Review of Various Routing Protocols for MANETs

Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma

***Abstract*—In recent years, a vast research has been seen going on in the field of Mobile Ad Hoc Networks (MANETs). Due to limited resources in MANETs, to design an efficient and reliable routing strategy is still a challenge. An intelligent routing strategy is required to efficiently use the limited resources. Also the algorithms designed for traditional wired networks such as link-state or distance vector, does not scale well in wireless environment. Routing in MANETs is a challenging task and has received a tremendous amount of attention from researchers around the world. To overcome this problem a number of routing protocols have been developed and the number is still increasing day by day. It is quite difficult to determine which protocols may perform well under a number of different network scenarios such as network size and topology etc. In this paper we provide an overview of a wide range of the existing routing protocols with a particular focus on their characteristics and functionality. Also, the comparison is provided based on the routing methodologies and information used to make routing decisions. The performance of all the routing protocols is also discussed. Further this study will help the researchers to get an overview of the existing protocols and suggest which protocols may perform better with respect to varying network scenarios.**

***Index Terms*—Mobile ad hoc networks, Routing Protocols comparison.**

I. Introduction

A Mobile ad hoc network is a group of wireless mobile computers (or nodes); in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points. A MANET is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. MANETs possess certain characteristics like Bandwidth-constrained, variable capacity links, Energy-constrained Operation, Limited Physical Security, Dynamic network topology, Frequent routing updates. Figure 1 shows a mobile ad hoc network with 6 nodes.

Manuscript received August 15, 2011; revised September 25 2011

Anuj K. Gupta is a research fellow in Punjab Technical University, Punjab, India. His research area is Mobile ad hoc networks, wireless networks & Data Communication. Currently he is working as faculty in CSE Dept. at RIMT-IET, Punjab. He is a member of IACSIT.

Dr. Harsh Sadawarti is Director at RIMT-IET, Punjab, India. He has a vast teaching and research experience of more than 20 years in the field of computer science. He is a member of IEEE.

Dr. Anil K. Verma is faculty in Computer Sci. & Engg. Dept. at Thapar University, Patiala, Punjab, India. He has a vast teaching & research experience of more than 20 years.

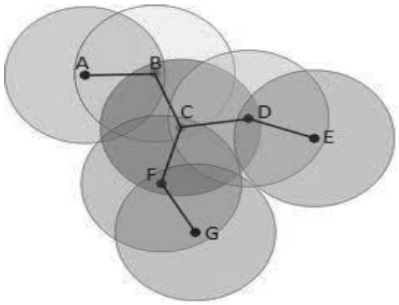

Fig. 1. A Mobile ad hoc network

Paper Outline

The rest of the paper is organized as follows: Section II presents routing in MANETs. Section III presents classification of various routing protocols. Sections IV, V, VI present the detailed analysis of all the three categories of ad hoc routing protocols and Section VII presents the overall comparison based on the review presented. Finally Section VIII concludes the paper.

II. Routing in MANETs

A Mobile Ad Hoc Network or spontaneous network is an infrastructureless, self-organized and multi-hop network with rapidly changing topology causing the wireless links to be broken and re-established on-the-fly [1]. A key issue is the necessity that the Routing Protocol must be able to respond rapidly to the topological changes in the network. In these networks, each node must be capable of acting as a router. As a result of limited bandwidth of nodes, the source and destination may have to communicate via intermediate nodes [2]. Major problems in routing are Asymmetric links, Routing Overhead, Interference, and Dynamic Topology.

Routing in MANETs has been an active area of research and in recent years numerous protocols have been introduced for addressing the problems of routing, reviewed in later sections. These protocols are divided into two broad classes – Reactive and Proactive [3]. In Reactive or on-demand RPs the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On-demand Distance Vector Routing Protocol (AODV). Wherein Proactive or Table-driven RPs the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and Destination Sequenced Distance Vector Protocol (DSDV). All these protocols are quite insecure because attackers can easily obtain information about the network topology [4]. In Section 2, first we focus on security aspects of MANET Routing Protocols and later in Section 3 we will present classification of the existing RPs, their types and review their characteristics. It also explores some of the proposed secure Routing Protocols, and Section

4 gives the qualitative comparison of their characteristics & categorizes them accordingly to their routing strategies & relationships [5]. Section 5 shows some assumptions in form of a chart based on the performance of Routing Protocols in terms of mobility and network size.

III. Classification of Routing Protocols

We will discuss the classification of existing wireless ad hoc routing protocols, their characteristic features & types. The Routing Protocols for ad hoc wireless networks can be divided into three categories based on the routing information update mechanism. They could be Reactive (On-demand), Proactive (Table-driven) or Hybrid [6]−[15]. Figure 2 shows the three categories of Ad hoc RPs and various proposed Protocols under each category [7, 8, 9]. The table-driven ad hoc routing approach is similar to the connectionless approach of forwarding packets, with no regard to when and how frequently such routes are desired.

