This is a draft version only.

Wireless Ad Hoc Networks

Zygmunt J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos, and S. Sajama
Cornell University
School of Electrical and Computer Engineering
323 Rhodes Hall
Ithaca, NY 14853
Tel: (607) 255-3454, Fax: (607) 255-9072
e-mail: {*haas, jing, liang, papadp, sajama*}*@ece.cornell.edu*
URL: http://www.ece.cornell.edu/~haas/wnl/html

Abstract

A mobile ad hoc network is a relatively new term for an old technology - a network that does not rely on pre-existing infrastructure. Roots of this technology could be traced back to the early 1970s with the DARPA PRNet and the SURAN projects. The new twitch is the application of this technology in the non-military communication environments. Additionally, the research community has also recently addressed some extended features of this technology, such as multicasting and security. Also numerous new solutions to the "old" problems of routing and medium access control have been proposed. This survey attempts to summarize the state-of-the-art of the ad hoc networking technology in four areas: routing, medium access control, multicasting, and security. Where possible, comparison between the proposed protocols is also discussed.

Keywords: ad hoc networks, MANET, MAC protocols for ad hoc network, routing protocols for ad hoc networks, proactive routing protocols, reactive routing protocols, hybrid routing protocols, multicasting for ad hoc networks, security for ad hoc networks,

1. Introduction[1]

1.1 The Notion of the Ad Hoc Networks

A Mobile Ad Hoc Network (MANET) is a network architecture that can be rapidly deployed without relying on pre-existing fixed network infrastructure. The nodes in a MANET can dynamically join and leave the network, frequently, often without warning, and possibly without disruption to other nodes' communication. Finally, the nodes in the network can be highly mobile, thus rapidly changing the node constellation and the presence or absence of links. Examples of the use of the MANETs are:

- tactical operation - for fast establishment of military communication during the deployment of forces in unknown and hostile terrain;
- rescue missions - for communication in areas without adequate wireless coverage;
- national security - for communication in times of national crisis, where the existing communication infrastructure is non-operational due to a natural disaster or a global war;

[1] Perkins, Charles E., AD HOC NETWORKING, pp.221-225, © 2001 Addison Wesley Longman, Inc. Reprinted by permission of Pearson Education, Inc.

- law enforcement - for fast establishment of communication infrastructure during law enforcement operations;
- commercial use - for setting up communication in exhibitions, conferences, or sales presentations;
- education - for operation of wall-free (virtual) classrooms; and
- sensor networks - for communication between intelligent sensors (e.g., MEMS[2]) mounted on mobile platforms.

Nodes in the MANET exhibit nomadic behavior by freely migrating within some area, dynamically creating and tearing down associations with other nodes. Groups of nodes that have a common goal can create formations (clusters) and migrate together, similarly to military units on missions or to guided tours on excursions. Nodes can communicate with each other at any time and without restrictions, except for connectivity limitations and subject to security provisions. Examples of network nodes are pedestrians, soldiers, or unmanned robots. Examples of mobile platforms on which the network nodes might reside are cars, trucks, buses, tanks, trains, planes, helicopters or ships.

MANETs are intended to provide a data network that is immediately deployable in arbitrary communication environments and is responsive to changes in network topology. Because ad-hoc networks are intended to be deployable anywhere, existing infrastructure may not be present. The mobile nodes are thus likely to be the sole elements of the network. Differing mobility patterns and radio propagation conditions that vary with time and position can result in intermittent and sporadic connectivity between adjacent nodes. The result is a time-varying network topology.

MANETs are distinguished from other ad-hoc networks by rapidly changing network topologies, influenced by the network size and node mobility. Such networks typically have a large span and contain hundreds to thousands of nodes. The MANET nodes exist on top of diverse platforms that exhibit quite different mobility patterns. Within a MANET, there can be significant variations in nodal speed (from stationary nodes to high-speed aircraft), direction of movement, acceleration/deceleration or restrictions on paths (e.g., a car must drive on a road, but a tank does not). A pedestrian is restricted by built objects while airborne platforms can exist anywhere in some range of altitudes. In spite of such volatility, the MANET is expected to deliver diverse traffic types, ranging from pure voice to integrated voice and image, and even possibly some limited video.

1.2. The Communication Environment and the MANET Model

The following are a number of assumptions about the communication parameters, the network architecture, and the network traffic in a MANET.

- Nodes are equipped with portable communication devices. Lightweight batteries may power these devices. Limited battery life can impose restrictions on the transmission range, communication activity (both transmitting and receiving) and computational power of these devices.
- Connectivity between nodes is **not** a transitive relation; i.e., if node *A* can communicate directly with node *B* and node *B* can communicate directly with node *C,* then node *A* **may**

[2] **M**icro-**E**lectro-**M**echanical-**S**ystems

not, necessarily, be able to communicate directly with node *C.* This leads to *the hidden terminal problem* [Tob75].

- A hierarchy in the network routing and mobility management procedures could improve network performance measures, such as the latency in locating a mobile. However, a physical hierarchy may lead to areas of congestion and is very vulnerable to frequent topological reconfigurations.
- We assume that nodes are identified by fixed IDs (based on IP [Pos81] addresses, for example).
- All the network nodes have equal capabilities. This means that all nodes are equipped with identical communication devices and are capable of performing functions from a common set of networking services. However, all nodes do not necessarily perform the same functions at the same time. In particular, nodes may be assigned specific functions in the network, and these roles may change over time.
- Although the network should allow communication between **any** two nodes, it is envisioned that a large portion of the traffic will be between geographically close nodes. This assumption is clearly justified in a hierarchical organization. For example, it is much more likely that communication will take place between two soldiers in the same unit, rather than between two soldiers in two different brigades.

A MANET is a *peer-to-peer* network that allows direct communication between any two nodes, when adequate radio propagation conditions exist between these two nodes and subject to transmission power limitations of the nodes. If there is no direct link between the source and the destination nodes, *multi-hop* routing is used. In multi-hop routing, a packet is forwarded from one node to another, until it reaches the destination. Of course, appropriate routing protocols are necessary to discover routes between the source and the destination, or even to determine the presence or absence of a path to the destination node. Because of the lack of central elements, distributed protocols have to be used.

The main challenges in the design and operation of the MANETs, compared to more traditional wireless networks, stem from the lack of a centralized entity, the potential for rapid node movement, and the fact that all communication is carried over the wireless medium. In standard cellular wireless networks, there are a number of centralized entities (e.g., the base-stations, the Mobile Switching Centers (MSCs), the Home Location Register (HLR), and the Visitor Location Register (VLR)). In ad-hoc networks, there is no preexisting infrastructure, and these centralized entities do not exist. The centralized entities in the cellular networks perform the function of coordination. The lack of these entities in the MANETs requires distributed algorithms to perform these functions. In particular, the traditional algorithms for mobility management, which rely on a centralized HLR/VLR, and the medium access control schemes, which rely on the base-station/MSC support, become inappropriate.

All communications between all network entities in ad-hoc networks are carried over the wireless medium. Due to the radio communications being vulnerable to propagation impairments, connectivity between network nodes is not guaranteed. In fact, intermittent and sporadic connectivity may be quite common. Additionally, as the wireless bandwidth is limited, its use should be minimized. Finally, as some of the mobile devices are expected to be hand-held with limited power sources, the required transmission power should be minimized as well. Therefore, the transmission radius of each mobile is limited, and channels assigned to mobiles are typically spatially reused. Consequently, since the transmission radius is much smaller than the network span, communication between two nodes often needs to be relayed through intermediate nodes; i.e., multi-hop routing is used.

Because of the possibly rapid movement of the nodes and variable propagation conditions, network information, such as a route table, becomes obsolete quickly. Frequent network reconfiguration may trigger frequent exchanges of control information to reflect the current state of the network. However, the short lifetime of this information means that a large portion of this information may never be used. Thus, the bandwidth used for distribution of the routing update information is wasted. In spite of these attributes, the design of the MANETs still needs to allow for a high degree of reliability, survivability, availability, and manageability of the network.

Based on the above discussion, we require the following features for the MANETs:

- **Robust routing and mobility management algorithms** to increase the network's reliability and availability; e.g., to reduce the chances that any network component is isolated from the rest of the network;
- **Adaptive algorithms and protocols** to adjust to frequently changing radio propagation, network, and traffic conditions;
- **Low-overhead algorithms and protocols** to preserve the radio communication resource
- **Multiple (distinct) routes** between a source and a destination - to reduce congestion in the vicinity of certain nodes, and to increase reliability and survivability;
- **Robust network architecture** to avoid susceptibility to network failures, congestion around high-level nodes, and the penalty due to inefficient routing.

In this paper, we present a survey of techniques used to establish communications in MANETs. In particular, we concentrate on four areas: the medium access control (MAC) schemes, the routing protocols, the multicasting protocols, and the security schemes.

2. MAC-Layer Protocols for Ad Hoc Networks

Applicability of the existing MAC-layer protocol, in particular the family of the *Carrier Sense Multiple Access (CSMA),* to the radio environment is limited by the following two interference mechanisms: the *hidden terminal* and the *exposed terminal* problems.

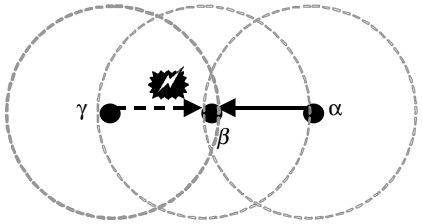

Fig. 1: An example of the *hidden terminal* problem

The *hidden terminal* problem occurs because the radio network, as opposed to other networks, such as a LAN, for instance, does not guarantee high degree of connectivity. Thus, two nodes, which maintain connectivity to a third node, do not, necessarily, can hear each other. Consider the situation in Figure 1.

