A REVIEW ON MANET ROUTING PROTOCOLS AND ITS VULNERABILITIES

Himadri Nath Saha¹, Dr. Debika Bhattacharyya² Bipasha Banerjee³ Sulagna Mukherjee⁴ Rohit Singh⁵ and Debopam Ghosh⁶

¹,²,³,⁴,⁵,⁶ Institute of Engg & Management, Department of Computer Science, Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex Kolkata - 700 091, West Bengal, India

ABSTRACT: Mobile Ad-hoc Network (MANET) is a wireless network model which is infrastructure-less and consists of mobile nodes which are free to move. Since MANET does not have any centralized base station and is robust in nature, it is a major center of attraction both in telecommunication industries as well as academics. Due to the open nature, lack of any centralized infrastructure and access to trusted authorities, the security in MANET poses a huge threat. Also energy constraint is another factor to be considered and thus, routing in MANET is a big challenge this paper we have discussed in depth about the various on-demand, proactive and hybrid routing protocols in MANET. We have also discussed and compared their vulnerabilities in form of attacks.

KEYWORDS: REACTIVE, PROACTIVE, HYBRID, MANET, POSITION BASED ROUTING.

1. INTRODUCTION

1.1 BACKGROUND

Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes which communicate over relatively bandwidth constrained wireless links. MANETs differ from conventional wireless networks, such as cellular networks and IEEE 802.11 (infrastructure mode) networks; in that they are self-containing the network nodes can communicate directly with each other without reliance on centralized infrastructures such as base stations. Additionally, MANETs are self-organizing and adaptive; they can therefore form and de-form on-the-way without the need for any system administration. These unique features make MANETs very attractive for scenarios requiring rapid network deployment, such as search and rescue operations. The decentralized nature of MANETs, notably the absence of centralized entities, and hence the avoidance of single point of failures, makes these network paradigms also ideal for military and commercial applications that require high degree of robustness. MANET (mobile ad-hoc network) is a collection of mobile nodes which are dynamically connected to transfer information without the presence of any centralized infrastructure. It is a fully self organized network as it does not rely on any established infrastructure for the network initialization and operation. Initially it was conceptualized mainly for crisis situations like battle-fields and so on. Nodes can be any wireless device like personal computers (laptops), mobile phones etc.

Figure 1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the nodes wirelessly communication among them.

Figure 1 MANET Overview

1.2 Current challenges:

There are some challenging security issues which need to be addressed before MANETs are ready for widespread commercial or military deployment. One of the core security issues is trust management. Trust is generally established and managed in wired and other wireless networks via centralized entities, such as certificate authorities (CAs) or key distribution centers. The absence of centralized entities in MANETs makes trust management a rather challenging problem, primarily due to the unavailability of trusted authorities to perform necessary functions such as the revocation of digital certificates.

Another intriguing MANET security problem is the issue of secure routing in the presence of selfish or malicious nodes, which selectively drop packets they are required to forward; and in so doing, these selfish or malicious entities can cause various communication problems. Also since the network is self-organizing, the topology changes randomly. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.

Nodes in an ad hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life. Due to presence of a fixed supporting structure, limits the adaptability wireless system is required easy and quick deployment of wireless network. Recent advancements of wireless technologies like Bluetooth[1],IEEE 802.11[2] introduced a new type of wireless system known as Mobile ad-hoc network (MANETs)[3][4][5][6], which operate in the absence of central access point. It provides...
high mobility and device portability that allow nodes to connect to network and communicate to each other. It allows the devices to maintain connections to the network as well as add and remove devices to and from the network. User can design such networks at cheapest costs and minimum time. MANET has the following characteristics, such as:

- Weaker in security
- Device size Limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

2. ROUTING PROTOCOLS

2.1 Definition:
In an ad hoc network, all the nodes may not be within the transmission range of each other; hence, nodes are often required to forward network traffic on behalf of other nodes. Consider for example the scenario in Fig 2–1, if node S sends data to node D, which is three hops away, the data traffic will get to its destination only if A and B forward it. The process of forwarding network traffic from source to destination is termed routing.

Figure 2: Multihop scenario[47]

2.2 Overview of routing approaches in MANETs:
Before proceeding to describe each of the routing protocols of MANET, it is fitting to list some desirable qualitative properties of these protocols. This list is adopted from an Internet Engineering Task Force (IETF) MANET Working Group memo [7].

