

DVR-BASED MANET ROUTING PROTOCOLS TAXONOMY

Mrinal Kanti Debbarma¹, Santanu Kumar Sen² and Sudipta Roy³

¹Department of Information Technology, Triguna Sen School of Technology, Assam
University, Silchar-788011, India

mkdb06@gmail.com

²Dept. of Computer Science & Engineering
Guru Nanak Institute of Technology, Sodepur, Kolkata-700114

santanu_hello@yahoo.com

³Department of Information Technology, Triguna Sen School of Technology, Assam
University, Silchar-788011, India

sudipta.it@gmail.com

ABSTRACT

In ad hoc network, each node is equipped with a wireless transmitter and receiver (transceiver) that is powered by a battery. Two nodes willing to communicate with each other need to be either in the direct common range of each other or should be helped by other nodes to act as routers forwarding their packets. A node in a Mobile Ad hoc Network (MANET) acts as dual role of a host and a router as well. Designing routing algorithm for MANET is a difficult job compared to designing routing algorithm for wired networks. The important challenges in routing in MANET are due to same intrinsic characteristic of MANET, like limited battery power, highly dynamic nature of network topology, limited bandwidth, asymmetric links, scalability, mobility of nodes etc. In this paper, we analyzed DVR based routing protocols aiming to find suitable path through special neighbours between hops in MANET. This paper classified various routing protocols based on DVR for MANET and compared on the characteristics (routing metrics), performance and complexity.

KEYWORDS

DVR based routing protocols, Proactive routing protocols, Reactive routing protocols, Special neighbor, Neighbours Notification

1. INTRODUCTION

Mobile ad hoc network (MANET) is a form of wireless ad hoc network, and is a self-configuring network of mobile devices connected by any quantity of wireless links. One of the major fundamental problems in mobile ad hoc networks is routing. An ad hoc network is a peer-to-peer mobile network consisting of large number of mobile nodes MANET is different from the classic networks in the character such as node mobility, limited bandwidth and the frequent change of the network topology. It is IP based, nodes have to be configured with a free IP address to receive unicast message. Every device in a MANET is also a router because it is required to forward traffic unrelated to its own use. Each MANET device is free to move independently, in any arbitrary direction, and thus each device will potentially change its links to other devices on a regular basis. The main challenge to setup a MANET is that each device has to maintain the information required to route traffic properly. Ad hoc network is used because it is easy and fast to deploy, and less dependent on infrastructure to overcome the hectic and error prone manual intervention of the network manager. Designing a routing protocol for MANET has several difficulties. Firstly, MANET has a dynamically changing topology as the nodes are mobile. This behaviour favours routing protocols that dynamically discover routes (e.g. Dynamic Source Routing [1], TORA [2], Associativity Based Routing (ABR) [3] etc.) over conventional distance vector routing protocols (DVR) [2]. Secondly, the fact that MANET lacks

any structure and thus makes IP subnetting inefficient. Thirdly, limitation of battery power and power depletion of nodes due to large no of message passed during cluster formation. Links in mobile networks could be asymmetric at times. If a routing protocol relies only on bi-directional links, the size and connectivity of the network may be severely limited; in other words, a protocol that makes use of unidirectional links can significantly reduce network partitions and improve routing performance.

1.1 MANET applications and Challenges:

The primary application of the MANET is in battle field, disaster recovery, reuse operation, natural calamity, fast traffic information delivery on highways, network extension, local interconnection network, ubiquitous computing, sensor network, urban sensing, vehicular networking, home and enterprise networking, Wireless Local Area Network (WLAN), Private Area Network (PAN), health monitoring, tracking application, monitoring the aquatic environment, localization application, law enforcement, emergency service, educational application, conference/meeting/lectures, wildlife monitoring, intelligent home applications, urban areas, ubiquitous Internet access, delivery of location-wise information/service, entertainment, multiuser games, robotic pets and etc. However, a slight variation, namely wireless sensor networks (WSN) [4], Vehicle Ad hoc Networks (VANET) which are ad hoc in nature, do possess wide applicability in the modern electronics world. Routing in such ad hoc networks possess a vital role in transmission of messages for what they are intended to. Routing is the heart of a network and optimality and reliability are the keen requirements for the success of such a routing protocol.

The important challenges in routing in MANETs are due to same intrinsic characteristic of MANETs, like limited battery power, highly dynamic nature of network topology, limited bandwidth, asymmetric links, scalability, mobility of nodes etc.

Recent challenges for ad hoc wireless networks comprise:

- Multicast [5]
- QoS support
- Power-aware routing [6]
- Location-aided routing [7]

Multicast is appropriate to support cooperative /multiparty wireless communications. The multicast tree is highly dynamic in nature (i.e., its topology is subject to change over time), the multicast routing protocol must be able to handle with mobility, including multicast membership dynamics (e.g., join and leave). In case of QoS, it is insufficient to consider QoS simply at the network level without considering the underlying MAC layer [8]. Again, as nodes are dynamic in nature, the problems associated with the hidden station, and inconsistent link characteristics, supporting end-to-end QoS is a nontrivial issue that involves in-depth analysis and research. In recent years, there is a trend toward an adaptive QoS approach as a substitute of the “plain” resource reservation method with hard QoS guarantees. An additional important factor is the limited power source in handheld nodes, which can seriously forbid packet forwarding in an ad hoc mobile environment. Therefore, routing traffic based on nodes’ power metrics is one way to differentiate routes that are more prolonged than others. Finally, as a substitute of using beacon or broadcast search Location-Aided Routing (LAR) uses positioning information to define associated regions at the routing is spatially concerned with. This is comparable to associativity-oriented and restricted broadcast in Associativity Based Routing (ABR).

2. BACKGROUND DETAILS

The conventional routing protocols, though simple and easier to implement, face some problems in MANETs due to highly dynamic nature of the nodes and limited bandwidth available for communication. Many routing protocols, based on different conventional routing protocols, have been proposed for MANET so far, each one claiming to offer some advantages over the other. But, in general, there are some common desirable properties that any routing protocol for an ad hoc network should possess. These are as follows:

- **Loop free:** Presence of loops in the path from the source to the destination result in to inefficient routing. In the worst-case situation, the packets may keep traversing the loop indefinitely and never reach their destination.
- **Distributed control:** In a centralized routing scheme, one node stores all the topological information and makes all routing decisions; therefore, it is neither robust, nor scalable.
- **Minimal control overhead:** The routing protocols should not unnecessarily transmit the control packet; which reduces the power of the batteries in the nodes, leading to shorten the life of network.
- **Unidirectional link support:** Unidirectional links vary frequently in ad hoc networks creating misunderstandings between the nodes about the reachability between them and leads to packet drops.
- **Localized reaction to topological changes:** Topological changes in one part of the network should lead to minimal changes in routing strategy in other distant parts of the network. This will keep the routing update overheads in check and make the algorithm scalable.
- **Multiplicity of routes:** Even if node mobility results in disruption of some routes, other routes should be available for packet delivery.
- **Power efficient:** A routing protocol should be power efficient. That is, the protocol should distribute the load; otherwise shut-off nodes may cause partitioned topologies that may result in inaccessible routes.
- **Secure:** A routing protocol should be secured. We need authentication for communicating nodes, non-repudiation and encryption for private networking to avoid routing deceptions.
- **QoS aware:** A routing protocol should also be aware of Quality of Service. It should know about the delay and throughput for a source destination pair, and must be able to verify its longevity so that a real-time application may rely on it.