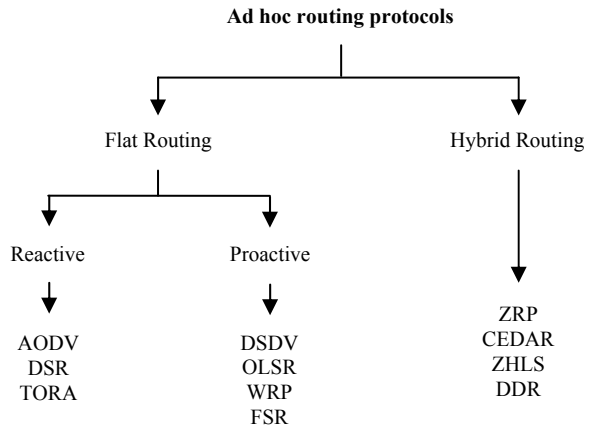

Fig. 2. Classification of Ad hoc Routing Protocols

This is not the case, however, for on-demand routing protocols. When a node using an on-demand protocol desires a route to a new destination, it will have to wait until such a route can be discovered. On the other hand, because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed [10]. In this paper we have presented a critical analysis of the above mentioned secure routing protocols. First we present a comparison between the two broad classes of routing protocols based on their routing methodology and other network parameters shown in Table 3.

IV. Proactive Protocols

These protocols always maintain up-to-date information of routes from each node to every other nodein the network. These protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. Different protocols keep track of different routing state information [11]. These protocols require each node to maintain one or more tables to store up to date routing information and to propagate updates throughout the network. As such, these protocols are often also referred to as table-driven. These protocols try and maintain valid routes to all communication mobile nodes all the time, which means before a route is actually needed. Periodic route updates are exchanged in order to synchronize the tables. Some examples of table driven ad hoc routing protocols include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV) [12], Optimized Link State Routing Protocol (OLSR) [13] and Wireless Routing Protocol (WRP) [14]. These protocols differ in the number of routing related tables and how changes are broadcasted in the network structure.

A. DSDV

DSDV is proposed by Perkins and Bhagwat. The Destination-Sequenced Distance-Vector (DSDV) [14] Routing protocol is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements such as making it loop-free. The distance vector routing is less robust than link state routing due to problems such as count to infinity and bouncing effect. In this, each device maintains a routing table containing entries for all the devices in the network. In order to keep the routing table completely updated at all the time each device periodically broadcasts routing message to its neighbor devices. When a neighbor device receives the broadcasted routing message and knows the current link cost to the device, it compares this value and the corresponding value stored in its routing table. If changes were found, it updates the value and re-computes the distance of the route which includes this link in the routing table.

B. OLSR

Clausen and Jacquet proposed the Optimized Link State Protocol, a point-to-point proactive protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying [16, 17]. It optimizes the pure link state routing protocol. Optimizations are done in two ways: by reducing the size of the control packets and by reducing the number of links used for forwarding the link state packets. Here each node maintains the topology information about the network by periodically exchanging link-state messages among the other nodes. OLSR is based on the following three mechanisms: neighbor sensing, efficient flooding and computation of an optimal route using the shortest-path algorithm. Neighbor sensing is the detection of changes in the neighborhood of node. Each node determines an optimal route to every known destination using this topology information and stores this information in a routing table. The shortest path algorithm is then applied for computing the optimal path. Routes to every destination are immediately available when data transmission begins and remain valid for a specific period of time till the information is expired.

C. WRP

The Wireless Routing Protocol, as proposed by Murthy and Garcia-Luna-Aceves [18], is a table-based protocol similar to DSDV that inherits the properties of Bellman-

Ford Algorithm. The main goal is maintaining routing information among all nodes in the network regarding the shortest distance to every destination. Wireless routing protocols (WRP) is a loop free routing protocol. WRP is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. Each node in the network uses a set of four tables to maintain more accurate information: Distance table (DT), Routing table (RT), Link-cost table (LCT), Message retransmission list (MRL) table. In case of link failure between two nodes, the nodes send update messages to their neighbors. WRP belongs to the class of path-finding algorithms with an important exception. It counters the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. This eliminates looping situations and enables faster route convergence when a link failure occurs.

D. STAR

The STAR protocol [19] is also based on the link state algorithm. Each router maintains asource tree, which is a set of links containing the preferred paths to destinations. This protocol has significantly reduced the amount of routing overhead disseminated into the network by using a least overhead routing approach (LORA), to exchange routing information. The optimum routing (ORA) approach obtainsthe shortest path to the destination while LORA minimizes the packet overhead. Garcia–Luna–Aceves and Spohn propose STAR where each node maintains a source tree which contains preferred links to all possible destinations. Nearby source trees exchange information to maintain up-to-date tables. The routes are maintained in a routing table containing entries for the destination node and the next hop neighbor. The link state update messages are used to update changes of the routes in the source trees. Since these packets do not time out, no periodic messages are required.

E. FSR

Pei et al. propose the FSR protocol [20] which takes inspiration from the ‘‘fisheye’’technique of graphic information compression proposedby Kleinrock and Stevens. When adapted to a routing table, this technique means that a node maintains accuracy distanceand path quality information about its immediate vicinity, but the amount of detail retained decreases with the distance from the node. Each node considers a number of surrounding fish-eye scopes, areas which can be reachedwith 1, 2 ... hops. FSR reduces the size of the update messages by updating the network information for nearby nodes at a higher frequency than for theremote nodes, which lie outside the fisheye scope. This makes FSR more scalable to large networks than the protocols.