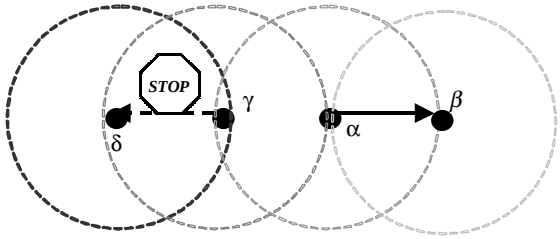

Fig. 2: An example of the *exposed terminal* problem

Node α is in communication with node β. Node α is currently transmitting. Node γ wishes to communicate with node β as well. Following the CSMA protocol, node γ listens to the medium, but since there is an obstruction between node α and node γ, node γ does not detect node' sα transmission, declaring the medium is free. Consequently, γ accesses the medium, causing collisions at β.

The second problem, the *exposed terminal* problem, is depicted in Figure 2. In the figure, node α is transmitting to node β, while node γ wants to transmit to node δ. Following the CSMA protocol, node γ listens to the medium, hears that node α transmits and defers from accessing the medium. However, there is no reason why node γ cannot transmit concurrently with the transmission of node α, as the transmission of node γ would not interfere with the reception at node β due to the distance between the two. The culprit here is, again, the fact that the collisions occur at the receiver, while the CSMA protocol checks the status of the medium at the transmitter.

In general, the *hidden terminal* problem reduces the capacity of a network due to increasing the number of collisions, while the *exposed terminal* problem reduces the network capacity due to the unnecessarily deferring nodes from transmitting.

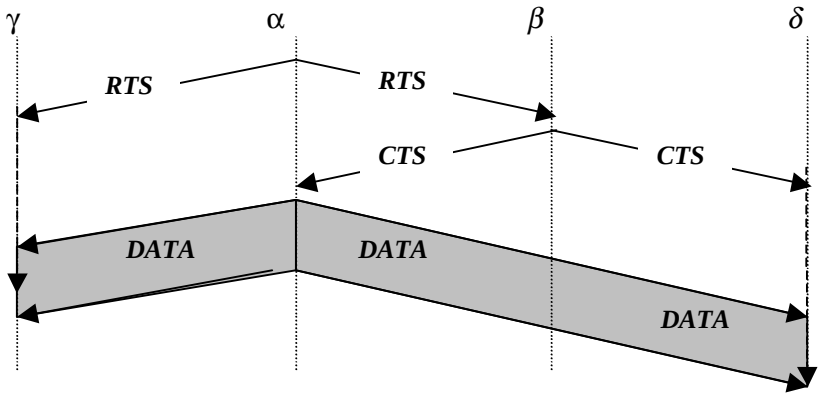

Fig. 3: The *RTS/CTS dialogue* reduces the chances of collisions

Several attempts have been made in the literature to reduce the ill effect of these two problems. The necessity of a dialogue between the transmitting and the receiving nodes that preempts the actual transmission and that is referred to as the *RTS/CTS dialogue*, has been generally accepted.

The *RTS/CTS dialogue* is depicted in Figure 3. A node ready to transmit a packet, send a short control packet, the *Request To Send (RTS),* with all nodes that hear the RTS defer from accessing the channel for the duration of the *RTS/CTS dialogue*. The destination, upon reception of the RTS responds with another short control packet, the *Clear To Send (CTS).* All nodes that hear the CTS packet defer from accessing the channel for the duration of the DATA packet transmission. The reception of the CTS packet at the transmitting node acknowledges that the *RTS/CTS dialogue* has been successful and the node starts the transmission of the actual data packet. Although the RTS/CTS dialogue does not eliminate the *hidden* and the *expose terminal* problems, it does provide some degree of improvement over the traditional CSMA schemes.

In what follows, we present a number of attempts to further improve the performance of the MAC-layer protocols for ad hoc networks.

2.1 The *Multiple Access Collision Avoidance (MACA)* scheme

In *Multiple Access Collision Avoidance (MACA)* [Kar90], Karn proposed the use of RTS/CTS dialogue for collision avoidance on the shared channel. Through the use of the RTS/CTS dialogue, the MACA scheme reduces the probability of data packet collisions caused by hidden terminals.

The RTS packet in the MACA scheme has a similar function as that of the packet preamble in the *RI-BTMA* scheme. The *RI-BTMA* scheme does not have the CTS packet because it uses a busy tone to notify the communication initiator. Since the CTS packet may suffer from packet collisions, the notification from CTS packets is not as safe as that from the busy tone in the RI-BTMA scheme. An example is the reception failure of CTS packet at some hidden nodes because of transmissions from other nodes. These hidden nodes, without receiving any CTS packet notification, may transmit new RTS packets when the CTS packet sender is receiving its data packet. This leads to data packet collisions. It is clear that additional continuous notification is necessary to protect data packets.

2.2 The *MACAW* scheme

Bharghavan [Bha94] suggested the use of the RTS-CTS-DS-DATA-ACK message exchange for a data packet transmission in the MACAW protocol. Two new control packets were added to the packet train: DS and ACK packets. When the transmitter receives the CTS packet from its intended destination, it sends out a DS (Data Sending) packet before it transmits the data packet. The DS packet notifies neighbor nodes of the fact that a RTS/CTS dialogue has been successful and a data packet will be sent. The ACK packet was implemented for immediate acknowledgment and the possibility of fast retransmission of collided data packets instead of upper-layer retransmission.

A new back-off algorithm, the Multiple Increase and Linear Decrease (MILD) algorithm, was also proposed in the paper to address the unfairness problem in accessing the shared channel. In the MILD back-off algorithm, successful nodes decrease their back-off interval by one step and unsuccessful nodes increase their back-off interval by multiplying them with 1.5. Back-off interval is also put into the header of the transmitted packet, so that the nodes overhearing successful packet transmission can copy the back-off interval on the packet into a local variable and use it (back-off copy mechanism). Compared with the Binary Exponential Back-off algorithm, the MILD algorithm has milder oscillation of the back-off intervals. Additional features of the MILD algorithm, such as multiple back-off intervals for different destinations, further improve the fairness performance of MACAW. The drawback of the MACAW scheme is inherited from the MACA scheme: the RTS/CTS packet collisions in a network with hidden terminals degrade its performance.

2.3 The *Floor Acquisition Multiple Access (FAMA)* schemes

In [Ful94], Fullmer and Garcia-Luna-Aceves proposed the *Floor Acquisition Multiple Access (FAMA)* scheme. In FAMA, each ready node has to acquire the channel (the “floor") before it can use the channel to transmit its data packets. FAMA uses both carrier sensing and RTS/CTS dialogue to ensure the acquisition of the "floor" and the successful transmission of the data packets. FAMA performs as well as MACA, when hidden terminals are present and as well as CSMA otherwise. In [Ful97], FAMA was extended to FAMA-NPS (FAMA Non-persistent Packet Sensing) and FAMA-NCS (FAMA Non-persistent Carrier Sensing). FAMA-NPS requires nodes sensing packets to back off. FAMA-NCS uses carrier sensing to keep neighbor nodes from transmitting while the channel is being used for data packet transmission. The length of the CTS packet is longer than that of the RTS packet, maintaining the dominance of CTS packets in the situation of collisions. Nodes can sense the carrier of the CTS packet when there is a collision between an RTS and a CTS packet and keep quiet; hence the data packet is protected at the receiver.

It was quantitatively shown [Ful97] that FAMA-NPS did not perform well in situations with hidden terminals present, unless multiple transmissions of the CTS packet are used. The reason is the possible packet collisions resulting from hidden terminals. FAMA-NCS, by combining the carrier sensing and floor acquisition schemes together, out-performs non-persistent CSMA and previous FAMA schemes in multi-hop networks.

The problem of the FAMA-NCS scheme is the false detection of CTS dominance. In the FAMA-NCS scheme, a node sensing the carrier of collided packets is required to keep silent for the duration of a data packet transmission even if the collisions were merely caused by RTS packets. Hence the shared channel will be idle and wasted. The false detection of CTS dominance introduces unnecessary long idle time to the shared channel, lowering the channel throughput.

2.4 The *Dual Busy Tone Multiple Access (DBTMA)* scheme

In the *Dual Busy Tone Multiple Access (DBTMA)* scheme [Haa02], in addition to the use of an RTS packet, two out-of-band busy tones are used to notify neighbor nodes of the channel status. When a node is ready to transmit, it sets up its Transmit Busy Tone and sends out an RTS packet to its intended receiver. On reception of the RTS packet, the receiver sets up a busy tone (the Receive Busy Tone) and waits for the incoming data packet. The Receive Busy Tone operates similarly to the busy tone of the RI-BTMA scheme. However, with the help of the second busy tone (the Transmit Busy Tone), the probability of RTS packets being collided is decreased and the performance is improved.

The *DBTMA* scheme completely solved the *hidden terminal* problems and the *exposed terminal* problems. It forbids the hidden terminals to send any packet on the channel while the receiver is receiving the data packet. It allows the exposed terminals to initiate transmission by sending out the RTS packets. Furthermore, it allows the hidden terminals to reply RTS packets by setting up the Receive Busy Tone and initiate data packet reception.

3. Routing Protocols for Ad Hoc Networks

Traditionally, the network routing protocols could be divided into *proactive protocols* and *reactive* protocols. Proactive 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. The early protocols that were proposed for routing in ad hoc networks were proactive Distance Vector protocols based on the *Distributed Bellman-Ford (DBF)* algorithm [Ber92]. To address the problems of the DBF algorithm - convergence and excessive control traffic, which are especially an issue in resource-poor ad hoc networks - modifications were considered (i.e., [Che89], [Gar93], and [Per94]). Another approach taken to address the convergence problem is the application of the Link State protocols to the ad hoc environment. An example of the latter is the Optimized Link State Routing protocol (OLSR) [Jac98]. Another approach taken by some researchers is the proactive Path Finding algorithms. In this approach, which combines the features of the Distance Vector and Link State approaches, every node in the network constructs a Minimum Spanning Tree (MST), using the information of the MSTs of its neighbors, together with the cost of the link to its neighbors. The Path Finding algorithms allow to reduce the amount of control traffic, to reduce the possibility of temporary routing loops, and to avoid the "counting-to-infinity" problem. An example of this type of routing protocols is the *Wireless Routing Protocol (WRP)* [Mur95] and [Mur96].