2.1. MANET Routing Protocols: Taxonomy

A large number of different routing protocols for MANETs are either in use or have been suggested in the literature. Figure 1, below shows the names of many of them. These routing protocols can be classified on the basis of, what routing information is exchanged; when and how the routing information is exchanged, when and how routes are computed and so on. Some classifications are as follows:

- (a) Link state routing vs. distance vector routing
- (b) Pre-computed routing vs. on-demand routing
- (c) Periodical update vs. event-driven update
- (d) Flat structure vs. hierarchical structure
- (e) Decentralized computation vs. distributed computation
- (f) Source routing vs. hop-by-hop routing
- (g) Single path vs. multiple paths
- (h) Isolated routing vs. Distributed routing

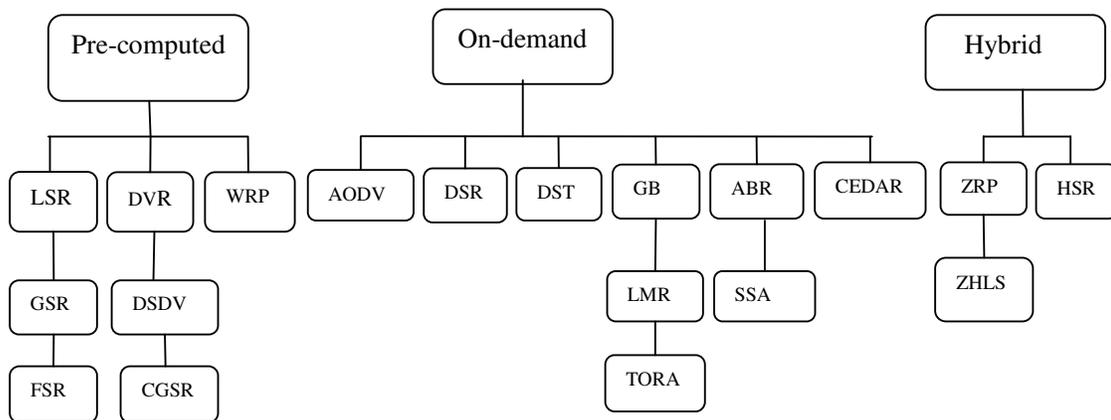


Figure 1: MANET routing protocols classification based on design strategy

(a) **Link state routing (LSR) vs. distance vector routing (DVR)**

In Link state routing (LSR), routing information is flooded in the network by each router, in the form of link vectors. Any link change is flooded by the concerned routers into the entire network immediately. Every node can construct and maintain a global network topology when it receives this link vector from every other router and computes the length of its shortest path to each destination and stores this information - its routing table along with the identity of the neighbour which provides the first path in the shortest path. LSR leads to very high control overhead because the ideology of the Ad-Hoc Networks is very dynamic and every change in the link takes a flood in the network.

In DVR [2], every node periodically exchanges distance vectors, containing its shortest path to every router in the network with its neighbors. When a node receives distance vectors from all its neighbors, it computes new routes (current shortest path) to every router and updates its distance vector. Every node reaches a remote destination via a neighbour who is acting as a forwarding node for that destination in its routing table. The problems with DVR are slow convergence in case of link faults in the tendency of creating routing loops.

(b) **Pre-computed routing vs. on-demand routing (Proactive vs. Reactive)**

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. In this approach, the routes to all destinations are computed a priori. In order to compute routes in advance, nodes need to store the entire or partial information about link states and network topology. In order to keep the information up to date, nodes need to update their information periodically or whenever the link state or network topology changes. The advantage of pre-computed routing is that when a source needs to send packets to a destination, the route is already available, i.e. there is no route discovery delay. The disadvantage is that some routes may never be used, although the dissemination of routing information consumes a lot of the scarce wireless network bandwidth and node battery power when the link state and network topology change fast (this is especially true in a wireless ad hoc network). The conventional LSR and DVR are examples of proactive routing.

On-demand routing is also called reactive routing. In this method, the route to a destination may not exist in the routing table in advance and it is computed only when the route is needed.

Route discovery: When a source needs to send packets to a destination, it first finds a route or several routes to the destination. This process is called route discovery.

Route maintenance: After the route is discovered, the source transmits packets along the route. During the transmission of packets, the route may be broken because the node on the route move away or go down. The broken route needs to be rebuilt. The process of detecting route breakage and rebuilding the route is called route maintenance. The major advantage of on-demand routing is that the precious bandwidth of wireless ad hoc networks is greatly saved because it limits the amount of bandwidth consumed in exchange of routing information by maintaining routes to only those destinations to which the routers need to forward data. On-demand routing removes the need for disseminating routing information periodically. The primary problem with on-demand routing is the large latency at the beginning of the transmission caused by route discovery.

Finally, the hybrid protocols try to combine the both Proactive and Reactive protocols and also take advantage of the recent availability at low cost of the Global Positioning System (GPS), for achieving improved performance through location dependent routing. Most of the proposed hybrid routing protocols for MANET are Zone-based routing protocol i.e., network is partitioned into various zones by each node and other group node are partitioned into clusters or trees.

(c) **Periodical update vs. event-driven update**

Periodical update protocols disseminate routing information periodically. Periodical updates will simplify protocols and 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 will be disseminated which would waste the precious bandwidth of a wireless network.

In an event-driven update protocol, when events occur (such as when a link 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 up a lot of precious bandwidth, and furthermore, may cause too much fluctuation of routes. One solution is to use some threshold.

Periodical update and event-driven update mechanisms can be used together, forming what is called a hybrid update mechanism. For example, in DSDV, a node broadcasts its distance-vector periodically. Moreover, whenever a node finds that a link is broken, it distributes a message immediately.