- Loop-free: It is desirable that routing protocols prevent packets from circling around in a network for arbitrary time periods.
- Demand-based operation: In order to utilize network energy and bandwidth more efficiently, it is desirable that MANET routing algorithms adapt to the network traffic pattern on a demand or need basis rather than maintaining routing between all nodes at all time.
- Proactive operation: This is the flip-side of demand-based operation. In cases where the additional latency—which demand-based operations incur—may be unacceptable, if there are adequate bandwidth and energy resources, proactive operations may be desirable in these situations.
- “Sleep” period operation: It may be necessary—for reasons such as the need for energy conservation—for nodes to stop transmitting or receiving signals for arbitrary time periods. Routing protocols should be able to accommodate sleep periods without adverse consequences.

Security: It is desirable that routing protocols provide security mechanisms to prohibit disruption or modification of the protocol operations.

There are two general categories of MANET routing protocols: Topology-based and Position-based. Firstly we start by classifying MANET routing protocols as given in Figure 3 followed by a brief overview of each of the protocols in sections 2.3 and 2.4.

Figure 3 General Categories of Routing Protocols

2.3. Position-based routing protocols
Position-based routing protocols employ nodes’ geographical position to make routing decisions. In order to utilize a position-based routing protocol, a node must be able to ascertain the geographical position of it and that of all the nodes it wishes to communicate with. This information is typically obtained via Global Positioning System (GPS) and location services.

Greedy
The Greedy Routing Protocol by G.Finn[8]. In the greedy forwarding approach, a node selects for the next hop, the node that is closest to the destination of the packet. In Figure 2.3 if S has data traffic to send to D which is outside its transmission range. This protocol dictates that S sends the traffic through B, since B is the node within transmission range which is closest to destination D.

Figure 4: Greedy forwarding[47]
Greedy forwarding tries to bring the message closer to the destination in each step using only local information. Thus, each node forwards the message to the neighbor that is most suitable from a local point of view. This can lead into a dead end, where there is no neighbor closer to the destination. Alternatively, one can consider another notion of progress, namely the projected distance on the source-destination-line, for example, MFR; or the minimum angle between neighbor and destination for example, Compass and Randomized Compass.

Compass
The Compass routing algorithm was developed by Kranakis et al.[9]. In this scheme, a node S which has data traffic to send to a destination node D, forwards the traffic to its neighbor N which has the smallest angle $\angle N$ SD, where N is a neighboring node to the forwarding node S and D is the destination. So for example, in Figure 2.4, S forwards the traffic for D to A since the angle $\angle ASD$ is smaller than angle $\angle N$ SD where N is a node within S transmission range. Notably, Stojmenovic and Lin [10] showed that the Compass Algorithm is not Loop free.

Randomized compass
The Randomized Compass routing algorithm [11] is a variation of the Compass algorithm which avoids loops with random decision s. Consider a line between a node S and a destination node D. The Random Compass forwarding approach chooses the next hop for a packet by randomly selecting between the nodes $N_i$ and $N_j$ which has the smallest angle $\angle N_i$ SD and $\angle N_j$ SD between the imaginary line NS (between a node N and the forwarding node S) and SD, above and below the imaginary line SD, respectively. So for example in Figure 2.4, node S would randomly select node A or B for forwarding packets to D since $\angle ASD$ is the smallest angle (between a line connecting S and a node that is within S transmission range, and the line SD) above the line SD and $\angle BSD$ is the smallest angle below the line SD.

Most Forwarded within Radius (MFR)
Takagi and Kleinroc proposed MFR [12]. Consider an imaginary line SD between a node S and a destination node D; in MFR forwarding, S forwards data traffic for D to a node A which maximizes the progress along the imaginary line SD. A is therefore the node which minimizes the dot product $DA \cdot DS$. So in Figure 2.5, S forwards packets for D to A since A is the node within S transmission range which provides the most progress along the line SD.

Some of the protocols which uses the above mentioned approaches are as follows:

Greedy Perimeter Stateless Routing (GPSR) [13]
GPSR, by Karp and Kung, also uses the location of the node to selectively forward the packets based on the distance. The forwarding is carried out on a greedy basis by selecting the node closest to the destination. This process continues until the destination is reached. However, in some scenarios, the best path may be through a node which is farther in geometric distance from the destination. In this case, a well known right hand rule is applied to move around the obstacle and resume the greedy forwarding as soon as possible.

Distance Routing Effect Algorithm for Mobility (DREAM) [14]
Basagni et al. propose the DREAM protocol which also uses the node location information from GPS systems for communication. DREAM is a part proactive and part reactive protocol where the source node sends the data packet “in the direction” of the destination node by selective flooding.