The main issue with the application of proactive protocols to the ad hoc networking environment stems from the fact, that as the topology continuously changes, the cost of updating the topological information may be prohibitively high. Moreover, if the network activity is low, the information about the actual topology is may even not be used and the investment of limited transmission and computing resources in maintaining the topology is lost.

On the other "end of the spectrum" are the *reactive* routing protocols, which are based on some type of "query-reply" dialog. Reactive protocols 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.* Examples of reactive protocols include the Temporally Ordered Routing Algorithm (TORA) [Par97], the *Dynamic Source Routing (DSR)* [Joh96], and *Ad hoc On Demand Distance Vector (AODV)* [Per99]. In *TORA*, the route replies use controlled flooding to distribute the routing information through a form of a Directed Acyclic Graph (DAG), which is rooted at the destination. The DSR and the AODV protocols, on the other hand, use unicast to route the reply back to the source of the routing query, along the reverse path of the query packet. The reversed path is "inscribed" into the query packet as "accumulated" route in the DSR and is used for source routing. In AODV, the path information is stored as the "next hop" within the nodes on the path. Although the reactive approach can lead to less control traffic, as compared with proactive Distance Vector or Link State schemes, in particular when the network activity is low and the topological changes frequent, the amount of traffic is can still be significant at times. Moreover, due to the network-wide flooding, the delay associated with reactive route discovery may be considerable as well.

So, both of the routing "extremes," the proactive and the reactive schemes, may not perform best in a highly dynamic networking environment, such as in ad hoc networks. Although proactive protocols can produce the required route immediately, they may waste too much of the network resources in the attempt to always maintain the updated network topology. The reactive protocol, on the other hand, may reduce the amount of used network resources, but may encounter excessive delay in the flooding of the network with routing queries. Another approach to address the routing problem was through the *hybrid* protocols, which incorporate some aspects of the proactive and some aspects of the reactive protocols. The Zone Routing Protocol (ZRP) [Pea99] is an example of the hybrid approach. In ZRP, each node proactively maintains the topology of its close neighborhood only, thus reducing the amount of control traffic relative to the proactive approach. To discover routes outside its neighborhood, the node reactively invokes a generalized form of controlled flooding, which reduces the route discovery delay, as compared with purely reactive schemes. The size of the neighborhood is a single parameter that allows optimizing the behavior of the protocol based on the degree of nodal mobility and the degree of network activity.

In what follows, we present a number of examples of routing protocols that were developed for the ad hoc networking environment.

3.1 Single-Scope Routing Protocols

3.1.1 Advantages and Disadvantages

The main advantage of the single-scope routing protocols, in comparison with the multi-scope routing protocols, is their lower complexity. There is no distinction of nearby or faraway nodes, and there is no need to maintain a hierarchical structure. Therefore, they are generally simpler

to implement, both in simulations and in practical systems. The current activities within the IETF MANET group predominantly involve single-scope routing.

However, inefficient resource management can result from treating nodes equally, regardless of their relative location. For example, it may not be necessary for a node to maintain very accurate link-state tables or route caching information of faraway nodes. Therefore, the single-scope routing protocols may not scale well as the network size increases.

The single-scope routing protocols can be categorized into reactive (or on-demand) and proactive (or table-driven) ones. The main advantage of the reactive protocols is that no routing-table updating is required unless a route is used. Therefore, battery power and wireless bandwidth can be conservatively utilized. However, when a route is needed, the source node needs to query for the route. That can lead to routing delay. Furthermore, an efficient route querying mechanism is required in order to prevent overloading the network with query packets.

On the other hand, the proactive protocols generally provide a source node with readily available routes to all other nodes. They incur no routing delay or query traffic. The disadvantage of the proactive protocols is that they may incur unnecessary control traffic in maintaining up-to-date topology information, whether that information is needed for routing or not.

3.1.2 Reactive/On-Demand Routing Protocols

3.1.2.1 Ad Hoc On-Demand Distance Vector Routing (AODV)

AODV [Per99] incorporates the destination sequence number technique of *Destination-Sequenced Distance-Vector Routing (DSDV)* routing into an on-demand protocol. (DSDV is discussed in the sequel.)

Each node keeps a next-hop routing table containing the destinations to which it currently has a route. A route expires if it is not used or reactivated for a threshold amount of time.

If a source has no route to a destination, it broadcasts a route request (RREQ) packet using an *expanding ring search* procedure, starting from a small Time-To-Live value (maximum hop count) for the RREQ, and increasing it if the destination is not found. The RREQ contains the last seen sequence number of the destination, as well as the source node's current sequence number. Any node that receives the RREQ updates its next-hop table entries with respect to the source node. A node that has a route to the destination with a higher sequence number than the one specified in the RREQ unicasts a route reply (RREP) packet back to the source. Upon receiving the RREP packet, each intermediate node along the RREP routes updates its next-hop table entries with respect to the destination node, dropping the redundant RREP packets and those RREP packets with a lower destination sequence number than one previously seen.

When an intermediate node discovers a broken link in an active route, it broadcasts a route error (RERR) packet to its neighbors, which in turn propagate the RERR packet up-stream towards all nodes that have an active route using the broken link. The affected source can then re-initiate route discovery if the route is still needed.

3.1.2.2 Dynamic Source Routing (DSR)

DSR [Joh96] is a source routing on-demand protocol with various efficiency improvements.

In DSR, each node keeps a *route cache* that contains full paths to known destinations. If a source has no route to a destination, it broadcasts a route request packet to its neighbors. Any node receiving the route request packet and without a route to the destination appends it's own ID to the packet and re-broadcasts the packet. If a node receiving the route request packet has a route to the destination, the node replies to the source with a concatenation of the path from the source to itself and the path from itself to the destination. If the node already has a route to the source, the route reply packet will be sent over that route. Otherwise, depending on the underlining assumption of the directionality of links, the route reply packet can be sent over the reversed source-to-node path, or piggy-backed in the node's route request packet for the source.

When an intermediate node discovers a broken link in an active route, it sends a route error packet to the source, which may re-initiate route discovery if an alternate route is not available.

DSR has efficiency improving features. One of such features is the *promiscuous* mode, in which a node listens to route request, reply, or error messages not intended to itself and updates its route cache correspondingly. Another DSR feature is the *expanding ring search* procedure, in which the route request packets are sent with a maximum hop count, which can be increased if the destination is not found within the hop-count limit. Finally, adding *jitter* in sending the route reply messages to prevent *route reply storms* and *packet salvaging* to extract correct routes from route error packets are yet two other features that improve DSR performance.

3.1.2.3 Temporally Ordered Routing Algorithm (TORA)

Temporally Ordered Routing Algorithm (TORA) [Par00] is a merger of the proactive link-reversal algorithm for destination-oriented Directional-Acyclic-Graph creation proposed in [Gaf81] and the on-demand query-reply mechanism of Lightweight Mobile Routing (LMR) [Cor95].

In TORA, routes to a destination are defined by a Directional Acyclic Graph (DAG) rooted at the destination. Each link in the network is assumed to be bi-directional, but in order to form the DAG with respect to a destination, a logical direction of the link is defined by giving *height* values to the two nodes at the ends of the link. Since time is part of the height value, TORA requires synchronized clocks across all nodes.

If a source has no route to a destination (i.e., the source node has no out-going edge in the DAG), it broadcasts a route query packet (QRY), which is propagated outwards by its neighbors. After receiving the QRY, a node that has a route to the destination broadcasts a route update packet (UPD) containing its own height. Receiving the UPD, each node that doesn't have a route to the destination updates its height to reflect the creation of an out-going edge.

Route maintenance is achieved through height adjustment and UPD exchange. Network partition can be detected by a node receiving UPD's reflected from the partition boundary, in which case a clear message (CLR) is used to update all routes within the partition.

TORA also supports a proactive mode, in which the destination initiates the route creation process by sending a packet that is processed and forwarded by the neighboring nodes.

3.1.3 Proactive/Table-Driven

3.1.3.1 Destination-Sequenced Distance-Vector Routing (DSDV)

Destination-Sequenced Distance-Vector Routing (DSDV) [Per94] provides improvements over the conventional Bellman-Ford distance-vector protocol. It eliminates route looping, increases convergence speed, and reduces control message overhead.

In DSDV, each node maintains a next-hop table, which it exchanges with its neighbors. There are two types of next-hop table exchanges: periodic full-table broadcast and event-driven incremental updating. The relative frequency of the full-table broadcast and the incremental updating is determined by the node mobility.

In each data packet sent during a next-hop table broadcast or incremental updating, the source node appends a sequence number. This sequence number is propagated by all nodes receiving the corresponding distance-vector updates, and is stored in the next-hop table entry of these nodes. A node, after receiving a new next-hop table from its neighbor, updates its route to a destination only if the new sequence number is larger than the recorded one, or if the new sequence number is the same as the recorded one, but the new route is shorter.

In order to further reduce the control message overhead, a *settling time* is estimated for each route. A node updates to its neighbors with a new route only if the settling time of the route has expired and the route remains optimal.

3.1.3.2 Wireless Routing Protocol (WRP)

The ***Wireless Routing Protocol (WRP)*** [Mur96] provides improvements over the Bellman-Ford distance-vector protocol. It reduces the amount of route looping, and has a mechanism to ensure the reliable exchange of update messages.

In WRP, each node maintains a distance-table matrix, which contains all destination nodes, and, for each destination node, all neighbors through which the destination node can be reached. For each neighbor-destination pair, if a route exists, the route length is recorded. Also recorded is the *predecessor*, the last node along a route before the destination node.

Each node neighbor broadcasts its current best route to selected destinations on an event-driven incremental basis. After a broadcast, acknowledgments are expected from all neighbor nodes. If some acknowledgments are missing, the broadcast will be repeated, with a *message retransmission list* specifying the subset of neighbors that need to respond. A node, after receiving the route updating packets from a neighbor, updates its own routing table only if the consistency of the new information is checked against the predecessor information from all its neighbors.

3.2 Multi-Scope Routing Protocols

3.2.1 Advantages and Disadvantages

The multi-scope routing protocols distinguish nodes by their relative positions. More resource is devoted to maintaining the topology information of more nearby, and hence more frequently used, part of the network. Therefore, scalability is the main advantage of the multi-scope routing protocols.

