new routing philosophy that provides a scalable solution to large size of network topologies. The design follows the idea that each node send routing packets only when communication is requested. By this way, the routing overhead is reduced. An on-demand routing protocols consists of the following two main phases. First, route discovery is conducted to search a route between two nodes. Second, route maintenance is conducted to repair a broken route or search a new route in the presence of route failures. There are different types of on-demand routing protocols such as Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV) [3][4].

In MANETs, another classification of routing protocols can be made in terms of the number of paths a protocols delivers per source destination pair. There exist unipath and multipath routing protocols. For a unipath routing protocol, a single route is used to deliver data from the source node to the destination node. Most of the routing protocols in MANETs form a single-path, such as DSR and AODV. Single-path routing protocols need to repair routes each time the route is broken. This route repair generates a lot of control packets, and increases the end-to-end delay. In order to overcome these drawbacks of the single path routing, multipath routing schemes have been proposed. In a multipath routing protocol, more than one route is used to deliver the data [5][6]. Multipath routing is a technique which can improve the reliability of the transmission. In addition, multipath routing has the advantages of balancing load, minimizing end-to-end delay, increasing fault-tolerance, reducing the frequency of route inquiries and achieving a lower overall routing overhead . The objective of designing a multipath routing protocol is to provide enhanced robustness to node or link failures. If one could provide multiple paths from a source to a destination, one could envision the transmission of redundant information on various paths would help the receiver in reconstructing the transmitted information even if a few of the paths were to fail [7].

The rest of this paper is organized as follows. Section 2 summarizes the challenges in designing multipath routing protocols. Section 3 describes the major issues (disadvantages) in multipath routing protocols. Section 4 briefly explains two popular on-demand routing protocols, namely, DSR and AODV. Section 5 provides detailed operational descriptions, objectives, limitations and comparison of the multipath protocols. Section 6 concludes the paper and discusses possible lines of future work.

2. Challenges in designing multipath routing protocols

While designing a multipath routing protocol, the following three major challenges have been addressed in the literature [8][9][10].

i. **How to discover multiple paths**
The basic route discovery process of on-demand routing protocols like DSR and AODV is usually used to discover multiple routes from the source to the destination. This route discovery mechanism needs to be modified in order for it to discover multiple paths. In many multipath routing applications, disjoint paths are favoured due to the independence of the paths. There are two types of disjoint paths, i.e., *node-disjoint* and *link-disjoint*. Node-disjoint paths do not have any nodes in common, except the source and the destination. In contrast, link-disjoint paths do not have any link in common. Hence, the route discovery mechanisms of the existing routing protocols need to be modified to discover a maximum number of nodes- disjointed or link-disjoint paths.

ii. **How to select a path**
A multipath routing protocol should decide how to select a path for sending data packets after all the routes are discovered. According to Lee et al. [30] if a number of routes are discovered, it is required to know how many of these routes should be used (some or all of them). If only a small number of paths are used, the performance of a multipath routing protocol would be similar as that of the shortest path routing protocol. On the other hand, if all these paths are used, there is a chance of selecting an excessively long path, which may adversely affect the performance of a multipath routing protocol.

iii. **How to distribute the load**
A multipath routing protocol should determine how to use these multiple routes during the transmission of data packets. When a path or a set of paths are selected, there arises another challenge, specifically, how a source node should send a packet. It may divide a packet into multiple segments and send these segments by using different paths or it may send duplicate copies of a packet by using different paths.

3. Issues in multipath routing

Most of the proposed multipath protocols are based on an on-demand routing protocol, e.g., AODV or DSR. In fact, on-demand multipath routing protocols improve network performances, e.g., load balancing, delay and energy efficiency. However, they also bear some disadvantages as below [8][11][12].

- **Route request storm:**
A huge quantity of route request messages are created by the on-demand multipath routing protocols. The intermediate nodes have to process duplicate route request messages and lots of redundant overhead packets are introduced in the networks.
- **Inefficient route discovery:**
The route discovery process of a multipath routing protocol may not be as efficient as that of the DSR and AODV protocols. To find node-disjoint or link-disjoint paths, some multipath routing protocols prevent an intermediate node from sending a reply from its route cache. Hence, the source has to wait till it gets a reply from the destination. Thus the process of route discovery performed by the multipath routing protocol needs more time when compared with DSR or AODV protocols.
- **Longer paths:**
In a multipath routing protocol, packets usually travel longer hops than in shortest path routing protocol. Hence, packets suffer longer delay. To avoid using excessively long paths, a multipath routing protocol should not use all the discovered paths. Instead, the protocol should use a carefully selected number of paths. For example, the split multipath routing (SMR) protocol [30] uses two paths.
- **Special control message:**

In addition to the control messages incurred by route discovery and route maintenance, a multipath routing protocol uses some other control messages. The other control messages are used by a mobile node to collect information about its neighbors so that suitable (node- disjoint or link-disjoint) paths are discovered. For example, a special control message called *Hello* is used in the Cluster based Multipath Dynamic Source Routing (CMDSR) protocol [34]. When the network is large, the control messages used in a multipath routing can flood the network. These messages can consume a significant portion of the available bandwidth thereby adversely affecting the performance of the network.

- **Duplicate packet processing:**
  To ensure reliable data transfer, some multipath routing protocols (e.g. AODVM [7], SMR [30]) send duplicate packets using different paths. Duplicate packets create redundancy and thus consume limited bandwidth. Moreover, special arrangements are required to generate duplicate packets at the source and to filter out these duplicate packets at the destination.

4. On-demand routing protocols for MANETs

Routing in mobile ad hoc networks presents a great challenge, which becomes more difficult when the network size becomes larger. The challenge comes mainly from two aspects: 1) node mobility, which causes frequent topological changes, and 2) limited network bandwidth, which restricts the timely topological updates at each router [13][14]. In On-demand protocols, a route between nodes is initiated whenever there is a desire to establish a link. This is done via a routing discovery process, which is initiated whenever there is a need to transmit data packets to a destination [15]. Most multipath routing protocols mentioned in this paper are based on the principles of the AODV or DSR protocols as shown in Figure 1. However, all multipath routing protocols share a common characteristic, i.e., they discover *multiple* routes between a pair of source-destination nodes [16]. In order to have an understanding of the multipath routing protocols it is necessary to know the basic mechanisms in the DSR and AODV protocols.

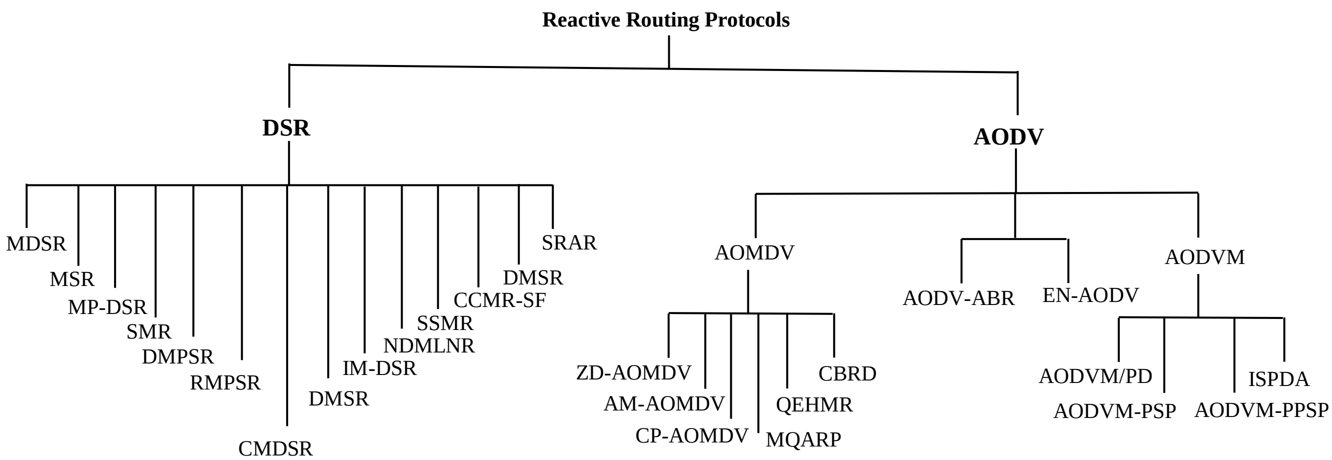

Fig. 1. Multipath routing protocols

4.1 The DSR protocol

The distinct feature of Dynamic Source Routing (DSR) [3][17][18] is the use of source routing. Source routing is a routing technique in which the sender of a packet adds the whole route up to the destination node to the packet header. The intermediate nodes use this to forward packets towards the destination and maintain a route cache containing routes to other nodes. DSR protocol is based on two basic mechanisms: route discovery and route maintenance.

Route discovery involves both *route request* and *route reply* messages. In the route discovery phase, when a node wants to send a packet, it first checks the cache whether there is an entry for that. If yes then it uses that path to transmit the packet and also it attaches its source address on the packet. If it is not there or the entry has expired, the source broadcasts route request packet (RREQ) to all its neighbors asking for a path to the destination. The RREQ message includes a route record which specifies the sequence of nodes traversed by the message. When an intermediate node receives a RREQ, it checks whether it is already in the route record. If yes, it drops the message. This is to prevent routing loops. If the intermediate node had received the RREQ before, then it also drops the message. The intermediate node forwards the RREQ to the next hop according to the route specified in the header. When the destination receives the RREQ, it sends back a route reply (RREP) message. If the destination has a route to the source in its route cache, then it can send a RREP message along this route. Otherwise, the RREP message can be sent along the reverse route back to the source. If an intermediate node has a route to the destination in its cache, then it can append the route to the route record in the RREQ, and send a RREP back to the source containing this route. This can help limit flooding of the RREQ. However, if the cached route is outdated, it can result in the source receiving stale routes.

In the route maintenance phase, when a node detects a broken link while trying to forward a packet to the next hop, it sends a route error (RERR) packet back to the source containing the link in error. When a RERR packet is received, all routes containing the link in error are deleted at that node.

4.2 The AODV protocol

Ad hoc On-demand Distance Vector (AODV) [3][8][17][19][20] is an improvement of the Destination-Sequenced Distance Vector routing (DSDV) protocol. The AODV protocol is called a pure on-demand routing protocol because a mobile node does not have to maintain any routing information if it is not located in an active path. However, as opposed to DSR, which uses source routing, AODV uses hop-by-hop routing by maintaining routing table entries at intermediate nodes. The structure of the route request packet in AODV protocol is different from that of the DSR protocol. To distinguish a fresh route from a stale route, each node maintains two counters called node sequence ID and broadcast ID. Each route request packet contains information about the destination sequence ID and the source sequence ID in addition to the source address and the destination address.

In the route discovery phase, when a source node desiring to send messages does not already have a valid route to the destination, it initiates a route discovery process by broadcasting a RREQ packet to its neighbors, which then forwards the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is reached. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies a RREQ. Along with the node's sequence number and the broadcast ID, the RREQ includes the most recent sequence number it has for the destination.

When an intermediate node knows an active route to the requested destination, it sends a RREP packet back to the source node in unicast mode. Once the destination node or a node with a valid route to the destination has received the RREQ, it will create a RREP intended for the source. The RREP will be unicast along the reverse path. A valid path from the source to the destination will be established when the RREP message arrives at the source node.

In the route maintenance phase, If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbor notices the move and propagates a link failure notification message to each of its neighbors to inform them of the breakage of that part of the route. These nodes in turn propagate the link failure notification to their upstream neighbors, and so on until the source node is reached. The source node may then choose to re-initiate route discovery for that destination if a route is still desired.

5. Multipath routing protocols

Due to multipath routing protocols generally are considered more reliable and robust than single-path routing protocols [21]. Furthermore, whenever a link failure is detected in a primary route, the source node can select the optimal route among the other available routes. This mechanism enhances route availability and consequently reduces control overhead. It also saves energy, enhances data transmission rate, and increases the network bandwidth. Recently, several multipath routing protocols have been proposed, and many of them are based on two popular on-demand routing protocols, DSR and AODV. In this section we will present a selection of them.

5.1 Protocols based on DSR

Multipath Dynamic Source Routing

A multipath extension of DSR protocol called multipath dynamic source routing (MDSR) was proposed by Nasipuri and Das [22]. The main motivation of this protocol is to reduce and efficiently control the frequency of route discovery floods, since these intrinsic parts of on-demand protocol takes up a significant amount of available network bandwidth [23].

