ISSN: 2321-7782 (Online)
Volume 3, Issue 5, May 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

An Overview of Classification in AD HOC Routing Protocols

Dr. G. Samuel Vara Prasad Raju[1]
Professor
Andhra University
AP, India

K S R Murthy[2]
Research scholar
CSSE, Andhra University College of Engineering
AP, India

Abstract: ***In this paper, we identified some of the important design issues of routing protocols for sensor networks and also compared and contrasted the existing routing protocols. As our study expose, it is not possible to design a routing algorithm which will have good performance under all scenarios and for all mobile ad-hoc network applications. Routing protocols have been proposed for sensor networks, many issues still remain to be addressed. This work is an attempt towards a comprehensive performance evaluation of three commonly used mobile ad hoc routing protocols (AODV, DSR, and TORA). Over the past years, new standards have been introduced to enhance the capabilities of ad hoc routing protocols.***

Keywords: Wireless Sensor networks, Design issues, Routing protocols, Applications.

I. INTRODUCTION TO ROUTING PROTOCOL

A MANET environment is characterized by nodes (Mobile Hosts), bandwidth-constraints, variable-capacity wireless links and dynamic topology, leading to frequent and unpredictable connectivity changes. Therefore, traditional link- state and distance vector routing algorithms (Designed and fine-tuned under the assumption of a fixed and wired network) are not effective in this environment [28].

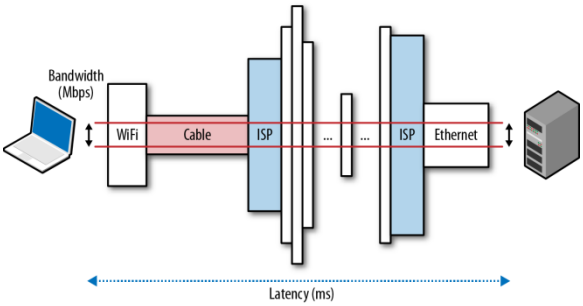
The network layer is responsible for all of the aspects of end-to-end packet delivery, including logical message addressing and routing packets between different networks. The main goal of a routing strategy is to efficiently deliver data all the way from the source to the destination.

Routing in a MANET depends on many factors including topology, selection of routers, and location of request initiator, and specific underlying characteristics that could serve as a heuristic in finding the path quickly and efficiently. The routing strategy has a significant impact on the performance of Ad hoc networks, especially since the nodes act as routers. First, routing protocols for Ad hoc networks have to be robust to the unreliable wireless links in Ad hoc networks, which are due to interference variations and mobility. Second, node mobility introduces another degree of complexity over wired or infrastructure networks, especially because of the lack of a central network controller. Third, energy awareness is crucial in Ad hoc network routing protocols. Because the nodes also act as routers in Ad hoc networks, energy depletion of some nodes could mean loss of connectivity in the network. A characterizing feature of routing protocols is the manner in which they disseminate

routing state among the nodes. The topology of a routing protocol also impacts performance related to energy efficiency, delay, and throughput.

II. MANET NETWORK ROUTING CHALLENGES

Routing in MANETs is more challenging than routing in traditional, wired networks. The factors responsible for are as follows-



- The mobile devices are usually resource-constrained and have limited wireless transmission range.
- Unlike traditional networks, the mobile devices must rely on the broadcast nature of the wireless medium. Issues like hidden terminal problem makes routing more complex.
- Generally wireless transmission medium is lesser as compared to its wired counterpart. As a result, the routing protocols must consider higher packet losses due to transmission errors.
- The mobile devices can change their locations while the message is being sent. In high-mobility environments, routing mechanisms are often subjected to additional overheads to fall out of supporting mobility is that, nodes which were formerly sending/receiving packets, move out of transmission coverage and attributing to mobility-induced packet losses.
- Battery constraints [57] as often the devices used are cellular phones or PDAs which can only run for a matter of hours and their battery must be preserved as much as possible.
- We must also account for potentially frequent network partitions. This might imply that simply no path exists from a mobile node to another as the intermediate routing stations have moved too far apart.
- The security aspects are of paramount importance [30-33]. The broadcast nature of wireless networks lends itself to passive eavesdropping attacks without malicious nodes being detected. By exploiting the specific aspects of wireless routing protocols being used, more damaging attacks are possible [34-36].

Reason to Analyze Existing MANET Routing Protocols [35, 37]

In Ad hoc networks, we need to analyze existing routing protocols to find new routing protocols because of the following reasons:

- Nodes in Ad hoc networks are mobile and topology of interconnections between them may be quite dynamic.

- Existing protocols exhibit least desirable behavior when presented with a highly dynamic interconnection topology.
- Existing routing protocols place too heavy computational burden on each mobile computer in terms of the memory-size, processing power and power consumption.
- Existing routing protocols are not designed for dynamic and self starting behavior as required by users wishing to utilize Ad hoc networks.
- Existing routing protocols like Distance Vector Protocol take a lot of time for convergence upon the failure of a link, which is very frequent in Ad hoc networks.
- Existing routing protocols suffer from looping problems either short lived or long lived. Methods adopted to solve looping problems in traditional routing protocols may not be applicable to Ad hoc networks.
- Most of the existing protocols use unipath routing. The new protocol must involve multiple paths between source and destination because when a path breaks an alternate path is used instead of initiating a new route discovery and multipath routing also achieves load balancing and is more resilient to route failures.

Table : Classification of Routing Protocols

Classification	Criteria used
Pre-Computed Routing Vs. On-Demand Routing	Depending on when the route is computed
Periodical Update vs. Event-Driven Up-Date	Based on when the routing information will be disseminated
Flat Structure vs. Hierarchical Structure	Based on the number of levels (clusters) used
Decentralized Computation vs. Distributed Computation	Based on how (or where) a route is computed
Source Routing Vs. Hop-By-Hop Routing	Based on routing information available in packet header
Single Path (unipath) Vs. Multiple Paths (multipath)	Based on number of paths established

III. Feature Desired for a Routing Protocol in Ad Hoc Networks

- he protocols to be used in the Ad hoc networks should have the following features [65-67]
- The protocol should adapt quickly to topology changes.
- The protocol should provide loop free routing.
- The protocol should provide multiple routes from the source to destination and this would solve the problems of congestion to some extent.
- The protocol should have minimal control message overhead due to exchange of routing information when topology changes occur.
- The protocol should allow for quick establishment of routes so that they can be used before they become invalid.

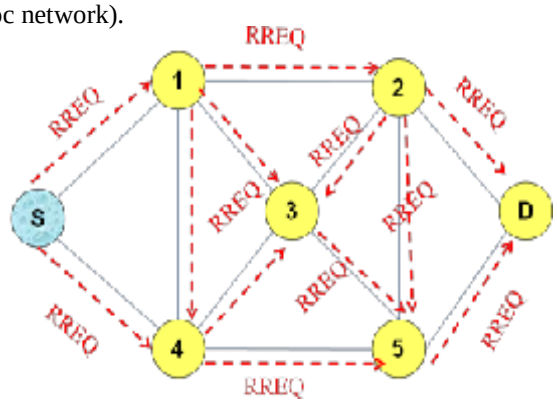
CLASSIFICATION OF ROUTING PROTOCOLS

There are different criteria [68] for designing and classifying routing protocols for wireless Ad hoc networks as shown in table below.