Their disadvantage is their relative complexity in comparison with the single-scope routing protocols. Ranking mechanisms that distinguish the nodes are required. Furthermore, they generally need to be reconfigurable, in order to adapt to the changing network topology and the varying node traffic and movement patterns.

Multi-scope routing can be categorized into the flat protocols and the hierarchical protocols. The main advantage of the flat protocols, in comparison with the hierarchical ones, is that they do not require specialized nodes. All nodes serve the same set of functions. Therefore, they are relatively simple to implement, and they avoid the control message overhead and non-uniform loading involved in node specialization. However, since the flat structure does not have special nodes that can provide locally centralized functionality, the nodes between nearby local scope exchange link information in a strictly distributive manner. Thus, the lack of coordination can lead to inefficiency.

On the other hand, the hierarchical protocols utilize specialized nodes, such as the cluster heads, group leaders, or the route gateways, to coordinate the dissemination of local link information. Furthermore, the relative position of the specialized nodes can provide directional guidance to routing between the regular nodes. However, the dynamic maintenance of the hierarchy can potentially take away a large amount of the battery power and wireless bandwidth from routing itself, especially when the network is highly mobile. Furthermore, mechanisms are needed to avoid overloading the local controllers and to alleviate the traffic hot spots.

3.2.2 Flat Routing Protocols

3.2.2.1 Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) [Pea99] provides a hybrid routing framework that is locally proactive and globally reactive. Each node proactively advertises its link state a fixed number of hops, called the zone radius. These local advertisements give each node an updated view of its routing zone -- the collection of all nodes and links that are reachable within the zone radius. The routing zone nodes that are at a minimum distance of the zone radius are called peripheral nodes. The peripheral nodes represent the boundary of the routing zone and play an important role in zone based route discovery. Each node has an associated routing zone, and routing zones of neighboring nodes overlap.

ZRP uses knowledge of routing zone connectivity to guide its global route discovery. Rather than blindly broadcasting route queries from a node to all its neighbors, ZRP employs a service called *bordercasting*, which directs the route request from a node to its peripheral nodes via multicast. Special query control mechanisms are used to identify those peripheral nodes that have been covered by the route query (i.e. that belong to the routing zone of a node that

already has bordercast the query) and prune them from the bordercast's query distribution tree. This encourages the query to propagate outward, away from its source and away from covered regions of the network.

Routing zones also help improve the quality and survivability of discovered routes, by making them more robust to changes in network topology. Once routes have been discovered, routing zones offer enhanced, real-time, route maintenance. Multiple hop paths within the routing zone can bypass link failures. Similarly, sub optimal route segments can be identified and traffic can be re-routed along shorter paths.

3.2.2.2 Optimized Link State Routing (OLSR)

Optimized Link State Routing (OLSR) [Jac00] is a link-state protocol where the link information is disseminated through an efficient flooding technique.

The key concept in OLSR is *multipoint relay* (MPR). A node's MPR set is a subset of its neighbors whose combined radio range covers all nodes two hops away. Heuristics are proposed for each node to determine its minimum MPR set based on its two-hop topology. Each node obtains the two-hop topology through its neighbors' periodic broadcasting of HELLO packets containing the neighbors' lists of neighbors.

As with a conventional link-state protocol, a node's link information update is propagated throughout the network. However, in OLSR, when a node forwards a link updating packet, only those neighbors in the node's MPR set participate in forwarding the packet (similar to ZRP's border-casting with *1-hop* zone radius).

Furthermore, a node only originates link updates concerning those links between itself and the nodes in its MPR set. Therefore, routes are computed using a node's partial view of the network topology.

3.2.2.3 Fisheye State Routing (FSR)

The fisheye routing concept is based on the premise that changes in a network region's topology have less effect on a router's packet forwarding decisions as the distance (in hops) between the router and the network increases. This relationship can be exploited in order to reduce routing traffic by relaying topology updates for distant regions less often than updates for nearby regions. Given an approximate view of the distant parts of the network, a node can forward a packet in the proper direction toward the destination. As the packet progresses toward the destination, the view of the destination's region becomes more accurate, providing for more precise packet forwarding.

This fisheye technique is applied in the *Fisheye State Routing (FSR)* protocol [Iwa99], an adaptation of *Global State Routing (GSR)* [Che98]. In the original GSR protocol, link state information is propagated through the network by periodic link state table exchanges between neighbors. In FSR, a node exchanges individual link state table entries at different rates, depending on the distance to the link's source. In particular, FSR defines *scopes* of increasing radii (in hops) around each node. A node relays a link state table entry if the link's source lies within the largest scope covered by the current table exchange. The first level (innermost) scope is covered by every table exchange. The k^{th} level scope is covered by every Xk^{th}

interval, where X_k is an integer multiple of X_{k-1}. This relationship ensures that an exchange covering a level k^{th} scope coincides with the more frequent updates of all the interior scopes.

3.2.3 Hierarchical Routing Protocols

3.2.3.1 Core-Extraction Distributed Ad hoc Routing (CEDAR)

Core-Extraction Distributed Ad hoc Routing (CEDAR) [Siv99] employs a set of core nodes, at least one of which is within one hop of each node, in its routing mechanism. The core nodes are selected using a highest-degree scheme. A core node dominates each non-core node. Through periodic updating, the non-core nodes maintain a list of the IDs of their neighbors and their neighbors' respective dominators. The state information of each link is disseminated towards the core nodes away from the link, and the higher is the capacity of link, the further the information travels. Each core node keeps a local link-state table containing only the stable, high capacity, and nearby links.

Global route search is carried out reactively. Similarly to CBRP, the dominator of a source node determines a *core path* to the dominator of the destination node by an efficient flooding over the core. Using its local link-state, the dominator of the source computes a ``shortest-widest-furthest'' QoS-admissible path to an intermediate node, along the core path towards the destination. It then sends a route-forwarding request to the dominator of the intermediate node, which then starts the same QoS-admissible path search using its own local link-state table. The process continues until the QoS-admissible path reaches the destination. Source routing is then carried out to forward the data packets.

3.2.3.2 Zone-based Hierarchical Link State (ZHLS)

In ***Zone-based Hierarchical Link State (ZHLS)*** [Joa99], the system coverage area is divided into non-overlapping physical zones. The nodes are equipped with geo-location devices such as the GPS receivers, so that each node can determine its zone membership by comparing its physical location with the zone map. Furthermore, if the nodes within a zone are partitioned, logical sub-zones are created, each containing one of the partitions. Every node maintains an intrazone routing table and an interzone routing table. The intrazone routing table enables a node to reach all other nodes within the zone. Inter-zone communications are carried out through the *gateway* nodes near the zone edges. The gateway nodes broadcast the status of the virtual links between zones to the entire network. A node aggregates all gateway broadcasts to form the interzone routing table.

When a source node needs to transmit data to a destination node outside of the source node's zone, global zone query is used to determine the zone identity of the destination node. Using its interzone routing table, the source node sends the query to all zones in the network. After receiving the query message, the gateway nodes whose zone contains the destination node sends back to the source node the destination node's zone identity. The source node then sends out the data packets with the destination node's zone ID and node ID specified in their headers. The packets are then forwarded to the destination node according to both the interzone and the intrazone routing tables at the intermediate nodes.

3.2.3.3 Landmark Ad hoc Routing (LANMAR)

The original landmark scheme for wired networks was proposed in [Tsu88]. ***Landmark Ad hoc Routing (LANMAR)*** [Pei00] adopts that scheme for ad hoc network routing. In LANMAR, the network consists of pre-defined logical subnets, each with a pre-selected *landmark*. All nodes in a subnet are assumed to move as a group, and they remain connected to each other via *Fisheye State Routing*.

The routes to the landmarks, and hence the corresponding subnets, are proactively maintained by all nodes in the network through the exchange of distance-vectors. Every node has a lifetime hierarchical address identifying the subnet where it belongs. A source node specifies the hierarchical address of a destination node in the data packet headers. The packets are then forwarded towards the landmark of the subnet where the destination node belongs. When a packet reaches a node in the subnet where the destination node belongs, the node forwards the packet to the destination node using its subnet routing table.

3.3 Geographically-routed Protocols

3.3.1 Location-Aided Routing (LAR)

In ***Location-Aided Routing (LAR)*** [Ko98], a source node estimates the range of a destination's location, based on the destination's last reported velocity, and broadcasts route request only to nodes within a geographically defined *request zone*. LAR requires each node to obtain its geographic location through external devices such as GPS.

3.3.2 Distance Routing Effect Algorithm for Mobility (DREAM)

In ***Distance Routing Effect Algorithm for Mobility (DREAM)*** [Bas98], each node obtains its geographic location through external devices such as GPS, and periodically transmits its location coordinates to other nodes in the network. The period of location transmission depends on the node's velocity and the geographic distance to nodes to which the location information is intended.

A source sends a data packet to a subset of its neighbors in the direction of the destination. The intermediate nodes similarly forward the data packet towards the destination.

4. Multicasting Protocols for Ad Hoc Networks

Multicasting is an efficient communication tool for use in multi point applications. Many of the proposed multicast routing protocols, both for the Internet and for ad hoc networks, construct trees over which information is transmitted. Using trees is evidently more efficient than brute force approach of sending the same information from the source individually to each of the receivers. Another benefit of using trees is that routing decisions at the intermediate nodes become very simple: a router in a multicast tree that receives a multicast packet over an in-tree interface forwards the packet over the rest of its in-tree interfaces.

Multicast routing algorithms in the Internet [Pau98] can be classified into three broad categories:

- Shortest Path Tree algorithms [Ber92],
- Minimum Cost Tree algorithms [Cho91], [Wax93],
- Constrained Tree algorithms [Kad83], [Kom93].

There are two fundamental approaches in designing multicast routing - one is to minimize the distance (or cost) from the sender to each receiver individually (shortest path tree algorithms) and the other is to minimize the overall (total) cost of the multicast tree. Practical considerations lead to a third category of algorithms, which try to optimize both constraints using some metric (minimum cost trees with constrained delays). The majority of multicast routing protocols in the Internet is based on shortest path trees, because of their ease of implementation. Also, they provide minimum delay from sender to receiver, which is desirable for most real-life multicast applications. However shared trees are used in some more recent protocols (like PIM [Dec96] and CBT [Bal97]) in order to minimize the state stored in the routers.