In the DSR protocol, a destination node replies to every received request packet. But in MDSR protocol, a destination replies only to a selected set of queries. After receiving all requests, the destination replies back only to those route requests that are link-disjoint from the primary source route (i.e., the shortest path route). The primary source route is the route taken by the first query reaching the destination. The destination node keeps record of the shortest path. Based on the shortest path information, it figures out which later requests to respond to [8]. At the end of the route discovery process, the source is equipped with multiple disjoint routes to the destination. A source keeps all the routes received on reply packets in a cache. When the primary route breaks, then the shortest remaining alternate route is used. A new route discovery is initiated when all routes in the cache are broken [24].

Figure 2 illustrates the idea of the MDSR [9][23] protocol and the utility of the multiple routes maintained at each intermediate node. The source node **S** uses the primary route for sending the data packets until it fails as described by the link sequence $L_1 - L_2 - - - L_k$. Each mobile node in the primary route N_i has its alternative route P_i to the destination node **D**. Whenever the primary route fails to transfer the data packet to the destination, an alternative route will respond by replacing it with a primary route. This process will continue until a link in the route P_i breaks. If a link in the alternative route P_i breaks, it will propagate a route error message backward to the node N_{i-1} and switches the data packets to its own alternative route P_{i-1}. Therefore, whenever the link failure occurs, an intermediate mobile node has to replace the broken link with new alternative route. However, based on the simulation results in MDSR, the alternative route is normally longer than the primary route. Thus, the end-to-end delay packet is increased although the frequency of the route discovery process is decreased.

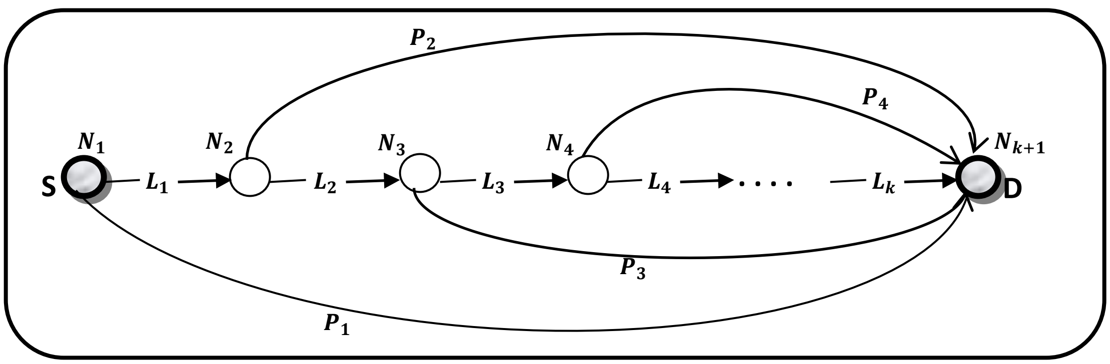

Fig. 2: MDSR protocol. The primary route is depicted by the sequence of links $L_1 - L_2$ -- - L_K. Each node in the primary route N_i , has an alternate path P_i to the destination.

Multipath Source Routing Protocol

Multipath source routing (MSR) protocol was proposed by Wang et al. [25][26] as an extension to the DSR protocol. It aims at improving the throughput of TCP and UDP and the packet delivery ratio, reducing the end-to-end delay and the queue size, while adding little extra overhead. As a result, MSR decreases the network congestion quite well in a simulated MANET environment.

MSR uses almost similar route discovery process in DSR except that multiple disjoint routes are discovered instead of only one used route. Disjoint routes are preferred in MSR protocol because the path independence is very important between routes in multipath routing approach [9]. In this protocol, the source node is responsible for load balancing. Delay is used as the metric to distribute packets over multiple routes [27]. In order to monitor real-time delay information along each path, a feedback control mechanism is used A special type of packet called probing packet is sent periodically to each path to estimate the round trip time (RTT) for each path. This delay information about a path is taken into account while distributing traffic along a path. For example, if a path has a long delay, less traffic is dispatched to that path in order to alleviate congestion [8]. By load balancing, the MSR protocol not only improves the network utility but also balances the energy consumption of each node so increasing the network lifetime.

As an optimization for MSR, the intermediate nodes can reschedule the packets on the fly according to their local multipath load distributing processes, if the intermediate nodes have paths to a destination and they would like to do so. This will allow cascaded multipath routing, which makes full use of network resources without additional protocol overhead.

However, the MSR protocol has its own drawbacks. It needs more routing table space and more processing complexity due to the maintenance of link failure. It needs to handl the route error messages for the extra routes per destination.

Multipath Dynamic Source Routing Protocol

Leung et al. [28][29] proposed a multipath dynamic source routing (MP-DSR) protocol based on the DSR protocol. The objective of this protocol is to provide QoS support in terms of end-to-end reliability, and to probabilistically guarantee the required connection lifetime. This reliability considers the probability of having a successful data transmission between two mobile nodes within the time period from t_0 to t_0 + t, where t_0 is any time instant. Mathematically, this is defined as:

$$P(t) = 1 - \prod_{k \in K}(1- \prod_{S,D}^{k}(t)) \quad (1)$$

Where:

$$\prod_{S,D}^{k}(t) = \prod_{(m,n)\in k} A_{m,n}(t) \quad (2)$$

$$\prod_{lower} = 1 - \sqrt[m0]{1 - P_u} \quad (3)$$

P(t) is the end-to-end reliability of multiple paths, $\prod_{S,D}^{k}$(t) is the path reliability of Ķth path between the source node S and the destination node D, $A_{m,n}(t)$ is the link availability of connecting node m and node n in a time period of t, and $\prod_{lower}$ is the lowest path reliability requirement for each RREQ message.

After the value of $\prod_{lower}$ and the number of paths to be discovered are set, the source node floods a RREQ packet for a set of paths (neighbor nodes). Each RREQ packet contains additional parameters such as $\prod_{lower}$, the path it has traversed (T), the corresponding path reliability ($\prod_{acc}$), etc. When an intermediate node receives a RREQ, it checks whether the RREQ meets the path reliability requirement ($\prod_{acc} > \prod_{lower}$). If yes, the intermediate node adds itself and sends out multiple copies of this RREQ to its neighbors. Otherwise the RREQ packet is discarded [5].

When the destination receives all the RREQ packets, it sorts all the feasible paths (gathered from the RREQ packet) according to the path reliabilities, and selects a set of disjoint paths that together satisfy the end-to-end reliability requirement. A set of RREP packets are sent through each disjoint path back to the source. When the source receives the RREPs, it can begin using the multiple paths to route data [29].

The route maintenance process in MP-DSR contains two scenarios. The first scenario occurs when the time window t_w at the source node expires. The route maintenance in this scenario needs to check the update of reliability before deciding whether a new route discovery process is required or not. The second scenario is the time instant when all paths are broken. In this scenario, the source node directly initiates a new route discovery process without any examination [9][28].

There are two drawbacks in the MP-DSR protocol. First, the mobile nodes in mobile ad-hoc networks cannot move too fast to render QoS routing impossible. Second, the protocol performs some periodical message exchanges, which results in a large number of overhead packets.

Split Multipath Routing protocol

A multipath extension of DSR protocol called split multipath routing (SMR) protocol was developed by Lee and Gerla [8][30]. The main objective of SMR is to reduce the frequency of route discovery processes and thereby reduce the control overhead in the network. The protocol uses a per packet allocation scheme to distribute a load into multiple paths of active sessions.

When the source node has data packets to send but does not have the route to the destination, it floods a *RREQ* packet into the network. Due to flooding, several duplicate *RREQ* messages reach the destination along various different paths. Source routing is used since the destination needs to select multiple disjoint paths to send the *RREP* packet [17].

In SMR, intermediate nodes do not reply to RREQs even if they have routes to the destination. In addition, intermediate nodes forward those RREQ packets received from a different incoming link rather than the link from which the first RREQ is received, provided its hop count is less than the first RREQ [23].

If the first RREQ packet arrives at the destination node, a RREP is generated and sent back on the reverse path which is the "s*hortest delay path*". Then the destination node waits for a period of time to receive more RREQs selects a route that is maximally disjoint to the first route, and sends another RREP packets back to the source via the second route selected [5].

There are three drawbacks in SMR protocol. First, there is extra routing overhead because the duplicate route request packets are not discarded at the intermediate nodes when each node floods too many route request packets. This will result in very high routing load and make SMR inefficient. Second, it builds a maximally backup disjoint route that leads to increasing the power consumption in the network because the data packets travel a long route to the destination. Third, the routing overhead of SMR starts to decrease when the number of nodes exceeds 50. The reason is that when there are more than 50 nodes, the network becomes congested and many control packets are dropped. In such networks, the delivery ratio of data packets is below 10 % [9][31].

Disjoint Multipath Source Routing protocol

Disjoint multipath source routing (DMPSR) was developed by Wisitpongphan and Tonguz [32] as an improvement to the DSR protocol. DMPSR aims to minimize the maintenance cost and achieve a higher level of robustness than DSR. It is expected that DMPSR can reduce the routing overhead and the delay caused by route reconstruction if topology changes frequently. In DMPSR, a source node uses multiple disjoint routs to transmit packets. DMPSR consists of three phases: route discovery, route maintenance, and route destruction. When a source node needs to start the communication, it initiates the Route Discovery process by "gossiping" or broadcasting a Route Request (RREQ) packet with a probability of P=1. The other nodes re-broadcast this request packet with a probability of P<1. Thus, the overhead is minimized in the gossiping approach. According to percolation theory, this probability P can be chosen in such a way that all the other mobile nodes can hear this route request regardless of where the RREQ originates from. This probability is sometimes referred to as the *critical probability* below which the network is in disconnectivity.

When an intermediate node knows how to reach the destination or the destination itself receives a RREQ packet, it generates and sends a RREP packet back to the source node. The source node gathers information from these packets and selects as many disjoint routes as possible. The purpose of choosing disjoint routes is to increase the connectivity of the network (i.e., the source stays connected to the destination for as long as at least one of the routes is active).

In the case of the link breakage, the source continues to send packets over available routes and only reinitiates the route discovery process if all the routes are broken. This approach reduces the routing overhead which can incur if the network topology changes frequently. At the end of the communication session, the source notifies the destination and all the relay nodes about closing the connection so that they release the resources. A node can either choose to erase the route information from its cache or wait for the timer to expire before deactivating the route.

Robust Multipath Source Routing protocol

In order to improving the video communication, the robust multipath source routing (RMPSR) protocol is an extension of DSR protocol introduced by Wei and Zakhor [33]. The main design goal of RMPSR is to minimize video packet loss caused by the changes of network topology. Multipath routing is an efficient choice for video applications in mobile ad-hoc networks because the number of broken links are much less compared to the single path routing approach.

The RMPSR protocol aims to discover multiple nearly disjoint routes between a source and a destination. The primary route connects a source and a destination node. Other alternative routes connect an intermediate node to a destination. The two route sets are nearly disjoint. The route discovery process of DSR is modified to increase the probability of discovering multiple paths. The route sets are constructed at the destination. A destination node collects multiple copies of a request within a given time window. It then builds nearly disjoint multiple paths. A destination node returns the primary route to a source and the secondary route to an intermediate node [8]. The RMPSR uses a per-packet allocation scheme to distribute video packets over two primary routes of two route sets. When one primary route in transmission is broken, the intermediate node that corresponds to the broken link will send a Route Error packet (RERR)to the source node. Upon receiving the RERR packet, the source node removes the broken links from its route cache and switches the transmission to another primary route.

To better support video applications, three new schemes are introduced. First, when the transmitting route is broken, alternative routes are used to salvage packets. This scheme improves the delivery ratio of video packets without retransmission. Second, RMPSR triggers a new route request process before the connectivity is entirely lost. In this implementation, the protocol triggers a new route request when there is only one primary route left in the route cache of the sender. Third, RMPSR protocol increases the probability of discovering multiple disjoint routes at the expense of control overhead. To alleviate the control overhead in the network, both RMPSR and DSR are deployed at each node with different classes of traffic. Video traffic is given higher priority under RMRSR, whilst other traffic is given lower priority under DSR. This scheme helps to maintain high quality of video applications when the amount of data traffic in the network increases.

There are two drawbacks in RMPSR protocol as follows. First, each intermediate node still sends a route error message back to the source node upon link failure. Second, if there are other primary routes available in the route cache, the source needs to start again the route discovery process which results in both large end-to-end delay and consumption of the overall network resources [9].

Cluster based Multipath Dynamic Source Routing protocol

To enhance the scalability of the DSR, A cluster based multipath dynamic source routing (CMDSR) protocol was introduced by An et al. [34]. CMDSR protocol is designed to be adaptive according to network dynamics. It uses a hierarchy to perform the route discovery mechanism and distribute traffic among diverse multiple paths. The main idea of this protocol is to prevent the network flooding and minimize the routing overhead control messages.