Location-aided routing (LAR)
Ko and Vaidya[15][16]present the LAR protocol which utilizes location information to minimize the search space for route discovery towards the destination node. LAR aims to reduce the routing overhead for the route discovery and it uses the Global Positioning System (GPS) to obtain the location information of a node. LAR essentially describes how location information such as GPS can be used to reduce the routing overhead in an ad hoc network and ensure maximum connectivity. According to the performance study in [17] LAR schemes introduce less routing overhead than that introduced by the pure flooding scheme. However, it is considered as a two sided solution, as more resources are required, namely, GPS. However, it is considered as a two sided solution, as more resources are required, namely, GPS.

Position-based routing protocols are completely on GPS (Global Position System) for routing. GPS demands external battery power and hence results in a battery life. These systems are also not well run in real
time for all models, because if there is any malfunction with the GPS system, then the Position Based Routing fails. Hence this is the main cause of using Topological based Routing Protocols.

2.4 Topology based routing protocol

Topology based routing mechanism utilizes topology information to make routing decisions at each node. Topology information means separate route management process, like Route Request, Route Reply, etc. There are three major categories of Topology-based routing protocols: On-demand (Reactive), Proactive & Hybrid protocols.

In this section, we briefly describe some of the most prominent existing MANET topology-based routing protocols. We commence with proactive protocols.

2.4.1 Proactive protocols:

Proactive protocols are also referred to as periodic protocols. It maintains one or more tables representing the entire topology of the network, which are updated from time to time. There are many proactive protocols, as shown in Figure 2.2., out of which some of them are described as follows,

Destination-sequenced Distance-Vector (DSDV) [18]

utilizes the classical Distributed Bellman-Ford Distance-Vector algorithm [19][20][21]. DSDV (Perkins & Bhagwat, 1994) is a distance vector routing protocol that ensures loop-free routing by tagging each route table entry with a sequence number.

Fisheye State Routing (FSR)

This protocol reduces the amount of traffic for transmitting the update messages. The basic idea is that each update message does not contain information about all nodes. Instead, it contains update information about the nearer nodes more frequently than that of the farther nodes. Hence, each node can have accurate and exact information about its own neighboring nodes. The novelty of FSR is that it uses a special structure of the network called the ‘fisheye.’

Source Tree Adaptive Routing (STAR)

The Source Tree Adaptive Routing (STAR) protocol [22] has significantly decreased the routing overhead disseminated in the network by employing a least overhead routing approach (LORA) to exchange routing information. It also employs optimum routing approaches (ORA) if required. This protocol scales very well for large networks since it has significantly reduced the bandwidth consumption for routing updates.

Optimised Link-State Routing (OLSR)

(Jacquet, Muhlethaler, Clausen, Laouiti, Qayyum, & Viennot, 2001)[23] optimises the linkstate algorithm by compacting the size of the control packets that contain link-state information and reducing the number of transmissions needed to flood these control packets to the whole network.

Clusterhead gateway switch routing (CGSR) [24]

The CGSR protocol, by Chiang et al., uses a distributed algorithm called the Least Cluster Change (LCC). By aggregating nodes into clusters controlled by the cluster heads, a framework is created for developing additional features for channel access, bandwidth allocation and routing. Nodes communicate with the cluster head which in turn communicates with other cluster heads within the network.

Wireless routing protocol (WRP) [25]

Murthy and Garcia–Luna–Aceves propose WRP which builds upon the distributed Bellman-Ford algorithm. The routing table contains an entry for each destination with the next hop and a cost metric. The route is chosen by selecting a neighbor node that would minimize the path cost. Link costs are also defined and maintained in a separate table and various techniques are available to determine these link costs.

Global state routing (GSR) [26]

Chen and Gerla propose the GSR protocol, where the control packet size is adjusted to optimize the MAC throughput. Each node maintains the neighbor list and three routing tables containing the topology, the next hop, and the distance respectively. The neighbor list contains all neighbors of the current node. The topology table contains the link state information and a timestamp indicating the time in which the link state information is generated. The next hop table contains a list of next hop neighbors to forward the packets while the distance table maintains the shortest distance to and from the node to various destinations. A weight function computes the distance of a link which may be replaced by other QoS routing parameter.

<table>
<thead>
<tr>
<th>Table 1: Comparison of Proactive Routing Protocol [48]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>DSDV</td>
</tr>
<tr>
<td>WRP</td>
</tr>
<tr>
<td>CGSR</td>
</tr>
<tr>
<td>GSR</td>
</tr>
<tr>
<td>FSR</td>
</tr>
</tbody>
</table>
In general, every node maintains a list of destinations and their routes by processing periodic topology changes originated by each node in the network, which increases the routing table space and requires periodic routing [27]. When a packet arrives, the node checks its routing table and forwards the packet accordingly. Each node monitors its neighboring links and every change in connectivity with any neighbor results in a topology broadcast packet that floods over the entire network, hence causing excessive traffic in the network.