Multicasting in ad hoc networks is more challenging than in the Internet, because of the need to optimize the use of several resources simultaneously. Firstly, nodes in ad hoc networks are battery-power limited. Furthermore, data travels over the air and wireless resources are scarce. Secondly, there is no centralized access point or existing infrastructure (like in the cellular network) to keep track of the node mobility. Thirdly, the status of communication links between routers is a function of their positions, transmission power levels, etc. The mobility of routers and randomness of other connectivity factors lead to a network with a potentially unpredictable and rapidly changing topology. This means that by the time a reasonable amount of information about the topology of the network is collected and a tree is computed, there may be very little time before the computed tree becomes useless.

Work on multicast routing in ad hoc networks gained momentum in the mid 90s. Some early approaches to provide multicast support in ad hoc networks consisted of adapting the existing Internet multicasting protocols; For example Shared Tree Wireless network Multicast [Chi97]. ODMRP [Lee99], AMRIS [Wu99], CAMP [Gar98] and others [Roy99b], [Bom98], [Lee00], [Bri00], [Zho00], [Con00], [San98], [Sin99] and [Wie99] have been designed specifically for ad hoc networks. ODMRP is a mesh based, on-demand protocol that uses soft state approach for maintenance of the message transmission structure. It exploits robustness of mesh structure to frequent route failure and gains stability at the expense of bandwidth. The *Core Assisted Mesh Protocol (CAMP)* attempts to remedy this excessive overhead, while still using a mesh by using a core for route discovery. AMRIS constructs a shared delivery tree rooted at a node, with ID-numbers increasing as they radiate from the source. Local route recovery is made possible due to this property of ID numbers, hence reducing the route recovery time and also confining route recovery traffic to the region of link failures.

In what follows, we present a number of examples of multicasting protocols that were developed for the ad hoc networking environment.

4.1 *Core Assisted Mesh Protocol (CAMP)*

Core Assisted Mesh Protocol (CAMP) [Gar98] builds and maintains a multicast mesh for information distribution within each multicast group. A router is allowed to accept unique packets coming from any neighbor in the process of forwarding packets through the mesh. Because a member router of a mesh has redundant paths to any other router in the mesh, this protocol is more resilient to topology changes than tree based protocols.

Cores are used to limit the control traffic needed for receivers to join multicast groups. In contrast to CBT[Bal97], one or multiple cores can be defined for each mesh and cores need not be part of the mesh of their group. Routers can join a group even if all associated cores become unreachable using an expanded ring search. CAMP ensures that all reverse shortest

paths between sources and receivers are part of groups mesh by means of "heart beat" messages. In the event of link failure and partition, the operation of mesh components continues. Different components merge by sending join requests to cores as soon as connectivity with a core is re-established.

CAMP is designed to support very dynamic ad-hoc networks. According to the performance analysis presented in the paper, CAMP performs better than the *On Demand Multicast Routing Protocol (ODMRP)* in terms of percentage of packets lost by routers, average packet delay and total number of control packets received by each router. (ODMRP is described in the sequel.)

4.2 *Multicast Operation of Ad-hoc On-Demand Distance Vector Routing Protocol*

This is an extension of AODV to support multicasting and it builds multicast trees on demand to connect group members. Route discovery in MAODV [Roy99b] follows a route request/route reply discovery cycle. As nodes join the group, a multicast tree composed of group members is created. Multicast group membership is dynamic and group members are routers in the multicast tree. Link breakage is repaired by downstream node broadcasting a route request message. The control of a multicast tree is distributed so there is no single point of failure. One big advantage claimed is that since AODV offers both unicast and multicast communication, route information when searching for a multicast route can also increase unicast routing knowledge and vice-versa.

In [Roy99b], an ad-hoc network consists of laptops in a room (50-100m width, 10m range) talking to each other, moving at 1 m/s. The results presented only verify working of AODV and do not compare performance with other multicasting protocols. They show that AODV attains a high goodput ratio and is able to offer this communication with a minimum of control packet overhead. They also demonstrate its operation under frequent network partitions.

4.3 *AMRIS : A Multicast Protocol for Ad Hoc Wireless Networks*

AMRIS[Wu99] is an on-demand protocol, which constructs a shared delivery tree to support multiple senders and receivers within a multicast session. Each participant in the multicast session has a session-specific multicast session member id (*msm-id*). These msm-ids increase in numerical value as they radiate away from a central node known as SID. Tree initialization is done by the SID broadcasting a new session message. All nodes of the network calculate their msm-id to be larger than the msm-id of the node they received the new session message from. There are beacon messages exchanged between nodes, which help a node to calculate its new msm-id after it moves to a new location.

AMRIS does not depend on the unicast routing protocol to provide routing information to other nodes as it maintains a neighbor-status table. It is the child's responsibility to reconnect to the tree if link failure occurs. If it has potential parents, i.e., neighboring nodes with lower msm-ids, it sends a join request to them, which in turn try to join the tree in the same way. If there are no potential parents, the node transmits a join request message.

In the simulation given in [Wu99], the authors vary membership from 50-100 and the speed of nodes is up to 20 m/s. The simulation results presented study various performance parameters in terms of network conditions but do not compare performance with other protocols. The paper studied the effect of beacon intervals, membership sizes and mobility on packet delivery

ratio and concludes that there is an optimum beacon interval. Control overhead is verified to be higher when the beacon interval is small. They also show that the relationship between end-to-end packet delay and packet delivery ratio is robust with respect to membership.

4.4 *AMRoute: Ad hoc Multicast Routing protocol*

AMRoute [Bom98] presents an approach for robust IP multicast in ad hoc networks by exploiting user-multicast trees and dynamic logical cores. It creates a bi-directional shared tree for data distribution using only group senders and receivers as tree nodes. Unicast tunnels are used as tree links to connect neighbors on the user-multicast tree. Hence the AMRoute protocol needs not to be supported by other nodes in the network and also the tree structure does not change even in the case of dynamic network topology and hence reduces signaling. Each node is aware of its tree neighbors only and forwards data on the tree links to its neighbors. This saves node resources.

Certain tree nodes are designated by AMRoute as logical cores and are responsible for initiating and managing the signaling component of AMRoute, such as detection of group members and tree setup. Unlike CBT and PIM-SM, they are not a central point for data distribution and can migrate dynamically among member nodes. Hence there is no single point of failure. Like DVMRP, AMRoute provides robustness by periodic flooding for tree construction. However, AMRoute periodically floods a small signaling message instead of data.

AMRoute simulations were done with TORA as the underlying unicast protocol. The mobility of the network was emulated by keeping the node location fixed and breaking/connecting links between neighbors. The simulation results show that broadcasting signaling traffic generated by AMRoute is independent of group size and inversely proportional to network mobility. Unicast signaling traffic is proportional to group size and inversely proportional to network mobility. Total signaling traffic is independent of the data rate. Both signaling traffic and join latency are relatively low for typical group sizes. They verify that group members receive a high proportion of data multicast by a sender, even in the case of a dynamic network.

4.5 *ODMRP : On Demand Multicast Routing Protocol*

ODMRP [Lee99] is a mesh based rather than a conventional tree based scheme and uses a forwarding group concept (only a subset of nodes forwards the multicast packets via scoped flooding). By maintaining a mesh instead of a tree, the drawbacks of multicast trees in ad hoc networks like frequent tree reconfiguration and non-shortest path in a shared tree are avoided. ODMRP applies "on-demand" routing techniques to avoid channel overhead and improve scalability.

The source starts a session by flooding a "join data" control packet with data payload attached, which is subsequently broadcast at regular intervals to the entire network to refresh membership information and update the routes. The mesh is created by the replies of receivers to this packet received via various paths. When receiving a multicast data packet, a node forwards it only when it is not a duplicate, hence minimizing traffic overhead.

Because the nodes maintain soft state, finding the optimal flooding interval is critical to ODMRP performance. ODMRP uses location and movement information to predict the duration of time that routes will remain valid. With the predicted time of route disconnection, a "join data" packet is flooded when route breaks of ongoing data sessions are imminent. In

[Lee99], the authors present a comparison with DVMRP and show that ODMRP is better suited for ad hoc networks in terms of bandwidth utilization.

4.6 *MCEDAR: Multicasting Core-Extraction Distributed Ad hoc Routing*

This scheme [Sin99] is a multicast extension of CEDAR, which was a routing scheme proposed for unicast communication in ad hoc networks. MCEDAR relies on the Core Extraction and the Core Broadcast components of the CEDAR architecture. The Core extraction algorithm used is a distributed, heuristic for finding a good approximation to a minimum dominating set. Each core node has the following state stored in it: its nearby core nodes, the nodes it dominates; i.e., each core node has enough local information to reach the domain of its nearby nodes and set up virtual links. Core broadcast is used instead of flooding in order to discover a route to the destination. This is done by making each node cache every RTS and CTS packet it hears on the channel for core broadcast packets. So a node knows whether a packet has been received by the destination already. If it has, it does not transmit the packet and hence suppresses the duplicate transmission.

The infrastructure for a multicast group resides entirely within the core broadcast mechanism, which is used to perform data forwarding. Each multicast group extracts a subgraph of the core-graph to function as "mgraph". Data forwarding is done on the mgraph using the core broadcast mechanism. In this way the forwarding is tree-based, though the structure is robust because it is a mesh.

5. Security of Ad Hoc Networks

The provision of security services in the MANET context faces a set of challenges specific to this new technology. The insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes have been identified [Zho99,Sta99] in literature as such challenges. Nevertheless, the single most important feature that differentiates MANET is the absence of a fixed infrastructure. No part of the network is dedicated to support individually any specific network functionality, with routing (topology discovery, data forwarding) being the most prominent example. Additional examples of functions that cannot rely on a central service, and which are also of high relevance to this work, are naming services, certification authorities (*CA*), directory and other administrative services.