The CMDSR protocol is based on the 3-level hierarchical scheme, which is given in Figure 3. The 0-node is the first level of the cluster. The 1-cell cluster is the second level of cluster. Here each node of the cell is one hop away from the cluster head. The 2-server cluster gathers a set of cells of which the Server is the leader [35]. Due to node mobility, the clusters change dynamically. The neighbor node information is exchanged among nodes and a cluster head is selected among these nodes. The procedure of choosing a cluster head is based on owning token first (OTF) and minimum ID (MI). A token is an attribute of a node that defines whether a node can be a cluster head or not. In this procedure, a node owning the token becomes the cluster head or the node with minimal ID is selected as the cluster head when many nodes own the token. [10]. Hello messages are used by a cluster head to update the cluster information. When a cluster member does not receive three Hello messages continuously from its cluster head, it assumes that the link is broken. Then the member node can select another cluster head and if it cannot hear from any cluster head, it becomes a cluster head itself. The cluster heads work together to select a server among themselves. During the route discovery mechanism, many paths are discovered from a source to a destination. The quality of a path is considered important in CMDSR. CMDSR selects a reliable path only. The path reliability is calculated based on the availabilities of all the links along a path [8].

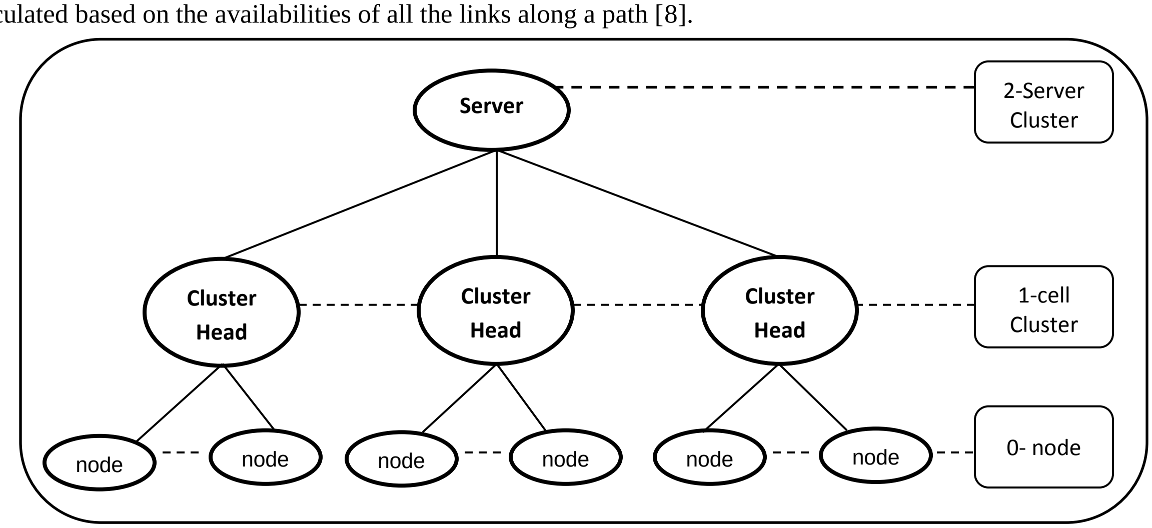

Fig. 3. Cluster based multipath routing .

There are two drawbacks in CMDSR protocol. First, every node needs to broadcast HELLO messages regularly. Second, the path-sorting algorithm is required to sort all the feasible paths in a descending order according to their accumulated path reliabilities.

Dynamic Multipath Source Routing

DMSR is an extension of DSR protocol proposed by Yang and Huang [36] to transmit the data packet over multiple routes simultaneously. The main design goal of DMSR is to improve the packet delivery ratio and reduce the routing overhead. As the traffic load and topology changes are more significant, the protocol advantage is more remarkable. In most of the scenarios in DMSR, the data packets are transmitted over 2 or 3 routes simultaneously which can decrease the end-to-end delay and increase the reliability of the network.

When a source node initiates a QoS request which includes (*SourceID*, *RREQID*, *Routing_list*, H_{max} and B_{min}), it firstly checks whether it has the routing information to the destination node. If not, it begins to broadcast RREQ to its neighborhoods. When the intermediate nodes receive this RREQ, it follows the following steps.

Step 1 If the current node is in the Routing_list of RREQ, it will discard the RREQ to avoid the routing loop. Otherwise, goto step 2;

Step 2 If the Source ID and RREQID is not included in the routing table, which means the current node receives this RREQ for the first time, it calculates the corresponding value of the bandwidth. If the value can't meet the requirement denoted by B_{min}, the RREQ will be discarded. Otherwise, goto step 3;

Step 3 Add the value of bandwidth to the RREQ. Then the RREQ will be forwarded. Goto step 1. When the destination node receives the first RREQ, it caches the RREQ and sent RREP to the source node. During the period of time the destination node collects other arriving RREQs which will be used to select node disjoint multipath routing. Through all RREQs' *Routing_list*, the destination node can construct a certain topology of the network.

In the routing maintenance of DMSR, due to the dynamic changes of resources, a node may have not enough resources to reserve after it receives RREP. For the moment, RERP will be sent to start the error processing. In the stage of error processing, the node which is unable to meet the conditions for reserving resources will send a failure message to the destination node along the feasible path and release the resources already reserved.

In the case of nearly static topology, the overhead of DMSR is higher than in a dynamic topology because it needs to build a stable multipath routing which causes more control packets. However, the decrease of pause time of nodes will lead to more disconnected links.

Improvement of Dynamic Source Routing

The IM-DSR multipath protocol is an extension of DSR protocol proposed by Khazaei [37] to improve fault tolerance and QoS. The main goal of IM-DSR is to reduce the packet loss and increase the reliability of the network. To achieve this goal, the IM-D SR protocol has modified the route discovery, route reply and route maintenance process of DSR protocol.

There are two techniques used in the IM-DSR protocol namely, local recovery, and alternative route. The alternative routes are created from the source to the destination during the route reply and route maintenance processes. Local recovery techniques are very useful despite the fact that they consume the limited energy of each node.

Suppose that a link is broken while sending a packet. At first, a node chechs the route cache and deletes all routes containing the broken link, and then one of the following actions is done by the type of packet.

- If transitional packet is a RREQ, it will not send RRER to the source node.
- If transitional packet is a RREP, it will send RRER to the node which makes the RREP.
- If transitional packet is a RRER, it will examine how many times the packet will be saved. If it is the first time, the packet will be saved by examining a route cache and finding alternative route. The RRER is sent to the destination through that route then the RRER is made and it will report the broken link to the source of RRER. If it is not the first time or if an alternative route is not in the route cache, the RRER will be deleted and only a RRER will be sent to the source node.
- If transitional packet is a data packet, it will examine how many times the packet will be saved. If it is less than three, the data packet will be sent by examining their route cache and alternative route then it will send

a RRER to the source node. If it is more than three or if an alternative route is not in the route cache, the data packet will be deleted and only a RRER will be sent to the source node.

The simulation results show that IM-DSR is very effective in decreasing the packet loss and increasing the fault tolerance. In all of the cases, IM-DSR has the higher packet delivery ratio than the DSR protocol. It also maintains acceptable overhead by improving route maintenance. Therefore the IM-DSR protocol is very useful for the applications that need a high level of reliability.

Node Disjoint Multipath Routing Link and Node Stability

Shuchita and Charu [9][38] proposed a node disjoint multipath routing link and node stability (NDMLNR) protocol based on DSR protocol. The main objective of NDMLNR is to find the multiple node disjoint routes from source to a given destination and keep track of the route bandwidth which is used by the source to select the optimal routes. In NDMLNR protocol, some modifications are made to the Route Request (RREQ) and Route Reply (RREP) packets of DSR protocol to enable the discovery of link stable node disjoint paths. Link stability derived from the factor stability depends directly on mobility factor and inversely on the energy factor. Hence, Link Stability Degree is defined as:

$$\textbf{LSD = Mobility factor / Energy factor} \qquad \textbf{(4)}$$

The LSD defines the stability degree of the link. The higher the value of LSD, the stability of the link is higher. When the LSD of a node falls below LSD_{thr}, it informs its predecessor node of the failure by sending the NODEOFF packet. Once a node receives such a packet, it sends the ROUTEDISABLE packet to the source node. The source can then reroute the packets through the backup routes. If no backup route exists, the source then starts the route discovery procedure again.

Simple Split Multipath Routing

SSMR is an improvement of the SMR protocol proposed by Liyan et al. [39], in order to reduce the number of control packets, balance the load and improve the packet delivery. In the SMR protocol, instead of dropping every duplicate RREQ, intermediate nodes forward the duplicate packets whose hop count is not larger than that of the first received RREQ. This leads to the increase of routing load and makes protocol inefficient. Therefore, SSMR is proposes an approach to record the number of RREQ forwarded by intermediate nodes, and limits this number up to four. When the number of forwarded RREQ reaches four, the others are dropped directly. This leads to the decrease of the number of RREQ and reduction of the routing load. When the destinations receive the first RREQ, they send the first RREP immediately. Then they send another RREP when the number of RREQ reaches four. This approach not only gets sufficient RREQ to send RREP, but also decreases the end-to-end delay through restricting the number of RREQ received by the destinations.

The route discovery and route maintenance processes of SSMR are based on the SMR protocol. However, to construct a maximally backup disjoint route in SSMR protocol, the energy consumption in the network will be increased because the data packets flow travels via a long route to the destination node. In addition, the SSMR has high routing loads when mobility is present.

Congestion Controlled Multipath Routing Algorithm based on Path Survivability Factor

A multipath extension of the DSR protocol called Congestion Controlled Multipath Routing Algorithm (CCMR-SF) protocol was developed by Daniel et al. [40]. The main goal of CCMR-SF is to find the alternate mechanism that will find out optimal and reliable paths in terms of congestion and number of hop counts. In this protocol, the route maintenance process is different from that of DSR because the use of **delay time** and **alert packets**. Alert packet is a type of acknowledgement packet. It is sent from destination to source at regular intervals of time (*delay time)* to tell the source that the current path is still valid. Delay time is 2.5 times the average time required by the alert packet to traverse the most distantly separated nodes in the network at the condition of average congestion level. The delay time will be governed by two factors. The first, factor is the traffic, which is the average congestion that can exist in longest path of the network for timely delivery of alert packet. The Second is the distance between two farthest pair.

The route discovery process of CCMR-SF is based on the DSR protocol. However, after receiving the first route reply, the source sends all the data packets to the destination using the path retrieved from the RREP. Additional

RREP that source node gets will act as an **alternate** to the current path. The RREP packet contains three parametric values of that path:

i. Number Of Hops Travelled (N): It is the number of nodes traversed.
ii. Traffic Load (T) At Any Node:
Traffic Load (T) = (Outgoing traffic at that node) - (Incoming traffic at that node).
iii. Bandwidth (B): It is the minimum bandwidth value of all links that the RREP traverses.

Depending on these three parameters, Survivability Factor for every path will be calculated by:

SF=function (B, T, N) (5)

The priority of the paths is based on SF. After determining the first path, the node will start sending the packets and for all subsequent route replies it shall calculate SF for them and prioritize them accordingly. In CCMR-SF, a very useful data structure tree has been employed for the accomplishment of the set of objectives of the algorithm. Besides giving multiple paths it identifies the exact location of the link failure. Also as the paths are arranged in order of decreasing survivability factor (how much survivable or reliable the path is), the the path with more value of survivability factor is chosen first.

Traffic Sensitive Dynamic Source Routing Protocol

A multipath extension of the DSR protocol called traffic sensitive dynamic source routing (TSDSR) was proposed by Kulkarni and Chimkode [41]. The main goal of this protocol is to improve the performances of a network in terms of throughput, packet delivery ratio, delay and normalized routing load as compared to the DSR protocol. This protocol modifies DSR to find node disjoint paths in increasing order of the Individual Fishing Quota (IFQ) occupancy (traffic), such that the IFQ occupancy at none of the intermediate nodes exceed the threshold value (60 %).

When intermediate nodes receive RREQ packets, there are two possibilities. First, if the source has the intermediate node's address then the node discards the RREQ packet, to avoid duplicate RREQ's. Second, if the intermediate node's address is not there in the source route then the node adds its address and forwards the RREQ after recording the IFQ occupancy at the node. When a RREQ packet is reached at a destination, the destination replies back to a source using the RREP packet. While RREP is traveling to the source node the IFQ occupancy at each intermediate node it visits is checked. If the IFQ occupancy exceeds the threshold (60 %) then the intermediate node will discard the RREP packet.

After receiving RREP messages, a source prepares as many disjoint paths as possible by using the information content of a route reply packet. The maximum number of paths from the source to any destination is restricted to three. A source sends packets using the path that has less traffic. When reverse routes are used in all probability, the source will first receive the least traffic path, as the path taken by RREP packet is also along the nodes with less traffic. If a route is broken, a source continues sending packets by using other alternative paths. If all routes are broken, a source initiates another route discovery.

