Volume 1 No. 6, October 2011 ISSN-2223-4985
International Journal of Information and Communication Technology Research

http://www.esjournals.org

Survey of Routing Protocols for Mobile Ad-hoc Network

Humayun Bakht
Taitec College
Manchester , United Kingdom

ABSTRACT

Routing is a challenging issue in mobile ad-hoc network. Concerning routing various solutions have been reported. In this context, only few of the proposed solutions are commonly evaluated and less attention has been paid to mention some other schemes. The contribution of this paper is to critically analyze most of the routing protocols which are reported in the available literature. This will help in having a wider understanding of the problem domain and can also be used to develop or some new or to extend already proposed schemes.

Keywords: *component, MANET; Routing Protocols, MAODDP, On-Demand Routing, Tables Driven Routing, Hybrid Routing*

I. INTRODUCTION

Mobile ad-hoc network is deployed in applications such as disaster recovery and distributed collaborative computing, where routes are mostly multi-hop and network hosts communicate via packet radios[1]. Routing is one of the challenging issues in mobile ad-hoc network. Existing protocols for ad-hoc network can generally be categorized into pro-active and re-active protocols types. It is a well known fact that most of these protocols have certain weaknesses. Some of the main problem includes Limitation: Most of the well known protocols in this area are limited to a particular scenario i.e. does not perform well in all environments; Lack of analytical studies: not sufficient work has been done to evaluate their performance with respect to other techniques of similar types. Moreover, proposed schemes focus on routing without considering their affects on some other routing relates issues[2].

The contribution of this paper is to collect and critically evaluate all those protocols that are proposed as a routing solution for mobile ad-hoc network. We believe via analyzing some of the unknown and famous routing schemes a wider knowledge of the problem could be developed. Moreover, it could also be used to either extend existing schemes or to develop new routing solutions. Rest of this paper has been organized as follows. In section 2 of this paper some of the protocols currently under consideration by IETF will be analyzed before rest of the schemes covered in section 3 and conclusions are given in section 4.

II. PROTOCOLS UNDER REVIEW BY IETF

Destination distance sequence vector (DSDV) [3] of tables driven , Ad-hoc on-demand distance vector (AODV) [4] of on-demand and Zone routing protocol(ZRP) [5] of hybrid type are under consideration by IETF. In the following section each of these protocols is analyzed.

A. Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

The destination sequenced distance vector routing protocol (DSDV) is an extension of classical bellman ford routing mechanism [3]. DSDV maintains consistent network view via periodic routing updates. Routing information is stored inside routing tables maintained by each node. New route broadcasts contain the address of the destination, the number of hops to reach destination, the sequence number of the destination and a new sequence number unique to broadcast. A route with a recent sequence number is considered as a fresh route. If sequence numbers are found to be the same than the route with better metric will be selected.

A1. Critiques of DSDV

DSDV requires nodes to periodically transmit routing table updates packets regardless of the network traffic [6]. When the number of nodes in the network grows the size of the routing tables and the bandwidth required to update them also grows[6]. This overhead is considered as the main weakness of DSDV. DSDV also pose a period of convergence before which routes will not be known and packets will be dropped [6]. This could also limit the number of nodes that can connect to the network since the overhead grows as O (N^2). Moreover, DSDV works only with bidirectional links [6]. In addition, in DSDV routing loops can occur while the network is reacting to a change in the topology.

DSDV use distance vector shortest-path routing as the underlying routing protocol. It has a high degree of complexity especially during link failure and additions [6]. Maximum settling time is difficult to determine in DSDV. DSDV does not support multi-path routing. Fluctuation is another problem of DSDV. In some simulation studies, DSDV is much more conservative in terms of routing overhead but because link breakages are not detected quickly more data packets are dropped. Specification of DSDV is silent over security issue [6]. DSDV assumes that all nodes are trust worthy and cooperative. Once the

false sequence has been established the attacker will continuously send out new packets to update the value. Therefore more hosts will be cheated [6] as a single misbehaving node can pose a serious threat for the entire network.

B. Ad-hoc On-demand Distance Vector Routing (AODV)

AODV is a combination of both DSR [7] and DSDV [3]. AODV provides both multicast, and unicast connectivity in a mobile ad-hoc environment. The main feature of AODV is quick response to link breakage in active route [50]. AODV[4,8] builds routes using a route request and route reply query cycle. For destination source nodes with no prior information it broadcasts a route request (RREQ) packet. Nodes receiving RREQ update their information and set-up backward pointers to the source node. When the source node receives the RREP it begins to forward data packets to the destination.

B1. Critiques AODV

AODV is an on demand approach but still use periodic broadcast of „hello message" to track neighboring nodes. This periodic propagation causes network overhead in AODV [6]. In AODV a route has to discover prior to the actual data packet transmission. This initial search latency may degrade the performance of interactive applications [6]. Similarly the quality of path is not known prior to call set-up. It can be discovered only while setting up the path. Moreover quality of path must be monitored by all intermediate nodes in an active session at the cost of additional latency and overhead penalty [6]. That makes AODV quite unsuitable for real life applications. AODV cannot utilize routes with asymmetric links between nodes and thus require symmetric links [6]. Nodes in AODV store only route that are needed. Nodes use the routing caches to reply to route queries. These results in „uncontrolled" replies and repetitive updates in hosts" caches yet early queries cannot stop the propagation of all query messages which are flooded all over the network.

C. Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) [5] is a hybrid routing protocol. It combines both proactive and reactive routing techniques. Each node has a predefined zone centered at itself in terms of number of hops. For nodes within the zone it uses proactive routing protocols to maintain routing information. For those nodes outside of its zone it does not maintain routing information on a permanent base. Instead, on-demand routing strategy is adopted when inter-zone connections are required.

The ZRP protocol consists of three components. In the zone proactive Intra-zone Routing Protocol (IARP) is used to maintain routing information. IARP can be link state routing or distance vector routing depending on the implementation. For nodes outside the zone, reactive Inter-zone Routing Protocol (IERP) is performed. IARP provides a route to nodes within a node"s zone. IERP uses the route query (RREQ) route reply (RREP) packets to discover a route very similar to some on-demand routing protocol.

C1. Critiques of ZRP

ZRP limits the proactive overhead to only the size of the zone. It also limits reactive search overhead to only select border nodes. Potential inefficiency may occur when flooding of the RREQ packets goes through the entire network. To some extent this protocol can provide a better solution in terms of reducing communication overhead and delay. But this benefit is subjected to the size of a zone and the dynamics of a zone. ZRP does not provide an overall optimized shortest path if the destination has to be found through IERP [6]. Moreover with the increase of network size ZRP could create unpredictable large overhead. In ZRP each path to a destination may be suboptimal. This also means that each node will have higher level topological information. Thus poses a higher memory requirement and an extra burden on the network resources.

III. OTHER ROUTING ALGORITHMS

Besides above mentioned protocols, there are some other routing protocols which are reported in the existing literature. In this section all of those protocols will be critically evaluated.

A. Dynamic Source Routing (DSR)

Dynamic source routing protocol [7] is a reactive protocol. DSR requires no periodic updates of any kind at any level within the network. DSR uses source routing through which sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache. A data packet carries the source route in the packet header. The DSR protocol consists of two mechanisms, route discovery and route maintenance. Route discovery process functions by flooding the network with route request (RREQ) packets. Each node receiving a RREQ packet rebroadcasts it unless it is the destination or it has a route to the destination. The route carried back by the RREP packet is cached at the source for future use. For route maintenance whenever a link on a source route is broken the source node is notified using a route error (RER) packet.

A1. Critiques of DSR

DSR is not designed to track topology changes occurring at a high rate [6]. Two sources of bandwidth overhead in DSR are route discovery and route maintenance[6]. These occur when new routes need to be

discovered or when the network topology changes. In DSR this overhead can be reduced by employing intelligent caching techniques in each node at the expense of memory and CPU resources. The remaining source of bandwidth overhead is the required source route header included in every packet. This overhead cannot be reduced by techniques outlined in the protocol specification [6].

DSR is based on source routing thus requires considerably greater routing information. In DSR a route has to discover prior to the actual data packet transmission. This initial search latency may degrade the performance of interactive applications [6]. Moreover, the quality of path is not known prior to call setup. It can be discovered only while setting up the path. This quality of path needs monitoring by all intermediate nodes during a session. It increases the cost of additional latency and overhead penalty [6].

Due to source routing DSR has major scalability problem. Nodes use routing caches to reply to route queries. This results in an „uncontrolled" replies and repetitive updates in hosts" caches. In addition, early queries cannot stop the propagation of all query messages which are flooded all over the network. Therefore when the network becomes larger, the control packets and message packets also become larger. This could degrade the protocol performance after a certain amount of time.

B. Temporary Ordered Routing Algorithm (TORA)

TORA [9] is a distributed routing protocol which is based on a link reversal algorithm. TORA is designed to discover routes on demand. At each node in the network a separate copy of TORA is run for each destination. When a node needs a route it broadcasts a query request to all other nodes. This query packet contains the address of the destination for which it requires a route. This packet propagates throughout the network until it reaches either to the destination or to the closest node having route to the destination. This node then broadcasts an update packet listing its height with respect to the destination. When this reply packet propagates through the network each node that receives the update sets its height to a value greater than the height of the neighbor node from which the update was received. It has the effect of creating multiple links from one node to the other.

B1. Critiques of TORA

TORA is one of the largest protocol thus requires extra memory for different operations. Each node must maintain a structure describing the node"s height as well as the status of all connected links per connection supported by the network. TORA requires each node to be in constant coordination with neighboring nodes, to detect topology changes and coverage which pose high bandwidth and CPU requirements. The main drawback of TORA is the exorbitant assumptions that it makes. Not only does it require bi-directional links and a link-level protocol but it actually depends on correct and in-order transmission of all packets. TORA uses internodal co-ordination and it exhibits instability behavior similar to "count-to-infinity" problem in distance vector routing protocols. Thus there is a potential for oscillations to occur especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other. Though such oscillations are temporary and route convergence will ultimately occur, it poses real threat to utilize TORA at its full.