F. CGSR

The Cluster head Gateway Switch Routing protocol differs from the other protocols as it uses hierarchical network topology, instead of a flat topology. As proposed by Chiang, it organizes nodes into clusters, which coordinate among the members of each cluster entrusted to a special node named cluster head. Least Cluster Change (LCC) algorithm [21] is applied to dynamically elect a node as the cluster head.Each node must keep acluster member table where it stores the destination cluster head for each mobile node in the network. These cluster member tables are broadcast by each node periodically using the DSDV algorithm. CGSR is an extension of DSDV and hence uses it as the underlying routing scheme. It has the similar overhead as DSDV. However, it modifies DSDV by using a cluster (hierarchical) routing approach to route traffic from source to destination. CGSR improves the routing performance by routing packets through the cluster heads and gateways.

Summary

In proactive protocols the topological information is exchanged among all the nodes in a network. In contrast to source initiated routing, table driven routing has extensive precedents in the research done for routing in the wired domain. Also wired routing protocols have inspired their own classes of protocolsin table driven ad hoc routing. One of these classes is the distance vector protocols where the nodes maintain only a local topology, and use the distributed Bellman-Ford algorithm to maintain the routing tables, the other class of protocols is the link state routing protocols, where the routers exchange full topology information, and then use a graph-theoretic shortest path algorithm (Dijkstra’s) on the resulting graph. However**,** these protocols differ in the way routing information is updated and detected, the number of routing tables used, the type of information stored in each table and the changes that are periodically broadcasted in the network. This class of routing protocols has its own advantages and disadvantages. One of its main advantages is the fact that nodes can easily get routing information and it‘s easy to establish a session. The disadvantage is too much data stored by the nodes for route maintenance and it is slow to restructure when there is a failure in a particular node link. TABLE 1 shows the comparison of some of the existing proactive routing protocols.

TABLE 1: COMPARISON OF PROACTIVE ROUTING PROTOCOLS

Parameters	DSDV	WRP	OLSR
Route updates	Periodic	Periodic	Periodic
Loop free	Yes	Yes	Yes
Routing overhead	High	High	Low
Caching overhead	Medium	High	High
Throughput	Low	Low	Medium
Routing tables	2	4	4

V. REACTIVE PROTOCOLS

The reactive or on-demand routing protocols are based on Query-Reply topology in which they do not attempt to continuously maintain the up-to-date topology of the network. When a route is desired, a procedure is invoked to find a route to the destination node. The major goal of on demand or reactive routing protocols is to minimize the network traffic overhead. These routing protocols are based on some type of "query-reply" dialog. They do not attempt to continuously maintain the up-to-date topology of the network. Rather, when the need arises, a reactive protocol

invokes a procedure to find a route to the destination; such a procedure involves some sort of flooding the network with the route query. As such, such protocols are often also referred to as on demand. The common element in reactive protocols is the mechanism used for discovering routes. The source node emits a request message, requesting a route to the destination node. This message is flooded, i.e. relayed by all nodes in the network, until it reaches the destination. The path followed by the request message is recorded in the message, and returned to the sender by the destination, or by intermediate nodes with sufficient topological information, in a reply message. Thus multiple reply messages may result, yielding multiple paths - of which the shortest is to be used. Some examples of source initiated ad hoc routing protocols include the Dynamic Source Routing Protocol (DSR) [22], Ad Hoc On-Demand Distance Vector Routing Protocol (AODV) [23], and Temporally-Ordered Routing Algorithm (TORA) [24].\

A. AODV

AODV is a widely accepted on-demand routing protocol in ad hoc networks proposed by C. E. Perkins and E. M. Royer. Ad hoc On-demand Distance Vector (AODV) [25] is a combination of both DSR and DSDV. It follows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. It uses destination sequence numbers to ensure loop freedom at all times and by avoiding the Bellman-Ford "count-to-infinity" problem offers quick convergence when the ad hoc network topology changes. AODV finds routes only when required and hence is reactive in nature. The major vulnerabilities present in AODV protocols are: Deceptive increase of sequence number and Deceptive decrease of hop count. Zapata [26] applies security extensions to AODV using one-way hash functions to serve metric fields in Route Request (Route Discovery). He introduced Secure-AODV (SAODV) [27] where he suggests using digital signatures to authenticate non-mutable data in an end-to-end manner. Hash chains are used to secure mutable fields such as hop count. It is an extension to AODV Routing Protocol. It is used to protect Route Discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation [28]. AODV does not repair a broken path locally. When a link breaks, which is determined by observing the periodical beacons or though ACK messages, the source and the destination nodes are notified (end nodes). The source node then reestablishes the route with the destination using higher layers. AODV does not provide any type of security.

B. TORA

The Temporally-Ordered Routing Algorithm (TORA) was developed by Park and Corson. Temporarily ordered routing algorithm **(**TORA) is highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. It uses directed acyclic graphs (DAG) to define the routes either as upstream or downstream. This graph enables TORA to provide better route aid for networks with dense, large population of nodes [28]. However to provide this feature TORA needs synchronization of the nodes which limits the application of the protocol. TORA is a fairly complicated protocol but what makes it unique and prominent is its main feature of propagation of control messages only around the point of failure when a link failure occurs. In comparison, all the other protocols need to re-initiate a route discovery when a link fails but TORA would be able to patch itself up around the point of failure. This feature allows TORA to scale up to larger networks but has higher overhead for smaller networks. TORA involves four major functions: creating, maintaining, erasing and optimizing routes. Since every node must have a height, any node which does not have a height is considered as an erased node and its height is considered as null. Sometimes the nodes are given new heights to improve the linking structure. This function is called optimization of routes.