Stable Route Aware Routing

Dhanda and Chaudhry [42] propose a stable route aware routing (SRAR) protocol based on DSR protocol to construct a stable and reliable path. The objective of this protocol is to reduce routing overhead and energy consumption at the same time with improving packet delivery ratio and throughput, especially in high mobility scenarios.

The SRAR protocol introduces dynamic power management (DPM) awareness into the routing decisions and finds multiple stable routes from the source to the destination. DPM technique supports energy conservation by making mobile nodes to sleep when no data communication is taking place. In this protocol, the route uptime factor (RUF) is defined as a metric which indicates the earliest up time when the link between any pair of adjacent nodes on a route is going to be interrupted due to one (or both) of the nodes being put to sleep. The RUF contains the all link uptime value between two nodes which satisfied the transmission threshold value. Then each node stores the link uptime vector which contains the all stable links between two nodes from the source to the destination.

The SRAR protocol adds four new entry types to the RREQ packet as below.

i. Link uptime vector ($t_i^{auptime}$; I Є (1,… N-1)) for the route.
ii. Partial route R_{ij}=(V_i , V_{i+1} ,..... V_k ,............. V_j, V_{j+1}).

iii. Earliest up-time of last-upstream node ($t_i^{auptime}$).

iv. Threshold value (Th = t_{data} transmission time of each data packet).

Where t^{uptime} is the uptime of the link and V_i is the source node. This protocol also adds three new entry types to RREP packet:

a) Source route R_{ij}=(V_i , V_{i+1} ,..... V_k ,............. V_j, V_{j+1}).

b) Link uptime vector ($t_i^{auptime}$; i Є (1,… N-1)).

c) Earliest up time. The minimum of all the Link Uptime Vector elements.

d) Estimated transmission time.

To identify the stable path, the SRAR protocol work in the following steps:

1) Source node initiates the data transmission request.
2) Check for the destination node in route cache. If found then forward the data packet to destination.
3) If the destination node is not found in the route cache then broadcast the route request packet to their neighbor node.
4) Calculate the link uptime value $t_i^{auptime}$ between the node V_i to V_{i+1}.

$$t_i^{auptime} = \text{average } (t_i^{up}, t_{i+1}^{up}) \qquad (6).$$

5) If $t_i^{auptime}$ > Th (Threshold) then add in to the link uptime vector and data packet is forwarded to the next node.

$$L_{ij} =(t_i^{auptime} , t_{i+1}^{auptime} , t_k^{auptime} , t_{k+1}^{auptime} , t_{j-1}^{auptime}) \qquad (7)$$

6) If any intermediate node receives more than two RREQ packets, it does not forward these all RREQ packets to their neighbor node. When the uptime of previous RREQ is greater than to the received RREQ, discard the received RREQ and forward the previous RREQ uptime.
7) Repeat step 3 to step 6 until the destination is found.
8) If destination found then store all routes in the routing table in decreasing order of **Route Uptime Factor**.

$$RUF_{ij} = \max (t_i^{auptime} , V_i \in , t_i^{auptime} \in L_{ij}) \qquad (8)$$

and send RREP to the first entry of the routing table. In the route reply phase, the destination node only sends the RREP packet which contains the first entry of the routing table. Hence, it leads to reducing the total transmission time between source to destination.

The drawback of SRAR protocol is hard in the sense that it may discard any RREQ which is predicted to be non-stable and thus might lead to a scenario where the source node fails to discover any stable path to the destination node.

5.1.1 **Comparison**

The key distinguishing features of the on-demand protocol DSR are loop-free and source-based. But it provides only single path routing, although, it could be improved to support multipath routing. In DSR, each data packet carries the complete path from the source to the destination as a sequence of IP addresses. When the network becomes larger, control packets and message packets also become larger. Clearly, this has a negative impact due to the limited available bandwidth. The DSR protocol also suffers from a scalability problem due to the nature of source routing.

A large number of multipath routing protocols can be seen as attempts to improve the performance of the DSR protocol under various operating scenarios. Some of these scenarios involve improving QoS and the throughput of TCP and UDP, or minimize packet loss and traffic congestion.

One of the main improvement directions has been the finding of multiple disjoint routes. Various approaches have been taken by the protocols. MDSR [22] (using an alternate path to the destination), MSR [25] (based on delay), MP-DSR[28] (based on end-to-end reliability), SMR [30] (depending on hop count), DMPSR [32] (based on gossiping), RMPSR [33] (improving video communication), DMSR [36] (using Delay-Bandwidth metric), NDMLNR [38] (based on the stability of the link), SSMR [39] (restricting the number of RREQ up to four), TSDSR [41] (depending on Individual Fishing Quota).

There are other directions considered by the protocols, e.g., QoS as in IM-DSR [37], hierarchy to perform the route discovery, as inCMDSR[34]. Finally, there are some protocols which extend upon the DSR by considering various additional networking challenges, such as congestion controlled (CCMR-SF [40]) and stable route (SRAR [42]).

Table 1summarizes the protocols reviewed in this section and compares some of their key features.

Table 1: Multipath routing protocols extension of DSR

Protocols	Tool	Objective	Num. of Paths	Drawback
MDSR 1999	An alternate disjoint route to the destination.	To reduce and efficiently control the frequency of route discovery flooding.	<=2	Increased end to end packet delay due to that the alternative route is longer than the primary route.
MSR 2000	Probing mechanism and Round Trip Time (RTT) for each path.	To improve the throughput of TCP and UDP, packet delivery ratio and reduce the end-to-end delay and the queue size.	Set of disjoint paths	requiring more routing table space and increased processing complexity for the maintenance of link failure.
MP-DSR 2001	End-to-end reliability, path reliability, link availability.	To provid QoS support in terms of end-to-end reliability and guarantee the required connection lifetime.	Set of disjoint paths	1. The mobile node cannot move too fast to render QoS routing impossible. 2. Periodic message exchanges result in a large number of overhead packets.
SMR 2001	Forward of duplicated RREQ and build maximally disjoint multiple paths.	To reduce the frequency of route discovery and the control overhead in the network.	2	1. Extra routing overhead because the duplicates route request packets are not discarded from the intermediate node. 2. Building a maximally backup disjoint route leads to the increase of power consumption in the network because the data packets travel via a long route to the destination. 3. The delivery ratio of SMR starts to decrease below 10% when the number of nodes exceeds 50. The reason is that for more than 50 nodes, the network becomes congested and many control packets are dropped.
DMPSR 2003	Gossip based route discovery mechanism.	To minimize the maintenance cost and achieve a higher level of robustness than DSR.	Set of disjoint paths	Data rate per route becomes very small and decays slowly while the overall distance continues to increase linearly as the spatial density increases.
RMPSR 2004	Discover multiple nearly disjoint routes.	To minimize video packet loss caused by network topology changes.	2	1. The intermediate node still sends a route error message back to the source node upon link failure. 2. If there is other primary route available in the route cache, the source needs to start again the route discovery process which results in large end-to-end delay and consumes network resources
CMDSR 2005	Utilizing clustering algorithm	To reduse the routing overhead and improve the network scalability.	Set of disjoint paths	1. Every node should broadcast HELLO messages regularly. 2. Path-sorting algorithm is required, which it sorts all feasible paths in a descending order according to their accumulated path reliabilities.
DMSR 2008	B_m : The minimum bandwidth metric.	To increases the packet delivery ratio and routing overhead.	3	In the case of nearly static topology, the overhead of DMSR is much higher than in dynamic topology because it needs to build a more stable multipath route causing more control packets and the decrease of pause time of nodes leads to more proken links.
IM-DSR 2010	Using local recovery techniques and alternate route.	To reduce the packet loss ratio and increase the data transfer to improve fault tolerance and QoS.	3	1. Local recovery techniques consume the limited power of each node. 2. The data packet needs to be saved for three times.
NDMLNR 2010	The degree of the link stability (LSD).	To find the multiple node disjoint routes and keep track of the route bandwidth which can be used by the source to select the optimal routes.	2	If there are no backup routes in the route cache, the source re-initiates route discovery process.
SSMR 2010	Record the number of RREQ forwarded by the intermediate nodes and restrict the request packet up to four only	To reduce the number of the control packets, routing load and improve packet delivery.	2	1. The energy consumption in the network will be increased because of the data packets flow traveling via a long route to the destination node. 2. It has high routing loads when mobility is present.
CCMR-SF 2011	Survivability factor	To find out optimal and reliable paths in terms of congestion and number of hop counts.	Set of paths	The paths are arranged in order of decreasing survivability factor that leads to the increase of the power consumption in the network.
TSDSR 2012	Individual Fishing Quota (IFQ)	To improve the network performance in terms of throughput, packet delivery ratio, delay and normalized routing load	3	Building a maximally disjoint path leads to the increase of the power consumption in the network because the data packets travel via a long route to the destination.

SRAR 2013	DPM and RUF	To reduce routing overhead and the energy consumption and to improve packet delivery ratio and throughput, especially in high mobility scenarios.	Set of paths	It is hard in the sense that it may discard any RREQ which is predicted to be non-stable and thus might lead to a scenario where the source node fails to discover any stable path to the destination node.

Tools: mechanism of selecting multiple routes in the protocol.

5.2 **Protocols based on AODV**

On-demand Multipath Distance Vector Routing protocol

A multipath extension of AODV protocol called on demand multipath distance vector (AOMDV) protocol was proposed by Marina and Das [17][43][44]. The main idea of AOMDV protocol is to provide efficient fault tolerance in the sense of fast and efficient recovery from route failures in highly dynamic networks where link failures and route breakages occur frequently. It reduces end-to-end delay more than a factor of two, and is also able to reduce routing overhead and the frequency of route discoveries by about 20% but increases the number of delivered packets. The AOMDV protocol consists of two main components, i.e., a rule for route updates to find multiple loop-free paths at each node, and a distributed protocol to compute the link-disjoint paths.

In this protocol, each route arriving at a node during route discovery potentially defines an alternate route to the source or the destination. Accepting all of them to construct routes will lead to routing loops. In order to eliminate any possible loops, the AOMDV uses new metric of “advertised hop count”. The advertised hopcount represents the maximum hop counts of each of those available multiple paths. The protocol only allows to accept alternate route with lower hop counts. This metric is necessary to guarantee loop free. The AOMDV protocol computes link-disjoint paths per route discovery. With multiple redundant paths available, the protocol switches routes to a different path when an earlier path fails. Thus a new route discovery is avoided. For efficiency, only link disjoint paths are computed so that the paths fail independently of each other.

Note that link disjoint paths are sufficient for our purpose, that is, using multipath routing for reducing routing overhead rather than for load balancing. Therefore, node disjoint paths are more useful, as switching to an alternate route is guaranteed to avoid any congested node. The AOMDV protocol [31][45]achieves the best performance in high mobility scenarios. When increasing the network density, the protocol’s performance decreases and it has the additional overhead of more RREPs per route discovery.

On-demand Distance Vector Multipath

A multipath extension of AODV protocol called on demand distance vector multipath (AODVM) protocol was proposed by Ye et al. [7][21]. The main goal of AODVM is to primarily design a multipath routing framework for providing enhanced robustness to node failures. In order to provide the reliability of paths and security, AODVM introduces reliable path segments, which is formed by reliable nodes. Nodes that join two segments have to be reliable nodes.

In AODVM protocol, instead of discarding the duplicate RREQ packets, intermediate nodes store the information contained in these packets in a table called RREQ table. When an intermediate node receives a RREQ packet, it records the following information in its RREQ table: the source ID, the destination ID, the neighbor list as shown in Figure 4. Furthermore, an intermediate node located between a source and a destination is not allowed to send a reply to the source.

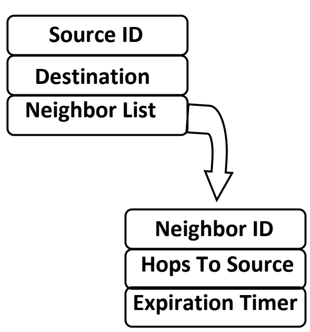

Fig. 4. The Structure of each RREQ table entry in AODVM

When the destination receives the RREQ packet, it updates its sequence number and generates a RREP packet. The RREP packet contains an additional field called ***last hop ID*** to indicate the neighbor from which the particular copy of RREQ packet is received. A destination node generates RREP packets for each RREQ packet received from its neighbors. When an intermediate node receives a RREP packet from a neighbor, it deletes the entry corresponding to this neighbor from its RREQ table and adds a routing entry to its routing table (shown in Figure 5) to indicate the discovered route from itself to a destination node. The node determines the neighbor in the RREQ table via the shortest path to the source, and forwards the RREP packet to that neighbor. Then, the entry corresponding to this neighbor is deleted from the RREQ table. When an intermediate node receives RREP packet and if it is unable to forward received packet (no entries in its RREQ table), it generates a Route Discovery Error (RDER) packet and sends it to the neighbor that the RREP is received from.