Even if such services were assumed, their availability would not be guaranteed, either due to the dynamically changing topology that could easily result in a partitioned network, or due to congested links close to the node acting as a server. Furthermore, performance issues such as delay constraints on acquiring responses from the assumed infrastructure would pose an additional challenge.

The absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separating nodes into trusted and non-trusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials and the ability for nodes to validate them. In the MANET context, there may be no ground for an *a priori* classification, since all nodes are required to cooperate in supporting the network operation, while no prior security association can be assumed for all the network nodes. Additionally, in MANET freely roaming nodes form transient associations with their neighbors; join and leave MANET sub-domains independently and without notice. Thus it may be difficult in most cases to have a clear picture of the ad hoc network

membership. Consequently, especially in the case of a large-size network, no form of established trust relationships among the majority of nodes could be assumed.

In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. The mechanisms currently incorporated in MANET routing protocols cannot cope with disruptions due to malicious behavior. For example, any node could claim that is one hop away from the sought destination, causing all routes to the destination to pass through itself. Alternatively, a malicious node could corrupt any in-transit route request (reply) packet and cause data to be misrouted.

The presence of even a small number of adversarial nodes could result in repeatedly compromised routes, and, as a result, the network nodes would have to rely on cycles of time-out and new route discoveries to communicate. This would incur arbitrary delays before the establishment of a non-corrupted path, while successive broadcasts of route requests would impose excessive transmission overhead. In particular, intentionally falsified routing messages would result in a *denial-of-service (DoS)* experienced by the end nodes.

Despite the fact that security of MANET routing protocols is envisioned to be a major "roadblock" in commercial application of this technology, only a limited number of works has been published in this area. In the sequel, we review some schemes related to the problem of incorporating security provisions within the context of ad hoc communication.

5.1 Overview of security schemes for ad hoc networks

Efforts to incorporate security measures in the ad hoc networking environment have mostly concentrated on the aspect of data forwarding, disregarding the aspect of topology discovery. On the other hand, solutions that target route discovery have been based on approaches for fixed-infrastructure networks, defying the particular MANET challenges.

For the problem of secure data forwarding, two mechanisms that (i) detect *misbehaving* nodes and report such events and (ii) maintain a set of metrics reflecting the past behavior of other nodes [Mar00] have been proposed to alleviate the detrimental effects of packet dropping. Each node may choose the 'best' route, comprised of relatively well-behaved nodes; i.e., nodes that do not have history of avoiding forwarding packets along established routes. Among the assumptions for the above-mentioned work are a shared medium, bi-directional links, use of source routing (i.e., packets carry the entire route that becomes known to all intermediate nodes), and no colluding malicious nodes. Nodes operating in promiscuous mode overhear the transmissions of their successors and may verify whether the packet was forwarded to the downstream node and check the integrity of the forwarded packet. Upon detection of a misbehaving node, a report is generated and nodes update the rating of the reported misbehaving node. The ratings of nodes along a well-behaved route are periodically incremented, while reception of a misbehavior alert dramatically decreases the node rating.[3] When a new route is required, the source node calculates a path metric equal to the average of the ratings of the nodes in each of the route replies, and selects the route with the highest metric.

The detection mechanism exploits two features that frequently appear in MANET*:* the use of a shared channel and source routing. Nevertheless, the plausibility of this solution could be questioned for several reasons and, indeed, the authors provide a short list of scenarios of incorrect detection. The possibility of falsely detecting misbehaving nodes could easily create a situation with many nodes falsely suspected for a long period of time. In addition, the metric construction may lead to a route choice that includes a suspected node, if, for example, the

[3] The initial rating, 0.5, is increased by 0.01 every 200 ms. Suspected nodes have a rating equal to –100, with the option for a long timeout period after which the negative rating is changed back to a positive value.

number of hops is relatively high, so that a low rating is "averaged out." Finally, the most important vulnerability is the proposed feedback itself; there is no way for the source, or any other node that receives a misbehavior report to validate its authenticity or correctness. Consequently, the simplest attack would be to generate fake alerts and eventually disable the network operation altogether. The protocol attempts new route discoveries when none of the route replies is free of suspected nodes, with the excessive route request traffic degrading the network performance. At the same time, the adversary can falsely accuse a significant fraction of nodes within the time-out period related to reinstating from a negative rating and, essentially, partition the network.

A different approach [But00] is to provide incentive to nodes, so that they comply with protocol rules; i.e., properly relay user data. The concept of fictitious currency is introduced, in order to *endogenize* the behavior of the assumed greedy nodes, which would forward packets in exchange for currency. Each intermediate node purchases from its predecessor the received data packet and sells it to its successor along the path to the destination. Eventually the destination pays for the received packet.[4] This scheme assumes the existence of an overlaid geographic routing infrastructure and a *Public Key Infrastructure (PKI).* All nodes are pre-loaded with an amount of currency, have unique identifiers, are associated with a pair of private/public keys and all cryptographic operations related to the currency transfers are performed by a physically tamper-resistant module. The applicability of the scheme, which targets wide-area MANET, is limited by the assumption of an on-line Certification Authority in the MANET context. Moreover, nodes could flood the network with packets destined to non-existent nodes and possibly lead nodes unable to forward purchased packets to starvation. The practicality of the scheme is also limited by its assumptions, the high computational overhead (hop-by-hop public key cryptography, for each transmitted packet), and the implementation of physically tamper-resistant modules.

The protection of the route discovery process has been regarded as an additional Quality-of-Service (*QoS*) issue [Yi01], by choosing routes that satisfy certain quantifiable security criteria. In particular, nodes in a MANET subnet are classified into different trust and privilege levels. A node initiating a route discovery sets the sought security level for the route; i.e., the required minimal trust level for nodes participating in the query/reply propagation. Nodes at each trust level share symmetric encryption and decryption keys. Intermediate nodes of different levels cannot decrypt in-transit routing packets, or determine whether the required *QoS* parameter can be satisfied, and simply drop them. Although this scheme provides protection (e.g., integrity) of the routing protocol traffic, it does not eliminate false routing information provided by malicious nodes. Moreover, the proposed use of symmetric cryptography allows any node to corrupt the routing protocol operation within a level of trust, by mounting virtually any attack that would be possible without the presence of the scheme. Finally, the assumed supervising organization and the fixed assignment of trust levels does not pertain to the MANET paradigm. In essence, the proposed solution transcribes the problem of secure routing in a context where nodes of a certain group are assumed to be trustworthy, without actually addressing the global secure routing problem.

An extension of the *Ad Hoc On-demand Distance Vector* (*AODV*) [Per99] routing protocol has been proposed [Gue01] to protect the routing protocol messages. The *Secure*-AODV (S-AODV) scheme assumes that each node has certified public keys of all network nodes, so that intermediate nodes can validate all in-transit routing packets. The basic idea is that the originator of a control message appends an *RSA signature* [Riv78] and the last element of a *hash chain* [Lam81] (i.e., the result of *n* consecutive hash calculations on a random number). As the message traverses the network, intermediate nodes cryptographically validate the

[4] An alternative implementation, with each packet carrying a purse of fictitious currency from which nodes remove their reward, faces different challenges as well.

signature and the hash value, generate the k^{th} element of the hash chain, with k being the number of traversed hops, and place it in the packet. The route replies are provided either by the destination or intermediate nodes having an active route to the sought destination, with the latter mode of operation enabled by a different type of control packets.

The use of public-key cryptography imposes a high processing overhead on the intermediate nodes and can be considered unrealistic for a wide range of network instances. Furthermore, it is possible for intermediate nodes to corrupt the route discovery by pretending that the destination is their immediate neighbor, advertising arbitrarily high sequence numbers and altering (either decreasing by one or arbitrarily increasing) the actual route length. Additional vulnerabilities stem from the fact that the *IP* portion of the *S-AODV* traffic can be trivially compromised, since it is not (and cannot be, due to the AODV operation) protected, unless additional hop-by-hop cryptography and accumulation of signatures is used. Finally, the assumption that certificates are bound with *IP* addresses is unrealistic; roaming nodes joining MANET sub-domains will be assigned *IP* addresses dynamically (e.g., *DHCP* [Dro97]) or even randomly (e.g., *Zero-Configuration* [Hat01]).

A different approach is taken by the *Secure Message Transmission (SMT)* [Pap02a] protocol, which, given a topology view of the network, determines a set of diverse paths connecting the source and the destination nodes. Then, it introduces limited transmission redundancy across the paths, by dispersing a message into N pieces, so that successful reception of any M-out-of-N pieces allows the reconstruction of the original message at the destination. Each piece, equipped with a cryptographic header that provides integrity and replay protection along with origin authentication and is transmitted over one of the paths. Upon reception of a number of pieces, the destination generates an acknowledgement informing the source of which pieces, and thus routes, were intact. In order to enhance the robustness of the feedback mechanism, the small-sized acknowledgments are maximally dispersed (i.e., successful reception of at least one piece is sufficient) and are protected by the protocol header as well. If less than M pieces were received, the source re-transmits the remaining pieces over the intact routes. If too few pieces were acknowledged or too many messages remain outstanding, the protocol adapts its operation, by determining a different path set, re-encoding undelivered messages and re-allocating pieces over the path set. Otherwise, it proceeds with subsequent message transmissions.

The protocol exploits MANET features such as the topological redundancy, interoperates widely with accepted techniques such as source routing, relies on a security association between the source and the destination, and makes use of highly efficient symmetric-key cryptography. It does not impose processing overhead on intermediate nodes, while the end nodes make the routing decisions, based on the feedback provided by the destination and the underlying topology discovery and route maintenance protocols. The fault-tolerance of *SMT* is enhanced by the adaptation of parameters such as the number of paths and the dispersion factor (i.e., the ratio of required pieces to the total number of pieces). *SMT* can yield *100%* successful message reception, even if *10* to *20* percent of the network nodes are malicious. Moreover, algorithms for the selection of path sets with different properties, based on different metrics and the network feedback, can be implemented by *SMT*. *SMT* provides a flexible, end-to-end, secure traffic engineering scheme tailored to the MANET characteristics.