Existed Pre-Computed Routing Vs. On-Demand Routing [62]

Depending on when the route is computed, routing protocols can be divided into two categories: Pre-computed routing and On-demand routing. Pre-computed routing is also called proactive routing or table driven routing [32]. In Proactive routing, routes to all destinations are computed a priori and link states are maintained in node's routing tables in order to compute routes

in advance. In order to keep the information up to date, nodes need to update their information periodically. The main advantage of proactive routing is when a source needs to send packets to a destination, the route is already available, i.e., and there is no latency. The disadvantages of proactive routing are some routes may never be used and dissemination of routing information will consume a lot of the scarce wireless network bandwidth when the link state and network topology change fast. (This is especially true in a wireless Ad hoc network).



On-demand routing is also called reactive routing. In Reactive (on-demand) routing, protocols update routing information when a routing requirement is presented i.e. a route is built only when required. The main advantage reactive routing is that the precious bandwidth of wireless Ad hoc networks is greatly saved. And the main disadvantage is if the topology of networks changes rapidly, a lot of update packets will be generated and disseminated over the network, which will use lot of precious bandwidth, and furthermore, may cause too much fluctuation of routes.

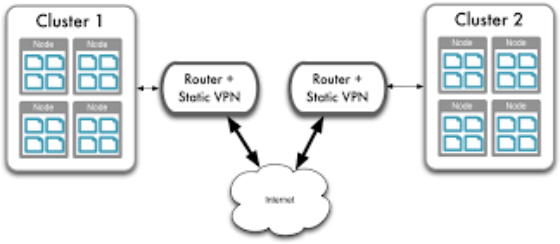
Periodical Update Vs Event-Driven Update [62]

Routing information needs to be disseminated to network nodes in order to ensure that the knowledge of link state and network topology remains up-to-date. Based on when the routing information will be disseminated, we can classify routing protocols as periodical update and event-driven update protocols. Periodical update protocols disseminate routing information periodically. Periodical updates will maintain network stability, and most importantly, enable (new) nodes to learn about the topology and the state of the network. However if the period between updates is large, the protocol may not keep the information up-to-date. On the other hand, if the period is small, too many routing packets will be disseminated which consumes the precious bandwidth of a wireless network. In an event-driven update protocol, when events occur, (such as when a link fails or a new link appears), an update packet will be broadcast and the up-to-date status can be disseminated over the network soon. The problem might be that if the topology of networks changes rapidly, a lot of update packets will be generated and disseminated over the network, which will use a lot of precious bandwidth, and furthermore, may cause too much fluctuation of routes. One solution [69, 70] is to use some threshold which imposes maximum limit to update packets .

Flat Structure Vs. Hierarchical Structure

In a flat structure, all nodes in a network are at the same level and have the same routing functionality. Flat routing is simple and efficient for small networks. The problem is that when a network becomes large, the volume of routing information will be large and it will take a long time for routing information to arrive at remote nodes. For large networks, hierarchical (cluster-based) routing may be used to solve the above problems [69, 71]. In hierarchical routing the nodes in the network are dynamically organized into partitions called clusters, and then the clusters are aggregated again into larger partitions called super clusters and so on. Organizing a network into clusters help to maintain a relatively stable network topology. The high dynamics of membership and network topology is limited within clusters. Only stable and high level information such as the cluster level or the super cluster level will be propagated across a long distance, thus the control traffic (or routing overhead) may be largely reduced [26, 69]. Within a cluster, the nodes may have complete topology information about its cluster and proactive routing may be used. If the destination is in a different cluster from the source, inter cluster routing must be used. Inter cluster routing is generally reactive, or a combination of proactive and reactive routing [72]. Similar to cellular structure in

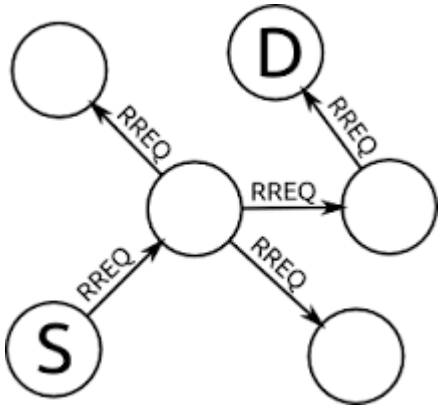
cellular systems, a hierarchical cluster is readily deployable to achieve some kind of resource reuse such as frequency reuse and code reuse [73] and interference can be reduced when using different spreading codes across clusters.



MANET Decentralized Computation Vs. Distributed Computation

Based on how (or where) a route is computed, there are two categories of routing protocols: decentralized computation and distributed computation. In a decentralized computation-based protocol, every node in the network maintains global and complete information about the network topology such that the node can compute the route to a destination itself when desired. The route computation in LSR is a typical example of decentralized computation. In a distributed computation-based protocol, every node in the network only maintains partial and local information about the network topology. When a route needs to be computed, many nodes collaborate to compute the route. The route computation in DVR and the route discovery in on demand routing belong to this category

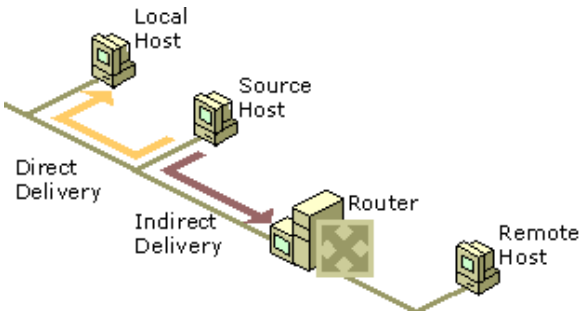
MANET Source Routing Vs. Hop-by-Hop Routing [45]



Some routing protocols place the entire route (i.e., nodes in the route) in the headers of data packets so that the intermediate nodes only forward these packets according to the route in the header. Such a routing is called “source routing”. Source routing has the advantage that intermediate nodes do not need to maintain up-to-date routing information in order to route the packets they forward, since the packets themselves already contain all the routing decisions. This fact, when coupled with on demand route computation, eliminates the need for the periodic route advertisement and neighbor detection packets required in other kinds of protocols [51]. The major problem with source routing is that when the network is large and the route is long, placing the entire route in the header of every packet will waste a lot of scarce bandwidth.

In a hop-by-hop routing, the route to a destination is distributed in the “next hop” of the nodes along the route. When a node receives a packet to a destination, it forwards the packet to the next hop corresponding to the destination. The problems are that all nodes need to maintain routing information and there may be a possibility of forming a routing loop.