C. DSR

DSR is an on-demand protocol designed by D. B. Johnson, Maltz and Broch to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols. The distinguishing feature of Dynamic Source Routing (DSR) [29] is the use of source routing. DSR is a reactive protocol i.e. it doesn't use periodic updates. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. There are two basic parts of DSR protocol: route discovery and route maintenance. Every node maintains a cache to store recently discovered paths. When a node wants to send a packet, it first checks the cache whether there is an entry for that. If yes then it uses that path to transmit the packet. Also it attaches its source address on the packet. If there is no entry in the cache or the entry is expired, the sender broadcasts a route request packet to all its neighbors asking for a path to the destination. Until the route is discovered, the sender host waits. When the route request packet arrives to any other nodes, they check whether they know the destination asked. If they have route information, they send back a route reply packet to the destination. Otherwise they broadcast the same route request packet. Once the route is discovered, the sender will send its required packets using the discovered route as well as insert an entry in the cache for future use. Also the node keeps the age information of the entry to recognize whether the cache is fresh or not. When any intermediate node receives a data packet, it first sees whether the packet is sent to itself or not. If it is the destination, it receives that else it forwards the packet using the path attached on the packet.

D. LAR

Location-Aided Routing (LAR) protocol is proposed by Ko and Vaidya [30]. It is based on flooding algorithms such as DSR. The goal of LAR is to reduce the routing overhead by the use of location information. Position information will be used by LAR for restricting the flooding to a certain area. LAR is a reactive protocol which is based on the DSR. This

Routing Protocol uses location information to diminish routing overhead of the mobile ad-hoc network. In the LAR routing technique, *RouteRequest* and *RouteReply* packets similar to DSR and AODV are being proposed. When using LAR, any node needs to know its physical location by using the Global Positioning System (GPS). LAR designates two geographical regions for selective forwarding of control packets, namely, Expected Zone and Request Zone. The request zone is fixed from the source, and nodes which are not in the request zone do not forward a *Route Request* to their neighbors. The source or an intermediate node will forward the message to all nodes that are closer to the destination than the node itself. The Expected Zone is the region in which the destination node is expected to be present.LAR uses flooding. The nodes decide to forward or discard the control packets based on two algorithms, LAR1 and LAR2 described in [31].

E. ARA

Gunes et al. [32] present a novel technique for ad hoc routing by using concepts of swarm intelligence and the ant colonymeta-heuristic. This class of algorithms aims to solve thecomplex optimization and collaboration problems withoutdirect communication among the participants. Indirect communication is achieved by stigmergy, the process ofleaving traces in the environment, similar to the behaviorof ants leaving pheromone signals. Route discovery is done by flooding a forward ant to the destination, similar to Route Request in AODV. Duplicate packetsare identified by the use of a sequence number and are deleted bysystem. When a route is found to the destination, a backward ant is created similar to Route Reply in AODV. The backward ant follows the path with the shortest trip time detected by theforward ant. The amount of pheromone deposited by both ants is a function of route length associated with pheromone. The route maintenance phase is responsible for updating the routinginformation during the communication. The algorithm updatesboth the forward and the backward path with an equal amount ofpheromone (presumed as 0.1). ARA also allows for theevaporation of pheromones [33]. ARA achieves loop free paths using sequence numbers. If a nodereceives a duplicate packet, it sets the DUPLICATE_ERROR flag and returns the packet to the previousnode, and removes the link. According to Gunes et al ARA performs comparatively better in terms of overhead ratio and delivery rate.

F. CBRP

In Cluster Based Routing Protocol (CBRP), unlike the on-demand routing protocols, the nodes are organized in a hierarchy [34]. The nodes in CBRP are grouped into clusters. Eachcluster has a cluster-head, which coordinates the data transmission within the cluster and to otherclusters. The advantage of CBRP is that only cluster heads exchange routing information, therefore the number of control overhead transmitted through the network is far less than the traditional flooding methods. The protocol suffers from temporaryrouting loops. This is because some nodes may carry inconsistent topology information due to long propagation delay.

G. DYMO

DYMO (Dynamic MANET On-demand) routing protocol is newly intended for use by mobile nodes in wireless multi-hop networks [35]. MANET working group uses it as the current research in on-demand routing issue. DYMO is a descendant of the design of MANET reactive protocols, such as AODV and DSR. The basic operations of the DYMO protocol are route discovery and route management. During route discovery, the originating node initiates dissemination of a Route Request (RREQ) throughout the network to find the target node. When the target node receives the RREQ, it responds with a Route Reply (RREP) unicast toward the originating node. When the originating node receives the RREP, routes have then been established between the originating node and the target node in both directions. RERR is sent to the packet source to indicate the current route is broken. Once the source receives the RERR, it can perform route discovery. DYMO uses sequence numbers as they have been proven to ensure loop freedom. In addition, DYMO protocol can be used both in IPv4 and IPv6 network and people may use it to connect with the Internet. It can adapt to changes of the network topology, and establish a unicast route between the target node and the originating node. The DYMO routing protocol is successor to the popular Ad hoc On-Demand Distance Vector (AODV) routing protocol and shares many of its benefits. DYMO protocol has the similar basic functions and operations to AODV. As a reactive protocol, DYMO does not explicitly store the network topology. Instead, nodes compute a unicast route towards the desired destination only when needed. As a result, little routing information is exchanged, which reduces network traffic overhead and thus saves bandwidth and power. DYMO is applicable to memory constrained devices. AODV supports unicast, multicast and broadcast. The DYMO only supports unicast routing established between the on-demand nodes in the network [36]. DYMO routing protocol with excellent performance is simple, compact, easy to implement and highly scalable characteristics, and is a very promising protocol.

