CHAPTER 1

Algorithms for Mobile Ad Hoc Networks

AZZEDINE BOUKERCHE

School of Information Technology and Engineering, University of Ottawa, Ottawa,
Ontario K1N 6N5, Canada

DANIEL CÂMARA and ANTONIO A. F. LOUREIRO

Department of Computer Science, Federal University of Minas Gerais, Belo Horizonte, Brazil

CARLOS M.S. FIGUEIREDO

FUCAPI—Analysis, Research, and Technological Innovation Center, Belo Horizonte, Brazil

COPYRIGHTED MATERIAL

1.1 INTRODUCTION

In the fourth century B.C., the Greek writer Aeschylus wrote the play *Agamemnon*, which provides a detailed description of how fire signals were supposedly used to communicate the fall of Troy to Athens over a distance of more than 450 km. This very same idea is present in the third movie of the trilogy "The Lord of the Rings," where fire signals were used to call for help of an ally army. In both cases, as well as in others found mainly in the literature and movies, the problem with a fire signal is that there is only one meaning associated with it—in the examples above, the fall of Troy and the call for help, respectively. This limitation of using fire signals to relay a message was realized by Polybius, one of the most famous ancient Greek historians who lived 200 years after Aeschylus in the second century B.C. To overcome this limitation, Polybius proposed a very simple fire signal mechanism based on fire torches that could be used to relay different messages. He described the procedure a person should follow before they start transmitting a message to another one (i.e., how a connection could be established between a pair of communicating entities), and he also described how messages could be coded using fire torches. Since this was basically a visual communication system, other people could see the same message (broadcast) and the people responsible for relaying messages could be mobile.

Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, Edited by Azzedine Boukerche
Copyright © 2009 by John Wiley & Sons Inc.

Polybius can probably be considered the first data communication engineer for mobile ad hoc networks. What it is more amazing is that his ideas were used during the next 2000 years for relaying messages among people in scenarios similar to the ones described above.

A mobile ad hoc network (MANET)[1] is comprised of mobile hosts that can communicate with each other using wireless links. It is also possible to have access to some hosts in a fixed infrastructure, depending on the kind of mobile ad hoc network available. Some scenarios where an ad hoc network can be used are business associates sharing information during a meeting, emergency disaster relief personnel coordinating efforts after a natural disaster such as a hurricane, earthquake, or flooding, and military personnel relaying tactical and other types of information in a battlefield.

In this environment a route between two hosts may consist of hops through one or more nodes in the MANET. An important problem in a mobile ad hoc network is finding and maintaining routes since host mobility can cause topology changes. Several routing algorithms for MANETs have been proposed in the literature, and they differ in the way new routes are found and existing ones are modified.

Mobile ad hoc networks can be realized by different networks such as body area network (BAN), vehicular ad hoc network (VANET), wireless networks (varying from personal area network to wide area network), and wireless sensor network (WSN). Furthermore, MANETs can be realized by different wireless communication technologies such as Bluetooth, IEEE 802.11, and Ultra-Wide Band (UWB). However, each one of these networks combined with the communication technologies pose various challenges in the design of algorithms for them as discussed in the following.

1.2 DESIGN CHALLENGES

The design of algorithms for MANETs poses new and interesting research challenges, some of them particular to mobile ad hoc networks. Algorithms for a MANET must self-configure to adjust to environment and traffic where they run, and goal changes must be posed from the user and application.

Data communication in a MANET differs from that of wired networks in different aspects. The wireless communication medium does not have a foreseeable behavior as in a wired channel. On the contrary, the wireless communication medium has variable and unpredictable characteristics. The signal strength and propagation delay may vary with respect to time and environment where the mobile nodes are. Unlike a wired network, the wireless medium is a broadcast medium; that is, all nodes in the transmission range of a transmitting device can receive a message.

The bandwidth availability and computing resources (e.g., hardware and battery power) are restricted in mobile ad hoc networks. Algorithms and protocols need to save both bandwidth and energy and must take into account the low capacity and

[1] Ad hoc is a Latin expression that means "*for the particular end or case at hand without consideration of wider application*". An ad hoc network means that the network is established for a particular, often extemporaneous service customized to applications for a limited period of time.