Single Path (unipath) Vs. Multiple Paths (multipath)



Some routing protocols will find a single route from a source to a destination, which results in simple protocol and saves storage. Other routing protocols will find multiple routes, which have the advantages of easy recovery from a route failure and being more reliable and robust. Single path routing protocols have been extensively discussed and examined in the past [46, 47]. A more recent research topic for MANETs is multipath routing protocols. Multipath routing protocols establish multiple disjoint paths from a source to a destination and are thereby improving resilience to network failures and allow for network load balancing. These effects are particularly interesting in networks with high node density (and the corresponding larger choice of disjoint paths) and high network load (due to the ability to load balance the traffic around congested networks).

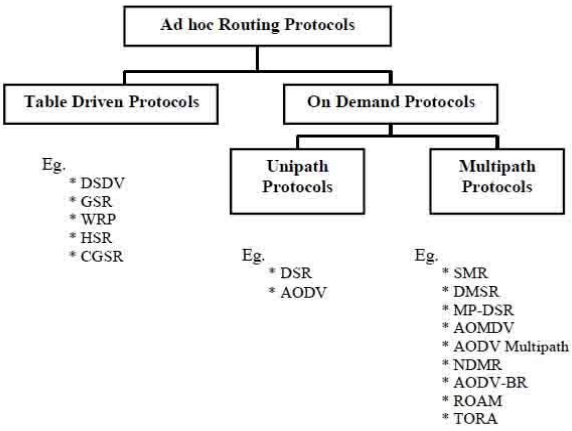


Fig : Classification of Routing Protocols

IV. OVERVIEW OF THE ROUTING PROTOCOL

In this section we discuss the two different route disseminate strategies that Ad hoc network routing protocols adopt viz.

(1) Table Driven (Proactive)

(2) On demand (Reactive) as depicted in Fig

Proactive (Table Driven) Routing Protocols

In Table-driven routing protocols [48] each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables periodically so as to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain consistent and up to date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables.

Destination Sequenced Distance Vector routing (DSDV) [10,49]

DSDV is an adaptation of a conventional routing protocol to Ad hoc networks. DSDV is based on the Bellman-Ford algorithm for shortest paths [8]. Consequently

DSDV only makes use of bi-directional links.

Topology and routing table as shown in Fig. table2 illustrates the operation of DSDV. Every node maintains the next hop and distance information to all other nodes in the network. In order to maintain table consistency, DSDV periodically transmits routing table updates. Here each table must contain the destination node address, the minimum number of hops to that destination (metric) and the next hop in the direction of that destination.

characteristic	servers	broadband	random
paths probed	378	1,139	1,636
vantage points	67	67	67
failure events	1,486	7,560	10,619
failed paths	294	999	1,395
failed links	337	1,052	1,455
classifiable failure events	962	5,723	7,024
last-hop	151 (16%)	3,406 (60%)	2,568 (37%)
non-last-hop	811 (84%)	2,317 (40%)	4,456 (63%)
unclassifiable failure events	524	1,837	3,595

The tables in DSDV also have an entry for sequence numbers for every destination. These sequence numbers form an important part of DSDV as they guarantee that the nodes can distinguish between istale and new routes. Here the value of the sequence number is incremented only by the node the sequence number is associated with. Thus, these increasing sequence numbers here emulate a logical clock. [If a node receives two updates from the same source, then the receiving node makes a decision as to which update is to be incorporated in its routing table based on the sequence number]. A higher sequence number denotes a more recent update sent out by the source node. Therefore it can update its routing table with more actual information and hence avoid route loops or false routes. DSDV determines the topology information and the route information by exchanging these routing tables, which each node maintains. The nodes here exchange routing updates whenever a node detects a change in topology. When a node receives an update packet, it checks the sequence number in the packet and process the packet as shown in packet process algorithm 4.1 In case of broken link, a cost of □‡ metric with a new sequence number (incremented) is assigned to it to ensure that the sequence number of the metric is always greater than or equal to the sequence number of that node. The updates sent out in this case, by nodes resulting from a change, can be of two types that is either a full update or a partial update. In case of full updates, the complete routing table is sent out and in case of a partial updates only the changes since last full update are sent out.

1. If the new packet has higher sequence number, the node chooses the route with the higher sequence number and discards the old sequence number. If the sequence number of the incoming packet is identical to one that the receiving node has already in its routing table, then the route with the least cost is chosen.
2. All the metrics chosen from the new routing information are incremented.
3. This process continues until all the nodes are updated. If there are duplicate updated packets, the node considers keeping the one with least cost metric and discards the rest.

Global State Routing (GSR) [50, 51]

Global State Routing (GSR) is similar to DSDV, with changes to reduce the overhead, which normal DSDV would incur with increasing network sizes. This protocol is based on Link State routing [25], which has the advantage of routing accuracy. Each node maintains a neighbor list, a topology table, a next hop table and a distance table. The neighbor list contains the list of nodes adjacent to the node. The topology table contains the link state information reported by a destination and a timestamp indicating the time at which this is generated. The next hop table and the distance table contain the next hop and the distance of the shortest path for each destination respectively. Initially, each node learns about its neighbors and the distance of the link to it (generally hop count equals one) and broadcasts this information to its neighbors. Upon receiving the link state message from its neighbors, each node updates the link state information corresponding to that neighbor in the topology table to the most up

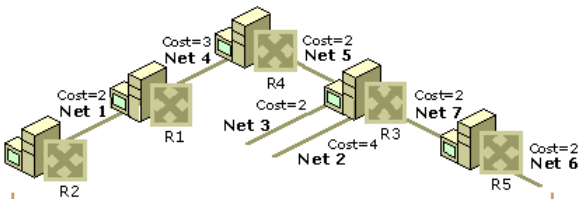
to date information. Then the node rebuilds the routing table based on newly computed topology table and broadcasts it to its neighbors. The routing table information is exchanged periodically with the neighbors only. GSR is suitable for a mobile environment where mobility is high and bandwidth is high. The drawbacks of GSR are the large size of the routing message, which consumes considerable bandwidth and the latency of the link state change propagation, which depends on update period.

Wireless Routing Protocol (WRP) [51]

WRP is another protocol based on distributed Bellman-Ford algorithm (DBF). It substantially reduces the number of cases in which routing loops (count-to-infinity problem) can occur. It utilizes information regarding the length and second-to-last hop (predecessor) of the shortest path to each destination Each node maintains a distance table, a routing table, a link-cost table and a message retransmission list. The distance table of a node contains tuples <destination, next hop, distance, predecessor (as reported by next hop) > for each destination and each neighbor. The routing table of a node contains tuples <destination, next hop, distance, predecessor, and marker for each known destination where marker specifies whether the entry corresponds to a simple path, a loop or a destination that has not been marked. The link-cost table contains the cost of the link to each neighbor and the number of periodic update periods elapsed since the node received any error-free message from it. The message transmission list (MRL) contains sequence number of update message, retransmission counter, and acknowledgement required flag vector with one entry per neighbor, and a list of updates sent in the update message. It records which updates of an update message have to be retransmitted and which neighbors should be requested to acknowledge such retransmission.

This avoids count-to-infinity problem by forcing each node to check consistency of predecessor information reported by all its neighbors. When a link fails or a link-cost changes, the node re-computes the distances and predecessors to all affected destinations, and sends to all its neighbors an update message for all destinations whose distance or predecessor have changed.