Summary

Reactive routing is best adapted to the most challenging incarnations of the adhoc networks. Their major goal is to minimize the network traffic overhead. The baseline for this class of protocols is set by AODVand DSR; both of them have several independent implementationsfor various operating systems. The common elements in reactive protocols are the mechanisms used for discovering and maintaining routes. The source node emits a request message for requesting a route to the destination node. This message is then flooded, i.e. forwarded by all nodes in the network, until it reaches the destination. The path followed by the request message is recorded and returned to the sender by the final destination, or by intermediate nodes with sufficient topological information. Thus there exist multiple reply messages which yield to multiple paths from source to destination node, of which the shortest is chosen. No periodic updates are required for these protocols but the routing information is only available when needed. However, this class of routing protocols is bandwidth efficient as compared to its counterpart i.e. proactive. Route

is built as and when it is desired by sending route requests across the network. But still there are few disadvantages with this class also. One of them is that a large amount of time is wasted finding routes. The other disadvantage is in case of excessive flooding, there might be a possibility of network clog. TABLE 2 shows the comparison of some of the existing reactive routing protocols.

TABLE 2: COMPARISON OF REACTIVE ROUTING PROTOCOLS

Parameters	AODV	DSR	TORA
Route Creation	By source	By source	Locally
Periodic updation	No	No	No
Performance Metrics	Speed	Shortness	Speed
Routing overhead	High	High	High
Caching overhead	Low	High	Medium
Throughput	High	Low	Low
Multipath	No	Yes	Yes
Route updation	Non-periodic	Non-periodic	High routing overhead

VI. HYBRID ROUTING PROTOCOLS

These protocols try to incorporate various aspects of proactive and reactive routing protocols. They are generally used to provide hierarchical routing; routing in general can be either flat or hierarchical. The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption. Some examples of Hybrid Routing Protocols include CEDAR [37], ZRP [38] and SRP [39]. In what follows, we present a few of the proposed routing protocols from each class developed for the ad hoc networks. The most important protocols and those which dominate recent literature are AODV, DSR, SRP, ZRP, DSDV and TORA.

A. ZRP

Haas and Pearlman proposed Zone Routing Protocol. ZRP [40] is a hybrid routing protocol for mobile ad hoc networks which localizes the nodes into sub-networks (zones). It incorporates the merits of on-demand and proactive routing protocols. Within each zone, proactive routing is adapted to speed up communication among neighbors. The inter-zone communication uses on-demand routing to reduce unnecessary communication. The network is divided into routing zones according to distances between mobile nodes. Given a hop distance *d* and a node N, all nodes within hop distance at most *d* from N belong to the routing zone of N. Peripheral nodes of N are N's neighboring nodes in its routing zone which are exactly *d* hops away from N. An important issue of zone routing is to determine the size of the zone. An enhanced zone routing protocol, Independent Zone Routing (IZR), which allows adaptive and distributed reconfiguration of the optimized size of zone, is introduced in [41]. Furthermore, the adaptive nature of the IZR enhances the scalability of the ad hoc network. Every node periodically needs to update the routing information inside the zone. Additionally, some local route optimization is performed at each node, which includes the following actions: removal of redundant routes, shortening of routes, detecting of link failures.

B. ZHLS

ZHLS is based on hierarchical structure in which the network is divided into non-overlapping zones. According to Joa and Lu [42], each node is assigned one unique node ID and a zone ID, which are calculated using geographical information. Hence the network follows a two-level topology structure: node level and zone level. Respectively, there are two types of link state updates: the node level LSP (Link State Packet) and the zone level LSP. A node level LSP contains the node IDs of its neighbors in the same zone and the zone IDs of all other zones. A node periodically broadcast its node level LSP to all other nodes in the same zone. Therefore, through periodic node level LSP exchanges, all nodes in a zone keep similar node level link state information. Before transmission, the source node first checks its intra-zone routing table. If the destination lies in its zone, the routing information is already present. Otherwise, the source sends a location request to all other zones through gateway nodes, which in turn replies with a location response containing the zone ID of the desired destination. The header of the data packets originated from the source contains the zone ID and the node ID of the destination node. ZHLS has a low routing overhead as compared to AODV and DSR. Also the routing path is adaptable to the dynamic topology as only node ID and zone ID are required for routing. So as long as the destination remains in the zone no further search is required.

C. CEDAR

Core Extraction Distributed Ad hoc Routing (CEDAR) proposed by Sivakumar, Sinha and Bharghavan [43] is a partitioning protocol, integrates routing with QoS support. Each partition includes a core node called dominator node. A Dominator set (DS) of a graph is defined as a set of nodes in the graph such that every node is either present in DS or is a neighbor of some node present in DS. The core nodes use a reactive source routing protocol to outline a route from a source to a destination. CEDAR has three key phases:

1. The establishments and maintenance of self-organizing routing infrastructure (core) for performing route computations
2. The propagation of the link-states of high-bandwidth and stable links in the core
3. A QoS route computation algorithm that is executed at the core nodes using only locally available state.

QoS routing in CEDAR is achieved by propagating the bandwidth availability information of stable links in the core sub-graph. To propagate the link information, slow-moving increase-waves and fast moving decrease waves are used, which denotes increase of bandwidth and decrease of bandwidth respectively.