C. Associativity Based Routing (ABR)

Associativity based routing is a new and different approach which claims to be free from loops, deadlock and packet duplicates [10]. It defines a routing metric for mobile ad-hoc network. This metric is known as the degree of association stability. A route is selected based on the degree of association stability of mobile nodes. All nodes generate a beacon to signify its existence. When received by neighbouring nodes this beaconing causes their associatively tables to be updated. Most of the functions of ABR operate very similar as some of the other on-demand protocols such AODV and DSR.

C1. Critiques of ABR

ABR adopts the basic idea of maintaining routing information via continuous beacon updates. It is fairly known that such schemes are not very impressive due to extra burden they pose on certain network resources. Moreover, due to the nature of mobile ad-hoc network, it is highly unlikely to maintain strong link connectivity among mobile nodes. ABR has used in some of the simulation studies. In general, results were mixed however in some studies, ABR showed weak performance in comparison with other simulated protocols.

D. Signal Stability Routing (SSR)

Signal Stability based adaptive protocol (SSR) is an on-demand protocol [11]. SSR selects routes based on the signal strength between nodes and on node"s location stability. SSR can split into two cooperative protocols i.e. the dynamic routing protocol (DRP) and the static routing protocol (SST). DRP is responsible for maintaining the signal stability table (SST) and routing table (RT). SST records the signal strength of neighboring nodes. This signal strength is obtained by periodic beacons from the link layer of each neighboring node. Signal strength is either marked as a strong or weak channel. When a link failure is detected within the network the intermediate nodes send an error message to the source indicating which channel has failed.

D1. Critiques of SSR

A partial route discovery mechanism is not valid to SSR. Therefore if a link failure is detected route discovery has to be initiated from the source. Broken links are locally detected but not repaired and the multiple flooding of RouteRequest messages restricts the bandwidth. One other weakness of SSR is the failure of the intermediate nodes to reply to route request which are forwarded towards the destination. This drawback adds more delay during the route discovery process. SSR does not suggest any mechanism to address those packets which receive over the weak channel. In a mobile ad-hoc network environment it is expected that channel strength could vary and maintaining strong signals on consistent basis is not easy. In SSR the absence of mechanisms to differentiate between different types of packets could results in large number of packet dropped.

E. Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) maintains routing information among all nodes in the network [12, 13]. Each node maintains four tables i.e. distance table, routing table, link-cost table and message retransmission list (MRL) table. Each entry of the MRL contains the sequence number of the update message a retransmission counter and an acknowledgement required flag vector with one entry per neighbor and a list of updates sent in the update message. The MRL records updates in an update message need to be retransmitted and which neighbors should acknowledge their transmission.

E1. Critiques of WRP

Nodes in WRP maintain four tables thus require sufficiently higher memory than some other table driven protocols. WRP also use Hello packets to keep updated routing information. It has been mentioned before that such message consumes different network resources. Overall latency associated in routing is comparatively less in WRP as it maintains separate tables. However, it is of more use when a link failure occurs. WRP use distance vector shortest-path routing as the underlying routing protocol and it has certain degree of complexity during link failure and additions. WRP focuses on broadcasting packet to the node in close vicinity, it may be concluded that node may not have adequate information about nodes not in their vicinity. Therefore, it limits effective data transmission in a small area. Update messages are limited to the neighboring node. This limits the network view for nodes not operating in the close vicinity.

F. Cluster-head Gateway Switch Routing Protocol (CGSR)

The Cluster-head gateway switch routing protocol (CGSR) is a clustered multi-hop mobile wireless network with several heuristic routing schemes. In CGSR a cluster head controls a group of mobile nodes. A framework for code separation and channel access through which routing and bandwidth allocation is achieved. A cluster head selection algorithm is utilized to select a node as the cluster head using a distributed algorithm within the cluster. Using LCC cluster-heads only change when two cluster heads come into contact or when a node moves out of contact of all other cluster-heads. The main problem is transmission power limited by the number of cluster head changes in mobile ad-hoc network. The CGSR is the only table driven protocol that follows a hierarchical routing philosophy and does not use any hello messages.

F1. Critiques of CGSR

LCC clustering algorithm introduces additional overhead and complexity in the formation and maintenance of clusters [14]. The disadvantage of having a cluster head scheme is that frequent cluster head changes can adversely affect routing protocol performance since nodes are busy with cluster head selection rather than packet relaying. Cluster head table also pose additional requirement to the memory. CGSR use distance vector shortest-path routing as the underlying routing protocol. It has the certain degree of complexity during link failure and additions. In CGSR cluster heads and gateway nodes have higher computation and communication load than other nodes. The network reliability may also be affected due to single points of failure of these critical nodes. Hence instead of invoking cluster head reselection every time the cluster membership changes clustering algorithm is introduced.

G. Global State Routing (GSR)

Global State Routing (GSR) improve link state routing by avoiding flooding of routing messages [15]. Each node maintains a Neighbors list, a topology table, a next hop table and a distance table. Neighbors list of a node contains the list of its neighbors here all nodes that can be heard by a node are assumed to be its neighbors. The routing messages are generated on a link change as in link state protocols. On receiving a routing message the node updates its topology table if the sequence number of the message is new than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbors.