The delivery of packet data is much more inefficient in Proactive Protocols and they are not adaptive with respect to topology changes. Proactive routing protocols provide fast responses to topology changes by maintaining routing information for all network destinations and react to changes in the network. However, the price to pay is the signaling overhead incurred in maintaining routing information for those destinations in which large numbers of nodes have no interest. On the other hand, reactive routing protocols provide routing information on a need-to-have basis and, at least in theory, can reduce the signaling overhead incurred in maintaining routing tables compared to proactive approaches [27].

### 2.4.2. On-demand protocols:

On-demand protocols are also referred to as reactive protocols. Unlike proactive protocols which seek to maintain routes to all destinations and maintain an up-to-date routing table for the entire network calls for excessive communication between the nodes, as periodic and triggered updates are flooded throughout the network. On-demand protocols establish routes on a per-need basis. There are larger collections of existing on-demand protocols compare to proactive protocols. We present brief description of some of the more widely known on-demand protocols below.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Type</th>
<th>Mobile</th>
<th>CO</th>
<th>MO, Reduced</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAR</td>
<td>List</td>
<td>One and Five Lists</td>
<td>Conditi onal</td>
<td>Employs LORA and ORA</td>
<td>High MO, processing overhead</td>
</tr>
<tr>
<td>OLSR</td>
<td>Three</td>
<td>Periodic</td>
<td>Reduced CO and connecti on</td>
<td>2-hop neighbor knowledge required</td>
<td></td>
</tr>
<tr>
<td>DREAM</td>
<td>One</td>
<td>Mobility Based</td>
<td>Low CO and MO</td>
<td>Requires GPS</td>
<td></td>
</tr>
</tbody>
</table>

SSA (Signal Stability-Based Adaptive Routing):

SSA routing protocol as proposed by DUBE[30] provides an on-demand route discovery by selecting longer-lived routes based on signal strength and location stability. The rational being that links which exhibit the strongest signal for the maximum amount of time leads to longer-lived routes and less route maintenance.

In SSA routing, a source S sends out a route discovery request when it has data to send to a destination D that is not in its routing table. S broadcasts the route request to all its neighbors. Each neighboring node propagates the route request if it received it over a strong channel and the request has not been propagated previously. A channel is characterized as strong or weak based on the average signal strength at which the packets are exchanged exchanged between the nodes at either end of the channel. The route search packet continues to traverse the network until it reaches the destination, and it stores the address of each intermediate node it traversed. The first route search
packet which arrives at the destination D is selected and a route reply packet is constructed and returned to S using the selected route. Each intermediate node in the selected route, on receiving the route reply packet, includes the new next-hop, destination pair in its routing table.

These measurements are used to classify the links as either stable or unstable. SSA tries to find a completely stable path form the beginning, a process that if succeeded to find a path, it will be a very positive side of SSA. On the other hand if this process fails to find a path it may start the procedure from the beginning allowing paths with unstable link, which means additional effort to find a path.

**ABR (Associativity-Based Routing)**

C-H Toh developed the Associativity-Based Routing (ABR) [31]. ABR utilizes the observation that a mobile node’s association with its neighbor changes as it migrates and its transiting period can be identified by the associativity “ticks”. Associativity ticks are updated by the mobile node’s data-link protocol which periodically transmits beacons identifying itself and updates its associativity ticks in accordance with the mobile nodes in its neighborhood. A mobile node exhibits high associativity ticks (high association stability) with its neighbors when it is in a state of low mobility. Conversely, a state of high mobility is associated with low associativity ticks.

In ABR routing, a node S which desires a route to a destination D broadcasts a broadcast query (BQ) message which propagates through the MANET in search of a node which has a route to the given destination. When an intermediate node \( n_i \) receives a BQ message it has not previously seen, \( n_i \) appends its address, associativity ticks with its neighbors, its relaying load, link propagation delay and its hop count to the appropriate fields of the BQ, and broadcasts the BQ to its neighbors. The next succeeding intermediate node will then erase its upstream node’s neighbors’ associativity ticks entries and retain only those concerning itself and its upstream nodes. When the destination node D receives the BQ packets, it selects a route based on the following selection criteria: routes consisting of nodes with higher associativity ticks has higher preference even over routes with smaller number of hops. For routes with equal number of associativity ticks, the route with the smaller hop count is selected. If the routes have the equal number of associativity ticks and hop counts, one of the route is randomly selected. The selected route is used to construct a REPLY packet and returned to the source S via the selected route. The intermediate nodes on the route from D to S will consequently mark their routes to D as valid and subsequently inactivate all other possible routes to D.