D. DDR

Nikaein et al. [44] propose a tree-based routing protocol without the need of a root node. In this strategy tree are constructedusing periodic beaconing messages, whichis exchanged by neighboring nodes only. These trees within the network form a forest withthe created gateway nodes acting as links between the treesin the forest. These gateway

nodes are regular nodesbelonging to separate trees but within transmission rangeof each other. A zone naming algorithm is used to assign aspecific zone ID to each tree within the network. Hence,the overall network now comprises of a number of overlappingzones The DDR algorithm comprise of the following sixphases: (i) preferred neighbor election; (ii) intra-tree clustering; (iii) inter-tree clustering; (iv) forest construction; (v) zone naming; and (vi) zone partitioning. To determine routes, hybrid ad hoc routing protocols (HARP) [45] is used. HARP uses the intra-zone and inter-zone routing tables created by DDR to determine a stable path between the source and the destination. The advantage of DDR is that unlike ZHLS, it does not rely on a static zone map to perform routing and it does not require a root node or a cluster-head to coordinate data and control packet transmission between different nodes and zones.

E. DST

The nodes in the network are grouped into a number of trees [46]. Each tree has two types of nodes; route node, and internal node. The root controls the structure of the tree and whether the tree can merge with another tree, and the rest of the nodes within eachtree are the regular nodes. Each node can be in one three different states; router, merge and configure depending on the type of task that it trying toperform. DST proposes two strategies to determine a route between a source and a destination pair:

Hybrid Tree Flooding (HTF): In this scheme, the sourcesends the control packets to all the neighbors and adjoining bridges in the spanning tree. Each packet is remained static at these places for a specific holding time.

Distributed Spanning Tree (DST) shuttling: In this approach, the source sends the control packets to the tree edges till each of them reaches a leaf node. When a packet reaches the leaf node, it is forwarded to a shuttling level.

The drawback with such architecture is the existence of a single point of failure for the entire tree. If the root node fails, the entire routing structure falls apart. Furthermore, the holding time used to buffer the packets may introduce extra delays in to the network.

Summary

Hybrid protocols are a new generation of protocols, a combination of both proactive and reactive protocols. They have the potential toprovide higher scalability than pure reactive orproactive protocols. Another noveltyof hybrid routing protocols is that they attempt toeliminate single point of failures and creating bottleneck nodes in the network. This is achieved by allowing any number of nodes to performrouting or data forwarding if the preferred pathbecomes unavailable. They are generally used to provide hierarchical routing. The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. These protocols have the great potential to provide higher scalability than the other two classes. They attempt to minimize the number of re-broadcasting nodes by defining a zone, which allows the nodes to work together. The best or most suitable nodes can then be used to perform route discovery. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which requires more memory and power consumption. Out of these ZRP combines the best features of both reactive and proactive routing protocols. TABLE 3 shows the comparison of some of the existing hybrid routing protocols.

TABLE 3: COMPARISON OF HYBRID ROUTING PROTOCOLS

Parameters	ZRP	ZHLS	DST	DDR
Routing Structure	Flat	Hierarchical	Hierarchical	Hierarchical
Multiple routes	No	Yes	Yes	Yes
Beacons	Yes	No	No	Yes
Route information stored in	Intrazone & Interzone tables	Intrazone & Interzone tables	Route tables	Intrazone & Interzone tables
Route metric	Shortest path	Shortest path	Forwarding using the tree neighbors	Stable routing
Advantage	Reduced transmissions	Low control overhead	Reduced transmission	No zone coordinator or zone map
Dis-advantage	Overlapping zones	Static zone map required	Root node	Neighbors may become bottlenecks

TABLE 4: COMPARISON BETWEEN THE THREE CATEGORIES OF ROUTING PROTOCOLS

Parameters	Table-Driven (Proactive)	On-Demand (Reactive)	Hybrid
Storage Requirements	Higher	Dependent on no. of routes maintained or needed	Depends on size of each zone or cluster
Route Availability	Always available	Computed as per need	Depends on location of destination
Periodic Route Updates	Required always	Not required	Used inside each zone
Delay	Low	High	Low for local destinations and high for Interzone
Scalability	100 nodes	> 100	> 1000
Control Traffic	High	Low	Lower that other two types
Routing Information	Keep stored in table	Doesn't store	Depends on requirement
Routing Philosophy	Mostly flat	Flat	Hierarchical

VII. COMPARISON OF PROTOCOLS

In this section we have presented a comparison between existing routing protocols. TABLE 4 below provides an overall comparison of the three categories of routing protocols. The comparisons basically consider the characteristic properties of routing protocols in high load networks. In order to make flat addressing more efficient, the number of routing overheads introduced in the networks

must be reduced. The hybrid routing protocols employ both reactive and proactive properties bymaintaining intra-zone information proactively and inter-zone information reactively. Another way to reduce routing overheads is by using conditional updates ratherthan periodic ones. In on-demand routing protocols, the flooding-based routing protocols such as DSRand AODV will also have scalability problems. In order to increase scalability, the route discovery and route maintenance must be controlled. Hybrid routing protocols such as the ZHLS may also perform well in large networks. ZRP is another hybrid routing protocol which is designed to increase the scalability of MANETs.It maintains strong network connectivity (proactively) within the routing zones while determining remote route (outside the routing zone) quicker than flooding. Also it can incorporate other protocols to improve its performance. Although newer protocols have built upon the earlier ones, we cannot identify a single best protocol. Table 4 shows the comparison of all the three categories of ad hoc routing protocols.