(d) **Flat structure vs. hierarchical structure**

In a flat structure, all nodes in a network are at the same level and have the 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. In hierarchical routing, the nodes in the network are dynamically, organized into partitions called clusters, then the clusters are aggregated again into larger partitions called

super-clusters and so on. Organizing a network into clusters 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. Within a cluster, the nodes may have complete topology information about is 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. 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 and interference can be reduced when using different spreading codes across clusters.

(e) Decentralized computation vs. 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.

(f) Source routing vs. hop-by-hop routing

Some routing protocols place the entire route (i.e., nodes in the route) in the Traders of data packets so that the intermediate nodes simply forward these packets according to the specified 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, sauce 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 and neighbor detection packets required in other kinds of protocols. The biggest 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 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 for 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.

(g) Single path vs. multiple paths

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 thus making routing algorithm reliable and robust. Moreover, the source can not only select the best one among multiple available routes, but also distribute the load among them thus presenting possible congestion in the network.

The routing technique of using multiple predetermined routes between two routers is called static multipath routing. In many networks, several paths exist between each pair of routers and some of these paths may be almost equally good. Under such circumstances, choice of multiple

paths, instead of a single path (usually, the shortest), offers two important advantages. First, delay performance of the network is improved by distributing the whole traffic among different paths as this reduces the load on each of the communication lines. Second, and more important, reliability of the network is considerably improved because of the availability one or more alternative routes to each destination. Static multipath routing is probably the only static routing that is used in practice.

(h) Isolated routing vs. Distributed routing

Isolated routing is the simplest form of dynamic routing in which routing decisions are independently taken by each router, based solely on its own information; i.e., the router does not exchange routing information with either other routers or with an RCC, but tries to adapt to changes in topology and traffic, totally by itself.

Distributed Routing adapts a compromise between the two extreme approaches adapted by the centralized routing (a fully global but centralized approach) and isolated routing (a purely local approach) by sharing the knowledge about the network gained by other routers. This makes Distributed Routing perform much better than the other two dynamic routing algorithms and, as a result, most of today's routing algorithms are distributed in nature.

2.2 Mostly used Routing Algorithms

Broadly, the routing algorithm in MANET has been classified into three categories, viz. proactive or table-driven, reactive or on-demand and the hybrid. The dominant algorithm used in the wired network are proactive in nature but some of the features of a MANET make a reactive approach perform better under many situations. Because of this observation, hybrid approach is gaining in importance.

In this section, most popular routing protocols for MANETs which are primarily based on proactive / reactive approach. The first one is most well-known proactive protocol, the other two are reactive in nature and, additionally one of the reactive protocols employ source routing for MANET.

2.2.1. Table-driven or Proactive protocols

Proactive or table-driven protocols are based on one of the old techniques of routing. These protocols maintain route to all the nodes present in the network, all the time. To ensure the freshness of the routing tables, these protocols adopt different mechanisms, e.g., sending the "hello" messages containing the address of transmitting node, at regular intervals. Some of the popular table-driven routing protocols (proactive) for MANETs are listed below:

- (a) Destination Sequence Distance Vector routing protocol (DSDV)
- (b) Wireless Routing Protocol (WRP)
- (c) Cluster-head Gateway Switch Routing (CGSR)
- (d) Optimized Link State Routing Protocol (OLSR)
- (e) Fisheye State Routing protocol (FSR)
- (f) Global State Routing protocol (GSR)
- (g) Topology Broadcast based on Reverse-Path Forwarding routing protocol (TBRBF)

(a) The Destination Sequence Distance Vector (DSDV)

DSDV [9] is the most well-known pro-active routing scheme. It is based on the classical Distributed Asynchronous Bellman Ford (DBF) routing algorithm which has long been used in for wired networks. DSDV is a table driven routing algorithm and maintains routing tables containing route for each station present in the network.

DSDV uses the sequence number to keep the route fresh and to avoid the Loop. Each entry in the routing table must contain, destination id, destination number, the next hop for this destination. The sequence number is with each node, which increases monotonically. The information with sequence number is treated as fresh information.

The nodes exchange routing updates whenever they detect a change in topology. Two types of updates are used in DSDV, namely, full dumped and incremental update. In case of full updates, the complete routing table is sent out and in case of an incremental or partial updates only the changes since full dump are out. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dumps are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent.

DSDV is well suited for the less dynamic and small networks. When the mobility increases the packet delivery ratio decreases very rapidly.

(b) Wireless Routing Protocol (WRP)

The WRP protocol [10] also guarantees loops freedom and it avoids temporary routing loops by using the predecessor information. However, four routing tables is required in each node in WRP protocol. This presents a significant amount of memory overhead at every node as the network size increases. Another disadvantage of WRP is that it ensures connectivity through the use of hello message.

(c) Cluster-head Gateway Switch Routing (CGSR)

A cluster-based routing protocol is the most popular hierarchical routing strategy. It uses a particular clustering algorithm for election of cluster head in which mobile nodes are grouped into clusters by geographic vicinity. Cluster heads look into all responsibility on behalf of the cluster for membership management and routing functions. Cluster head Gateway Switch Routing (CGSR) [11] is an example of a cluster-based MANET routing protocol. The Hierarchical State Routing (HSR) protocol [12] also supports a multi-level cluster arrangement. The CGSR protocol differs from the previous protocol in the type of addressing and network group structure employed. Instead of a “flat” network, CGSR is based on a clustered multihop mobile wireless network with several heuristic routing structures.

(d) Optimized Link State Routing Protocol (OLSR)

OLSR [13] is a point-to-point routing protocol based on the traditional LSR algorithm. In this scheme, every node maintains topology information about the network periodically replacing link-state messages. The originality of OLSR is that it minimizes the size of each control message and the number of rebroadcasting nodes during each route update by employing multipoint replaying (MPR) approach. During each topology update, each node in the particular network selects a set of intermediate/neighbouring nodes to retransmit/forward its own packets. This set of nodes is termed the multipoint relays of that node. Any node which is not in the set can read and process each packet but do not retransmit. To select the MPRs, each node periodically broadcasts a list of its one hop neighbours using hello messages from the list of nodes in the network.

(e) Fisheye State Routing protocol (FSR)

FSR [14] decreases the size of the update messages in GSR by updating the network information neighbour nodes at a higher frequency than for the isolated nodes, which lie outside the fisheye scope. This makes FSR more scalable to dense networks than the protocols described. However, scalability originates at the price of reduced accuracy. This is because as mobility grows the routes to remote destination become less accurate. This can be overcome by making the frequency at which updates are sent to remote destinations proportionate to the level of mobility.

(f) Global State Routing protocol (GSR)

The GSR protocol [15] is based on the traditional LSR algorithm. However, GSR has upgraded the way information is disseminated in LSR algorithm by restricting the update messages between intermediate nodes. In GSR, every node maintains a link state table (LST) based on the up-to-date information received from neighbouring nodes, and periodically interchanges its link state information with neighbouring nodes. However, the size of update messages is relatively dense, and as the size of the network increases they will get even larger. Therefore, a substantial amount of bandwidth is consumed by these update messages.