The main drawback of this approach is short beaconing interval to reflect association degree precisely

**AODV (Ad-hoc On-demand Distance Vector)**

Ad-hoc On-demand Distance Vector Routing was designed by Perkins and Royer [32]. The key feature of this protocol is that applying a distributed routing scheme. In contrast to the source routing applied by DSR, AODV depends on storing the next hops of a path as entries in the intermediate nodes, which is considered as an advantage. However this may require additional resources form the intermediate nodes, which is the negative side of AODV [33].

Each node using AODV maintains a route table entry for each destination of interest. A route table entry contains the destination D, next hop, number of hops to D, sequence number of the destination and the expiration time for the route table entry. When a node S has a packet to send to a destination D, S checks its routing table for an entry containing D as the destination with a sequence number equal to or greater than the last known destination sequence number of D. If there is no such entry, S broadcasts a route request (RREQ) packet, containing the source address, the source sequence number, broadcast id, destination sequence number and hop count. The source sequence number and the broadcast id are separate that are maintained by each node. Each piece of information in this packet has a use in the route setup process [34].

A node increments its broadcast id counter each time it constructs a new RREQ packet; whereas the node’s sequence number counter is incremented less frequently. The destination sequence number is the last known sequence number of the destination. When a node \( n_i \) receives a RREQ packet it has not previously seen, it sets up a reverse path to the source by recording the address of its neighbor from which it received the first copy of the RREQ. If \( n_i \) is not the destination and its routing table does not contain an entry for D, it increments the hop count and rebroadcasts the RREQ packet to its neighbors. If \( n_i \) however is the destination or if its routing table contains an entry with D as its destination with a destination sequence number that is equal to or greater than the destination sequence number in the RREQ packet, it constructs a route reply (RREP) packet and unicasts it to the neighboring node it received the RREQ from. An RREP packet contains the source address, destination address, destination sequence number, hop count and lifetime. When an intermediate node receives a RREP packet, it updates its routing table with the information the RREP contains, then unicasts it to the neighbor it received the first copy of the associated RREQ packet. The process continues until the RREP packet gets to S. S can now forward its packet to the next hop on the path to D.

**DYMO (Dynamic Manet Ondemand)**

DYMO was proposed by Perkins and Chakeres [35][36] is a successor to AODV reactive protocol. It is, however, slightly easier to implement and accumulates the routing information of all nodes in the path and does not support unnecessary HELLO messages and operation is purely based on sequence numbers assigned to all the packets. It
is a reactive routing protocol that computes unicast routes on demand or when required. It employs sequence numbers to ensure loop freedom.

DYMO implements three messages during the routing operation namely Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). Besides this the DYMO protocol mandates each node to maintain an unsigned unique integer called “sequence number” which guarantees the orderly delivery of packets to the destination and maintain loop-free routes similar to that in AODV and DSDV. Sequence numbers allow the nodes to evaluate the freshness of routing information and to avoid loops in the route.

If a source has no route entry to a destination, it broadcasts a RREQ message to its immediate neighbors. If a neighbor has a route to the destination, it replies with an RREP message else it broadcasts the RREQ message. While broadcasting the RREQ message, the intermediate node will attach its address to the message. Every intermediate node that disseminates the RREQ message makes a note of the backward path. Each intermediate node having a valid path to the destination keeps on adding its address and sequence number to the RREQ packet. The source node waits for a RREP message[36]. The RERR message must be generated by a node if and when a link to any other node breaks. The generating node multicasts the RERR message to only those nodes which are concerned with the link failure. Upon reception of a RERR message, the routing table is updated and the entry with the broken link is deleted.

One of the special features of DYMO is that it is energy efficient. If a node is low on energy, it has the option to not participate in the route discovery process. In such a case, the node will not forward any of the incoming RREQ messages. It however will analyze the incoming RREP messages and update its routing tables for future use.

The DYMO protocol [37], however, does not perform well with low mobility. The control message overhead for such scenarios is rather high and unnecessary. Another limitation lies in the applicability of the protocol as stated in the DYMO Draft which states that DYMO performs well when traffic is directed from one part of the network to another. It shows a degraded performance when there is very low traffic random and routing overhead outruns the actual traffic.

**TORA(Temporally-Ordered Routing Algorithm)**

Temporally-Ordered Routing Algorithm (TORA) was developed by Park and Corson [38]. It is a highly adaptive multipath, loop-free, distributed routing algorithm which was designed for highly dynamic MANET environments. A key design concept of TORA is the localization of routing control messages to a small set of nodes near the topological change.