G1. Critiques of GSR

The update message size in GSR is relatively large compared to those in some other scheme. Large message size and propagation delay wastes a considerable amount of network bandwidth . That makes it difficult to predict GSR performance on different size of network. It is not clear why routing information in GSR stored inside three tables besides maintaining neighbour list. This

approach is different from traditional link state routing protocol such as DSDV which uses single table for same purpose. Keeping information inside three different tables limits node performance to certain extent. Not limited to route or address management, these tables have their due affects on battery life of mobile nodes. Efficient retrieval of already stored addresses requires a search operation. Having distributed information could slow down the whole search process. Likewise storing new information could yield the same affect.

H. Fisheye State Routing (FSR)

Fisheye State Routing (FSR) is an improvement of GSR [16]. In FSR, each update message does not contain information about all nodes. Thereby reducing the size of the messages and saving a considerable amount of bandwidth. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size. So each node gets accurate information about neighbors. However, details and accuracy of information decreases as the distance from node increases. The scope is defined in terms of the nodes that can be reached in a certain number of hops. The centre node has most accurate information about all nodes in the white circle and so on. Even though a node does not have accurate information about distant nodes the packets are routed correctly because the route information becomes more and more accurate as the packet moves closer to the destination.

H1. Critiques of FSR

It is cleared from the above description that FSR could show better results in a small network. However, its efficiency could reduce as the network grows. In other words accuracy of information decreases as the distance between the nodes increases. Having an integrated node consist wider information than other nodes and reduces the response ability of other nodes in the network. It also reduces the view of the other nodes in comparison with the centre node. In addition, this semi integrated structure is not suitable for mobile ad-hoc network environment.

I. Source Tree Adaptive (STA)

In STAR each node maintains a source tree which consists of its preferred links to each destination[17]. The source tree is calculated on the information of its own links and the source trees reported by its neighbors. Any changes in a source tree are reported to the neighbors in an incremental manner. The source tree and neighbor information establish the partial topology information in each node. This information is used by a route selection algorithm to obtain the route table with destination and next hop. In STAR information is updated with link state updates. STAR can operate in several modes but there are two main modes namely optimum routing approach and the least overhead routing approach.

I1. Crítiques of STA

STAR requires new neighbors and leaving neighbors are detected in finite time. This could also limit the overall scope of this scheme. Likewise protocol requires a link layer capable of transmitting local broadcast messages without hidden terminal interference. Unlike some other link state protocol STAR does not follow any approach to clear outdated information from the routing table. This leaves a number of different side effects on the protocol performance. Over time routing tables will grow bigger. No doubt it will have its own negative impact on the available resources such as bandwidth. Likewise it could also degrade node performance. In situations where in already established network nodes have to look for destination of interests an extra amount of time is added to the initial node search process. Moreover, if nodes decided to search for a suitable route, the same response query packet will receive at all intermediate receiver¨s nodes. As a consequence the whole network will be slow down. Chances are as time passes the network performance will reach to such an extent where rebooting the entire network become necessary.

In STAR the link state information does not time out which makes it difficult to predict anything about the stability of the recorded links. STAR claims to reduce the routing overhead but protocol specification is silent about its effect on network resources such as bandwidth and battery power. At last, not enough literature highlighting STAR performance or comparison with other schemes is available. This also limits the possibility of gaining a wider understanding about protocol working and its performance in different networking environments.

J. Optimized Link State Routing (OLSR)

Optimized Link State Routing is another proactive link state protocol which is claimed to work best in large dense network [18].OLSAR each node selects a set of Multipoint Relays (MRP) from its neighbors. The radio range of the MRP set such that it should cover all two hops neighbors. Each node has the knowledge as to for which node it acts as a MRP. Thus OLSR requires bidirectional links. OLSR utilizes UDP to distribute routing packets. Each routing packet contains one or more OLSR messages. Messages exist for neighbor by the same originator as the route and send its reply via the reversed hop list in the received request.

J1. Critiques of OLSR

OLSR is suitable for network where frequent communication take place in collection of nodes rather than as a whole. It is not cleared what criteria nodes use to

form Multipoint Relays (MRP). Each routing packet in OLSR can have more than one message. Therefore more effective measures are required to differentiate different messages in a routing packet. OLSR use User Datagram Protocol (UDP) as communication medium. UDP provides very few error recovery services, offering instead a direct way to send and receive datagram"s over an IP network. Due to the nature of mobile ad-hoc network it is expected that network transmission would meet different types of error. Absence of effective error recovery mechanism could make it difficult to utilize OLSR at best.

K. Distance Routing Effect Algorithm for Mobility (DREAM)

Distance Routing Effect Algorithm for Mobility is a table driven protocol [19]. It is designed to provide distributed loop-free and multi-path routing. DREAM is also able to adapt to mobility. For routing update DREAM introduces two new mechanisms i.e. frequency and message life time. The principles are distance effect and mobility rate. In DREAM, each node records location information in a Location Table. With the location information stored at routing tables, data packets are partially flooded to nodes in the direction of the destination, and then it selects a set of one-hop neighbors that are located in the direction. If such steps are empty the data is flooded to the entire network. Otherwise, the set is enclosed in the data header and transmitted with the data. When the destination receives the data it responds with an ACK to the source in a similar way. However, the destination will not issue an ACK if the data is received via flooding. The source, if it does not receive an ACK for data sent through a designated set of nodes, retransmits the data again by pure flooding.