(g) Topology Broadcast based on Reverse-Path Forwarding routing protocol (TBRPF)

TBRPF [5] protocols is based on link-state based routing protocol, which implements hop-by-hop routing scheme. Reverse-path forwarding (RPF) is used to propagate its update packets information in the opposite direction along the spanning tree, which is made up of the minimum-hop path from the nodes leading to the source of the update message. In this routing approach, every node computes a source tree, by providing a path to all reachable destinations by applying a modified version of Dijkstra's algorithm (MDA) on the partial topology information stored in their topology table. In TBRPF, every node minimizes overhead by reporting only part of their source tree to their neighbours not all the nodes. The reportable part of each source tree is interchanged with neighbouring nodes periodically along with hello messages.

2.2.2. On-demand or Reactive routing protocols

The reactive routing protocols discover the route(s) to destination(s) only when it is needed. When a node requires a route to destination, it initiates route discovery process within the network. After getting some routes to the destination, the best among them is selected and used for forwarding the packets to the destination. Once a route is discovered, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or the route is no longer desired. Below is the list of some Reactive ad-hoc routing protocols.

- (a) Ant-based Routing Algorithm for Mobile Ad-Hoc Networks (ARA).
- (b) Associativity-Based Routing protocol (ABR)
- (c) Ad hoc On Demand Distance Vector routing protocol (AODV)
- (d) Dynamic Source Routing protocol (DSR)

(a) Ant-based Routing Algorithm for Mobile Ad-Hoc Networks (ARA).

This protocol is based on swarm intelligence and ant colony based Meta heuristic search. ARA [16] for ad hoc network attempt to reduce routing overheads by adopting the food searching techniques (FST) of ants. During ants search for food they start from their nest and walk in the direction of the food, while leaving behind a transient trail called pheromone. This directed the path that has been taken by the ant and allows rests to follow, until the pheromone disappears. Similar to AODV and DSR, ARA is also made up of two phases:

- Route discovery
- Route maintenance

Route discovery:

During route discovery forwarding ANT (FANT) is broadcast through the network (like a RREQ). At each hop, each node calculates total pheromone value depending on how many number of hops the FANT has taken to reach them. The nodes then forward the FANT to their neighbours. Once the destination is reached, it creates a Backward ANT (BANT), and returns it

to the source. When the source receives the BANT from the destination node, a path is determined and data packet propagation begins.

Route maintenance: For maintaining each route, each time a data packet travels between forwarding nodes the pheromone value is increased. Otherwise the pheromone value is decreased overtime until it expires. Making a broken link, the nodes check their routing table, if no route is found they inform their intermediate neighbours for a substitute route. If the neighbours do have a route they inform their neighbours by backtracking. If the source node is reached and no route is found, a new route discovery process is initiated.

Advantages: The advantage of these techniques is that the size of each FANT and BANT is tiny, which means the amount of overhead per control packet introduced in the network is minimized. However, flooding is used for route discovery, which means that the protocol may have scalability problems as the number of nodes and flows in the network grows.

(b) Associativity-Based Routing protocol (ABR)

ABR [17] protocol defines a new type of routing metric “degree of association stability” for MANETs. In this routing protocol, a selection of route is based on the degree of association stability of mobile nodes. Each node periodically generates beacon to broadcast its presence. Upon receiving the beacon message, a neighbor node updates its own associativity table. For each beacon received, the associativity tick of the receiving node with the beaconing node is increased. A high value of associativity tick for any particular beaconing node means that the node is relatively static. When any neighboring node moves out of the neighborhood then associativity tick is reset.

(c) Ad hoc On-Demand Distance Vector Routing Protocol (AODV)

Ad hoc On-Demand Distance Vector Routing Protocol (AODV) [18] is another reactive routing protocol, uses sequence number to avoid looping and maintains fresh routes to the destinations. This algorithm also consists of two phases, route discovery route maintenance.

Route discovery: If the route to the destination is not available in the routing table, a RREQ (Route Request) packet is broadcast throughout the MANET with a search ring technique. When a node receives this RREQ, the node creates a reverse routing entry towards the originator of RREQ, which is used to forward replies later. The destination or the intermediate node, which has a valid route towards the destination, answers with a RREP (Route Reply) unicast packet. On receipt of the RREP the reverse routing entry towards the originator of RREP is also created, the processing of RREQ. A precursor list is maintained to notify upstreams about the link failure of the downstream neighbour for a particular destination.

Route maintenance: Every node along an active route periodically broadcasts messages to its neighbours. If the node does not receive a HELLO message or data packet from a neighbour for a while, the link between itself and the neighbour is to be broken. RERR (Route Error) packet is sent to the neighbours in the list associated with the routing entry to inform them of the link failure. AODV gives all round good performance in small and medium size networks.

It is interesting to note that most of the successful and popular routing protocols like DSDV, AODV, ADV etc. used in MANETs are based on the fundamental principle of distance vector routing (DVR), which in turn, derived from the well-known Distributed Asynchronous Bellman Ford Algorithm (DABFA).

(d) Dynamic Source Routing Protocol (DSR)

DSR is a source routing protocol and behaves in a reactive manner for discovering the route to a destination. It does not maintain the routing table like other routing protocols. DSR has a route cache, where complete path (list of all intermediate nodes) to the destination is kept. The basic procedure of DSR is divided two phases:

Route discovery: If the source route entry towards a destination is not present in the route cache, a Route Request packet is broadcast throughout the MANET. Every receiving node, if it has the route to the requested destination, adds its id in the list in the request packet's header. When the destination receives the packet, it also discovers the route to reach the source in the similar way.

Route maintenance: Unlike the proactive routing protocols and the AODV, no HELLO message is sent in the DSR. Every node along the path is responsible for checking the validity of the downstream link connecting itself and the next hop in the source route, which could be detected by its MAC layer. If link breakage is found, the source of the route will be notified with a Route Error packet. The source then re-initiates a route discovery procedure.

Route cache is very helpful in reducing the control overhead in DSR. Gratuitous reply, multi-paths and packet salvaging are the features which takes help from cache. During route discovery phase, if the intermediate node has the route towards the destination in its routing cache, it can answer with a route reply packet and send a gratuitous route reply about the source to the destination at the same time. Multiple paths are available by the route discovery process. When an intermediate node detects the downstream link breakage when forwarding a data packet, but it has another source route in its routing cache towards the same destination, it forwards the packet along the new route, which is called packet salvaging. DSR is suited for the small to medium size networks, where the number of nodes is up to 200. Control overhead increases with the increase in number of nodes in between the source and destination, because it contains the full path in the packet.