Hierarchical State Routing (HSR) [53,54]



Network	Forwarding IP	Port	Metric
4	--	1	3
5	--	2	2
1	R1	1	5
3	R3	2	4
2	R3	2	6
7	R3	2	4
6	R3	2	6

Hierarchical State Routing (HSR) employs a multilevel clustering and logical partitioning scheme. The network is partitioned into clusters and a cluster-head is elected as in a cluster-based algorithm. Cluster heads again organize themselves into clusters up to any desired clustering level as shown in above table. Within a cluster, nodes broadcast their link information to one another. A cluster head summarizes its cluster information and sends it to neighboring clusters through a gateway node. A gateway node is one, which is adjacent to one or more cluster heads. Here cluster heads are members of a higher- level cluster. At each level, summarization and link information exchanges are performed. The way the information is exchanged in this hierarchy is, first information is collected among the nodes forming the base level cluster, it is then passed on to the cluster head which In turn passes to its next hierarchical cluster head and from there on the information is disseminated into other cluster heads and thus the information traverses down the hierarchy. Here each node has a hierarchical address, which may be obtained by assigning numbers from the top root to the bottom node.

But as a gateway can be reached from the root from more than one path, so a gateway can have more than one hierarchical address. Also, each subnet contains a location management server (LMS). All nodes in the subnet are registered with the local

LMS. LMS has to inform upper levels, and upper level information comes to local LMS server. When two nodes wish to communicate, they send their initial data to the LMS, and the LMS then forwards it to the destination. But if the source and destination know each other's hierarchical addresses, they communicate directly. The protocol is highly adaptive to network changes.

The cluster head can monitor all the traffic within the cluster and provide QoS service to real time applications simply by appending bandwidth and channel quality information to the link state information. The control traffic in HSR can be comparable to that of in on-demand protocols. The latency for access to non frequently used destinations is low. But, the average number of hops the packets takes, protocol complexity, packets dropped because of invalid routes is more in HSR when compared to that of in on-demand protocols.

Clustered Gateway Switch Routing protocol (CGSR) [55]

In this protocol, nodes are aggregated into clusters controlled by a cluster head elected using a distributed algorithm as shown in Fig 4.5. All nodes within the transmission range of the cluster-head belong to this cluster. CGSR uses a Least Cluster Chance (LCC) clustering algorithm in which a cluster-head chance occurs only when two cluster-heads come into one cluster or one of the nodes moves out of the range of all the cluster heads. Also, more priority is given to cluster heads during channel allocation to maximize channel utilization and minimize delay. The general algorithm is based on DSDV algorithm [10]. Each node maintains two tables, namely, a cluster member table which records the cluster head for each destination node and routing table which contains the next hop to the destination. The cluster member table is broadcasted periodically. A node will update its cluster member table when it receives a new one from its neighbors using sequence numbers as in DSDV. To route a packet to a destination, the node first selects the shortest (minimal hop) cluster-head corresponding to the destination from the cluster member table and routing table and then transmits the packet to the next hop according to the routing table entry corresponding to that cluster head. The general algorithm can be improved to route packets alternatively between cluster heads and gateways as shown in Fig below. A gateway is a node, which belongs to more than one cluster. First, the source sends the packet to its cluster head. Then, the packet gets forwarded to the gateway node that connects this cluster-head and the next cluster-head en route destination. The gateway sends it to that cluster head and so on till the packet reaches the destination cluster head, which then transmits the packet to the destination. Also, heuristic token scheduling and gateway code scheduling speed packets delivery along multi-hop paths and path reservation makes token scheduling and code scheduling more efficient, thus being capable of transmitting multimedia traffic.

Clustering provides framework for the development of important features such as code separation (among clusters), effective channel allocation and spatial reuse, routing and bandwidth allocation. But the selection of the cluster heads may cause complexity and overhead, thus degrading performance. Also, there are traffic bottleneck and single point failures at the cluster heads and gateways.

On-Demand Routing Protocols

The main motivation of the designing of on-demand routing protocols is to reduce the routing overhead in order to save bandwidth in Ad hoc networks. On-demand routing protocols execute the path finding process and exchange routing information only when there is a requirement by the station to initialize a transmission to some destination. On-demand routing protocols can be again classified as unipath (single path) on demand protocols and multipath on-demand protocols [57, 58].

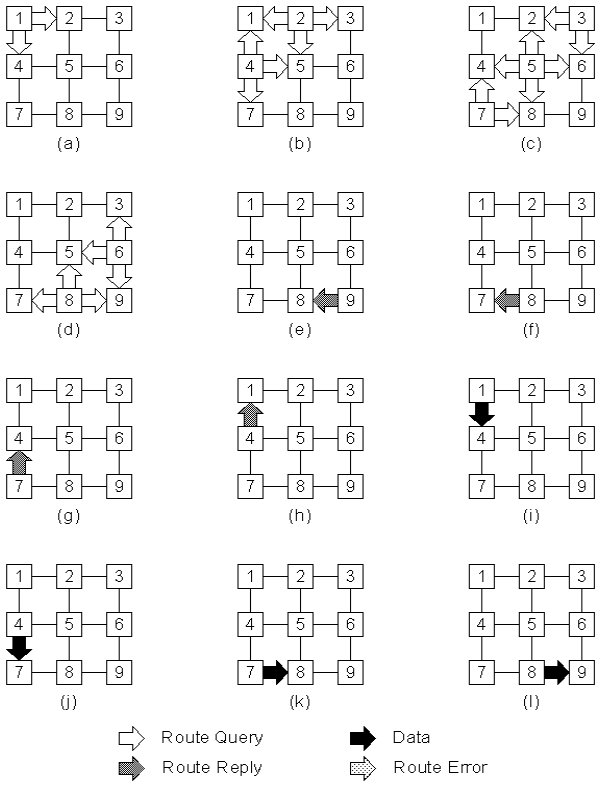
Unipath On Demand Routing Protocols

Most currently proposed routing protocols for Ad hoc networks are unipath routing protocols. In unipath routing, only a single route is used between a source and destination node. Two of the most widely used on-demand protocols are the Dynamic Source Routing (DSR) and the Ad hoc On-demand Distance Vector (AODV) protocols. An example of route discovery in a unipath Ad hoc network is shown in DSR Fig.

Dynamic Source Routing (DSR) [14, 57-62]

Dynamic source routing is a Source routed On-Demand routing protocol in Ad hoc networks. It uses Source Routing, which is a technique in which the sender of a packet determines the complete sequence of nodes through which the packets have to be traveled to reach destination.

The sender of the packet explicitly mentions the list of all nodes in the packet's header, identifying each forwarding 'hop' by the address of the next node to which to transmit the packet on its way to destination host. In this protocol the nodes don't need to exchange the Routing table information periodically and thus reduces the bandwidth overhead in the network. Each Mobile node participating in the protocol maintains a 'routing cache', which contains the list of routes that the node has learnt. Whenever the node finds a new route it adds the new route in its 'routing cache'.