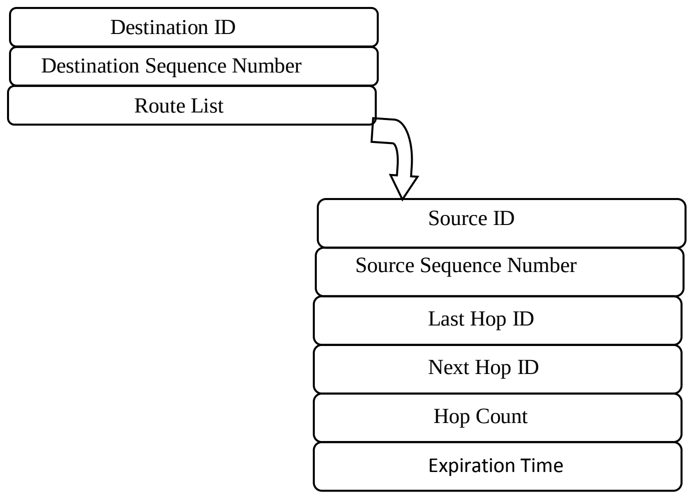

Fig. 5. Structure of the each routing table entry in AODVM

The neighbor, upon receiving the RDER packet, will try to forward the RREP to a different neighbor which forwards it further towards the source. Since an intermediate node makes decisions on where to forward the RREP packet (unlike in source routing), a source node and a destination node are unaware of that forwarding decision. Thus, when a source node receives a RREP packet, it should confirm each received RREP packet by sending a route request confirmation message (RRCM).

In AODVM protocol, the sequence number is used to prevent loops. When a source node initiates a RREQ, it increases its sequence number and the destination sequence number. If the destination receives a new RREQ packet, it computes a new sequence number and includes it in the RREP packet.

Multipath AODV with Path Diversity protocol

A multipath extension of AODVM protocol called on demand distance vector multipath with path diversity (AODVM/PD) protocol was proposed by Mueller and Ghosal [46]. The main objective of AODVM/PD protocol is to find diverse paths with a correlation factor between paths. It provides both smaller end-to-end delay than AODVM in networks with low mobility and better fault tolerance.

In AODVM/PD, the route discovery process is similar to that of the AODVM protocol. The main difference between AODVM/PD and AODVM is that AODVM/PD depends upon the correlation factor metric. The correlation factor of two node-disjoint paths is defined as the total number of links connecting the paths. In order to implement AODVM/PD, a node maintains three parameters during route discovery: (1) L*ocal Correlation Factor (LCF)*, which measure of how many RREPs associated with a given route discovery that a node has overheard. (2) A*rea Correlation Factor (ACF)*, which is the weighted average of a node's local correlation factor and the average of its neighbors' local correlation factors and (3) C*orrelation Threshold (CT)*, when a node's area correlation factor is over the correlation threshold, the node is no longer allowed to participate in any routes for the particular route discovery.

In AODVM/PD protocol, a modification is made to the route reply and route confirmation phases of AODVM. When a node overhears a RREP packet, it increments its local correlation factor by 1 as shown in Figure

6. When a node receives a RREP addressed to it and its ***ACF*** is greater than the ***CT,*** it sends a Route Discovery Error (RDER) packet to the sender. Otherwise, the node selects the neighbor from the RREQ table with the shortest hop count to the source, and forwards the RREP to that neighbor. If a node overhears an **RRCM**, it broadcasts a Correlation (CORR) packet containing its local correlation factor. When a node receives a CORR packet from a neighbor, it updates the local correlation of its neighbor in the RREQ table. The node then calculates its ***ACF***. If it's ***ACF*** is greater than the ***CT***, then it broadcasts another ***CORR*** packet with the OVER_THRESHOLD flag set to true. When a node receives a CORR packet with the OVER_ THRESHOLD flag set, it deletes the sending node from its RREQ table. When the destination receives an RRCM, it sends the next RREP to a neighbor from its RREQ table. The purpose of the route confirmation phase is to remove nodes with a relatively high area correlation from RREQ tables.

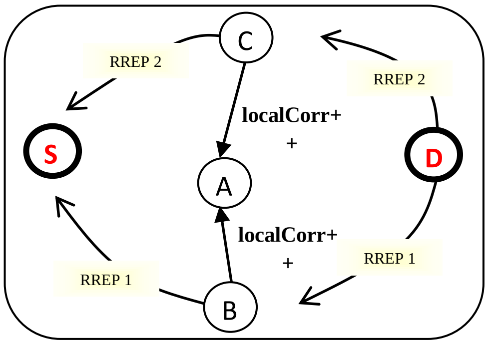

Fig. 6. Basic route reply operation of

The AODVM/PD protocol has two drawbacks as follows. First, when the mobility level of the nodes increases, the delay becomes greater than AODVM. Second, the control overhead is Increased due to the transmission of CORR packet during the route discovery phase.

Multipath AODV with Path Selection Probability

Ad hoc on demand distance vector multipath with path selection probability (AODVM-PSP) protocol was developed by Jing et al. [8][47] as an improvement to the AODVM protocol. It considers route probability value as the most important factor in selecting a route. The main objective of AODVM-PSP protocol is to provide load balancing, alleviate congestion and bottlenecks.

In AODVM-PSP, the route discovery process is similar to that of the AODV protocol. The multiple routes are set up in a similar manner as that of the AODVM protocol. The main difference between AODVM-PSP and AODVM is that AODVM-PSP depends on transmission delay time T_i (s,d) along a route while making a routing decision. When a node sends a packet to one of its destinations, the packet contains time information it was transmitted. The destination node or intermediate node can estimate the delay based on the information included in the packet. When the source node gets the transmission delay time of a packet transmitted between the source node *s* to the node *d* via the route *i* in the network, the route is selected according to the goodness (probability) of each route. The routing probability $P_i(s,d)$ is inversely proportional to the transmission delay time $T_i(s,d)$ as follows:

$$P_i(s,d) \infty \frac{1}{T_i(s,d)} \qquad (9)$$

In order to reduce overhead, a modified version of the probability of selecting a path has been defined as:

$$P_i(s,d) \quad \frac{\frac{1}{T_i(s,d)}}{\sum_{i=1}^{k} \frac{1}{T_i(s,d)}} \qquad (10)$$

Where **k** is the number of paths between a source and a destination. In the AODVM-PSP, the route discovery process and the route maintenance process avoid the keep-alive packet and provide route resilience, unlike AODVM.

The AODVM-PSP protocol consists of three limitations. First, there may be a possibility of missing efficient routes due to the fact that the re-discovery process is not initiated frequently. Second, the node forwards the data packet by the chosen route that may not be the best route. Third, the overhead of a route discovery in multi-path routing is much higher than that of single-path routing.

On-demand Multipath Routing Protocol with Preferential Path Selection Probabilities

Ad hoc on demand distance vector multipath with preferential path selection probability (AODVM-PPSP) protocol was developed by Jing et al. [48] as an improvement to the AODVM-PSP protocol which considers the least transmission delay time and node throughput values as the most important factors in selecting a route. The main objective of AODVM-PPSP protocol is to find multiple routes, with higher packet delivery ratio and lower routing packets.

In AODVM-PPSP, the route discovery process is similar to that of the AODV protocol. The multiple routes are set up in a similar manner as that of the AODVM protocol. The main difference between AODVM-PSP and AODVM-PPSP is that AODVM-PPSP depends on the transmission delay time T_i (s,d) and node throughput along a route while making a routing decision. According to the goodness (probability) of each route, the route is selected. In the AODVM-PPSP, the routing probability Pi(*s*,*d*) of a node *s* to *d* is constrained as follows:

$$\sum_{i=1}^{K} P_i\,(s,d) = 1,\ \ s,d \in [1,N] \qquad (11)$$

Where *N* is the number of nodes in the network. In order to reduce overhead, a modified version of the probability of a path has been defined as:

$$P_i(s,d) = \frac{\frac{1-a}{T_i\,(s,d)}}{\sum_{i=1}^{k}\frac{1}{T_i(s,d)}} \qquad i \in [2,K] \qquad (12)$$

Where a is the degree of preference for the selection of routes and it is obtained with the throughput (s) of node s.

$$a = f(\text{Throughput}(s)) \qquad (13)$$

The AODVM-PPSP protocol adapts the path selection activity to the varying data traffic status and preference the route with the least transmission delay time. In addition, It switches degree of preference considering node throughput. Whenever the node *s* get the new transmission delay time Ti(*s*,*d*)of the route *i*, the routing probability will be updated as same as routing probability obtaining. The multiple routes are efficiently selected and thereby resulted in a higher packet delivery ratio and lower routing packets.

The AODVM/PPSD protocol consists of two drawbacks as follows. First, the only exploration overhead of this protocol is a slight increase in the size of the packets. Second, it needs to update the routing table of the low probability routes with more data packets. At the same time, there is a drawback of repeated usage of low probability routes, which have a low performance record.

Adaptive Backup Routing protocol

A multipath extension of AODV-BR protocol called adaptive backup routing for mobile ad-hoc networks (AODV-ABR) protocol was proposed by Lai et al. [17][49]. It sets up a mesh and multipath routing using RREP packets and aims to reduce control overhead. The mesh structure can be created by overhearing the data packets transmitted from neighbor nodes. This helps to increase the adaptation to topology changes without transmitting extra control messages.

In AODV-ABR protocol, when a node detects a broken link, it will perform a handshake process. The handshake procedure is accomplished by two one-hop control signals: BRRQ (Backup Route Request) and BRRP (Backup Route Reply). The format of BRRQ and BRRP packets are shown in Figure 7. When the link between node B and node C breaks, node B will broadcast a BRRQ signal to its neighbors. Then node E and node F will send BRRP with the hop count to node B. Node B will choose node F as the next hop to the destination, and then transmit data packets to node F. Node B and F will update its routing tables to reflect these changes.

In AODV-ABR protocol, AODV–LR (Local Repair) repairs the link locally if the broken link is not far away from the destination, but AODV-ABR could repair the link anywhere along the primary route if alternate routes exist. Therefore, AODV-ABL process combines AODV-ABR with AODV-LR algorithm. If the distance

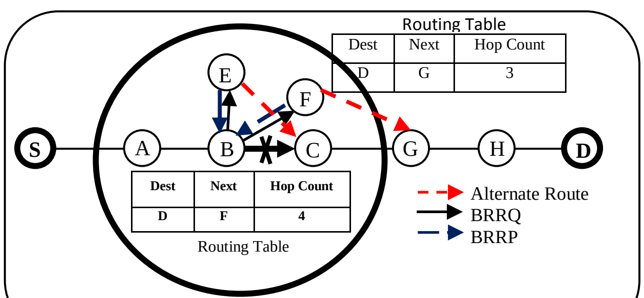

Fig. 7. Re-route of data packets in AODV-ABR.

between the broken link and the destination is less than MAX_REPAIR_TTL hops, AODV-ABL would try to repair the link by broadcasting a RREQ control signal as AODV-LR , otherwise the AODV-ABL will repair the link by a handshake process. When the data transmission rate is exceeded to 8 packets per second, AODV-ABL still has the best performance and AODV-ABR becomes slightly better than AODV–LR. The traffic load will become heavier, when more nodes participat in a wireless network. The probability of packet collisions will increase, resulting in the degradation in overall performance.

Zone-Disjoint On-Demand Multipath Distance Vector Routing

Javan et al. [50] proposed zone-disjoint on demand multipath distance vector (ZD-AOMDV) protocol [50] as an extension to the AOMDV protocol. It utilizes common omni-directional antennas, rather than directional ones and transfers data through multiple zone disjoint paths simultaneously. The objective of ZD-AOMDV is to increase the packet delivery ratio and achieve less average end-to-end packet delay as compared to AOMDV protocol.

The ZD-AOMDV uses the concept of "Active Neighbor". Active neighbors are the neighbor nodes which have already received and replied to the RREQ and it is probable that they exist on other paths for the same source and destination, so even though they are located on two disjoint paths they will still affect each other in simultaneous data transfer. In this protocol, the nodes in zone-disjoint paths have almost no neighbor in the other path. The ZD-AOMDV counts the number of active neighbors for each path from the source to the destination and choose paths that have the lowest total number of active neighbor nodes.

In this protocol, each node should save the RREQ messages it receives from other nodes in RREQ_Seen table. Also, there is an additional field in RREQ_Seen table, called After _Active _Neighbor _Count (After_A_N_C), which will be used to count the number of active neighbors. In order to make the subsequent nodes to know the total number of active neighbors of the traversed nodes along a path, a new field called ActiveNeighborCount is added to the headers of both RREQ and RREP packets.