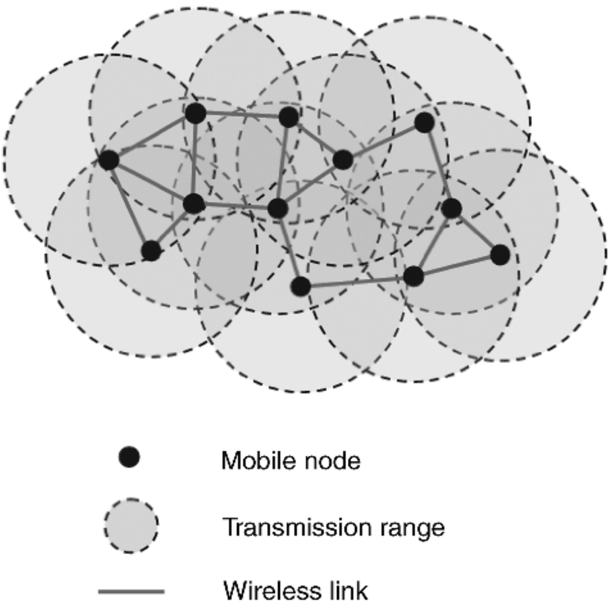

Figure 1.1. MANET topology.

limited processing power of wireless devices. This calls for lightweight solutions in terms of computational, communication, and storage resources.

An important challenge in the design of algorithms for a mobile ad hoc network is the fact that its topology is dynamic. Since the nodes are mobile, the network topology may change rapidly and unexpectedly, thereby affecting the availability of routing paths. Figure 1.1 depicts a snapshot of a MANET topology.

Given all theses differences, the design of algorithms for ad hoc networks are more complex than their wired counterpart.

1.3 MANETS: AN ALGORITHMIC PERSPECTIVE

1.3.1 Topology Formation

Neighbor Discovery. The performance of an ad hoc network depends on the interaction among communicating entities in a given neighborhood. Thus, in general, before a node starts communicating, it must discover the set of nodes that are within its direct communication range. Once this information is gathered, the node keeps it in an internal data structure so it can be used in different networking activities such as routing. The behavior of an ad hoc node depends on the behavior of its neighboring nodes because it must sense the medium before it starts transmitting packets to nodes in its interfering range, which can cause collisions at the other nodes.

Node discovery can be achieved with periodic transmission of beacon packets (active discovery) or with promiscuous snooping on the channel to detect the communication activity (passive discovery). In PRADA [1], a given source node sends periodically to its neighboring nodes a discovery packet, and in turn their neighbors reply with a location update packet (that might include, for instance, the node's geographical location). PRADA adjusts dynamically its communication range, called topology knowledge range, so it leads to a faster convergence of its neighboring nodes.

Packet Forwarding Algorithms. An important part of a routing protocol is the packet forwarding algorithm that chooses among neighboring nodes the one that is going to be used to forward the data packet. The forwarding algorithm implements a forwarding goal that may be, for instance, the shortest average hop distance from source to destination. In this case, the set of potential nodes may include only those in direct communication range from the current node or also the set of possible nodes in the route to the destination. The forwarding goal may also include some QoS parameters such as the amount of energy available at each node.

The following forwarding algorithms consider only nodes that are in direct communication range of the node that has a data packet to be forwarded, as depicted in Figure 1.2. The Most Forward within Radius (MFR) forwarding algorithm [2] chooses the node that maximizes the distance from node *S* to point *p*. In this case, as depicted in Figure 1.2, it is node 1. On the other hand, the Nearest Forward Progress (NFP) forwarding algorithm [3] chooses the node that minimizes the distance from node *S* to point *q*. In this case it is node 2. The Greedy Routing Scheme (GRS) [4] uses the nodes' geographical location to choose the one that is closest to the destination node *D*.

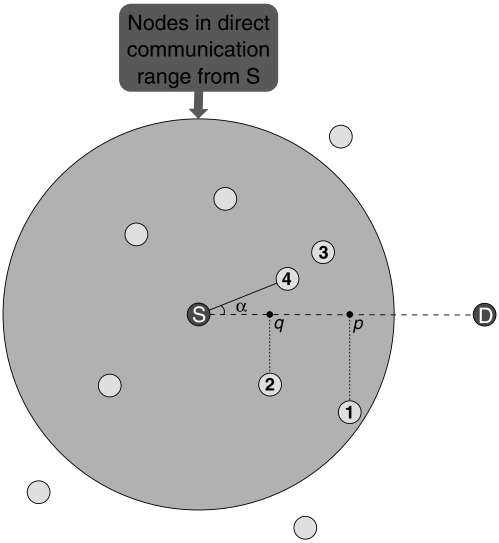

Figure 1.2. Strategies used by some forwarding algorithms.