Each mobile node also maintains a sequence counter 'request id' to uniquely identify the requests generated by a mobile host. The pair <source address, request id > uniquely identifies any request in the Ad hoc network.

The protocol does not need transmissions between hosts to work in bi-direction. The main phases in the protocol are Route Discovery process and Route Maintenance process.

Route Discovery:

Route discovery allows any host to dynamically discover the route to any destination in the Ad hoc network. In DSR, a source initiates a route discovery process when the source wants to send a packet to a destination to which it doesn't have a valid route. The Source, if has the valid route in its routing cache then it uses it otherwise it sends a route request packet by broadcasting it to the neighbors. The route request packet contains the source address; request id and a route record in which the sequence of hops traversed by the request packet before reaching the destination are noted down.. The route request travels the Ad hoc network until it reaches the destination node. Any node forwards the route reply packet by using a route in its route cache if it has one for the initiator node or by using the node reverses the route in the reply packet to which node it need to send the reply packet.

1. It checks to see if it has the pair <initiators address, request id> in its list of recently seen requests if so discards the packet.

2. Otherwise, if this host's address is already present in the route record of the request packet then it discards the packet. This eliminates the looping problem.

3. Otherwise, if the destination the source is looking for matches with its address then it sends the route reply packet to the initiator containing the list of nodes the request packet has traversed before it reached the destination.

4. Otherwise, it appends its own address to the route request packet and rebroadcasts it.

Route maintenance:

It is performed when there is an error with an active route. When a node that is part of some route detects that it cannot send packets to next hop, it will create a Route Error message and send it to the initiator of data packets. The Route Error message contains the addresses of the node that sent the packet and of the next hop that is unreachable. When the Route Error message reaches the initiator, the initiator removes all routes from its route cache that have address of the node in error. It then initiates route discovery for a new route if needed. The advantage of DSR is reduced overhead and is able to react very quickly to changes in the network. Route caching is the mechanism used in route discovery phase, which further reduces route discovery overhead. The disadvantage of DSR is packet header size grows with route length.

Ad hoc On-Demand Distance Vector (AODV) [15-17, 63]

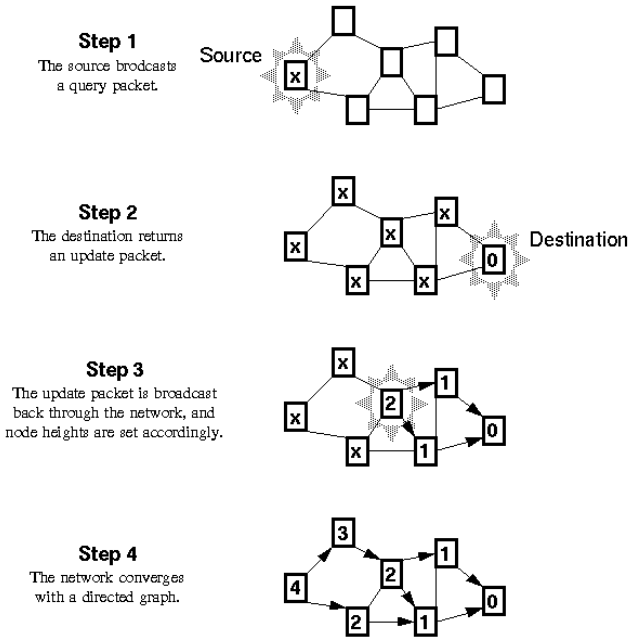


Table Structure of Routing Table Entries for AODV

Destination
Sequence number
Hop count
Next hop
Expiration timeout

AODV combines the use of destination sequence numbers in DSDV with the on-demand route discovery technique in DSR to formulate a loop-free, on-demand, single path, distance vector protocol. Unlike DSR, which uses source routing, AODV is based on hop-by-hop routing approach. Each node maintains a routing table, which contains a destination address, sequence number of destination; hop count (number of hops to reach the destination), and next hop to reach the destination and expiration timeout.

Route Discovery:

In AODV, a sender first broadcasts a Route Request Packet (RREQ) with the sender's id and a unique destination sequence number to all its neighbors. All neighbors that receive the RREQ rebroadcast it. Neighbors also store the neighbor's id from which they received the RREQ, which represents the reverse path to the destination. Any node that has already processed this RREQ discards any duplicate RREQs. If a valid route to the destination is available, then the intermediate node generates a RREP, else the RREQ is rebroadcast. Duplicate copies of the RREQ packet received at any node are discarded. Finally, when the destination node receives a RREQ, it sends a RREP, which eventually reaches the original sender through the reverse path links. The sender then proceeds with data transmission. Nodes in AODV maintain only next hop routing state, which provides AODV with a high degree of scalability

Route maintenance:

Route maintenance is done using route error (RERR) packets. When a link failure is detected (by a link layer feedback, for example), a RERR is sent back via separately maintained predecessor links to all sources using that failed link. Routes are erased by the RERR along its way. When a traffic source receives a RERR, it initiates a new route discovery if the route is still needed. Unused routes in the routing table are expired using a timer-based technique. Sequence Numbers and Loop Freedom- Sequence numbers in AODV play a key role in ensuring loop freedom. Every node maintains a monotonically increasing sequence number for itself. It also maintains the highest known sequence numbers for each destination in the routing table (called "destination sequence numbers"). Destination sequence numbers are tagged on all routing messages, thus providing a mechanism to determine the relative freshness of two pieces of routing information generated by two different nodes for the same destination. The AODV protocol maintains an invariant that destination sequence numbers monotonically increase along a valid route, thus preventing routing loops. AODV route update rule is given in A node can receive a routing update via a RREQ or RREP packet either forming or updating a reverse or forward path. Routing updates received via a RREQ or RREP are referred as "route advertisements." The update rule in algorithm 4.3 is invoked upon receiving a route advertisement. Hop-by-Hop routing in AODV eliminates the need for a source route in each data packet, which reduces the byte overhead of the protocol.

Route Discovery:

Route discovery consists of finding multiple routes between a source and destination node. Multipath routing protocols can attempt to find node disjoint, link disjoint, or non-disjoint routes. Node disjoint routes [93-95], also known as totally disjoint routes, have no nodes or links in common. Link disjoint routes have no links in common, but may have nodes in common. Non-disjoint routes can have nodes common and are therefore non-disjoint.

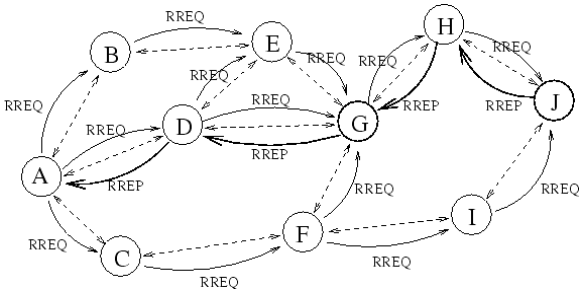
Traffic Allocation -:

Once the source node has selected a set of paths to the destination, it can begin sending data to the destination along the paths. The traffic allocation strategy used deals with how the data is distributed amongst the paths. The choice of allocation granularity is important in traffic allocation. The allocation granularity specifies the smallest unit of information allocated to each path. For instance, per-connection granularity would allocate all traffic for one connection to a single path. Per-packet granularity would distribute the packets from multiple connections amongst the paths. Per-packet granularity results in the best performance [84]. This is because it allows for finer control over the network resources.