RREQ_ Query and RREQ_Query_Reply are added to the route discovery process. Figure 8 shows an example of ZD-AOMDV protocol. When a source node S wants to send data to D, it first looks into the route table to find a route. If a source cannot find a route in its route table, the source initiates a route discovery mechanism by broadcasting a request packet to its neighbors and set the After_A_N_C to zero. When a neighbor A, B, and C of a source receive a request packet, it will insert its address into the RREQ packet and will store the information of the packet in RREQ_Seen table. Then each of them will broadcast RREQ_Query packet. After performing the queries, nodes A and C will each recognize node B as their active neighbor and increment ActiveNeighborCount by one. Node B will recognize both A and C as active neighbors and increment its ActiveNeighborCount by two. After that each nodes A, B, and C will broadcast their RREQ packet.

When a destination receives a RREQ packet through node B, the active neighbor value of this path (S-B-D) is two. Nodes E and F will receive the RREQ message and will initiate the query process, through which they recognize node B as their active neighbor and will increment the *ActiveNeighborCount* in their RREQ message. Since node B broadcasted the same RREQ message before; it will respond to node's E and F's queries with positive *RREQ_Query_Reply* and at the same time it will increment the *After_A_N_C* by one for each of those queries. As shown in figure 8-b, all the RREQ messages which arrive at the destination will have the same ActiveNeighborCount value as two. The destination node sends a RREP packet to every received RREQ packet and will also update the ActiveNeighborCount value of RREP packet with the same value in the RREQ.

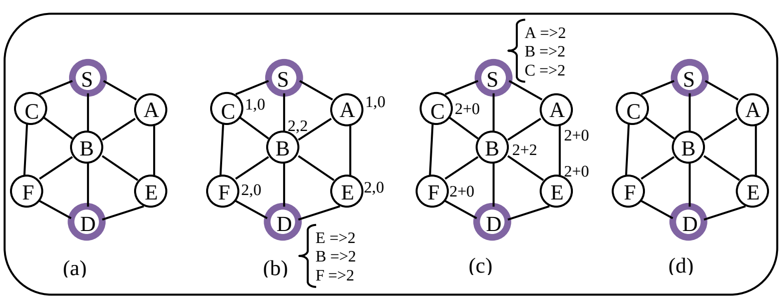

Fig. 8 An example of ZD-AOMDV protocol

Each intermediate node on the path will add its After_A_N_C value to the ActiveNeighborCount value in the RREP message it receives. As shown in Figure 8-c, only node B will change the ActiveNeighborCount value in the RREP and will increment it by two. When the source node receives the first RREP, it will set timer for another

RREP messages to arrive. After the timer expires the source will choose the paths which have lower ActiveNeighborCount values and will start sending data to the destination through these zone disjoint paths. In this example, the source will choose the two paths shown in Figure 8-d which are S-A-E-D and S-C-F-D for transmitting data.

The ZD-AOMDV protocol consists of two drawbacks as follows. First, the overhead of routing increases rapidly as the number of nodes increases. This is due to the increase in the number of query and query-reply packets sent between neighbors in the route discovery process. Second, the Route Discovery phase of this protocol takes more time than it takes in AOMDV.

Adaptive Multi-metric On-Demand Multipath Distance Vector Routing

Khimsara et al. [51] proposed adaptive multi-metric on-demand multipath distance vector routing (AM-AOMDV) protocol as an extension to the AOMDV protocol which considers multi-metric and local route update as the most important factors in selecting routes. The main objective of AM-AOMDV is to increase the packet throughput and route longevity, decrease the end-to-end latency, route discovery frequency and route overhead under high mobility environments.

There are three metrics included in AM-AOMDV: node-to-end Received Signal Strength Indication (RSSI), node-to-end latency and node occupancy, in addition to minimum hop-count to select the most efficient route from the source to the destination. The multiple metrics also help in avoiding the hot spots under heavy traffic conditions. These metric values are recorded in the routing table for each node and their corresponding paths. The node to-end RSSI metric is defined as the RSSI value of the path from any node to the destination. It uses the average value of RSSI. The RSSI value of each forward link is fed back to the nodes through the ACK packets. The node-to-end latency consists of two parameters (1) delay from the node to the source computed from the timestamp of the RREQ packet, and (2) the delay from the destination to the node computed from the RREP packet. The node occupancy is defined as the total number of data packets that any node processes per second and it plays an important role under heavy traffic conditions.

In AM-AOMDV, the route discovery procedure is similar to the AOMDV protocol. The source node begins forwarding packets, after receiving the first RREP from the destination. If a new RREP arrives, the source will change to the new route. This is because the protocol is adaptive and chooses the best available route, unlike AOMDV. The AM-AOMDV updates the route to the destination periodically using the local update algorithm. The local path updates in AM-AOMDV increase the route longevity. The end-to-end latency, the route discovery latency and routing overhead are much lower than in the AOMDV and hence it is more reliable than AOMDV. In a sparse network with lower number of connections, the AM-AOMDV shows higher route discovery delay than AOMDV.

Coverage prediction- On-Demand Multipath Distance Vector Routing

Coverage prediction- on-demand multipath distance vector routing (CP-AOMDV) protocol was developed by Aalam and Victoria [52] as an extension to the AOMDV protocol which considers the maximum coverage and highest stability as the most important factors in selecting multiple paths. The main objective of CP-AOMDV protocol is to improve routing overhead and power consumption over AOMDV.

The CP-AOMDV consists of three major processes. First, coverage prediction and stability estimation. Second, route discovery. Third, route maintenance. In order to keep track of the coverage area and link stabilities between a given node and its neighbors, each node periodically broadcasts *a Hello message* including the location of the broadcasting node. Based on the time interval between two neighboring HELLOs, it obtains the following steps:

i. Estimating the distance between the nodes.

ii. Calculating the probabilistic coverage area and stability estimation based on the following equations:

$$PL(U(I)) = 1 - \frac{y^{a+1}}{a} + \frac{y^{a+1}}{a+1} - \frac{y^{a+2}}{3(a+3)} + \frac{y^{a+3}}{6(a+3)} \qquad 14$$

$$LS_i = Q\left(\frac{\gamma - PL(U(T1))}{\sigma}\right) \qquad 15$$

Where PL(U(T1)) is the probability of the coverage prediction; LS_i is the link stability; ϒ is the threshold value and σ represents the variance of the propagation area.

iii. Storing the values in the routing table.

In the route discovery process, the source node starts to find stable routes by broadcasting RREQ packets to all its neighboring nodes. The RREQ packet includes two additional fields called coverage prediction and stability estimation. After an intermediate node receives a RREQ from its neighbor, it does not rebroadcast all received RREQs but only the RREQ attached with higher coverage area and larger route stability comparing to prior received RREQs in order to reduce control overhead. When the intermediate node decides to rebroadcast a specified RREQ, it calculates the stability of available routes (LS_i , PL(U(T1))) from the source to the intermediate node and it replaces the values of the PL(U(T1)) and LS_i in field of RREQ. When the RREQ reaches the destination node, the destination selects and sorts the multiple routes with the maximum coverage area and higher route stability. The destination will reply to the source node by sending a Route Reply (RREP) packet via intermediate nodes. The stable route with maximum route stability is discovered by the specified RREP and forward entries of the route tables to the source node. It accepts the selected route and begins to send data.

In route maintenance, the source node periodically sends the coverage prediction message to the destination node. When the intermediate node receives the coverage prediction message, it recalculates the estimations based on the coverage. it may choose the next hop. The destination node periodically updates the coverage probability through the coverage prediction message. When the destination node identifies weak coverage area it informs the source through the RREP, then the source selects another route.

The CP-AOMDV protocol consists of three drawbacks as follows. First, the packet delivery ratio decreases with increased packet rate. Second, more packets are dropped due to congestion. Third, throughput decreases with increased node mobility.

Multipath QoS Aware Routing Protocol

Balachandra et al. [53] proposed multipath QoS aware routing (MQARP) protocol as an extension to the AOMDV protocol to support delay, jitter and throughput. The objective of MQARP is to identify more than one route which is link reliable and delay aware. In this protocol, average timestamp and link life time ratio are used as a metric for QoS routing.

In MQARP protocol, the route discovery process is similar to that of the AOMDV protocol. The RREQ packet includes two additional fields called time stamp and link life time. In the new QoS Routing Protocol, the loss of unnecessary packet is avoided . Each of the packets broadcasted by the source node via the network contains a timestamp. As the nodes are updated in the routing table, the average timestamp value is calculated using the following equation:

$$T_{avg} = \frac{\sum_{i=0}^{i=n} T_i}{C} \qquad (16)$$

Where T_{avg} is the average timestamp, n stands for maximum simulation time, T_i is the timestamp of each packet and C is the total count of each entry made to the routing table. The positions of the node added to the routing table is known.

When the network topology changes, it is required to calculate the route reliability dynamically. Assume two mobile nodes A and B are within the radio transmission range of each other, let:

(X_A, Y_A): coordinate of mobile node A; X_B, Y_B: coordinate of mobile node B;
V_A: mobility speed of mobile node A; V_B: mobility speed of mobile node B;
Θ_A: direction of motion of mobile node A ($0<\Theta_A<2\pi$); Θ_B: direction of motion of mobile node B ($0<\Theta_B<2\pi$).
The link life time can be calculated by using the following equation:

$$\text{LLT} = \frac{-(ab+cd)\sqrt{(a^2+c^2)r^2-(ad-cb)^2}}{(a^2+c^2)} \qquad (17)$$

Where,
a= V_A Cos Θ_A - V_B Cos Θ_B , c= V_A Sin Θ_A - V_B Cos Θ_B
b= $X_A - Y_B$, d= $X_A - Y_B$

If node A is the previous hop of the packet for node B, it appends its position and movement information to the RREQ packet. When node B receives this packet, it calculates the life time of the link. The Route Life Time (RLT) is the minimum link life time along a routing path. Therefore, the RLT is equal to the minimum of LLTs for a route. The Percentage Life Time Ratio (PLTR) can be computed as below:

$$\text{PLTR} = \frac{RLT}{TTL} * 100 \qquad (18)$$

Where TTL is the time to live. If the PLTR is greater than 50% then the intermediate node allows the rebroadcasting of RREQ messages; otherwise the data packets will be dropped.

When the destination receives the RREQ packet, it generates a RREP packet. The RREP packet contains an additional field called ***Minimum link life time***. The reverse path is used to forward RREP packets from the destination to the source. When an intermediate node receives the RREP, it updates the routing table entries and forwards the data packets towards the source node.

The performance of MQARP is improved for the MANET with high density, high mobility and high speed situations. The jitter of MQARP has been always linearly varying. So this new protocol is suitable for video and audio data transmission.

QoS Enhanced Hybrid Multipath Routing Protocol

Devi and Rao [11] proposed multipath QoS enhanced hybrid multipath routing (QEHMR) protocol as an extension to the AOMDV protocol to enhance the packet delivery ratio, throughput, routing overhead and power consumption. This protocol combines the features of both proactive and reactive protocols.

The QEHMR protocol is composed of two main mechanisms, namely, proactive topology discovery and reactive route discovery. In topology discovery process, each node learns the battery power, queue length and residual bandwidth of every other nodes and stores them in the topology information table (TIT). By exchanging the TIT among the nodes, the topology is discovered. The consumed power (P(t)) is computed as follows:

$$\mathbf{P(t)} = \boldsymbol{DP_{tx} * \lambda + DP_{re} * \eta} \qquad \textbf{(19)}$$

Where DP_{tx} is the number of data packets transmitted by the node after time *t;* DP_{re} is the number of data packets received by the node after time *t*; $\boldsymbol{\lambda}$ and $\boldsymbol{\eta}$ are constants in the range of [0, 1]. When P_i denotes the initial power of a node, the residual power P_R of a node at time t , can be computed as:

$$\boldsymbol{P_R = P_i - P(t)} \qquad \textbf{(20)}$$

The average queue size that specifies the traffic load of the node can be computed as follows:

$$\boldsymbol{QL = \delta * QL_O + (1 - \delta) * QL_C} \qquad \textbf{(21)}$$

Where QL is the average queue length, QL_C is the current queue length, QL_O is the old queue length and δ is the constant in the range [0, 1].

Since the bandwidth is shared among neighboring nodes, by taking channel into consideration, the nodes calculate bandwidth based on the ratio of idle and busy times projected for a predefined interval of time (t). The local bandwidth (B_1) is estimated as follows:

$$\boldsymbol{B_1 = C_{ch} * \left(\frac{t_i}{t}\right)} \qquad \textbf{(22)}$$

Where C_{ch} is the channel capacity and t_i is the idle time in t. The residual bandwidth (B_R) is defined as the difference between the minimum bandwidth (B_{min}) and B_1 and is stored in the residual bandwidth register.