VIII. Conclusion

In this paper, we have presented and discussed the taxonomy of routing protocols in mobile ad hoc networks and provided comparisons between them. The protocols are divided into three main categories: (i) source-initiated (reactive or on-demand), (ii) table-driven (pro-active), (iii) hybrid protocols. For each of these classes, we reviewed and compared several representative protocols. While there are still many challenges facing Mobile ad hoc networks related to routing and security. Each routing protocol has unique features. Based on network environments, we have to choose the suitable routing protocol. The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. The main differentiating factor between the protocols is the ways of finding and maintaining the routes between sourcedestination pairs. The comparison we have presented between the routing protocols indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem against the existing security solutions. We hope that the taxonomy presented in this paper will be helpful and provide researchers a platform for choosing the right protocol for their work. At last we have provided the overall characteristic features of all routing protocols and described which protocols may perform best in large networks.Almost all the protocols we discussed in this paper have their own characteristic features and performance parameter combinations where they outperformtheir competitors. Still mobile ad hoc networks have posed a great challenge for the researchers due to changing topology and security attacks, and none of the protocols is fully secured and research is going on around the globe.

Acknowledgement

The authors wish to thank the reviewers and editors for their valuable suggestions and expert comments that help improve the contents of paper.

References

[1] A. K. Gupta and H. Sadawarti, "Secure Routing Techniques for MANETs," "*International Journal of Computer Theory and Engineering"*, vol. 1 no. 4, pp. 456-460, October 2009.
[2] C. E. Perkins, "*Ad hoc Networking*", Pearson Publication.
[3] P. G. Argyroudis and D. O'mahony, University Of Dublin, Trinity College, "*Secure Routing for Mobile Ad hoc Networks*".
[4] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, "*in Proceedings of ACM MOBICOM'02"*, 2002.
[5] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," "*EEE Network Magazine"* vol. 13, no.6, November/December 1999.
[6] A. K. Gupta, H. Sadawarti, and A. K. Verma, "A Review of Routing Protocols for Mobile Ad Hoc Networks," ""*SEAS Transactions on Communications"***,** ISSN: 1109-2742**,** Issue 11 Vol.10, November 2011, pp. 331-340.
[7] P. Papadimitratos and Z. J. Haas. "Secure routing for mobile ad hoc networks," "*SCS Communication Networks and Distributed Systems Modeling and Simulation Conference* (CNDS 2002)", Jan 2002.
[8] M. Zapata, N. Asokan, "*Securing ad hoc routing protocols*", WiSe'02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.
[9] E. M. Royer and Chai-Keong Toh, "*A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks*".
[10] N. S. Yadav and R.P. Yadav "Performance Comparison and Analysis of Table- Driven and On- Demand Routing Protocols for Mobile Ad-hoc Networks," "*International Journal of Information Technology"*, vol.4, no. 2, pp 101-109, 2007
[11] A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D.Turgut, "Routing protocols in ad hoc networks: A survey," "*Elsevier Computer Networks"*, 55 (2011) 3032–3080.
[12] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) for Mobile Computers," "*Proc. ACM Conf. Communications Architectures and Protocols"*, London, UK, August 1994, pp. 234-244.
[13] T. H. Clausen et al., "The Optimized Link-State Routing Protocol. Evaluation through Experiments and Simulation," "*Proc. IEEE Symp. Wireless Personal Mobile Communications 2001*", Sept. 2001.
[14] S. Murthy, C. Siva Ram and B.S. Manoj, "*Ad Hoc Wireless Networks: Architectures and Protocols*," Prentice Hall, Chapter 7, 2004.
[15] T. A.Wysocki, A. Dadej, and B. J. Wysocki , "Secure routing protocols for mobile ad-hoc wireless networks," "*in Advanced Wired and Wireless Networks*", Eds. Springer, 2004.
[16] L. Abusalah, A. Khokhar and M. Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", "*IEEE Communications Surveys & Tutorials"*, vol. 10 no. 4, 4th Quarter 2008.
[17] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, L.Viennot, "Optimized link state routing protocol for ad hoc networks," in: "*Proceedings of IEEE INMIC"*, December 2001, pp. 62–68.
[18] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," "*ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks"*, Oct. 1996, pp. 183–97.
[19] J. J. Garcia-Luna-Aceves, C. M. Spohn, "Source-tree routing in wireless networks," in: "*Proceedings of the Seventh Annual International Conference on Network Protocols Toronto"*, Canada, October 1999, p. 273.
[20] G. Pei, M. Gerla, T.-W. Chen, "Fisheye state routing in mobile ad hoc networks," in: "*Proceedings of IEEE ICDCS Workshop on Wireless Networks and Mobile Computing"*, April 2000, pp. D71–D78.
[21] J. Luo, D. Ye, X. Liu, and M. Fan, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks," "*IEEE Communications Surveys & Tutorials"*, vol. 11, no. 1, First Quarter 2009.
[22] D. B. Johnson, D. A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," "*Ad Hoc Networking, C.E. Perkins"*, Ed., Addison-Wesley, 2001, 139-172.
[23] C. E Perkins, E. M. Royer, and S. Das, "*Ad hoc On-demand Distance Vector (AODV)*," RFC 3561, July 2003.
[24] P. Papadimitratos and Z. J. Haas. "Secure routing: Secure Data Transmission in Mobile Ad Hoc Networks," "*Proc. ACM Wksp. Wireless Security 2003"*, Sept. 2003, pp. 41-50.