Split Multipath Routing (SMR) [102, 103]

It is a multipath version of DSR. Unlike many prior multipath routing protocols, which keep multiple paths as backup routes, SMR is designed to utilize multipath concurrently by splitting traffic onto two maximally disjoint routes. Two routes said to be maximally disjoint if the number of common links is minimum. SMR uses one route discovery process to accumulate

as many as possible routes to the destination node. This route discovery process runs in the same way as in DSR. However, there are more steps involved in processing RREQ packets at intermediate and destination nodes. If an intermediate node receives a RREQ packet, it adds its own address and rebroadcasts the RREQ packet. Whenever an intermediate node receives another RREQ from the same source node and with the same request id, i.e. a duplicated RREQ, the node checks the following two things. First, the RREQ packets are checked if they traversed through different incoming link. Second, the hop count (of the RREQ) is checked if it is not larger than that of the first received RREQ. Then the node appends its own id and forwards the RREQ packets. Otherwise the RREQ packet is discarded. Additionally, intermediate nodes are not allowed to reply directly with a RREP on a RREQ packet.



When a route fails, every entry, regardless of destination, in the source's routing table that shares common intermediate nodes with the fail route is removed. After this if the other route remains valid, either a new route discovery is initiated, or the protocol waits until the second route fails. SMR outperforms DSR in terms of delay and packet drops in an Ad hoc network. Furthermore, SMR is more efficient when new route discovery is initiated only when both routes are broken, as this scheme generates less control overhead.

AODV Multipath Router Approach (AODVM-R) [18]

When performing route discovery, the source and intermediate nodes maintain multiple routes to the destination. To ensure loop freedom the RREQ packet includes path information (path from the source to the router). Primary and secondary routes will have the same sequence numbers. When a link breaks, a node tries to reestablish the route using alternate paths. If still there is an unreachable destination, the node sends an RERR message to its neighbors. If the primary route works for a long time, alternate paths might timeout because they are not used. While the primary route is being used, send REFRESH message to the alternate routes occasionally to refresh them. The REFRESH packet is sent every active route_timeout / 2 seconds. The REFRESH packet is forwarded to the destination, refreshing the routes on the way. If an alternate route is detected to be broken, it is simply discarded from the route table. AODVM-R reduces number of route discoveries, but the total overhead is not significantly reduced because of refresh message overhead. Refresh message period can be carefully tuned to reduce overhead.

Temporally Ordered Routing Algorithm (TORA)[71,72]

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive loop free distributed routing algorithm based on the concept of link reversal. It is designed to minimize reaction to topological changes. A key design concept in TORA is that it decouples the generation of potentially far-reaching control messages from the rate of topological changes. Such messaging is typically localized to a very small set of nodes near the change without having to resort to a complex dynamic, hierarchical routing solution. Route optimality (shortest-path) is considered of secondary importance, and longer routes are often used if discovery of newer routes could be avoided. TORA is also characterized by a multi-path routing capability. Each node has a height with respect to the destination that is computed by the routing protocol. It is simply the distance from the destination node. TORA is proposed to operate in a highly dynamic mobile networking environment. It is source initiated and provides multiple routes for any desired source/destination pair. To accomplish this, nodes need to maintain routing information about adjacent (one-hop) nodes.

1. The protocol performs three basic Functions as follows-

a) Route creation

b) Route maintenance

c) Route erasure

2. From each node to each destination in the network, a separate directed acyclic graph (DAG) is maintained. When a node needs a route to a particular destination, it broadcasts a QUERY packet containing the address of the destination for which it requires a route. This packet propagates through the network until it reaches either the destination, or an intermediate node having a route to the destination.

Table ... : Summary of On-Demand Multipath Routing Protocols

Protocol	Base Protocol	Routing Choice Made at	Route Discovery	Motivation /Application
AODVM-R	AODV	Intermediate nodes	Link-disjoint paths.	Reduces number of route discoveries
AOMDV	AODV	Source node (Source routing)	Link-disjoint paths	Reduction in delay, routing load and the frequency of route discoveries
SMR	DSR	Source node (source routing)	Link/Node-disjoint paths	Splitting traffic provides better load distribution
AODV-Multipath	AODV	Source node (source routing)	Node-disjoint paths	Performs best in relatively static scenarios
NDMR	AODV	Intermediate nodes	Node-disjoint paths	Reduced routing overhead
DMSR	DSR	Source node (source routing)	Nodes disjoint	Increases the packet delivery ratio with lower routing overhead
MP-DSR	DSR	Source node (source routing)	Link/Node-disjoint paths	QoS applications with soft end-to-end reliability
AODV-BR	AODV	Intermediate nodes	Link-disjoint paths	Provides robustness to mobility and enhances protocol performance
TORA	link reversal	Source node (Source routing)	Link/Node-disjoint paths	Operate in a highly dynamic mobile networking environment.

V. CONCLUSION

This work is an attempt towards a comprehensive performance evaluation of three commonly used mobile ad hoc routing protocols (DSR, TORA and AODV). In this paper, using the latest simulation environment NS 2, Matlab and java we evaluated the performance of three widely used ad hoc network routing protocols using packet-level simulation. The simulation characteristics used in this research, that is, packet delivery fraction and end-to-end delay are unique in nature, and are very important for detailed performance evaluation of any networking protocol. We can summarize our final conclusion from our experimental results as:

- Increase in the density of nodes yields to an increase in the mean End-to-End delay.
- Increase in the pause time leads to a decrease in the mean End-to-End delay.
- Increase in the number of nodes will cause increase in the mean time for loop detection.

In short, AODV has the best all round performance. DSR is suitable for networks with moderate mobility rate. It has low overhead that makes it suitable for low bandwidth and low power network. TORA is suitable for operation in large mobile networks having dense population of nodes. The major benefit is its excellent support for multiple routes and multicasting.

References

1. S.R. Das, C.E. Perkins and E.M. Royer, "Performance comparison of two ondemand routing protocols for Ad-hoc networks", 19th Annual Joint Conference of the IEEE Computer and Communications letters, pages 3–12, 2000.
2. Ram Ramanathan and Jason Redi, "A brief over view of Ad hoc network: Challenges and direction", IEEE Communication Magazine, pages 20-22,May 2002.
3. C. E. Perkins, "Ad Hoc Networking", Addison-Wesley, ISBN: 0201309769, 2001.
4. P. Gupta and P. Kumar, "The capacity of wireless networks", IEEE Transactions on Information Theory, 46(2): pages 388-394, March 2000.
5. Lima, L. Calsavara, "A Paradigm Shift in the Design of Mobile Applications Advanced Information Networking and Applications Workshops", AINAW 008, 22nd International Conference on Vol. 25, Issue 28, pages 1631-1635,March 2008.