TORA builds and maintains a directed acyclic graph (DAG) rooted at the destination. The DAG, by design, ensures that all directed paths are loop-free and lead to the destination. Links between routers are directed (to form the DAG) based on a metric, maintained by the routers, that can conceptually be viewed as a “height”[39]

In TORA routing, each node, at any given point in time has an associated ordered quintuple consisting of the following elements: (1) a logical time of link failure (2) the unique ID of the node which defined the new reference level (3) a single bit which is used to divide each of the unique reference level into two unique sub-levels (4) a propagation ordering parameter and (5) the unique ID of the node. Conceptually, the quintuple represents the height of a node defined by a reference level and a delta with respect to the reference level.

The reference level is represented by the first three values of the quintuple while the last two values represent the delta. Each node i (other than the destination) maintains its height Hi which is initially set to NULL. \( H_i = (-, -, -,) \). The height of the destination is always ZERO, \( H_{DID} = (0, 0, 0, 0, Did) \), where DID represents the destination ID. In addition to its own height, each node maintains an height array with an entry \( HN_{ij} \) for each of its neighbor j. Each node i also maintains a link-state array for each of its links. The state of a link is determined by its height \( H_i \) and \( HN_{ij} \) and is directed from higher node to lower node.

When a node requires a route to a destination D it sends out a QRY packet. When a node i receives a QRY packet it has not previously seen, it reacts as follows: (a) i rebroadcasts the QRY packet if it has no downstream links; (b) if the receiving node has at least one downstream link and its height is NULL, it sets its height to the minimum height of it non NULL neighbors and broadcasts a UPD packet (which consists of a destination ID and the height of the node i which is broadcasting the packet); (c) if the receiving node has at least one downstream link and its height is non NULL, it first compares the time the last UPD packet was broadcast to the time the QRY packet arrived was active. If the link became active prior to the broadcasting of the UPD packet, i discards the QRY; otherwise, i broadcasts a UPD packet. When a node i receives a UPD packet it has not previously seen from a neighbor j, i updates the entry \( HN_{ij} \) in its height array with the height contained in the UPD packet, then do the following: if its height is NULL, i sets its height to the minimum height of its non NULL neighbor, updates all the entries in its link-state array then rebroadcasts the UPD packet which contains its new height. The process (broadcasting of QRY and UPD packets) continues until a directed acyclic graph (DAG) rooted at the destination (i.e. the destination is the only node with no downstream links) is formed. The DAG represents a route from the source S to the destination D.

This protocol can often falsely detect partitions. It even requires reliable and in-order delivery of route control packets. The main disadvantage of TORA is that...
the algorithm may also produce temporary invalid routes. TORA is not much used since DSR and AODV outperforms it.

### Table 2 Comparison of Reactive Protocols

<table>
<thead>
<tr>
<th></th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSR</strong></td>
<td>Intermediate nodes do not store route information; Can provide multiple paths</td>
<td>Stale caches and relay storm problems may arise in large and highly mobile MANETs. Communication overhead due to source routing.</td>
</tr>
<tr>
<td><strong>ABR</strong></td>
<td>Stable routes; Localised route repair mechanism</td>
<td>Suitable for small MANETs. Frequent beacons may result in extra bandwidth and power consumptions.</td>
</tr>
<tr>
<td><strong>SSA</strong></td>
<td>Stable routes</td>
<td>Introduces more delays than DSR to find routes. Does not have any localised route repair mechanism.</td>
</tr>
<tr>
<td><strong>AODV</strong></td>
<td>Adaptable to highly dynamic topologies; Multicast routing capability</td>
<td>Requires HELLO messages. Does not support multiple routes. Intermediate nodes need to store routing information. May not scale well with network size.</td>
</tr>
<tr>
<td><strong>DYMO</strong></td>
<td>It has a high throughput and packet delivery, low average end to end delay but incurs a low routing overhead.</td>
<td>Does not perform well with low mobility. It shows a degraded performance when there is very low traffic.</td>
</tr>
<tr>
<td><strong>RDMA</strong></td>
<td>Limits the propagation of routing control packets</td>
<td>Flooding is used if nodes do not have any prior communication. Suited for MANETs having low to moderate topological changes.</td>
</tr>
</tbody>
</table>