Protocols	Route/Method Computation	Structure	Number of Paths	Update period	Stored Information
LSR	Proactive/Flooding (itself)	Flat	Single or multiple	Hybrid	Entire topology
DVR	Proactive/distributed/Broadcast	Flat	Single	Periodical	Distance-vector
DSDV	Proactive/ Broadcast	Flat	Single	Hybrid	Distance-vector
WRP	Proactive/ Broadcast	Flat	Single	Hybrid	Distance/routing/link-cost tables, MRL
CGSR	Proactive/ Broadcast	Heirarchy	Single	Periodical	Cluster member table, Distance Vector
OLSR	Proactive/ Flooding	Heirarchy	Single	Periodical	Neighbour, Topology, Routing tables
GSR	Proactive/ Broadcast	Flat	Single or multiple	Periodical	Entire topology
FSR	Proactive/ Broadcast	Heirarchy	Single or multiple	Periodicals	Entire topology
TBRBF	Proactive/ Broadcast	Flat	Single but may multiple	Event-driven	Neighbour/Topology/Routing table
ARA	Reactive/on-demand/Flooding	Heirarchy	multiple	Event-driven	Alternate route/backtrack/neighbour
ABR	Reactive/ Broadcast	Heirarchy	Single	Periodicals	Strongest associativity/routing table/neighbor
AODV	Reactive/ Unicast	Flat	multiple	Event-driven	Next hop for desired destination
DSR	Reactive/ Unicast	Flat	multiple	Event-driven	Full path (From source to Destination)
ZRP	Proactive/ Reactive(hybrid)/ Broadcast	Flat	Single or multiple	Periodical	Local (within zone), topology
ZHLS	Proactive/ Reactive(hybrid)/ Broadcast	Heirarchy	Single/multiple	Periodical /Event-driven	Location request/shortest path
HSR	Proactive/ Reactive(hybrid)	Heirarchy	Single or multiple	Periodical	Routing tables

Table 2: Comparison of MANET Routing Protocols

2.3. DVR based Routing protocols in MANETs

DVR is a simple, elegant and widely used as the Internet Gateway Protocol (IGP) and Extended Gateway Protocol (EGP) [3] in the Global Internet as well as in the private Internets in the form of Routing Information Protocol (RIP)[2,3], RIP-2 and Boarder Gateway Protocol (BGP)[2,3]. The Distance Vector Routing Algorithm (DVRA) is a dynamic, distributed, asynchronous and iterative routing protocol where the routing tables are continuously updated with the information received from the neighbouring routers [2], [19].

As a distributed dynamic routing algorithm which is expected to adapt to changes in topology and traffic. The existing DVRA, though simple and conceptually elegant, suffers from some well-known problems like Count-to-Infirmity (CTI), slow convenience, looping, frequent route oscillation. Out of all these, the CTI is more vulnerable, which actually, made practical DVR out of race.

Though good amount of research has been done in the past towards the improvement of the basic DVRA [20], none of the proposed techniques like Hold-Down, Split Horizon and Poison Reverse have been able to satisfactory solve the problems in the DVRA.

DVRA is used in routing protocols similar to IGRP [20], ISO and Novell IPX due to its simplicity, elegance and flexibility.

We have investigated a modified DVRA (MDVRA), which uses a host of novel techniques to remove all the weaknesses, particularly the CTIP, inherent to the existing DVRA. Additionally, the goal is to augment the existing capabilities of the DVRA so as to make it efficient, robust, fully dynamic and fully fit to the environment of the MANET primarily and WSN in the extended phase.

2.3.1. Weakness of DVRA

There are some weaknesses of the asynchronous DVRA are as follows:

- Count-To-Infinity (CTI) Problem
- Slow Convergence Problem
- Oscillation Problem

2.3.1a. Count-To-Infinity (CTI) Problem

The DVRA cannot perform fine if there are topological changes in the internetwork. DVRA suffers from CTI problem due to link or router failure or due to unending routing loops. The CTI caused by routing loops involving more than two routers are providing in [21].

2.3.1b Slow Convergence Problem

When there is growth in terms of cost of any link or there is a failure in the link between two corresponding neighboring nodes in an internetwork, then it considered as worst case or requires unnecessary number of iterations to terminate.

2.3.1 c Oscillation Problem

Besides CTI and slow convergence the another important problem of the DVR or compatible shortest path routing protocols is that because of the need to always use the shortest path, there may be frequent switching of routes caused by even small increase or decrease in the link costs. This frequent route switching gives rise to instability in routing and this problem is known as the route oscillation problem [18]. If two paths to a destination have delays which are marginally different, then the choice of the lower delay path as the shortest path invites more traffic on this path so that it ceases to be the shortest path in no time and, as a result, the other

path becomes shorter than this path. As a consequence, more traffic now flows through the second path, thus increasing its delay and makes it lose the status of the shortest path to the original shortest path. The route oscillation problem degrades overall performance of a network and hence some mechanism is needed to dampen the oscillation, i.e., to reduce the frequency of route switching. It should be noted in this context that if hop count is used as the metric in the DVR, then the route oscillation problem does not arise at all because the traffic changes which cause changes in the link delays are ignored.

2.4 Key modification of MDVRA

There are some key modification ideas from the MDVRA [7] [8] have been developed in the design of the MDVRMANET. How these special neighbours are identified, primarily by using the DVRTs and how they are used towards making the MDVRA efficient and practical routing algorithm with fast convergence and no CTI problem. The first essential modification requires that each entry in the DV Tables (DVT), periodically exchanged between the neighbours in a DVRA, should include the next-hop identity for the route. This information is not included in the DVTs in the DVRA but is contained in every router's own DVR Table (DVRT). The second modification requires a router to perform in a more intelligent and proactive manner in trying to determine the alternative shortest path following a link failure. Final modification requires each router to identify some of its neighbours as special neighbours and use them for avoiding routing loops and/or achieving a very reliable and efficient node-to-node communication. The concept of the special neighbours and the benefits a node derives from each of them.