In this case it is node 3. The compass-selected routing (COMPASS) algorithm [5] chooses the node that minimizes the angle α but considers the nodes that are closer to node D. In this case it is node 4. The random process forwarding algorithm [6], as the name suggests, chooses a random node that is in direct communication range from S.

The Partial Topology Knowledge Forwarding (PTKF) algorithm [1] chooses a node using a localized shortest path weighted routing where routes are calculated based on the local topological view and consider the transmission power needed to transmit in that link.

1.3.2 Topology Control

Topology control algorithms select the communication range of a node, and they construct and maintain a network topology based on different aspects such as node mobility, routing algorithm, and energy conservation [7]. Broadly speaking, topology control algorithms for ad hoc networks can be classified in hierarchical or clustering organization, as well as in power-based control organization [7, 8]. Furthermore, these algorithms can be either centralized, distributed, or localized.

Clustering Algorithms. The clustering process consists in defining a cluster-head node and the associated communication backbone, typically using a heuristic. The goal is to avoid redundant topology information so the network can work more efficiently. Clustering algorithms are often modeled as graph problems such as the minimum connected dominating set (MCDS) [9]. This problem asks for the minimum subset of nodes V' in the original graph $G = (V, E)$ such that V' form a dominating set of G and the resulting subgraph of the MCDS has the same number of connected components of G. It means that if G is a connected graph, so is the resulting subgraph. MCDS is an NP-complete problem [10], and thus we must look for approximate solutions [7]. In the case of the clustering algorithm, nodes in the dominating set represent the cluster heads and the other nodes are their neighbors. An inherit characteristic of an ad hoc network, which makes this problem much more difficult, is that its topology is dynamic.

The cluster heads can be elected using either deterministic or nondeterministic approaches. A deterministic solution is similar to a distributed synchronous algorithm in the sense that it runs in rounds. In this case there is just one round, and after finishing it the cluster heads are chosen. Suppose we have a node and its neighboring nodes—that is, its one-hop neighborhood. The lowest ID solution selects the node with the lowest identifier among them to create the minimal dominating set (MDS) [10]. The max degree solution selects the node with the highest degree among them [11, 12]. The MOBIC solution examines the variations of RSSI (received signal strength indicator) signal among them to select the cluster head [13].

A nondeterministic solution runs multiple incremental steps to avoid variations in the election process and to minimize conflicts among cluster heads in their one-hop neighborhood. Examples of this approach are CEDAR [11], SPAN [14], and solutions based on a spanning tree algorithm [9].

Power-Based Control Algorithms. A mobile node in a MANET must rely on a energy source (typically a battery) to execute all its tasks. Batteries need to be recharged to provide a continuous energy supply for a node. To extend the lifetime of nodes in an ad hoc network, we need algorithms to determine and adaptively adjust the transmission power of each node so as to meet a given minimization goal and, at the same time, maintain a given connectivity constraint. Some possible minimization goals are to control the maximum or average power and define a maximum or average connectivity degree. Some connectivity constraints are a simplex communication or a full-duplex communication (biconnected). Ramanathan and Hain [2] propose a topology control algorithm that dynamically adjusts its transmission power such that the maximum power used is minimized while keeping the network biconnected.

1.3.3 Routing

The main goal of an ad hoc network routing algorithm is to correctly and efficiently establish a route between a pair of nodes in the network so a message can be delivered according to the expected QoS parameters [15, 16]. The establishment of a route should be done with minimum overhead and bandwidth consumption. In the current wired networks, there are different link state [17] and distance vector [18] routing protocols, which were not designed to cope with constant topology changes of mobile ad hoc environments. Link-state protocols update their global state by broadcasting their local state to every other node, whereas distance-vector protocols exchange their local state to adjacent nodes only. Their direct application to a MANET may lead to undesired problems such as routing loops and excessive traffic due to the exchange of control messages during route establishment.