K1. Critiques of DREAM

DREAM is claimed to be a loop free since the messages travel away from the node into a specific direction. This could be questioned since in a network with very high mobility the target direction can change even back to a node that has sent the message already. Another problem is that location table entries may be stale and that no close neighbor in the required direction can be found. DREAM requires each node to be equipped with GPS system. This additional requirement has several drawbacks. Normally GPS system is available under certain scenarios such as in battle field or in a disaster recovery. Availability of such system among normal users is not common. That not only limits the operational scope of DREAM but also pose a limit to its further practical implementation.

There are different conditions imposed by the protocol for routine network operations. It is common observation that normal network operation becomes complex due to excess of conditions. Conditions such as issuing an acknowledge message only if the packet is received via flooding pose an additional requirement. A node has to discover first how the packet is received. It could add the waiting time for packet in the queue. Likewise it could also delay in responding those packets which requires immediate action. Environment such as battle fields etc require smooth and effective transmission. These conditions could results in significant drops of protocol performance. At last no further work on DREAM has been reported in the cited literature but other routing schemes such as LAR[160] or FSR[35] did pick up some concepts of DREAM.

L. Zone-based Hierarchical Link State Routing Protocol (ZHLS)

In Zone-based Hierarchical Link State Routing Protocol (ZHLS), the network is divided into non-overlapping zones. ZHLS defines two levels of topologies – node level and zone level. A node level topology tells how nodes of a zone are connected to each other physically. A virtual link between two zones exists if at least one node of a zone is physically connected to some node of the other zone. Zone level topology tells how zones are connected together.

L1. Critiques of ZHLS

ZHLS could perform better in specific zones but it is difficult to maintain consistency across the network. The protocol to some extent can provide a better solution in terms of reducing communication overhead and delay, but this benefit is subjected to the size and the dynamics of a zone. It is expected that with the increase in the size of network, ZHLS could create unpredictable large overhead.

Efficient connectivity among various zone is it self an issue. Therefore if connectivity among mobile nodes in a zone is sound, it could be expected that the situation in other zone or the worst case in neighboring zone is not good enough. ZHLS proposed two different types of link state packets. In order to keep all nodes updated frequent propagation of this information is needed. Therefore, nodes should be capable of differentiating among various types of packets. That makes whole issue a bit complicated for the nodes. Engaging nodes in more jobs could affect and limit their ability to respond various network packets and consume node resources.

M. Hierarchical State Routing (HSR)

The characteristic feature of Hierarchical State Routing (HSR) is multilevel clustering and logical partitioning of mobile nodes. The network is partitioned into clusters and a cluster-head elected as in a cluster-based algorithm. In HSR, the cluster-heads again organize themselves into clusters and so on. A hierarchical address is enough to ensure delivery from anywhere in the network to the host. In addition, nodes are also partitioned

into logical sub-network and each node is assigned a logical address. Since logical address/hierarchical address are used for routing it is adaptable to network changes.

M1. Critiques of HSR

Continuously changing hierarchical addresses makes it difficult to locate and keep track of nodes[20]. This makes it difficult to achieve routing at a lower expense. It is expected that most of the time nodes will be busy locating different addresses. This also requires nodes to advertise their routes on frequent basis. It has been mentioned before that such scheme adds an extra burden on available network resources. Moreover, absence of efficient maintenance and error recovery mechanisms could also pose additional requirements in the address management of HSR.

N. Cluster Based Routing Protocols (CBRP)

In Cluster Based Routing protocol (CBRP) the nodes are divided into clusters. Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). In CBRP routing is done using source routing. In forwarding a packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism.

N1. Critiques of CBRP

CBRP and all those who focus on achieving routing in small partition of network face the same type of problems [21]. One important issue is connectivity among individual clusters. Network formation in such design is another issue i.e. how nodes will be allocated to different clusters or in zones such as in ZRP. It is mentioned in the specification of CBRP that new joining inside a cluster is based on broadcasting a message. But it is not cleared how nodes know in advance which cluster it wants to join. Moreover if the node receives replies from more than one clusters then how it will make its joining decision. Likewise in the case of clusters what scheme CBRP utilizes to aware all the cluster-heads about all other cluster-heads in the network. Specification details some error recovery mechanism but is silent about issues such as link satiability between clusters.

O. Hybrid Routing Protocol (HRP)

Hybrid routing protocols divides a set of nodes into zones in the network topology [39]. Then, the network is partitioned into zones and a proactive approach is used within each zone to maintain routing information. Hybrid routing adopts reactive approach to route packets between different zones. Therefore, in hybrid schemes a route to a destination that is in the same zone is established without delay while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The zone routing protocol (ZRP) zone-based hierarchical link state (ZHLS) routing protocol and distributed dynamic routing algorithm (DDR)[22] are three hybrid routing approaches.