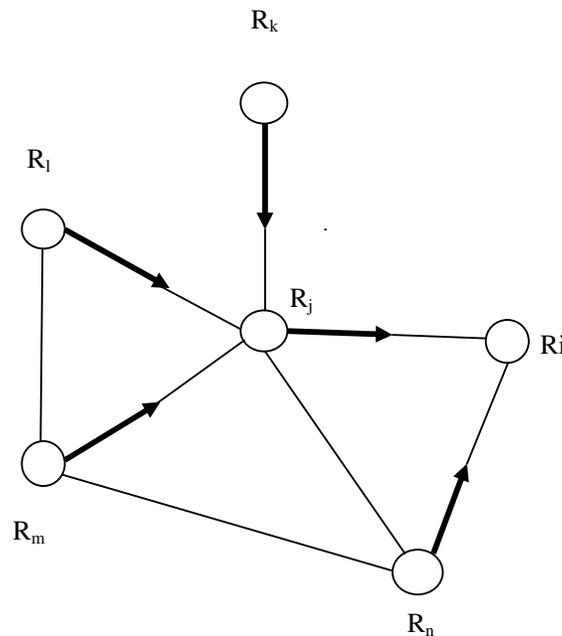


Figure 2: An Example network graph for illustrating concepts of some special neighbours.

(a) **Forwarding Neighbour (FN):** If a router R_j presently reaches a non-neighbour or remote destination R_i via its neighbour R_k (because R_k provides R_j with the current shortest path to reach R_i), then R_k is the FN of R_j for reaching R_i . In Figure 2, R_j is the FN of R_k , R_i and R_m (but not of R_n) for reaching R_i . In the MDVRA, we make an explicit distinction between a NH neighbour and a FN. Since a neighbour is always reached directly, i.e., never via another neighbour, each neighbour in the MDVRA is always its NH neighbour. But a neighbour is a FN only when it is used to forward packets to a remote or non-neighbour destination. Thus, in the

MDVRA, all neighbours are the NH neighbours for reaching themselves but all of them may not be FNs.

(b) **Dependent Neighbour (DN):** If a router R_k presently reaches a destination R_i via its neighbour R_j , i.e., if R_k depends on R_j for reaching R_i , then R_k is a Dependent Neighbour (DN) of R_j for reaching R_i . The routers R_k , R_l , and R_m , but not R_n , in Figure 2 are all DNs of R_j for reaching the destination R_i . Awareness about its DN(s) for each destination is extremely important to the router y because of two reasons. First, a DN x can never provide it with a shorter path to reach z so that the advertisements of the DN x for the destination z should just be ignored. Second, if y ever loses its present path (route) to z and looks for the shortest path to reach z , choosing the DN x as the next-hop must be avoided because that will create a routing loop between x and y .

(c) **Co-Neighbour (CN):** If three routers R_j , R_k and R_l , form a triangle in a network graph, then any two of the three routers are mutual CNs of each other for the third one, e.g., in Figure 2, R_k is a CN of R_j for R_l , R_l is a CN of R_j for R_k , R_j is a CN of R_k for R_l , and so on. Again for the router R_j , R_k has no CN, R_l has one CN, namely, R_m , R_m has two CNs, namely, R_l and R_n , R_n has two CNs, namely, R_m and R_l and, finally, R_l has one CN, namely, R_n .

(d) **Co-Dependent Neighbour (CDN):** If routers R_k and R_l are CNs of each other (i.e. mutual CNs) for the router R_j and, additionally, both R_k and R_l are also DNs of R_j for reaching a common destination R_i , i.e., R_j is their common FN for reaching R_i , then R_k and R_l are CDNs of R_j for the destination R_i . In accordance with the arrows shown in Figure 2, R_l and R_m are CDNs of R_j for reaching R_i . Incidentally, it may be noted that R_n would also have become, along with R_l and R_m , a CDN of R_j for reaching R_i , had the link R_n, R_i been absent.

(e) **Single-Connected Neighbour (SCN), Pendant Neighbour (PN), Sole Neighbour (SN) and Lost Destination (LD):** If y is the only neighbour of x , then y is the SN of x and x is a PN of y . A node in the network graph having a degree 1, i.e., a router which is connected only to a single router, is called a Single-Connected Neighbour (SCN) of the sole router to which it is connected. The sole router recognizes its SCN as a Pendant Node (PN) in the network. The router R_k in Figure 2 is a SCN of R_j and a PN in the network graph. It is obvious that a PN can only be a DN but never a FN. In case a SN loses communication with its PN, it views the PN as a LD, does not look for an alternative route to reach it (till its direct communication with the PN is re-established) and informs all other neighbours about this LD having become unreachable. This ensures that no more packets is generated for or forwarded to the LD by any router.

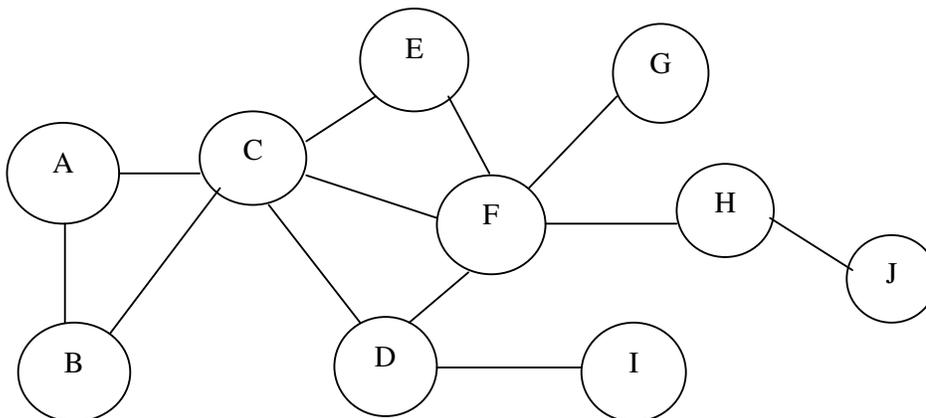


Figure: 3. A Sample Network to be used in discussing the special neighbours of router F

A DVRT has N entries one corresponding to each known router in the N-node network. Each entry has 3 fields, namely, the identity of a destination router, the estimated distance (metric) of this router and, finally, the identity of the next-hop (NH) router, i.e., the FN in case of any remote router, for reaching that destination. In this paper we shall normally consider delay as the metric since the MDVRA is expected to be fully adaptive, i.e., adaptive in respect of both topology and traffic. The short-form notations $DEST_i$, $DIST_i$ and NH_i will represent the values in the three fields of the i-th entry, $i=1, 2, 3, \dots, N$ in the DVRT of each router. The DVRT of the router R_j will be denoted by $DVRT_F$. It should be reiterated that the NH_i field will identify either the destination itself or the FN, depending upon the $DEST_i$ being a neighbour or a non-neighbour.