When a source (S) node wants to send data to the destination (D), it first verifies the TIT. After verification, S gathers all the information about the nodes towards D. Then node S computes the link metric (LM) using the data in its TIT which as shown below:

$$\boldsymbol{LM = \frac{\eta * QL}{(\alpha * P_R) + (\beta * B_R)}} \qquad \textbf{(23)}$$

Where α, β and η represents the normalization factor. The source chooses the nodes with minimum LM and initiates the packet transfer through the chosen node within 2-hop. The multipath Dijkstra algorithm is employed to transmit the data through multiple paths with the nodes holding minimum link metric.

When any intermediate node does not recognize the next 2-hop information from TIT towards destination, it broadcasts a RREQ packet to all neighboring nodes through the eligible links toward the destination and waits for the RREP packet. If any neighbor has an eligible route receiving the RREQ then it replies with RREP packet. On receiving the RREP, the node computes its link metrics and compares the link metrics with the value already stored in its TIT, and if satisfied the requirement, it starts sending data following that route and discards duplicate RREP packets.

The QEHMR protocol consists of three drawbacks as follows. First, when the number of nodes is increased from 30 to 110, the throughput and packet delivery ratio begin to reduce, as there are chances of more collisions. Second, the routing overhead decreases when there are up to 70 nodes and increases beyond 70 nodes. Third, the delay begins to increase when the node movement speed increases.

Congestion Based Route Discovery Protocol

Bawa and Banerjee [54] proposed a congestion based route discovery (CBRD) protocol as an extension to AOMDV protocol. The main advantage of this protocol is to check congestion on a node and then apply load balancing. The CBRD also aims at improving the throughput, delay and reducing packet loss during transmission as compared to AOMDV protocol.

The route maintenance of CBRD is similar to that of the AOMDV protocol, but route discovery is modified to find link disjoint as well as a node disjoint path from the source to the destination . The main difference between

CBRD and AOMDV is that CBRD considers the queue size of node while making a routing decision. When a source node sends a packet to a destination, the packet includes some value for congestion. When intermediate nodes receive the RREQ packet, they check value against their queue. If queue size is sufficient then that node can participate in the communication. Otherwise, the node discards it. The source node calculates congestion at each node and selects the best route. Packets are transferred based on minimum congestion on the route. At the end the best path is selected for communication and set as the primary path. Other paths are set as secondary paths for backup which are used when the primary path breaks up. Priorities are also set on paths to choose next primary path. When the route gets congested the source choose other paths for data transmission.

The CBRD protocol consists of two drawbacks as follows. First, when a node moves to other side trace file, the delay begins to increase. Second, some packets are lost when a node moves in another direction.

Energy supported On-demand Distance Vector Routing protocol

Sridhar et al. [55] proposed an energy supported on demand distance vector (EN-AODV) protocol as an extension to AODV protocol. It aims to improve the QoS parameters like throughput, packet delivery ratio and delay. The EN-AODV protocol calculates the energy levels of the nodes before they are selected for routing path. A threshold value is defined and nodes are considered for routing only if its energy level is above this threshold value.

The following are the main steps to implement EN-AODV routing protocol.

- Calculate the energy level.
- Recalculate and accumulate the energy value based on the routing path selected.
- Format, filter and transform.
- Identify the low energy nodes from the calculated value.
- Identify the reliable path among nearest reliable node.
- Change the routing path based on energy value of the node.
- Update the routing cache table.

The node energy level plays a very crucial role in MANET routing. When the energy levels are not sufficient, the EN-AODV protocol selects an alternate path to carry on routing successfully using reliable nodes. This protocol concentrates on identifying these unreliable nodes (running low on energy level) using the energy level values calculated for each node. Energy computation is based on nodes sending and receiving rate. It can be calculated by the difference between the initial energy level and the consumed energy level of a node. The procedure calculating energy value as follows.

Step 1: Set initial parameters values as initialenergy = 100, maxenergy=0, nodes=50 and Nodeid.
Step 2: Calculate Intermedenergy based on event time.
Step 3: Compute consumed energy for each node;

```
for (i inIntermednergy) {
Consumenergy [I] =initialenergy-Intermedenergy [I]
Totalenergy +=consumenergy [I]
If (maxenergy<consumenergy [I]) {
maxenergy=consumenergy[i]
nodeid=i }}
```

Step 4: Compute average energy
averagenergy=totalenergy/nodes.

The main drawback of the EN-AODV protocol is that the source itself may drain out. In such cases we may introduce external energy to the source node by utilizing virtual energy concepts. Other nodes have to store energy for future transmissions.

Improved Stability based Partially Disjoint AOMDV

Improved stability based partially disjoint (ISPDA) protocol was developed by Almobaideen et al. [56] as an improvement in the stability based partially disjoint AODVM (SPDA) protocol which considers node stability and hop count values as the most important factors in selecting a route. The main objective of ISPDA protocol is to improve the performance of SPDA protocol overcoming two weaknesses. First, SPDA does not take into consideration the number of hops of each path. Second, SPDA transmits packets over the shortest path until it becomes invalid before it tries to utilize other alternative paths.

Disjoint multipath routing protocols have been classified into maximally disjoint multipath (e.g. AOMDV protocol) and partially disjoint multipath protocols (e.g. ISPDA). The shared nodes or links between the partially disjoint paths are selected based on stability. Stability of the routes in MANET can be measured based on node stability or link stability. The ISPDA protocol chooses the most stable paths with the minimum number of hops in the path. This increases the lifetime of the selected paths and so reduces the opportunity of future path breaks, which in turn reduces packet transmission delay. This protocol transmits packets in parallel over all the discovered paths. It starts the transmission with the first discovered path.

When the destination receives the first RREQ packet, it considers as a primary route through which a RREP packet is sent back to the source node. When the destination receives other RREQs, it will check the number of hop counts the newly received RREQs has passed through. If this new path is shorter or equal to the primary route, then the destination checks the stability of each node in this path and it chooses the shortest paths with more stable links. The selected alternative paths will be used in parallel to transmit the data by the sender node in order to increase the utilization of available bandwidth.

In ISPDA protocol, the node stability is estimated based on the number of RREQs that passed through the node contained in the list of nodes carried by the receiving RREQs. An intermediate node is considered stable based on two factors. First, the number of times that a node has been traversed in various paths is greater than specific threshold. Second, the time of the last occurrence, when that node has been encountered in a path, is less than specific period of time.

ISPDA protocol outperforms SPDA protocol in terms of average end-to-end delay and throughput, but the discovery overhead of ISPDA is higher than that of SPDA.

5.2.1 Comparison

AODV is an improvement of the Destination-Sequenced Distance Vector routing (DSDV) protocol. AODV aims to reduce the number of broadcast messages forwarded throughout the network by discovering routes on-demand instead of keeping a complete up-to-date routing table. The advantages of AODV protocol are that it favors the least congested route instead of the shortest route and it also supports both unicast and multicast packet transmissions even for nodes in constant movement. It also responds very quickly to the topological changes that affect the active routes.

On the other hand, one of the major problems of AODV is the maintenance of only one route per a destination. This means that every time a path is broken, AODV has to initiate a route discovery process, which leads to more overhead, higher delays and higher packet loss in the network.

In order to alleviate the above-mentioned problems, a large number of multipath routing protocols were proposed to improve the performance of the AODV protocol under various operating scenarios. Some of these scenarios involve OoS improvement, load balancing, congestion alleviation, and power saving.

The main improvement direction has been about the finding of multiple disjoint routes. There are various approaches taken by the protocols, e.g., AOMDV [43] (using advertised hop count), AODVM [7] (based on reliable nodes and last hop ID), AODVM/PD [46] (depending on correlation factors metric), AODVM-PPSP [48] (based on transmission delay time and node throughput), AM-AOMDV [51] (depending on local route update and multi-metric i.e., node-to-end latency, node-to-end RSSI, and node occupancy, CP-AOMDV [52] (based on coverage prediction and route stability), MQARP [53] (depending on average timestamp and link life time ratio), QEHMR [11] (combining two main mechanisms, i.e, proactive topology and reactive route discovery, CBRD [54] (depending on the queue size of node).

There are other improvement direction such as route probability in AODVM-PSP[47] and backup route in AODV-ABR[49]. Meanwhile, some protocols extend upon the AODV by considering various additional networking challenges, such as energy levels in EN-AODV [55], zone disjoint paths in ZD-AOMDV [50] and partially disjoint path (ISPD [56]) (more stable than the maximally disjoint).

Table 2 summarizes the protocols reviewed in this section and compares some of their key features.

Table 2: Multipath routing protocols extension of AODV.

Protocols	Tool	Objective	Num. of Paths	Drawback
AOMDV (2001)	Multiple loop free (advertised hopcount) and link-disjoint paths.	To provide efficient fault tolerance in the sense of fast and efficient recovery from route failures in dynamic networks.	2-5	With the increase of the network density, the protocol's performance decreases and it has the additional overhead of more RREPs per route discovery.
AODVM (2003)	Using reliable nodes and last hop ID	To design a multipath routing framework for providing enhanced robustness to node failures.	At least 3 or 4	1. A sufficient number of node disjoint paths cannot be found without incurring a large amount of overhead. 2. It can only achieve better performance in scenarios with lower mobility and higher node density. 3. It severely suffers from packet loss when the network becomes dynamic.

AODVM/PD (2005)	Correlation Factors (LCF, ACF and CT).	To provides better fault tolerance and smaller end-to-end delay than AODVM in networks with low mobility.	3	1. With more nodes moving, the delay becomes greater than AODVM. 2. The control overhead is Increased due to the transmission of CORR packets during the route discovery phase.
AODVM-PSP (2005)	Transmission time delay and probability -selection scheme.	To balances load and alleviate congestion and bottlenecks that affect the throughput of the whole network.	Similar to AODVM	1. A possibility of missing efficient route due to the re-discovery process. 2. The node forwards the packet by the chosen route which may not be the good one. 3. More overhead than that of single-path routing.
AODVM-PPSP (2006)	Using the least transmission delay time and node throughput.	To find multiple routes, increase packet delivery ratio and reduce routing overhead.	Similar to AODVM	1. A slight increase in the size of the packets. 2. It needs to update the routing table of the low probability routes and use these routes repeatedly although they have a low performance record.
AODV-ABR (2007)	Using AODV-ABR and AODV-ABL.	To reduce control overhead.	Backup route	The traffic load becomes heavier when more nodes participate in a wireless network. The probability of packet collisions will increase, resulting in the degradation of overall performance.
ZD-AOMDV (2009)	Active neighbor	To increase the packet delivery ratio and decrease the end-to-end packet delay.	3	1. The routing overhead increases rapidly as the number of nodes increases. 2. The route discovery phase of this protocol takes more time than that of AOMDV.
AM-AOMDV (2010)	Multi-metric (node-to-end RSSI, node-to-end latency and node occupancy) and local route update.	To increase the packet throughput and route longevity, decrease the end-to-end latency, route discovery frequency and route overhead under high mobility environments.	2-5	In a sparse network (i.e., lower number of connections), the AM-AOMDV has a higher route discovery delay than AOMDV.
CP-AOMDV (2011)	Coverage prediction and link stability.	To improve routing overhead and power consumption over AOMDV.	Multiple paths	1. The packet delivery ratio decreases with increased packet rate. 2. More packets are dropped due to congestion. 3. Throughput decreases with increased node mobility.
MQARP (2012)	T_{avg}, LLT and PLTR.	To identify more than one route which is link reliable and delay aware.	Multiple disjoint path	If there is a particular node which is very far away such that its timestamp is higher than that of the average value, re-broadcasting of the RREQ from that node is not allowed. In this way, it saves the loss of packets and forces the Route Discovery Process to search for another route with limited time.
QEHMR (2012)	LM, P_R , B_R and QL	To enhance the packet delivery ratio, throughput, routing overhead and power consumption.	2	1. When the number of nodes is increased from 30 to 110, the throughput and packet delivery ratio begin to reduce, as there are chances of more collisions. 2. The routing overhead has increased beyond that since after 70 nodes. 3. The delay begins to increase when the speed increases.
CBRD (2013)	Queue size	To check congestion on a node and then apply load balancing	Multiple link disjoint paths	1. When a node moves to other side trace file, the delay begins to increase. 2. Some packets are lost when a node moves in another direction.
EN-AODV (2013)	Energy based	To improve the QoS parameters such as throughput, packet delivery ratio and delay.	Alternate path	The source itself may drain out.
ISPDA (2013)	Node stability and hop count.	To improve the performance of SPDA protocol	Ten partially disjoint paths	The discovery overhead of ISPDA is higher than that of SPDA.