An ad hoc network has a dynamic nature that leads to constant changes in its network topology. As a consequence, the routing problem becomes more complex and challengeable, and it probably is the most addressed and studied problem in ad hoc networks. This reflects the large number of different routing algorithms for MANETs proposed in the literature [15].

Ideally, a routing algorithm for an ad hoc network should not only have the general characteristics of any routing protocol but also consider the specific characteristics of a mobile environment—in particular, bandwidth and energy limitations and mobility. Some of the characteristics are: fast route convergence; scalability; QoS support; power, bandwidth, and computing efficient with minimum overhead; reliability; and security. Furthermore, the behavior of an ad hoc routing protocol can be further complicated by the MAC protocol. This is the case of a data link protocol that uses a CSMA (Carrier Sense Multiple Access) mechanism that presents some problems such as hidden stations and exposed stations.

In general, routing algorithms for ad hoc networks may be divided into two broad classes: proactive protocols and reactive on-demand protocols, as discussed in the following.

Proactive Protocols. Proactive routing algorithms aim to keep consistent and up-to-date routing information between every pair of nodes in the network by proactively propagating route updates at fixed time intervals. Usually, each node maintains this information in tables; thus, protocols of this class are also called table-driven algorithms. Examples of proactive protocols are Destination-Sequenced Distance Vector (DSDV) [19], Optimized Link-State Routing (OLSR) [20], and Topology-Based Reverse Path Forwarding (TBRPF) Protocols [21].

The DSDV protocol is a distance vector protocol that incorporates extensions to make its operation suitable for MANETs. Every node maintains a routing table with one route entry for each destination in which the shortest path route (based on the number of hops) is recorded. To avoid routing loops, a destination sequence number is used. A node increments its sequence number whenever a change occurs in its neighborhood. When given a choice between alternative routes for the same destination, a node always selects the route with the greatest destination sequence number. This ensures utilization of the route with the most recent information.

The OLSR protocol is a variation version of the traditional link state protocol. An important aspect of OLSR is the introduction of multipoint relays (MPRs) to reduce the flooding of messages carrying the complete link-state information of the node and the size of link-state updates. Upon receiving an update message, the node determines the routes (sequence of hops) to its known nodes. Each node selects its MPRs from the set of its neighbors such that the set covers those nodes that are distant two hops away. The idea is that whenever a node broadcasts a message, only those nodes present in its MPR set are responsible for broadcasting the message.

The Topology-Based Reverse Path Forwarding is also a variation of the link-state protocol. Each node has a partial view of the network topology, but is sufficient to compute a shortest path source spanning tree rooted at the node. When a node receives source trees maintained at neighboring nodes, it can update its own shortest path tree. TBRPF exploits the fact that shortest path trees reported by neighbor nodes tend to have a large overlap. In this way, a node can still compute its shortest path tree even if it receives partial trees from its neighbors. In this way, each node reports part of its source tree, called reported tree (RT), to all of its neighbors to reduce the size of topology update messages, which can be either full or differential. Full updates are used to send to new neighbors the entire RT to ensure that the topology information is correctly propagated. Differential updates contain only changes to RT that have occurred since the last periodic update. To reduce further the number of control messages, topology updates can be combined with Hello messages so that fewer control packets are transmitted.

Reactive Protocols. Reactive on-demand routing algorithms establish a route to a given destination only when a node requests it by initiating a route discovery process. Once a route has been established, the node keeps it until the destination is no longer accessible, or the route expires. Examples of reactive protocols are Dynamic Source Routing (DSR) [22] and Ad Hoc On-Demand Distance Vector (AODV) [23].

The DSR protocol determines the complete route to the destination node, expressed as a list of nodes of the routing path, and embeds it in the data packet. Once a node receives a packet it simply forwards it to the next node in the path. DSR keeps a cache structure (table) to store the source routes learned by the node. The discovery process is only initiated by a source node whenever it does not have a valid route to a given destination node in its route cache. Entries in the route cache are continually updated as new routes are learned. Whenever a node wants to know a route to a destination, it broadcasts a route request (RREQ) message to its neighbors. A neighboring node receives this message, updates its own table, appends its identification to the message and forwards it, accumulating the traversed path in the RREQ message. A destination node responds to the source node with a route reply (RREP) message, containing the accumulated source route present in the RREQ. Nodes in DSR maintain multiple routes to a destination in the cache, which is helpful in case of a link failure.