DEST	DIST	NH
C	D_{FC}	C
E	D_{FE}	E
G	D_{FG}	G
D	D_{FD}	D
H	D_{FH}	H
I	D_{FI}	D
A	D_{FA}	C
B	D_{FB}	C
J	D_{FJ}	H

Table 1: Routing Table of Router F ($DVRT_F$)

Notations used in example sample network graph, routing table are **DEST**: Destination, **DIST**: Distance, **NH**: Next-hop router, D_{FC} : distance between neighbor R_F and destination R_C , **FN**: Forwarding Neighbour, **CN**: Co-Neighbour, **CDN**: Co-Dependent Neighbour, **SCN**: Single Connected Neighbour, **PN**: Pendant Node, **LD**: Lost Destination, $DVRT_F$: Distance Vector Routing Table of node F, **NBbr**: Neighbour, N: Total no. of router entries in $DVRT_F$ i.e., total no. of nodes in the network, N_F : Total no. of neighbours of F, **NT_F**: Neighbouring Table of node F.

In order to build and update its DVRT and the DVT, each router employs the Distributed Asynchronous Bellman-ford Algorithm (DABFA) [22]. In the DABFA, a node R_j contained within a N-node weighted graph, having time varying weights, indefinitely executes the iteration given in Equation 1 for determining its current shortest distance D_{ji} to node R_i .

$$D_{ji} = \text{mid}[d_{jk} + D_{ki}] \quad \forall (R_j, R_i, R_k) \in S_N, i \neq j; \quad \forall R_k \in S_{nj}; \dots \dots \dots 1(a);$$

$$D_{jj}=0 \quad \forall R_j \in S_N; \quad \dots \dots \dots 1(b);$$

Where S_N and S_{nj} are, respectively, the set of all nodes in the network and the set of all neighbouring nodes of R_j , d_{jk} is the current distance of R_j to its neighbour R_k and D_{ki} is the distance of R_k to a remote (i.e., non-neighbour) destination R_i that was last reported by R_k to R_j . R_j executes the iteration in Equation 1 during all updates Periodic Update (PU) and triggered update (TU) and, accordingly, modifies its DVRT $DVRT_j$ and the DVT DVT_j , the entry in the $DVRT_j$ and the DVT_j , corresponding to destination R_i , is (R_i, R_i, D_{ji}) and (R_i, D_{ji}) respectively, if the current shortest path from R_j to R_i is via the neighbour R_i , i.e., if

$$D_{ji} = D_{ji/l} = d_{jl} + D_{li} \quad \forall (R_j, R_l, R_k, R_i) \in SN; \quad \forall (R_l, R_k) \in S_{nj}; \dots\dots\dots 2(a);$$

and $D_{ji/l} \leq D_{ji/k}, k \neq l \dots\dots\dots 2(b);$

where the notation $D_{ji/l}$ denotes the distance of R_j to R_i via neighbour R_l .

NBr	SCN	FN	CN	DN	CDN	PN
C	0	A,B	E,D	A,B	A,B	0
E	0	C	C	C	0	0
G	1	0	0	0	0	F
D	0	C	C	C	0	0
H	0	F	0	F	0	0

Table 2: Neighbour Table of Router F (NT_F)

For example, In Figure 3, router F creates its own neighbour-related tables like Neighbour Table (NT_F), for keeping track and utilizing its special neighbours (SCN, FN, CN, CDN, DN, SN, PN) i.e $DVRT_F$ as shown in Table 1 and in Table 2.

2.5 Identification and Use of the Neighbourhood

A router in the MDVRA always remains well-aware about its current neighbourhood so as to be able to use all the information that may be collected through them. This specially requires the router to identify its various special neighbours, namely, FN, DN, CN, CDN, SCN, PN, SN, LD. Based on the above method of identifying and utilizing each of these special types of neighbours, to meet the two major challenges in designing routing algorithms for MANET, specifically, highly dynamic changes in the MANET topology and the need to preserve battery power, a novel idea of neighbourhood monitoring has been employed. It was identified that DVR is based on a neighbour-exchange algorithm; a proactive approach to dealing with neighbours is much more desirable in a MANET than reacting to the discovery gains of neighbours after they actually occur.

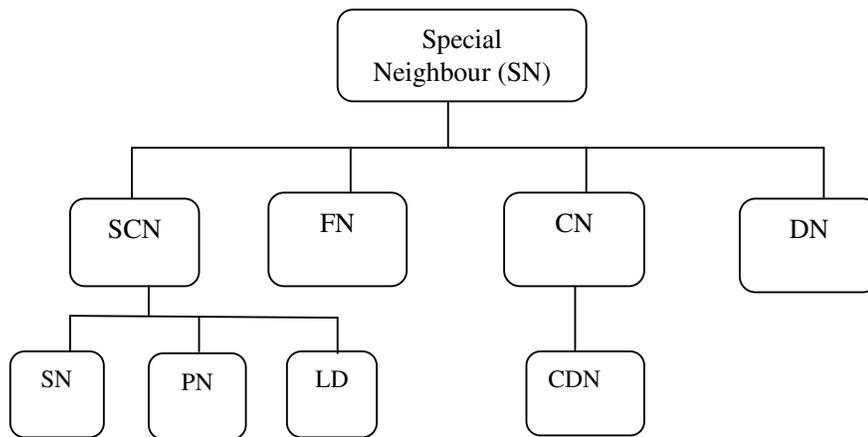


Figure 4: Interrelationship between different types special neighbours

2.6 Neighbour Notification (NN) and DVRT Packets: Periodic Interchange

DVRT periodically updates to enable each router, in an energy-aware manner, to both monitor its neighbours, the periodic DVRT exchange process in the DVRA has been divided in MDVRMANET into two separate exchanges, namely, more frequent exchange of Neighbour Notification (NN) packets and less frequent exchange of regular DVRT packets. Through the short NN packets, a node broadcasts to all neighbours its transmitted power as well as the list of its current RNs. DVRT packet contains all the information hold in an NN packet; it effectively replaces an NN packet. That is, during every 15-second- neighbour exchange cycle, each router synchronously sends and asynchronously receives from each neighbour 4 consecutive NN packets monitored by a DVRT packet.

3. CONCLUSIONS

This paper presented a review of the intrinsic problems of routing in MANETs and other such Ad Hoc Networks similar to wireless sensor networks (WSN), Vehicle Ad hoc Networks (VANET), etc are primarily because of the random topology changes mobility of the nodes, power constrain, limited bandwidth, asymmetric links, frequent link breakage due to random addition and deletion of nodes, for which, many routing protocols already proposed and/or in research, have not found stable and thus providing enough scope of improvement through research and investigations. The design or invention of new protocols is not find suitable solution until it is simple, elegant but robust in nature. In this paper, description of various routing schemes proposed for MANETs and classification of these schemes based on routing approach are provided with varying performance under various conditions.

This paper presented a DVR-based routing algorithm for MANETs because of its neighbour exchange based routing technique, through which a route can see its whole world only through a neighbour, and hence, need not to keep track of the whole network and thus reducing the burden of bandwidth and battery supply and alike overheads. This paper presented a of most recent DVR based routing protocols for MANETs and identified possible identification and use of the Special Neighbours (SN) and Neighbour Notification (NN) Neighbour Table (NT) and DVRT packets periodic exchange policy.