6. Conclusions and Future Work

Multipath routing has been a promising technique in MANETs. As opposed to their single path (e.g. DSR or AODV) counterparts, on-demand routing protocols with multipath capability can effectively deal with mobility-induced link failures in mobile ad hoc networks. The outcome of this fact is the multipath routing protocols that have been proposed for mobile ad hoc networks throughout the years. The technique proposes that the traffic can be distributed and carried by multiple simultaneously available paths, so that the available bandwidth can be better utilized by using multiple active transmission tasks especially under low traffic load conditions. It also provides a better fault tolerance for the system if a path fails.

In this survey, we have introduced a taxonomy of multipath routing protocols for mobile ad-hoc networks. We divide the multipath routing protocols into two categories: (i) multipath routing protocols extension of DSR, and (ii) multipath routing protocols extension of AODV. For each category, we have reviewed and compared around fourteen representative protocols. While different kinds of protocols operate under different scenarios, they usually share the common goal to reduce control packet overhead, maximize throughput, and minimize the end-to-end delay. The main differentiating factor between the protocols is the ways of finding and maintaining the routes between source–destination pairs.

Table 1 and Table 2 provide a summary of all the multipath routing protocols mentioned in this paper and provide a checklist that can help network designers to choose a suitable multipath routing protocol that can meet more than one performance objective.

To the best of our knowledge, We have grouped and summarized the weaknesses of the multipath routing protocols as mentioned in Table 1 and Table 2. These typical weaknesses include the increased end-to-end dealy, large routing table space, high processing complexity, large number of overhead packets, the increased power consumption, small data rate per route, the decreased performance when the network density increases, high packet loss, the increased packet size, the increased packet collisions and performance degradation, the reduced packet delivery ratio and throughput when the network size increases.

Our future work will focus on the design of multipath routing protocols that will overcome the aforementioned weaknesses Table 1 and Table 2.

References

1. NZ Ali, R. B Ahmad, and S. A. Aljunid, A Survey on On-Demand Multipath Routing Protocol in MANETs, IEEE, 2008.
2. S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications, Auerbach, 2008.
3. S. Mueller, R. P. Tsang, and D. Ghosal, Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges, Springer-Verlag Berlin Heidelberg, 2004, pp. 209–234.
4. B.Soujanya, T.Sitamahalakshmi, and C. D. AKAR, Study of Routing Protocols in Mobile Ad-Hoc Networks, International Journal of Engineering Science and Technology (IJEST), Vol. 3, April 2011.
5. A. Hassan, Simulations on Multipath Routing Based on Source Routing, Bachelor thesis, Bern University, 2008.
6. T. Okazaki, E. Kohno, T. Ohta, and Y. Kakuda, A Multipath Routing Method with Dynamic ID for Reduction of Routing Load in Ad Hoc Networks, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2010, pp 114-129.
7. Z. Ye, S.V. Krishnamurthy, and S.K. Tripathi, A framework for reliable routing in mobile ad hoc networks,IEEE INFOCOM, 2003, pages 270–280.
8. M. Tarique, K. Tepe, S. Adibi and S. Erfani, Survey of multipath routing protocols for mobile ad hoc networks, Journal of Network and Computer Applications, 2009, pp. 1125-1143.
9. N. A. Husieen, A Reliable Multipath Dynamic Source Routing Protocol for Multimedia Applications in Mobile Ad-hoc Networks, Doctor of Philosophy, University Utara Malaysia, 2013.
10. R. Kaur, R. Mahajan, and A. Singh, A Survey on Multipath Routing Protocols for MANETS, IJETTCS, Volume 2, Issue 2, 2013, P. 42-45.
11. P. R. Devi and D. S. Rao, QoS Enhanced Hybrid Multipath Routing Protocol for Mobile Ad hoc networks, International Journal of Distributed and Parallel Systems (IJDPS),Vol.3, 2012, pp 89-105.
12. J. Yi, A. Adnane, S. David, and B. Parrein, Multipath optimized link state routing for mobile ad hoc networks, Ad Hoc Networks, 2011, pp 28–47.
13. W. Lou, W. Liu, and Y. Zhang, Performance Optimization using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks, Kluwer Academic, 2005, pp 1-24.
14. V. B. Kute, and M. U. Kharat, Survey on QoS for Multi-Path Routing Protocols in Mobile Ad-Hoc Networks, International Journal of Machine Learning and Computing, Vol. 2, No. 4, 2012, pp 458-461.
15. H. Gharavi, Multichannel Mobile Ad Hoc Links for Multimedia Communications, IEEE,Vol. 96, No. 1, 2008, pp 77-95.
16. Xin Wang, Mobile Ad-Hoc Networks: Protocol Design, InTech, 2011.
17. A. Boukerche, B. Turgut, N. Aydin and M. Z. Ahmad, Routing protocols in ad hoc networks: A survey, Computer Networks, 2011, pp 3032-3080.
18. A. K. Gupta, H. Sadawarti , and A. K. Verma, A Review of Routing Protocols for Mobile Ad Hoc Networks, WSEAS TRANSACTIONS on COMMUNICATIONS, Vol. 10, 2011, pp 331-340.

19. C. de M. Cordeiro and D. P. Agrawal, Ad Hoc and Sensor Networks, World Scientific, 2006.
20. F. Yang and B. Sun, Ad hoc On-demand Distance Vector Multipath Routing Protocol with Path Selection Entropy, IEEE, 2011.
21. A. A. Etorban, The Design and Performance Evaluation of a Proactive Multipath Routing Protocol for Mobile Ad Hoc Networks, doctor's thesis, Heriot-Watt University, 2012.
22. A. Nasipuri and S. R. Das, On-Demand Multipath Routing for Mobile Ad Hoc Networks, IEEE, 1999, pp 64-70.
23. J. Tsai and T. Moors, A Review of Multipath Routing Protocols: From Wireless Ad Hoc to Mesh Networks, National ICT Australia (NICTA)1/ University of New South Wales, Australia.
24. A. Tsirigos, The Effect of Multipath Routing on the Packet Delivery Ratio, Master thesis, Cornell University, 2001.
25. L. Wang, L. Zhang, Y. Shu and M. Dong, Multipath Source Routing in Wireless Ad Hoc Networks, IEEE, 2000, P. 479-483.
26. Mohammad Ilyas, The Handbook of Ad Hoc Wireless Networks, CRC Press LLC, 2003.
27. Yihua Zhai, Implementing MSR and BSR in a wireless Ah Hoc Testbed, Master thesis, University of Ottawa, 2006.
28. R. Leung, J. Liu, E. Poon, A. C. Chan, B.Li, MP-DSR: A QoS-aware Multi-path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks, IEEE, 2001, pp 132-141.
29. YI Jiazi, Summary of routing protocols in mobile ad hoc networks, Polytechnic School of Univesity of Nantes, 2007.
30. S. Lee and M. Gerla, Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks, IEEE, 2001, pp. 3201-3205.
31. G. Parissidis, V. Lenders, M. May, and B. Plattner, Multi-path Routing Protocols in Wireless Mobile Ad Hoc Networks: A Quantitative Comparison, Springer Berlin Heidelberg, 2006, pp 313-326.
32. N.Wisitpongphan, O. K. Tonguz, Disjoint multipath source routing in ad hoc networks: transport capacity. In, IEEE , vol. 4, October 2003, p. 2207–2211.
33. W. Wei and A. Zakhor, "Robust Multipath Source Routing Protocol (RMPSR) for Video Communication over Wireless Ad Hoc Networks," in IEEE International Conference on Multimedia and Expo (ICME 04), vol. 2, Jun. 2004, pp. 1379 – 1382.
34. H. An, L. Zhong, X. C. Lu, and W. Peng, A Cluster-Based Multipath Dynamic Source Routing in MANET, IEEE, 2005, p369-p376.
35. M. Anupama and B. Sathyanarayana, Survey of Cluster Based Routing Protocols in Mobile Ad hoc Networks, International Journal of Computer Theory and Engineering, Vol. 3, No. 6, 2011, p806-p815.
36. P. Yang and B. Huang, Multi-path Routing Protocol for Mobile Ad Hoc Network, International Conference on Computer Science and Software Engineering, 2008, pp. 1024 – 1027.
37. M. Khazaei, Improvement Dynamic Source Routing Protocol by Localization for Ad hoc Networks, International Journal of Computer Science and Information Security (IJCSIS), vol. 8, No. 6, 2010, pp. 1 – 6.
38. S. Upadhayaya and C. Gandhi, Node Disjoint Multipath Routing Considering Link and Node Stability protocol: A characteristic Evaluation, IJCSI International Journal of Computer Science Issues, Vol. 7, 2010, pp 18-25.
39. L. Liyan, W. Muqing, C. Ziqing, and S. Jingfang, Analysis and Optimization of Multipath Routing Protocols based on SMR, 2nd International Conference on Signal Processing Systems (ICSPS), 2010, pp. 205 – 209.
40. A.K. Daniel, S. Dwivedi, T. Verma, and P. K. Dubey, A Congestion Controlled Multipath Routing Algorithm Based On Path Survivability Factor, International Journal on Computer Science and Engineering (IJCSE), Vol. 3, 2011, pp 1563-1572.
41. A. Kulkarni and S. Chimkode, Traffic Sensitive Dynamic Source Routing Protocol for Mobile Ad hoc Networks, International Journal of Computer Applications, Vol. 51, 2012, pp 9-13.
42. M. Dhanda and S. Chaudhry, Stable Route Aware Routing in Mobile Ad-Hoc Networks, International Journal of Computer Trends and Technology (IJCTT), vol. 4, 2013, pp 2049-2054.
43. M. K. Marina and S. R. Das, On-demand multipath distance vector routing in ad hoc networks, IEEE, 2001, pp. 14–23.
44. B. Kan and J. Fan, Interference activity aware multi-path routing protocol, EURASIP. J. Wireless Communication Network, 2012, pp. 1–13.
45. N. Nithya, R. Maruthaveni, A Survey on Routing Protocols in Mobile Ad Hoc Networks, IJSR, volume 2, Issue 1, 2013, pp. 350-354.

46. S. Mueller and D. Ghosal, Analysis of a Distributed Algorithm to Determine Multiple Routes with Path Diversity in Ad Hoc Networks, IEEE, 2005, pp. 277–285.
47. F. Jing, R.S. Bhuvaneswaran, Y. Katayama, and N. Takahashi, A Multipath On-Demand Routing with Path Selection Probabilities for Mobile Ad Hoc Networks, IEEE, 2005, pp 1099-1102.
48. F. Jing, R.S. Bhuvaneswaran, Y. Katayama, and N. Takahashi, On-Demand Multipath Routing Protocol with Preferential path Selection Probabilities for MANET, Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), IEEE, 2006.
49. W. K. Lai, S.-Yu Hsiao, Y.-Chung Lin, Adaptive backup routing for ad-hoc networks, Computer Communications,2007, pp 453–464.
50. N. T. Javan, R. Kiaeifar, B. Hakhamaneshi, and M. Dehghan, ZD-AOMDV: A New Routing Algorithm for Mobile Ad-Hoc Networks, ACIS International Conference on Computer and Information Science, IEEE, 2009, pp 852-857.
51. S. Khimsara, K. K.R. Kambhatla, J. Hwang, S. Kumar and J. D. Matyjas, AM-AOMDV: Adaptive Multi-metric Ad-Hoc On-Demand Multipath Distance Vector Routing, ICST Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, pp. 884-895.
52. S. S. Aalam and T. A. D. Victorie, A Probabilistic Approach of Coverage prediction in Mobile Ad hoc Networks, International Journal on Computer Science and Engineering (IJCSE), Vol. 3, 2011, pp 3824-3831.
53. M. Balachandra, P. K. V. FET, and Krishnamoorthy M., Enhancing the Quality of Service in MANETs by Improving the Routing Techniques, International Journal of Computer Applications, Vol. 51, 2012, pp 25-30.
54. O. S. Bawa and S. Banerjee, Congestion based route discovery AOMDV protocol, International Journal of Computer Trends and Technology- vol. 4, 2013, pp 54-58.
55. S.Sridhar, R.Baskaran and P.Chandrasekar, Energy supported AODV (EN-AODV) for QoS routing in MANET, Procedia - Social and Behavioral Sciences, 2013, pp 294 – 301.
56. W. Almobaideen, D. Al-Khateeb, A. Sleit, M. Qatawneh, K. Qadadeh, R. Al-Khdour, and H. A.Hafeeza, Improved Stability Based Partially Disjoint AOMDV, Int. J. Communications, Network and System Sciences, 2013, pp 244-250.