### Table 3. Complexity Comparison of The On-Demand Routing Protocols

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSR</strong></td>
<td>$O(2N)$</td>
<td>$O(2N)$</td>
<td>$O(2D)$</td>
<td>$O(2D)$</td>
</tr>
<tr>
<td><strong>ABR</strong></td>
<td>$O(N+r)$</td>
<td>$O(a+r)$</td>
<td>$O(D+c)$</td>
<td>$O(b+c)$</td>
</tr>
<tr>
<td><strong>SSA</strong></td>
<td>$O(N+r)$</td>
<td>$O(a+r)$</td>
<td>$O(D+c)$</td>
<td>$O(b+c)$</td>
</tr>
<tr>
<td><strong>AODV</strong></td>
<td>$O(2N)$</td>
<td>$O(2N)$</td>
<td>$O(2D)$</td>
<td>$O(2D)$</td>
</tr>
<tr>
<td><strong>DYMO</strong></td>
<td>$O(2N)$</td>
<td>$O(2N)$</td>
<td>$O(2D)$</td>
<td>$O(2D)$</td>
</tr>
<tr>
<td><strong>RDMA</strong></td>
<td>$O(2e)$</td>
<td>$O(2e)$</td>
<td>$O(2d)$</td>
<td>$O(2d)$</td>
</tr>
<tr>
<td><strong>TORA</strong></td>
<td>$O(2N)$</td>
<td>$O(2a)$</td>
<td>$O(2D)$</td>
<td>$O(2D)$</td>
</tr>
<tr>
<td><strong>CBRP</strong></td>
<td>$O(2m)$</td>
<td>$O(2a)$</td>
<td>$O(2D)$</td>
<td>$O(2b)$</td>
</tr>
</tbody>
</table>

The other On-demand routing protocols as mentioned in Figure 2.2 (for example ARA[40], CBRP[41], RDMAR[42], LMR[43]) are not so relevant to our work. So they have not been described in this section.

In Table 2 we try to present a comparative study between all the reactive protocols which we have described above.
Zone-Based Hierarchical Link State Routing Protocol (ZHLS)

In ZHLS protocol [46], the network is divided into non-overlapping zones as in cellular networks. Each node knows the node connectivity within its own zone and the zone connectivity information of the entire network. The link state routing is performed by employing two levels: node level and global zone level. The zone level topological information is distributed to all nodes. Since only zone ID and node ID of a destination are needed for routing, the route from a source to a destination is adaptable to changing topology. The zone ID of the destination is found by sending one location request to every zone.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>ZRP</th>
<th>ZHLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Philosophy</td>
<td>Flat</td>
<td>Hierarchical</td>
</tr>
</tbody>
</table>

Table 4: Comparison of Hybrid Routing Protocol [48]

<table>
<thead>
<tr>
<th>Routing class</th>
<th>PROACTIVE</th>
<th>REACTIVE</th>
<th>HYBRID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Overhead</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Route acquisition delay</td>
<td>Low</td>
<td>High</td>
<td>Lower for Intra-zone; Higher for Inter-zone</td>
</tr>
<tr>
<td>Bandwidth requirement</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Power requirement</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Table 5: Comparison Of Proactive And Reactive And Hybrid Routing Protocols In Manet [48]

2.4.3. Hybrid protocols:

These types of protocols combine proactive and reactive protocols to try and exploit their strengths. One approach is to divide the network into zones, and use one protocol within the zone, and another between them. It initially establishes some proactively prospected routes and then serves the demand from additional active nodes through reactive flooding. The main disadvantages are that the advantages depend on the no of nodes activated. Also the reaction to traffic demand depends on gradient of traffic volume.

Zone Routing Protocol (ZRP)

Zone routing protocol is a hybrid routing protocol which effectively combines the best features of proactive and reactive routing protocol [44][45]. The key concept is to use a proactive routing scheme within a limited zone in the r-hop neighborhood of every node, and use reactive routing scheme for nodes beyond this zone. An Intra-zone routing protocol (IARP) is used in the zone where particular node employs proactive routing whereas inter-zone routing protocol (IERP) is used outside the zone. The routing zone of a given nodes is a subset of the network, within which all nodes are reachable within less than or equal to the zone radius hops. The IERP is responsible for finding paths to the nodes which are not within the routing zone. When a node S wants to send data to node D, it checks whether node D is within its zone. If yes packet is delivered directly using IARP. If not then it broadcasts (uses unicast to deliver the packet directly to border nodes) the RREQ packet to its peripherals nodes. If any peripheral nodes find D in its zone, it sends RREP packet; otherwise the node re broadcasts the RREQ packet to the peripherals nodes. This procedure is repeated until node D is located.

---

*WCC: Worst Case Communication Complexity, i.e. number of messages needed to perform a route discovery or an update operation in worst case; WTC: Worst Case Time complexity, i.e. number of steps involved to perform a route discovery or an update operation in worst case; RD: Route Discovery; RM: Route Maintenance; N: Number of nodes in the network; D: Diameter of the network; a: Number of affected nodes; b: Diameter of the affected area; c: Diameter of the directed path of RREP; BANT: d: Diameter of the localised region; e: Number of nodes in the localised region; r: Number of nodes in the route reply path; m: Number of clusters in CBRP; #: Sends periodic probe packets along active routes;
their security. Hence, the requirement for secure routing protocols is inevitable.