The AODV protocol keeps a route table to store the next-hop routing information for destination nodes. Each routing table can be used for a period of time. If a route is not requested within that period, it expires and a new route needs to be found when needed. Each time a route is used, its lifetime is updated. When a source node has a packet to be sent to a given destination, it looks for a route in its route table. In case there is one, it uses it to transmit the packet. Otherwise, it initiates a route discovery procedure to find a route by broadcasting a route request (RREQ) message to its neighbors. Upon receiving a RREQ message, a node performs the following actions: checks for duplicate messages and discards the duplicate ones, creates a reverse route to the source node (the node from which it received the RREQ is the next hop to the source node), and checks whether it has an unexpired and more recent route to the destination (compared to the one at the source node). In case those two conditions hold, the node replies to the source node with a RREP message containing the last known route to the destination. Otherwise, it retransmits the RREQ message.

Some Comments. An important question is to determine the best routing protocol to be used in a MANET. This is not a simple issue, and the identification of the most appropriate algorithm depends on different factors such as QoS guarantees, scalability, and traffic and mobility pattern. Reactive protocols tend to be more efficient than proactive protocols in terms of control overhead and power consumption because routes are only created when required. On the other hand, proactive protocols need periodic route updates to keep information updated and valid. In addition, many available routes might never be needed, which increases the routing overhead. Proactive protocols tend to provide better quality of service than reactive protocols. In this class of protocols, routing information is kept updated; thus, a route to a given destination is available and up-to-date, which minimizes the end-to-end delay. Royer and Toh [15] present a comparison of these protocols in terms of their complexity, route update patterns, and capabilities.

The above classification is very broad, and there are other taxonomies to categorize routing protocols [24]. For instance, there are protocols that use a hybrid scheme to route messages; that is, they try to combine the advantages of some protocols, whereas there are protocols that use the node's geographical location to route messages.

It is interesting to observe that some IETF MANET Internet Drafts [mobile ad hoc networks (MANETs)] have reached a reasonable level of maturity, analysis, and implementation experience and became IETF standards. This includes the proactive protocols Optimized Link-State Routing (OLSR) [20] and Topology Dissemination-Based Reverse Path Forwarding (TBRPF) [21] and the reactive protocols Distributed Source Routing (DSR) [22] and Ad Hoc On-Demand Distance Vector (AODV) [23].

1.3.4 Multicasting and Broadcasting

An important aspect in the design of a routing protocol is the type of communication mode allowed between peer entities. Routing protocols for a MANET can be unicast, geocast, multicast, or broadcast. Unicast is the delivery of messages to a single destination. Geocast is the delivery of messages to a group of destinations identified by their geographical locations. Multicast is the delivery of messages to a group of destinations in such a way that it creates copies only when the links to the destinations split. Finally, broadcast is the delivery of a message to all nodes in the network.

Notice that, broadly speaking, there are two types of physical transmission technology that are largely used: broadcast links and point-to-point links. In a network with a single broadcast channel, all communicating elements share it during their transmissions. In a network that employs a wireless medium, which is the case of a mobile ad hoc network, broadcast is a basic operation mode whereby a message is received by all the source node's neighbors. In a MANET, the four communication modes that can be implemented by a routing protocol are realized by a wireless broadcast channel.

A multicast routing protocol is employed when a mobile node wants to send the same message or stream of data to a group of nodes that share a common interest. If there is a geographical area (location) associated with the nodes that will receive the message or stream of data, we use a geocast protocol. Thus, a geocast protocol is a special type of multicast protocol, such that nodes need their updated location information along the time to delivery a message. In a multicast communication, nodes may join or leave a multicast group as desired, whereas in a geocast communication, nodes can only join or leave the group by entering or leaving the defined geographical region.

In a MANET, a multicast communication can possibly bring benefits to the nodes such as bandwidth and energy savings. However, the maintenance of a multicast route, often based on a routing tree or mesh, is a difficult problem for mobile ad hoc multicasting routing protocols due to the dynamic nature of a MANET. In particular, the cost of keeping a routing tree connected for the purpose of multicast communication may be prohibited. In a multicast mesh, a message can be accepted from any router node, as opposed to a tree that only accepts packets routed by tree nodes. Thus, a multicast mesh is more suitable for a MANET because it supports a higher connectivity than a tree. The method used to build the routing infrastructure (tree or mesh) in a mobile ad hoc network distinguishes the different multicasting routing protocols.