O1. Critiques of HRP

The hybrid protocols can provide a better solution in terms of reducing communication overhead and delay. But this benefit is subjected to the size of a zone and the dynamics of a zone. Therefore with the increase of network size HRP could create unpredictable large overhead. This poses a limitation to the overall adaptability of HRP. Ideally zone could be bound to have some specific number of nodes to obtain consistent results. But this is not possible in a more practical environment. Hybrid approaches provide a compromise on scalability issue in relation to the frequency of end-to-end connection the total number of nodes and the frequency of topology change. Thus, the hybrid approach may not be a suitable approach for routing in some types of network.

P. Distributed Dynamic Routing Algorithm (DDR)

Distributed dynamic routing protocol (DDR) constructs a network from a network topology where each tree of the constructed network has to be optimal [22]. Each tree of the constructed network forms a zone. Once the network is partitioned into a set of non over-lapping dynamic zones each node calculates periodically its zone ID independently. Each zone is connected via the nodes that are not in the same tree but they are in the direct transmission range of each other. So the whole network can be seen as a set of connected zones. Thus each node from a zone can communicate with another node from another zone. Depending on features like node density rate of network connection and disconnection, node mobility and transmission power the size of zone increases and decreases dynamically. Mobile nodes can either be in a router mode or non-router mode regarding its position in its tree. This allows a more efficient energy consumption strategy. Each node is assumed to maintain routing information only to those nodes that are within its zone and information regarding only its neighboring zones.

P1. Critiques of DDR

In CEDAR selection of nodes for sub-net could be a problematic issue. Moreover where on one hand it could creates considerable delay before a network is formed. On the other hand, there is no guarantee that through such schemes entire network could be covered. Likewise, a specific mechanism is required to handle all joining and leaving requests from individual node. It has

to be done through packet transmission. It could also result in addition of extra update or similar type of packets. These packets could be a mean to add further burden on available bandwidth, thus could create network overhead. One final point is that most of the schemes that based on network partitioning to achieve routing suffer with one or more similar problems. One such problem is consistency. Ideally, this sort of scheme is more suitable for a small network of few nodes.

Q. Distributed Spanning Tree Protocol (DST)

DST[32] considers the variation of different regions in mobile ad-hoc networking environments[32]. DST proposed the establishment of a backbone network in the stable regions using a spanning tree algorithm. For the unstable regions a flooding or a shuttling approach is used to transmit the packet to the destination even through a very unstable area.

Q1. Critiques of DST

DST provides routing only in stable area. Moreover, it requires time before a clear view about the stable region could be established. In most of the cases, nodes require connection with other nodes or at-least with nodes of interest. It is not possible in DST as selection of stable regions requires time. DST is described in [168] and compared against pure flooding. However there was no comparison with other protocols. Moreover, the comparison focuses some of the small protocol and no comparisons have been done with some of the prominent protocols. Therefore it is difficult to add any further comments.

R. Flow Oriented Protocol (FORP)

FORP is deigned for real time traffic flows[33]. Like on-demand protocols, traffic flow is requested first and can be used after. In FORP, each link has a Link Expiry Time (LET) and the minimum of all LET"s for all links in a route gives the Route Expiry Time (RET). The destination sends a Flow-HANDOFF message which triggers another Flow-REQUEST thus finding a new route over which the current flow can be rerouted without interrupting it.

R1. Critiques of FORP

FORP is very similar to some other on-demand protocols. Therefore the draws back in the general sense are same as in some other on-demand protocols. No specific procedure is followed to reduce the power consumption which otherwise could consume when node will be busy in receiving and forwarding flow requests. Likewise no precautions have been taken to avoid message looping. Moreover, the whole scheme of flow requests without proper check could cause network overhead. Finally, no further work outlining FORP performance or comparison with other similar or related protocol is reported in the scientific literature.

S. Fuzzy Sighted Link State Algorithms (FSLS)

FSLS also focuses on the problem of limited dissemination of link state information. Links state information is sent with dynamically limited time-to-live and in certain intervals. It further depends on the number of hops the updates can travel. Far reaching link state information messages are sent much less frequent than short reaching link state information messages. Also these messages are only created if the state of a link has changed within the scope of the LSU (Link state unit). The length of the intervals and scope of the LSU"s is the design parameter of the class of FSLS algorithms. An extreme case is the discrete link state algorithm DLS in which each LSU is sent through the whole network. It differs from standard link state only in the fact that the LSU is not sent immediately after a link status changes but at the beginning of the next interval.

S1. Critiques of FSLS

It would be difficult to establish stable routing through out the network via FSLS. Maintaining limited information could also mean offering limited routing. Moreover, it is always an issue to achieve same data delivery in different sections of the network. To some extent the protocol also relies on updates. In case of mobile ad-hoc network where topology changes happen quite frequently, it is hard to maintain updated topology information without generating network overhead. Moreover, this sort of schemes could also cause mobile nodes to be engaged all the time. Engaging nodes throughout the network life could results nodes exhausting battery power, an extra burden on the available bandwidth and degradation both in nodes, efficiency and data delivery. No further work and comparison of FSLS is reported in the cited literature.