REFERENCES

Dang, W.Li and D.P. Agarwal, “Routing Security in wireless ad hoc networks”, IEEE Communications
Magazine, 0613-6804, pp. 70-75, October 2009.
evaluation considerations. Internet Request for Comments (RFC 2501). January 1999
[10] J. Stojmenovic and X. Lin. Loop-free hybrid single-path/odooing routing algo-
rithms with guaranteed
delivery for wireless networks. IEEE Transactions on
triangulations. In Proceedings of the 10th International Symposium on Algorithms and
Computation (ISAAC’99), Volume 1741 of Springer
257, 1984.
Routing for Wireless Networks, in: Proceedings of
Woodward, A distance routing effect algorithm for
mobility (DREAM), in: Proceedings of the ACM
MOBICOM, October 1998, pp. 76–84
[15] Y. Ko, N. Vaidya, Location-Aided Routing (LAR) in
mobile ad hoc networks, in: Proceedings of ACM
MobiCom, October 1998, pp. 66–75
[16] Y.-B. Ko, N.H. Vaidya, GeoTORA: A protocol for
geocasting in mobile ad hoc networks, in: Proceedings
Routing (LAR) in mobile adhoc networks, Proc. of
destination-sequenced distance- vector routing (dsdv)
for mobile computers. In Proceedings of ACM
SIGCOMM Conference on Communications
Architectures, Protocols and Applications, pages 234–
244, October 1994.
[21] C. Cheng, R. Riley, S. P. R. Kumar, and J. J. Garcia-
Luna-Aceves. A loop-
free bellman-ford routing
protocol without bouncing effect. In Proceedings of
ACM SIGCOMM ’89, pages 224–237, September
1989.
[22] J.J. Garcia Luna Aceves, C. Marcelo Spohn, Source
tree routing in wireless networks, Proceedings of the
Seventh Annual International Conference on
Network Protocols Toronto, Canada, p. 273,
October 1999.
[23] Optimized Link State Routing Protocol for Ad Hoc
Networks P.Jacquet, P.Mühlthaler, T.Clausen,
A.Lautiti,A. Qayyum,L.Viennot. Hipercom
Project,INRI Rocquencourt, BP 105, 78153 Le
Chesnay Cedex,France.
[24] W.L.C. Chiang, H. Wu and M. Gerla, Routing in
clustered multihop, mobile wireless networks, in:
Proceedings of IEEE SICON, April 1997, pp. 197–
211.
routing protocol for wireless networks, MONET 1 (2)
routing scheme for ad-hoc wireless networks, in:
175.
[27] Proactive or Reactive Routing: A Unified Analytical
Framework in MANETs Xianren Wu, Hui Xu, Hamid
R. Sadjadpour and J.J. Garcia-Luna-Aceves
[28] Johnson DB, Maltz DA, Hu Y. The dynamic source
routing protocol for mobile ad hoc networks
[29] D. Johnson and D. Maltz. Dynamic source routing in
ad-hoc wireless networks routing protocols. In
[40] ARA – The Ant-Colony Based Routing Algorithm for MANETs *Mesut Gunes*, Udo Sorges, Imed Bouazizi
[41] The Cluster-Based Routing Protocol:Tim Daniel Hollerung, University of Paderborn
[42] RDMAR: A bandwidth-efficient Routing Protocol for Mobile Ad hoc Networks:George Aggelou, Rahim Tafazolli Center for Communication Systems Research (CCSR), University of Surrey
[43] Label-based Multipath Routing (LMR) inWireless Sensor Networks Xiaobing Hou, David Tipper and Joseph Kabara,Department of Information Science & Telecommunications University of Pittsburgh, Pittsburgh, PA 15260

AUTHORS:

Prof Himadri Nath Saha :Prof. Saha is graduated from Jadavpur University. He did his post graduate degree from Bengal Engineering and Science university. He is Assistant Professor of Institute of Engg and Management. His research interest is security in MANET.

Prof.(Dr)Debika Bhattacharyya:

Prof.Bhattacharyya did Phd. from Jadavpur University in the dept. of ETCE. She is HOD in the Dept of CSE. Her research interest is security in MANET.

Bipasha Banerjee: She is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. Her research interest is MANET.

Sulagna Mukherjee: She is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. Her research interest is MANET.

Rohit Singh: He is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. His research interest is MANET.

Debopam Ghosh: He is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. His research interest is MANET.