It is noteworthy that *SMT* provides a limited protection against the use of compromised topological information, although its main focus is to safeguard the data forwarding operation. The use of multiple routes compensates for the use of partially incorrect routing information [Zho99], rendering a compromised route equivalent to a route failure. Nevertheless, the disruption of the route discovery can still be the most effective way for adversaries to consistently compromise the communication of one or more pairs of nodes.

Another approach to secure the route discovery procedures, the *Secure Routing Protocol (SRP)*, has been proposed in [Pap02b]. The scheme guarantees that a node initiating a route

discovery will be able to identify and discard replies providing false topological information, or, avoid receiving them. The novelty of the scheme, as compared with other MANET secure routing schemes, is that false route replies, as a result of malicious node behavior, are discarded partially by benign nodes while in-transit towards the querying node, or deemed invalid upon reception. The security goals are achieved with the existence of a security association between the pair of end nodes *only*, without the need for intermediate nodes to cryptographically validate control traffic.

The widely accepted technique in the MANET context of route discovery based on broadcasting query packets is the basis of the protocol. More specifically, as query packets traverse the network, the relaying intermediate nodes append their identifier (e.g., *IP* address) in the query packet header. When one or more queries arrive at the sought destination, replies that contain the accumulated routes are returned to the querying node; the source then may use one or more of these routes to forward its data.

Reliance on this basic route query broadcasting mechanism allows *SRP* to be applied as an extension of a multitude of existing routing protocols. In particular, the *Dynamic Source Routing* (*DSR*) [Joh96] and the *IERP* [Haa01a] of the *Zone Routing Protocol* (*ZRP*) [Haa01b] framework are two protocols that can be extended in a natural way to incorporate *SRP*. Furthermore, other protocols such as *ABR* [Toh97] for example, could be combined with *SRP* with minimal modifications to achieve the security goals of the *SRP* protocol.

In *SRP*, only the end nodes have to be securely associated, and there is no need for cryptographic validation of control traffic at intermediate nodes, two factors that render the scheme efficient and scalable. *SRP* places the overhead on the end nodes, an appropriate choice for a highly decentralized environment, and contributes to the robustness and flexibility of the scheme. Moreover, *SRP* does not rely on state stored in intermediate nodes, thus is immune to malicious acts not directed against the nodes that wish to communicate in a secure manner. Finally, *SRP* provides one or more route replies, whose correctness is verified by the route “geometry” itself.

6. Some Concluding Thoughts

The ad hoc networking technology has stimulated substantial research activity in the past 10 years or so. The rather interesting fact is that although the military has been experimenting and even using this technology for the last three decades, the research community has been coping with the rather frustrating task of finding a "killer" non-military application for ad hoc networks. A major challenge that has been perceived as a possible "show stopper" for technology transfer is the fact that commercial applications do not necessarily conform to the "collaborative" environment that the military communication environment does. In other words, why should a user forward someone else's transmission, depleting his or her own battery power and, thus, possibly restricting his or her use of the network in the future? This question may relate to the issue of billing - if billing is possible (and, in fact, desirable), then nodes that serve as "good citizens" could be rewarded. But billing is, by itself, a significant challenge in ad hoc networks.

Other challenges in deployment of ad hoc networks relate to the issues of manageability, security, and availability of communication through this type of technology.

Realizing that technology transfer has not been the motivating factor, the recent research interest in ad hoc networks could be, most probably, attributed to the intellectual challenges that are part of this type of communication environment.

Nevertheless, we believe that there is substantial commercial potential of ad hoc networks. Future extensions of the cellular infrastructure could be carried out using this type of technology and may, very well, be the basis for fourth generation (4G) of wireless systems. Other possible applications include sensing systems (also referred to as *Sensor Networks)* or augmentation to the wireless LAN technology.

7. Bibliography

[Bal97] A. Ballardie, "Core Based Trees (CBT Version 2) Multicast Routing - Protocol Specification," *RFC-2189,* September 1997

[Bas98] S. Basagni, I. Chlamtac, V.R. Syrotiuk, and B.A. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)," *ACMIEEE MobiCom,* Dallas, Texas, 1998

[Bel92] S.M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-based Protocols secure against dictionary attacks," *IEEE SympSecurity and Privacy,* May 1992

[Bel99] B. Bellur and R.G. Ogier, "A Reliable, Efficient Topology Broadcast Protocol for Dynamic Networks," *IEEE INFOCOM*, New York, March 1999

[Ber92] D. Bertsekas and R. Gallager, *Data Networks,* Second Edition, Prentice Hall, Inc., 1992

[Bha94] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless LAN's," in Proc*. ACM SIGCOMM'94*, pp.212-225, 1994

[Bia00] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," in *IEEE J.S.A.C.*, vol.18, no.3, pp.535-547, Mar.2000

[Bla99] M. Blaze, J. Feigenbaum, J. Ioannidis, A.D. Keromytis, "The KeyNote Trust-Management System," RFC 2074, *IETF,* September 1999

[Bom98] Bommaiah, McAuley, Talpade, and Liu. AMRoute: Ad hoc multicast routing protocol, Internet-Draft, *IETF,* August 1998

[Bri00] L. Briesemeister and G. Hommel, "Role-Based Multicast in Highly Mobile but sparsely Connected Ad Hoc Networks", *2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing,* 2000, pp. 45-50

[Bro98] J. Broch, D.A. Maltz, D.B. Johnson, Y.-CH, J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," *ACM/IEEE MobiCom*, pp85-97, 1998

[But00] L. Buttyan and J.P. Hubaux, "Enforcing Service Availability in Mobile Ad Hoc WANs," *1st MobiHoc,* Boston, Massachusetts, August 2000

[Che89] C. Cheng, R. Reley, S.P.R. Kumar and J.J. Garcia-Luna-Aceves, "A Loop-Free Extended Bellman-Ford Routing Protocol without Bouncing Effect," *ACM Computer Communications Review,* vol. 19, no. 4, 1989, pp. 224-236

[Che98] T.-W. Chen and M. Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks," *IEEE ICC,* pp171-175, June 1998

[Chi97a] C.-C. Chiang, H.-K. Wu, W. Liu, M. Gerla, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," *IEEE Singapore International Conference on Networks*, 1997

[Chi97b] C. Chiang, M. Gerla, and L. Zhang, "Shared tree wireless network multicast", *IEEE International Conference on Computer Communications and Networks (ICCCN'97),* September 1997

[Cho91] C.-H. Chow, "On multicast path finding algorithms," Proceedings of the *IEEE INFOCOM '91,* pp. 1274-1283, 1991

[Com00] G. D. Kondylis, S. V. Krishnamurthy, S. K. Dao and G. J. Pottie, "Multicasting Sustained CBR and VBR Traffic in Wireless Ad Hoc Networks", *International Conference on Communications*, 2000. pp 543-549

[Cor95] M.S. Corson and A. Ephremides, "A Distributed Routing Algorithm for Mobile Wireless Networks," *ACM/Baltzer Wireless Networks*, vol.1, no.1, pp.61-81, February 1995

[Das00] S.R. Das, C.E. Perkins, and E.M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE INFOCOM*, vol.1, pp.3-12, March 2000

[Dee96] S. E. Deering, D. Estrin, D. Farinacci, V. Jacobson, C-G Liu and L. Wei, "An Architecture for Wide-Area Multicast Routing," *IEEE/ACM Transactions on Networking*, Vol. 4, No. 2, pp. 153-162, April 1996

[Dro97] R. Droms, "Dynamic Host Configuration Protocol," IETF RFC 2131, Mar. 1997.

[Dub97] R. Dube, C.D. Rais, K.-Y. Wang, S.K. Tripathi, "Signal stability-based adaptive routing (SSA) for ad hoc mobile networks," *IEEE Personal Communications*, vol.4, no.1, pp.36-45, February 1997

[Eph87] A. Ephremeides, J.E. Wieselthier, and D.J. Baker, "A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling," *Proceedings of the IEEE*, vol.75, no.1, January 1987

[Fee01] L.M. Feeney, B. Ahlgren, A. Westerlund, "Spontaneous Networking: An Application-Oriented Approach to Ad Hoc Networking," *IEEE Communications Magazine*, vol.39, no.6, pp.176-181, June 2001

[Ful94] C.L. Fullmer, J.J. Garcia-Luna-Aceves, "Floor acquisition multiple access (FAMA) for packet-radio networks," in Proc. *ACM SIGCOMM'95*, pp.262-273, 1995

[Ful97] C.L. Fullmer, J.J. Garcia-Luna-Aceves, "Solutions to hidden terminal problems in wireless networks," in Proc. *ACM SIGCOMM'97*, pp.39-49, 1997

[Gaf81] E. Gafni and D. Bertsekas, "Distributed Algorithms for Generating Loop-Free Routes in Networks with Frequently Changing Topology," *IEEE Transactions on Communications*, vol.29, no.1, pp.11-15, January 1981

[Gar93] J.J. Garcia-Luna-Aceves, "Loop-Free Routing Using Diffusing Computations," *IEEE/ACM Transactions on Networking,* vol. 1, no. 1, February 1993, pp. 130-141

[Gar98] J.J. Garcia-Luna-Aceves, and E.L. Madruga, "The Core-assisted mesh protocol," *IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks*, vol.17, no.8, August 1998

[Ger95] M. Gerla and T.C. Tsai, "Multiuser, mobile multimedia radio network," *ACM/Balzer Journal of Wireless Networks*, 1995

[Ger99] M. Gerla, K. Tang and R. Bagrodia, "TCP Performance in Wireless Multi-hop Networks," in *Mobile Computing Systems and Applications*, pp.41-50, 25-26 Feb.1999

[Gla99] J.J. Garcia-Luna-Aceves and M. Spohn, "Source-Tree Routing in Wireless Networks,", *IEEE ICNP 99: 7th International Conference on Network Protocols*, Toronto, Canada, October 1999

[Glo99] *http://www.scienceforum.com/glomo/*

[Gue01] M. Guerrero, "Secure AODV", Internet draft sent to manet@itd.nrl.navy.mil mailing list, Aug. 2001

[Haa01a] Z.J. Haas, M. Perlman, P. Samar, "The Interzone Routing Protocol (IERP) for Ad Hoc Networks," draft-ietf-manet-zone-ierp-01.txt, IETF MANET Working Group, June 1st, 2001.