T. Lightweight Mobile Routing (LMR)

Lightweight mobile routing (LMR) is a link reversal routing protocol. Its operation depends on three basic messages i.e. query, reply and failure query. A query message is sent by the source node via limited broadcast. The source then waits for a reply packet which is issued by a node which has route to the destination. The directed flood caused by the reply messages forms a directed acyclic graph rooted in the originator of the reply. The route itself and the up and down stream links formed depend on the order of the reply transmissions. If a node

loses its last route to the destination and it has upstream neighbors a failure query is broadcasted to erase invalid routes. On reception of a failure query the node may either transmit a reply or another failure query if its last link was erased by the first failure query. So instead of a direct link reversal LMR erases the links and sets new links. Loop freedom is ensured by marking previous unassigned links as downstream-blocked if the node has already an upstream link. These markers time out after a while but it may happen that a downstream link cannot be used because of possible loop formation. Likewise to avoid deadlock a similar mechanism is used.

T1. Critiques of LMR

Limited broadcast in LMR may also mean that routing in a limited area. To some extent it could also improve different performance metric[34]. But LMR limits the network coverage and is not well suited for a larger network. Moreover, too many route queries could pose additional load on the network. Likewise the same factor could also be seen an additional burden on the limited network resources. LMR is cited in some of the available literature but mainly as a reference. The protocol lost interest with the development of TORA as a successor.

U. Link Reversal Routing (LRR)

LRR is designed specifically to aid routing in highly dynamic network. One of the main objectives is to minimize the amount of overhead [34]. In situations when topology changes need to be announced the maintained topology is reduced to a directed acyclic graph rooted in the destination. This graph is used to direct each link as either upstream or downstream to the destination. If a node in the graph becomes a local minimum i.e. it has no downstream one of its links is reversed. To achieve this notion of height is introduced thus the problem is similar to flow in a graph. The height of the minimum node is raised such that it is higher then the lowest of its neighbors thus reversing the direction of this link. The reversal can cause another node to become a minimum and the process continues.

U1. Critiques of LRR

In LLR no nodes knows about the distance of itself to the destination. Therefore optimizing metrics used in distance vector or link state algorithms cannot be used. This limits the adaptability of this approach at a wider level. Moreover, in the light of current specification of LLR, it could easily be concluded that scheme could produce results in a small area of few nodes. However, it"s difficult to predict any thing about a network with wider coverage. Thus LLR is well suited for small network.

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

Based on the reverse path forwarding algorithm [35, 36]. TBRPF is one of the tables driven or proactive link state protocol. Unlike traditional table driven protocol, TBRPF maintains a spanning tree in each node for each other node as the source. Each parent of the source node is responsible of this tree formation. A list of parents is kept at each node for every other node as well as full topology table including cost and sequence number of each link the node is aware of. The topology update messages are sent along these spanning trees but in the reverse direction. TBRPF support only bidirectional links. The topology updates are transmitted reliable. Very similar to tables driven protocols, A HELLO message is used for neighbor"s detection. This HELLO message also contains a list of router IDs and a sequence number such that each node can maintain its neighbor table. TBRPF also transmitted updated information which contains details of any changes in the router list.

V1. Critiques of TBRPF

The main problem in most of the schemes similar to TBRPF is the formation of spanning tree. Considerable amount of time is required to form spanning tree in each node. Moreover extra efforts are needed to maintain all such trees. Another aspect is the little consideration that has been given to address dynamic nature of ad-hoc network. Use of Hello messages in TBRPF could reduce node individual performance. Likewise it could also be a mean of reducing node and network limited resources.

W. Terminode Routing (TLR/TRR/AGPF)

Routing between terminodes is a hybrid process that routes packets based on the geographic position. The destination address is called location dependent address (LDA). From this LDA the closest friend-node is calculated and the packet is delivered to it. Terminodes use the concept of a virtual home region which is same for some approach. In other words for each node there exists such as home region which is specified by a fixed position and a radius. The region can be calculated by a hash function over the node"s id. Each node within the virtual home region of a certain node must maintain the current position of this node so that other node can obtain it.

The position based routing method is called Anchored Geodesic Packet Forwarding (AGPF). To avoid running into a maximum the route is oriented on set anchors along the path. An anchor is just a specific location. The anchored path is determined by the source using Friend Assisted Path Discovery (FAPD) and included into the packet. FAPD is based on small world graphs. Alternatively the path can be determined by Data Requirement Delivery (DRD) which just sends the packet to a set of neighbors whose angle is the smallest to the

right direction. The local routing method is no longer based on position information but only on a unique node identifier the target id. Two hops neighborhood information is maintained by each node by using HELLO packets. If the neighborhood is known and a packet can utilize local routing target to the node which received the packet, a path discovery is initiated to direct the packet to the destination.

W1. Critiques of TLR/TRR/AGPF

The protocol utilizes a number of different concepts of some of the earlier proposed schemes to offer routing. It uses Hello messages to maintain two hops neighbor information; similarly it relies on path discovery mechanism to direct the packet to the destination. Chances are both of these functions will be used extensively. It is mainly due to the dynamic nature of mobile ad-hoc network. It could results in unnecessary network resource consumption and likewise could also drop overall network data delivery and efficiency. It is cleared from the above mentioned specification that this scheme suits smaller network. The main reason is the difficulty to disseminate information across the network within the design frame of this protocol.