6. C. Petrioli, R. Rao, and J. Redi, "Guest editorial: Energy conserving protocols", ACM Mobile Networks and Applications (MONET), 6(3): pages207-209, June 2001.
7. C. Jones, K. Sivalingam, P. Agrawal, and J. Chen, "A survey of energy efficient network protocols for wireless networks", Wireless Networks, 7(4): pages 343-358, September 2001.
8. J. MacKie - Mason and H.Varian, "Pricing the Internet", in Public Access to the internet, Prentice Hall, New Jersey, 1994.
9. Yoo and D.P. Agrawal, "Why it pays to be selfish in MANETs", IEEE Wireless Communications Magazine, vol. 13, no.6, pages 87-97, 2006.
10. Grube Li, H, "Cellular Ad hoc network interoperation for coverage extension", Emerging Technologies: Frontiers of Mobile and Wireless Communication, Proceedings of the IEEE 6th Circuits and Systems Symposium, Vol. 2, pages 213-516, 2004.
11. S. Toumpis and D. Toumpakaris, "Wireless ad hoc networks and related Topologies applications and research challenges", vol. 123, no. 6, pages 232-241, June 2006.
12. Y.Natchetoi, H.Wu, "Service-oriented mobile applications for ad hoc networks", IEEE, ICSC, pages 405-412, 2008.
13. Jorma Jormakka, Henryka Jormakka, and Janne V, "A Lightweight Management System for a Military Ad Hoc Network", COIN 2007, LNCS 5200, pages 533–543, Springer-Verlag Berlin Heidelberg 2008.
14. Madhavi W. Subbarao, "Mobile Ad Hoc Data Networks for Emergency Preparedness Telecommunications – Dynamic Power-Conscious Routing Concepts", Interim project report National Communications Systems,2000.
15. Buttyan, L., and Hubaux, J. P, "Stimulating cooperation in self-organizing mobile ad hoc networks", Mobile Networks and Applications: Special Issue on Mobile Ad Hoc Networks, 8(5): pages 1-22, 2002.
16. Ostermaier, Benedi kt, Dotzer, Florian, "Enhancing the security of local danger warnings in VANETs, IEEE, pages 422-431,ARES-2007.
17. Kosch. T, "Local danger warning based on vehicle ad-hoc networks: Prototype and simulation", Proceedings of 1st International Workshop on Intelligent Transportation, pages 239-248, WIT- 2004.
18. Newsome J., Shi E., Song D. and Perrig A, "The Sybil attack in sensor networks: analysis & defenses", IPSN'04, Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268, ACM, 2004.
19. Hubaux J. P, Capkun S, Luo J, "Security and privacy of smart vehicles", IEEE Security & Privacy, vol.2, pages 49–55, 2004.
20. Ian F. Akyildiz, Weilian Su, Yogesh Sankaraubramaniam and Erdal Cayirci, "A Survey on sensor networks", IEEE Communications Magazine, vol.40, No.8, pages 102-114, Aug. 2002.
21. A. Mainwaring, J. Polastre, "Wireless sensor networks for habitat Monitoring", Proceedings of International workshop on WSNs and applications, Atlanta, Ga, USA , pages 88-97, Sep. 2002.
22. K. Romer, "Tracking real-world phenomena with smart dust", Proceedings.1st European Workshop on Wireless Sensor Networks (EWSN '04), pages 28–43, Berlin, Germany, January 2004.
23. L. Schwiebert, S. K. S. Gupta, and J. Weinmann, "Reserach challenges in wireless networks of biomedical sensors", Proceedings of the 7th ACM International Conference on Mobile Computing and Networking (MobiCom '01), pages 151-165, Rome, Italy, July 2001.
24. A. Acharya, A. Misra, S. Bansal, "High-performance architectures for IPbased multihop 802.11 networks", IEEE Wireless Communications 10 (5):pages 22–28, 2003.
25. A. Adya, P. Bahl, J. Padhye, A. Wolman, L. Zhou, "A multi-radio unification protocol for IEEE 802.11 wireless networks", International Conferences on Broadband Networks (BroadNets), 2004.
26. D. Aguayo, J. Bicket, S. Biswas, G. Judd, R. Morris, "Link-level measurements from an 802.11b mesh network", Proceedings of ACM Annual Conference of the Special Interest Group on Data Communication (SIGCOMM), pages 121–131 , August- 2004.
27. D. Aguayo, J. Bicket, S. Biswas, D.S.J. De Couto, R.Morris, "MIT Roofnet implementation", Available from: http://pdos.lcs.mit.edu/roofnet/design/,2004.
28. Andrew S. Tanenbaum, Vrije University, Amsterdam, Netherlands, Computer Networks, 3/E", Prentice Hall PTR, 1996, ISBN-10: 0133499456.
29. Goldsmith, A.J., and S.B. Wicker, "Design challenges for energy constrained ad hoc wireless networks", IEEE Wireless Communications 9 (4): Pages 8-27,2002.
30. H. Deng, W. Li, and Dharma P. Agrawal, "Routing Security in Ad Hoc Networks", IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol.40, No.10, pages 70-75,October 2002.
31. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Proceedings of the Tenth Annual Network and Distributed System Security Symposium (NDSS 2003)". ISOC, San Diego, CA,pages 57-73, February 2003.
32. Yi-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", WiSe 2003, September 19, 2003, pages 30-40, San Diego, California, USA, 2003.
33. Lidong zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, vol. 13, No. 6, pages 24-30, November/December 1999.
34. Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 2(3): pages 28-39, May/June 2004.
35. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks". IEEE Journal on Selected Areas in communications. 24(2):370-380, IEEE, February 2006.
36. S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks", Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, California, pages 299–302,2001.
37. Chaudrn, SR. Al-khcoidi, Acasecy, "Performance comparison of wireless multi hop adhoc-networks",WIMOU-2005,IEEE international onference.vol.3, pages 9-16, 2005.
38. S. R. Das, R. Castaneda, and J. Yan, "Simulation-based performance evaluation of routing protocols for mobile ad hoc networks", ACM/Baltzer Mobile Networks and Applications, pages 179–189, 2000.
39. V. C. Patil, Rajashree.V.Biradar, Dr. R. R. Mudholkar, Dr. S. R. Sawant,"Performance Comparison Of Multihop Wireless Mobile Ad Hoc Routing Protocols", Ubiquitous Computing and Communication Journal vol.4, pages696-703, 2009.
40. Smt. Rajashree.V. Biradar & Prof V. C. Patil, "Classification and Comparison of routing Techniques in Wireless Ad-hoc Networks", Proceedings of international Symposium on Ad-hoc Ubiquitous Computing (ISHUC'06), pages 7-11, 2006.
41. G. S. Lauer, "Packet-radio Routing in Communications Networks", (Ed M.teenstrup), pages 313–350, 2004.
42. A. Bokureche, "Performance evaluation of routing protocols for ad hoc wireless networks", ACM Mobile networks application, vol.9, no.4, pages333-342, august- 2004.
43. A. B. McDonald and T. F. Znati, "A mobility-based framework for adaptive clustering in wireless ad hoc networks", IEEE Journal on Selected Areas in Communications, 17(8): pages 1466–1487, August 1999.
44. M. Joa-Ng and I-Tai Lu, "A peer-to-peer zone-based two level Link state routing for mobile ad hoc networks", IEEE Journal on Selected Areas in Communications, 17(8): pages 1415– 425, August 1999.
45. A. Iwata, C. C. Chiang, G. Pei, M. Gerla and T. W. hen, "Scalable routing strategies for ad hoc wireless networks", IEEE Journal on Selected Areas in Communications, 17(8): pages 1369–1379, August 1999.
46. D. A. Maltz, J. Broch, J. Jetcheva and D. B. Johnso, "The effects of ondemand behavior in routing protocols for multihop ireless ad hoc networks", IEEE Journal on Selected Areas in Communications, 17(8): pages 1439–1453, August 1999.
47. M. R. Pearlman, Z. J. Haas, P. Sholander and S. S. Tabrizi, "On the Impact of Alternate Path Routing for Load Balancing in Mobile Ad Hoc Networks", Proceedings of the ACM MobiHoc, pages 3-10, 2000.
48. A. Nasipuri, R. Castaneda, and S. R. Das, "Performance of multipath routing for on-demand protocols in mobile ad hoc networks", Mobile Networks and Applications, vol. 6, pages 339-349, 2001.
49. E. M. Royer and C.K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks", IEEE Persona Communications, 6(2): pages 46–55, April 1999. Zhenqiang Ye, Srikanth V. Krishnamurthy, Satish K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks", University of California, IEEE INFOCOM, vol.1, pages 270-280, 2003.
50. T.W.Chen and M.Gerla, "Global State Routing: A New Routing Scheme for ad hoc Wireless Networks", Proceedings of IEEE ICC'98, Atlanta, GA, pages 171-175, Jun. 1998.