REFERENCES

- [1] Albeto Leon-Garcia and Indra Widjaja, *Communication Networks*, Tata McGraw Hill, 2000
- [2] N. H. Saeed, M.F. Abbod, and H S. Al-Raweshidy, "MANET Routing Protocols Taxonomy", *IEEE International Conference on Future Communication Networks*, PP-123-128, 2012
- [3] M. Abolhasan et al. "A review of routing protocols for mobile ad hoc networks" *Elsevier Ad Hoc networks 2* (2004) 1-22
- [4] Holger Karl and Andreas Willing, *Protocols and Architectures for Wireless Sensor Networks*, John Wiley & Sons, Ltd. 2005.
- [5] M. Gerla, C.C Chiang, and I. Zhang, "Tree Maulticast Strategies in Mobile, Multihop Wireless Networks," *ACM/Baltzer Mobile Networks and Apps. J.* 1988
- [6] S. Singh, M. Woo, and C. S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," *Proc. ACM/IEEE MOBICOM '98*, Oct. 1998.
- [7] Y. B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," *Proc. ACM/IEEE MOBICOM '98*, Oct. 1998.
- [8] S. Das, C. Perkins, E. Royer, Ad hoc on demand distance vector (AODV) routing, Internet Draft, draft-ietf-manetaodv-11.txt, work in progress, 2002.
- [9] Douglas E. Comer, David L. Stevens, *Internetworking with TCP/IP Vol-II*, 3rd Ed., Pearson Education (Singapore), LPE, 2005

- [10] G.V. Kumar et al. "Current Research Work on Routing Protocols for MANET: A Literature Survey" *International Journal on Computer Science and Engineering*, Vol. 02, No. 03, 2012, 706-713
- [11] <http://www.lockergnome.com/nexus/it/2006/08/17/distance-vector-and-link-state-routing-protocols/>
- [12] <http://www3.ietf.org/proceedings/98dec/I-D/draft-ietf-manet-appl-00.txt>
- [13] L. L. Peterson and B. S. Davie, *Computer Networks : A systems Approach*, 3rd Ed., Morgan Kaufman, 2003
- [14] S. K. Ray, J. Kumar, S. K. Sen and J. Nath, "Modified Distance Vector Routing Scheme for a MANET", Proc. Of the 13th National Conference on Communications (NCC) held at IIT, Kanpur during Jan 26-28, 2007, pp. 197-201.
- [15] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Third Edition, Pearson Education, Inc, Singapore, 2005
- [16] C. Toh, A novel distributed routing protocol to support ad-hoc mobile computing, in: IEEE 15th Annual International Phoenix Conf., 1996, pp. 480-486.
- [17] A. S. Tenenbaum, *Computer Networks*, 3rd Ed., PHI, 2000.
- [18] C. C. Chiang, T. C. Tsai, W. Liu, and M. Gerla, "Routing in clustered multihop, mobile wireless networks with fading channel," *The Next Millennium, Proceedings of IEEE Singapore International Conference on Networks*, SICON, pp. 197-221, 1997.
- [19] G. Pei, M. Gerla, X. Hong, and C. C. Chiang, "A wireless hierarchical routing protocol with group mobility," *IEEE Wireless Communications and Networking Conference, WCNC '99*, vol.3, pp. 1538-1542, New Orleans, LA, 1999.
- [20] D. Bertsekas and R. Gallagar: "Data Networks", 2nd Ed., Englewood cliffs, NJ, Prentice Hall, 1992
- [21] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, Optimized link state routing protocol for ad hoc networks, *IEEE INMIC, Pakistan*, 2001.
- [22] M. Gerla, Fisheye state routing protocol (FSR) for ad hoc networks, Internet Draft, draft-ietf-manet-aodv-03.txt, work in progress, 2002.
- [23] T.-W. Chen, M. Gerla, Global state routing: a new routing scheme for ad-hoc wireless networks, in: *Proceedings of the IEEE ICC*, 1998.
- [24] M. Gunes, U. Sorges, I. Bouazizi, Ara—the ant-colony based routing algorithm for manets, in: ICPP workshop on Ad Hoc Networks (IWAHN 2002), August 2002, pp. 79-85.
- [25] S. Murthy J.J. Garcia-Luna-Aceves, A routing protocol for packet radio networks, in: Proceedings of the First Annual ACM International Conference on Mobile Computing and Networking, Berkeley, CA, 1995, pp. 86-95.
- [25] <http://www.ietf.org/html.charters/manet-charter.html>
- [27] S.K. Sen "An Improved Network Routing Scheme Based on Distance Vector Principle" Ph.D Dissertation, Dept. of Comp. Sc. & Engg. Jadavpur University, January 2008
- [28] C.E. Perkins (ed). *Adhoc Networking*, Addison Wesley. 2001, ISBN 0-201-30976-9
- [29] <http://www.rfc.net/rfc2501.html>
- [30] E.M. Royer, S.B. Chai-Keong Toh, " A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks" *IEEE Personal Communications*, April 1999, PP-46-55

Authors

Mrinal Kanti Debbarma Research Scholar, Department of Information Technology, Triguna Sen School of Technology, Assam University, Silchar, Assam. His research interest include in MANET Routing Protocols, Wireless Sensor Networks, Software Engineering with special interest in Software metrics analysis and Regression testing. He has 12 years of academic and 5 years Industrial experience. He has published technical papers in various International Journals and Conferences. Mr. Debbarma is a member of IAENG, IACSIT. email: mmkdb06@gmail.com



Dr. Santanu Kumar Sen, Professor & Head, Department of Computer Science & Engineering, Guru Nanak Institute of Technology, Sodepur, Kolkata. His Research Interests are networking, Mobile Communication. He is presently guiding Ph.D students, post graduate students. He has around 18 years of experience in the field of Computer Science and Engineering in which 8 years in Industry and 10 years in Academics including Abroad. Prof. Sen has published papers more than 36 technical research papers in International and national journals and conferences. He is fellow member of FIET(UK), FIEC(USA), FIETE, FIE, LMISTE, SMCSI, MACM(USA), SMIEEE(USA). Prof. Sen has selected in the Marquis Who's Who in the World in Science & Engineering for the year 2012.



Dr. Sudipta Roy, Associate Professor & Head, Department of Information Technology, Triguna Sen School of Technology, Assam University, Silchar, Assam. His Research Interests are networking, signal processing and image processing. He is presently guiding Ph.D students, post graduate and graduate students. He has published numerous papers in International journals and national journals.