X. Witness Aided Routing (WAR)

Witness Aided routing makes use of the possibility to overhear a transmission in range of a node on a wireless channel in a unique way [37]. A node capable of overhearing a transmission from one mobile host to another over a relay can acts as a passive witness for that transmission. In situation when a relay is not able to reach the destination witness node i.e. node can overhear transmission becomes an active witness and tries to deliver the packet on behalf of the relay node, thus saving the packet even if the original route failed. Because many nodes can be witnessed of a certain transmission special care is taken to avoid contention.

The goal is to perform just one single successful delivery. To achieve this each witness host which intends to deliver the packet must get permission from the destination host. To get this permission the node sends a request to the destination host. If the target host did receive the packet before by the relay the request will be rejected otherwise the set of witness will be polled by the target until the packet could be successfully delivered.

The route discovery mechanism of WAR is very similar to DSR with the enhancement of multiple route selection criteria. The target can be instructed to await a certain amount of route requests or to wait for a certain time period and then choose the route to answer the route discovery according to some specified criteria. Alternate routes can be remembered to have them ready if the first choice breaks. Similar to DSR, WAR uses source routing to forward packets. Only that delivery is regarded as successful for which forwarding node receives an acknowledgement from either the intended relay node or from any witness. If not the route is considered broken and a route discovery process is initiated. Just like DSR the source route information in a relayed packet can be used to update local information.

X1. Critqiues Witness Aided Routing (WAR)

The main difficulty is the information about node that can overhear transmission. Even if the node is identified there are many reasons as to why this scheme might not work well. There are reasons as to why a node refuses to act as an intermediate node. One of those reasons is its own interest by conserving limited battery power for personal use. However, at present protocol features are silent to address this issue. For instance if a node is agreed to perform such service, it is an issue as to how long such a node can act? Moreover, having single or few nodes to cover the entire network is not easy to achieve specially in the context of mobile ad-hoc network. WAR also makes use of route discovery process which may be a means of generating extra network overhead. These factors pose a limit to the overall performance of WAR.

Y. Geographic Distance Routing (GEDIR)

GEDIR uses an approach based on progress to select the set of neighbors [38]. This set of neighbors is then use to forward the message to describe a set of related geographic routing protocols.

Y1. Critiques of GEDIR

Topology and efficiency of both mobile nodes and network as whole varies throughout the network life of mobile ad-hoc network. Any attempt to record such information would be a costly issue. Moreover, establishing routing based on stability of mobile nodes may not be an impressive idea in the context of mobile ad-hoc network. GEDIR also requires extra hardware which posed additional requirements to the protocol.

Z. Mobile Ad-hoc On Demand Data Delivery Protocol (MAODDP)

MAODDP [40] offers self starting; loop free routing among various hosts of a mobile ad-hoc network. The key feature of MAODDP is the route establishment and data delivery one after the other MAODDP requires no periodic updates of any kind at any level within the network. MAODDP enables mobile nodes to identify route breakage or expired routes so that such routes could be marked as invalid using the route error message. In

MAODDP, a joining message is broadcast to form a mobile ad-hoc network. All nodes who want to be part of the network are required to broadcast this message. Information such as node sequence number, IP address, route expiry time and hop-counter fields are part of the joining message. Information contained in the joining message serves as a starting point for initializing routing tables.

The hop-counter inside the „joining message" assists mobile nodes to locate their next-hop neighbours and the distance between two nodes in the mobile ad-hoc network. The hop-counter value increases as it reaches another node in the network. Data gathered through the "Joining message" if needed could also be used to transmit information from one node to the other node as long as the route is valid. However for destinations where the source node finds either no route or an expired route, it broadcasts a route query and data delivery packet (RQDD). From the application point of view MAODDP regards the RQDD packet as a part of its route query and data delivery process. The Acknowledge message (ACK) and the route error message are some of the messages types MAODDP defines. In MAODDP an acknowledge message serves two purposes i.e. an indication of successful data delivery and for updating routing tables. Route maintenance in MAODDP is achieved through route error (RER) messages very similar to some other [AG01, RT99] of mobile ad-hoc network. The route error (RER) message is used to track down different expired, broken or routes. MAODDP uses a combination of message broadcast ID and sequence number to avoid message looping. These broadcasts ID along with node sequence numbers are used to determine validity of the received packet.

IV. CONCLUSIONS

Among these conclusions some are of general types while rest varies from one scheme to the other. In general most of the schemes lack with practical implementation. Moreover, those who have been implemented are limited to a particular environment. Lack of the studies about these schemes is also an issue. Apart from some of the main schemes existing literature are silent about most of the schemes discussed in this paper. That makes it harder to evaluate these schemes in comparison with some of the schemes that follow same operational pattern. This fact also poses an additional obstacle in their further development. It is a well known fact that ad-hoc network suffer with different issues. Some of the most prominent issues are bandwidth constraints and limited power of mobile devices. Most of the schemes mentioned above clearly lacks in handling this and some other issues. Therefore there is definitely need of a routing solution that can not only offer a better routing solution but also address some of the other routing related issues.