51. Tsu-Wei Chen and Mario Gerla, "Global State Routing: A Routing Schemefor Ad-hoc Wireless Networks", Proceedings of IEEE ICC'98, pages 171-175,1998.
52. S. Murthy and J. J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks", ACM Mobile Networks Applications Journal, Special Issue on Routing in Mobile Communications, 1(2): pages 183–197, November 1996.
53. R. Ramanathan and M. Steenstrup, "Hierarchically-Organized, Multihop Mobile Wireless Networks for Quality-of-Service Support", ACM/Baltzer Mobile Networks and Applications, vol. 3, no. 1, pages 101-119, Jun. 1998.
54. A. Iwata, C.C. Chiang, G. Pei, M. Gerla and T.W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks", JSAC99, IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, pages 1369-1379, August 1999.
55. C. C. Chiang, H.-K Wu, W. Liu, and M. Gerla, "Routing in clustered multihop mobile wireless networks with fading channel", IEEE Singapore International Conference on Networks, pages 197–212, April 1997.
56. V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks", Proceedings of INFOCOM '97, vol. 3, pages 1405–1413, April 1997.
57. J. Raju and J. J. Garcia-Luna-Aceves, " An efficient path selection algorithm on-demand routing using link state hop by hop routing", Submitted to GLOBECOM 2000, vol.1, pages 577-581, December 2000.
58. S.R. Das, C.E. Perkins, and E.M. Royer, "Performance comparison of two ondemand routing protocols for Ad-hoc networks", Nineteenth Annual Joint Conference of the IEEE Computer and Communications, pages 3-12 , 2000 .
59. D. Johnson, D. Maltz and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks (DSR) ", Spriger US, vol.353, pages 151-181, 2004.
60. E.M. Royer and C.K. Toh, "Areview of current routing protocol for ad-hoc mobile wireless networks", IEEE Personal Communication Magazine, pages 46–55, April 1999.
61. Elizabeth Belding Royer, "Routing approaches in mobile Ad-hoc networks",IEEE Press Wiley, New York (2003).
62. D. Johnson, D. Maltz, and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Internet Draft,pages 139–172, 2001.
63. Qing Li, Meiyuan Zhao, Jesse Walker, Yih-Chun Hu, Adrian Perrig, and Wade Trappe, SEAr: "A secure efficient ad hoc on demand routing protocols for wireless networks", Proceedings of the 3rd annual ACM symposium Computer and Communications Security (ASIACCS 2008). ACM, Tokyo Japan, pages 201-204, March 2008.
64. Luo Liu, Laurie Cuthbert, "QoS in Node-Disjoint Routing for Ad Hoc Networks", PE-WASUN'07, Chania, Crete Island, Greece, pages 92-95, October 22, 2007.
65. Xuefei Li and Laurie Cuthbert, "Stable Node-Disjoint Multipath routing with low overhead in Ad Hoc Networks", MASCOTS-2004, pages 184-191, 2004.
66. Xuefei Li and Laurie Cuthbert, "A Reliable Node-Disjoint Multipath Routing with Low Overhead in Wireless Ad hoc Networks", Venezia, Italy MSWiM'04, October 4–6, 2004.
67. AHN Chunsoo SHIN Jitae and HUH Eui-Nam, "Enhanced multipath routing protocol using congestion metric in wireless ad hoc networks", International Conference on Embedded and Ubiquitous Computing, Seoul, COREE, REPUBLIQUE DE (2006), vol. 4096, pages 1089-1097,2006.
68. E. Yanmaz and O.R Tongwz, "Dynamic load balancing and sharing performance of integrated wireless communication", vol.22, no.5, pages 862-872, June 2004.
69. C. R. Lin and J. S. Liu, "QoS routing in ad hoc wireless Networks", IEEE journal on Selected Areas in Communications, 17(8):pages 1426–1438, August 1999.
70. Takeshi Murakami, Masaki Bandai and Twao Sasase, "Split Multi-Path Routing Protocol with Load Balancing Policy(SMR-LB) to Improve TCP Performance in Mobile Ad Hoc Networks", IEICE Tech. Rep., vol. 104, no. 381, CS2004-89, pages 7-12, Oct. 2004.
71. Vincent D. Park and M. Scott Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proceedings of INFOCOM'97, pages 1405–1413, April 1997.
72. Vincent D. Park and M. Scott Corson, "Temporally-Ordered Routing Algorithm (TORA) Version 1: Functional Specification", Internet-Draft, draftietf-manet-tora-spec-01.txt, August 1998.

AUTHOR(S) PROFILE

Dr. G. Samuel Vara Prasada Raju received the M.Tech degree in CSE from Andhra University in 1993. He received PhD degree from Andhra University in 1996. From 1994 to 2003 worked as Asst. Professor in the Dept. of CS&SE in Andhra University College of Engineering. From 2003 onwards worked as Associate Professor and Director of the CS&SE Department for School of Distance Education of Andhra University College of Engineering His research interest includes ecommerce, Network Security, Cryptography and Data Mining. He has more than 20 years experience in Academics and Research

Mr K S R Murthy an Assistant professor of the Department of Information Technology Sreenidhi Institute of science and technology, Hyderabad, A.P, India. He is an active Research Scholar at Andhra University in the areas of Ad hock networks Network Security, Cryptography and Mobile Computing, Data Mining.