[25] H. Dang, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," "*IEEE Communications Magazine"*, 0163-6804, pp. 70-75, October 2002.
[26] M. Zapata, N. Asokan, "Securing ad hoc routing protocols", WiSe'02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.
[27] M. G. Zapata. "Secure ad hoc on-demand distance vector (SAODV) routing," IETF MANET Mailing List, ftp://MANET.itd.nrl.navy.mil/pub/ MANET/2001-10.mail, October 8, 2001.
[28] A. K. Gupta, H. Sadawarti, and A. K. Verma, "Performance analysis of AODV, DSR & TORA Routing Protocols," "*IACSIT International Journal of Engineering and Technology*", vol.2, vo.2, April 2010.
[29] D. B. Johnson, D.A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," *"Ad Hoc Networking"*, C.E. Perkins, Ed., Addison-Wesley, 2001, 139-172.
[30] Y.-B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," "*in Mobile Computing and Networking (MOBICOM'98)*", Dallas, TX, USA, 1998, pp. 66–75.
[31] M. Mauve, J. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad-hoc networks," "*IEEE Network Magazine"*, vol. 15, no. 6, pp. 30–39, November 2001.
[32] M. Gunes, U. Sorges, and I. Bouazizi, "ARA -the ant-colony based routing algorithms for manets," in: "*Proceedings of IEEE ICPP Workshop on Ad Hoc Networks (IWAHN)*", August 2002, pp. 79–85.
[33] A. K. Gupta, A. K. Verma, and H. Sadawarti, "Analysis of various Swarm-based & Ant-based Algorithms," "*Proceedings of International Conference on Advances in Computing and Artificial Intelligence* (ACAI 2011)", an ACM Chapter Event, Chitkara University, Punjab, 21-22 July 2011, pp – 39-43.http://dl.acm.org/citation.cfm?id=2007052
[34] M. Jiang, J. Ji, Y. C. Tay, Cluster based routing protocol, Internet Draft, draft-ietf-manet-cbrp-spec-01.txt, work in progress, 1999
[35] Chakeres, C. Perkins, Dynamic MANET On-demand (DYMO) Routing, RFC draft, Boeing, Nokia, February 2008.
[36] R. E. Thorup "Implementing and Evaluating the DYMO," February 2007.
[37] A. A. Pirzada, C. McDonald and A. Datta, "Performance Comparison of trust-based Reactive Routing Protocols," "*IEEE Trans. Mobile Computing"*, vol. 5, issue 6, June 2006, pp. 695-710.
[38] Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of the Zone Routing Protocol," "*IEEE/ACM Transactions on Networking"*, vol. 9, no. 4, pp. 427-438, Aug 2001.
[39] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," *"in Proceedings of the International Conference on Network Protocols (ICNP)"*, pp. 78-87, 2002.
[40] Z. J. Haas and M. R. Pearlman, .ZRP: a hybrid framework for routing in ad hoc networks, pp. 221.253, 2001.
[41] P. Samar, M. R. Pearlman, and Z. J. Haas, "Independent zone routing: an adaptive hybrid routing framework for ad hoc wireless networks," "*in IEEE/ACM Transactions on Networking (TON)"*, vol. 12, 2004, pp. 595.608.
[42] M. Joa-Ng, I.-T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," "*IEEE Journal on Selected Areas in Communications* 17 (8) (1999) 1415–1425".
[43] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm," "*IEEE Journal on Selected Areas in Communications"*, vol 17, no 8, August 1999.
[44] N. Nikaein, H. Labiod, and C. Bonnet, "DDR: distributed dynamic routing algorithm for mobile ad hoc networks," in: "*Proceedings of ACM MobiHoc"*, August 2000, pp. 19–27.
[45] N. Nikaein, C. Bonnet, and N. Nikaein, "Harp-hybrid ad hoc routing protocol," in: *Proceedings of IST: "International Symposium on Telecommunications"*, September 1–3 Tehran, Iran, 2001.
[46] S. Radhakrishnan, N. Rao, G. Racherla, C. Sekharan, and S. Batsell, "DST – a routing protocol for ad hoc networks using distributed spanning trees," in: "*Proceedings of IEEE WCNC"*, September 1999, pp. 100–104.

Anuj K. Gupta is a research fellow in Punjab Technical University, Punjab, India. His research area is Mobile ad hoc networks, wireless networks & Data Communication. He has a teaching experience of above 10 years. Currently he is working as faculty in CSE Dept. at RIMT-IET, Punjab. He is a member of IACSIT. (email: seekanuj@gmail.com).

Dr. Harsh Sadawarti is Director at RIMT-IET, Punjab, India. He has a vast teaching and research experience of more than 20 years in the field of computer science. His areas of research are ad hoc networks, parallel computing & Distributed systems. He is a member of IEEE. (email: harshsada@yahoo.com).

Dr. Anil K. Verma is faculty in Computer Sci. &Engg. Dept. at Thapar University, Patiala, Punjab, India. He has a vast teaching & research experience of more than 20 years. His areas of research are mobile ad hoc networks, wireless sensor networks & Network Security. (email: akverma@thapar.edu).