[Haa01b] 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

[Haa02] Z.J. Haas and J. Deng, "Dual Busy Tone Multiple Access (DBTMA): A Multiple Access Control Scheme for Ad Hoc Networks," *IEEE Transactions of Communications,* to appear

[Hat01] M. Hattig, Editor, "Zero-conf IP Host Requirements," draft-ietf-zeroconf-reqts-09.txt, IETF MANET Working Group, Aug. 31st, 2001.

[IEE99] IEEE Std 802.11, “Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications,” *IEEE,* 1999

[Iwa99] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Ad Hoc Networks,* vol.17, no.8, pp.1369-1379, August 1999

[Jac98] P. Jacquet, P. Muhlethaler, and A. Qayyum, "Optimized Link State Routing Protocol,” *IETF MANET*, Internet Draft, Nov. 1998

[Jac00] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Lanouiti, L. Viennot, and T. Clausen, *IETF MANET Internet Draft "draft-ietf-MANET-olsr-02.txt,"* July 2000.

[Jia99] M. Jiang, J. Li, and Y.C. Tay, *IETF MANET Internet Draft "draft-ietf-MANET-cbrp-spec-01.txt,"* August 1999

[Joa99] M. Joa-Ng and 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, Special Issue on Wireless Ad Hoc Networks,* vol.17, no.8, pp.1415-1425, August 1999

[Joh96] D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in Mobile Computing, edited by T. Imielinski and H. Korth, chapter 5, pp.153-181, Kluwer Academic Publishers, 1996

[Joh99] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks," *ACM/IEEE MobiCom,* pp.195-206, August 1999.

[Jub87] J. Jubin and J.D. Tornow, " The DARPA packet radio network protocols,*" Proceedings of IEEE (Special Issue on Packet Radio Networks)*, vol.75, pp.21-32, January 1987

[Kad83] B. Kadaba and J. M. Jaffe. "Routing to multiple Destinations in Computer Networks," *IEEE Transactions on Communications*, vol. com-31, no. 3, pp. 343-351, March 1983

[Kar90] P. Karn, "MACA - A new channel access method for packet radio," in *ARRL/CRRL Amateur Radio 9th Computer Networking Conference,* pp.134-140, 1990

[Ker74] A. Kershenbaum and W. Chou, "A Unified Algorithm for Designing Multidrop Teleprocessing Networks," *IEEE Transactions on Communications,* vol. COM-22, pp.1762-1772, Nov. 1974

[Ko98] Y.-B. Ko and N.H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," *ACM/IEEE MobiCom,* Dallas, Texas, 1998

[Kom93] V. P. Kompella, J. C. Pasquale, and G. C. Polyzos, "Multicast routing for multimedia communication," *IEEE/ACM Transactions on Networking,* Vol. 1, No. 3, pp. 286-292, June 1993

[Kon00] G.D. Kondylis, S.V. Krishnamurthy, S.K. Dao, and G.J. Pottie, "Multicasting Sustained CBR and VBR Traffic in Wireless Ad Hoc Networks", *International Conference on Communications,* 2000, pp.543-549

[Lam81] L. Lamport, “Password Authentication with Insecure Communication,” *Communications of the ACM, 24 (11),* pp.770-772, November 1981

[Lee00] S. Lee and C. Kim, "Neighbor Supporting Ad Hoc Multicast Routing Protocol", *2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing,* 2000, pp. 37-44

[Lee99] S.-J. Lee, M. Gerla, and C.-C. Chiang, "On-Demand Multicast Routing Protocol", *IEEE WCNC'99*, New Orleans, LA, September 1999, pp.1298-1304

[Mar00] S. Marti, T.J. Giuli, K. Lai, M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” *6th MobiCom,* Boston, Massachusetts, August 2000

[Mur95] S Murthy and J.J. Garcia-Luna-Aceves, “A Routing Protocol for Packet Radio Networks,” Proc. of ACM Mobile Computing and Networking Conference, *MOBICOM’95,* Nov. 14-15, 1995

[Mur96] S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," *ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks,* October 1996

[Nik00] N. Nikaein, H. Labiod, and C. Bonnet, "DDR-Distributed Dynamic Routing Algorithm for Mobile Ad hoc Networks," *First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC),* August 2000

[NIS93] FedInfProcStandards, "Secure Hash Standard," Pub180, *NIST,* May 1993

[Pap02a] P. Papadimitratos and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks," submitted for publication.

[Pap02b] 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),* San Antonio, TX, January 27-31, 2002.

[Par97] V.D. Park and M.S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *IEEE INFOCOM '97*, Kobe, Japan, 1997

[Par00] V. Park and M.S. Corson, *IETF MANET Internet Draft "draft-ietf-MANET-tora-spec-03.txt,"* November 2000

[Pau98] S. Paul, Multicasting on the Internet and its Applications, Kluwer Academic Publishers, 1998

[Pea99] M.R. Pearlman and Z.J. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol," *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Ad Hoc Networks,* vol.17, no.8, pp.1395-1414, August 1999

[Pei00] G. Pei, M. Gerla and X. Hong, "LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility," *First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC),* August 2000

[Per01] Ad Hoc Networking, C.E. Perkins, editor, Addison-Wesley Longman, 2001

[Per94] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *ACM SIGCOMM: Computer Communications Review,* vol.24, no.4, pp.234-244, October 1994

[Per96] C. Perkins, "IP Mobility Support," RFC 2002, *IETF,* October 1996

[Per99] C.E. Perkins and E.M. Royer, "Ad-hoc On-Demand Distance Vector Routing," *Second IEEE Workshop on Mobile Computing Systems and Applications,* pp.90-100, February 1999

[Pos81] J. Postel, "Internet Control Message Protocol," RFC 792, *IETF,* September 1981

[Ram98] R. Ramanathan and M. Steenstrup, "Hierarchically-organized, multihop mobile wireless networks for quality-of-service support," *ACM/Baltzer Mobile Networks and Applications*, vol.3, no.1, pp.101-119, 1998

[Riv78] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining Digital Signatures and Public Key Cryptosystems," Comm. of ACM, 21 (2), pp. 120-126, Feb. 1978.

[Roy99a] E.M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications,* April 1999

[Roy99b] E. Royer and C.E. Perkins "Multicast operation of ad-hoc, on-demand distance vector routing protocol," *ACM/IEEE MobiCom ' 99*,August 1999

[Rup97] R. Ruppe and S. Griswald, "Near Term Digital Radio (NTDR) System," *IEEE MILCOM,* vol.3, pp.1282-1287, November 1997

[San00] C. Santivanez, "Asymptotic Behavior of Mobile Ad Hoc Routing Protocols with Respect to Traffic, Mobility and Size," Technical Report TR-CDSP0052, *Department of Electrical and Computer Engineering,* Northeastern University, Boston, MA

[San98] C. Sankaran and A. Ephremides, "Multicasting with Multiuser detection in Ad-Hoc Wireless Networks", *Conference on Information Sciences and Systems(CISS),* 1998, pp.47-54

[Sha87] N. Shacham and J. Westcott, "Future directions in packet radio architectures and protocols," *Proceedings of IEEE (Special Issue on Packet Radio Networks),* vol.75, pp.83-99, January 1987

[Sha96] J. Sharony, "An Architecture for Mobile Radio Networks with Dynamically Changing Topology Using Virtual Subnets," *ACM Mobile Networks and Applications,* vol.1, no.1, pp.75-86, 1996

[Sin99] P. Sinha, R. Sivakumar and V. Bharghavan, "MCEDAR: Multicast Core-Extraction Distributed Ad hoc Routing", *Wireless Communications and Networking Conference,* 1999, pp.1313-1318

[Siv99] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: A Core-Extraction Distributed Ad Hoc Routing Algorithm," *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Ad Hoc Networks,* vol.17, no.8, pp.1454-1465, August 1999

[Sta99] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, *7th International Workshop,* LNCS, Springer-Verlag, 1999

[Tob75] F.A. Tobagi and L. Kleinrock, "Packet switching in radio channels: part II - The hidden terminal problem in carrier multiple-access and the busy-tone solution," *IEEE Transactions on Communications,* vol. COM-23, no.12, pp.1417-1433, December 1975

[Toh97] C.K. Toh, "Associativity-Based Routing for Ad-Hoc Mobile Networks, " Wireless Personal Communications, Vol. 4, No. 2, pp. 1-36, Mar. 1997.

[Tsu88] P.F.Tsuchiya, "The Landmark Hierarchy: a new hierarchy for routing in very large networks," *Computer Communication Review*, vol.18, no.4, August 1988, pp.35-42

[Wax93] B. M. Waxman, "Performance Evaluation of Multipoint Routing Algorithms," Proceedings of *IEEE INFOCOM '93,* pp. 980-986, 1993

[Wie99] J.E. Wieselthier, G.D. Nguyen, and A. Ephremides, "Algorithms for Energy-Efficient Multicasting in Ad Hoc Wireless Networks", *IEEE Military Communications Conference (MILCOM),* 1999, pp.1414-1418

[Wu87] C. Wu and V.O.K. Li, "Receiver-initiated busy-tone multiple access in packet radio networks," in Proc*. ACM SIGCOMM'87*, pp.336-342, 1987

[Wu99] C.W. Wu and Y.C. Tay, "AMRIS: A Multicast Protocol for Ad hoc Wireless Networks," *IEEE MILCOM '99,* Atlantic City, NJ, November 1999

[Xu01] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?" *IEEE Communi.Magazine,* pp.130-137, June 2001

[Yi01] S. Yi, P. Naldurg, R. Kravets, "Security-Aware Ad-Hoc Routing for Wireless Networks," UIUCDCS-R-2001-2241 Technical Report, Aug. 2001

[Zho00] H. Zhou and S. Singh, "Content Based Multicast in Ad Hoc Networks", *2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing,* 2000, pp.51-60

[Zho99] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, vol,13, no.6, November/December 1999