Some of the route-tree-based multicast protocols for MANETs are AMRoute (Adhoc Multicast Routing Protocol) [25], DDM (Differential Destination Multicast) [26], and MAODV (Multicast Ad-hoc On-Demand Distance Vector routing) [27]. AMRoute uses an overlay approach based on bidirectional unicast tunnels to connect group members into the mesh. DDM is a stateless multicast protocol in the sense that no protocol state is maintained at any node except for the source node. Intermediate nodes cache the forwarding list present in the packet header. When a route change occurs, an upstream node only needs to pass to its downstream neighbors the difference to the forwarding nodes since the last packet. MAODV is the multicast version of the AODV protocol [23]. It uses a multicast route table (MRT) to support multicast routing. A node adds new entries into the MRT after it is included in the route for a multicast group. MAODV uses a multicast group leader to create an on-demand core-based tree structure.

Different from the previous route-tree-based multicast algorithms, LGT (Location-Guided Tree Construction Algorithm for Small Group Multicast) [28] uses the location information of the group members to build the multicast tree without the knowledge of the network topology. Two heuristics are proposed to build the multicast tree using location information: the Location-Guided *k*-rray tree (LGK) and the Location-Guided Steiner tree (LGS).

Some of the mesh-based multicast routing protocols for MANETs are CAMP (Core-Assisted Mesh Protocol) [29], FGMP (Forwarding Group Multicast Protocol) [30], and ODMRP (On-Demand Multicast Routing Protocol) [31]. CAMP generalizes the notion of core-based trees introduced for Internet multicasting. It uses core nodes for limiting the control traffic needed for the creation of a multicast mesh avoiding flooding. On the other hand, both FGMP and ODMRP use flooding to build the mesh. In the FGMP protocol, the receiver initiates the flooding process, whereas in the ODMRP the senders initiates it.

1.3.5 Transport Protocols

The Transmission Control Protocol (TCP) is by far the most used transport protocol in the Internet. It is the typical protocol for most network applications. TCP is a reliable connection-oriented stream transport protocol that has the following features: explicit and acknowledged connection initiation and termination; reliable, in-order, and not duplicated data delivery; flow control; congestion avoidance; and out-of-band indication of urgent data.

An important design issue of TCP is that it uses packet loss as an indication of network congestion, and it deals with this effectively by making corresponding transmission adjustment to its congestion window. In wired networks, error rates are quite low and the TCP's congestion avoidance mechanism works very well.

The mobile multihop ad hoc network introduces new challenges to the TCP protocol due to the frequent change in network topology, disconnections, variation in link capacity, and high error rate. In fact, issues present in the physical, MAC, and network layers can affect the performance of the TCP protocol. In a wireless mobile ad hoc network, packet losses are usually not caused by network congestion, but by error transmissions and frequent disconnections due to mobility, resulting in backoff mechanisms being inappropriately invoked. This reduces the network throughput and increases the delay for data transmission. The variation in link capacity, the presence of asymmetric links, and delayed acknowledgment of messages can seriously affect the

TCP's dynamic congestion window mechanism. In summary, standard TCP flow control and congestion control mechanisms do not work well in mobile ad hoc networks. The error control mechanisms of MAC protocols can affect the TCP performance. Timeouts in TCP and MAC can cause different perceptions for both protocols. For a MAC protocol as opposed to the TCP protocol, it is easier to distinguish a link failure from a congestion failure. Finally, the characteristics of the underlying routing protocol can impact the TCP performance. For instance, some reactive routing protocols (such as DSR) send back a path failure message to the source node whenever there is a broken link to the destination node. The source nodes starts a new route computation, thereby increasing the time to route packets and, probably, leading TCP to experience timeouts during each route computation time, especially if there is heavy traffic in the network.

There are at least two strategies to adapt the TCP protocol to a mobile ad hoc network [32]. The first one is to make TCP mobility-aware by adding to it mechanisms and support from the underlying protocols to diminish the impact caused by mobility. ELFN (explicit link failure notification) [33] provides the TCP sender with information about the link status and route failures. In this way, whenever there is some physical problem, the TCP avoids triggering the congestion avoidance mechanism (as if a congestion occurred) and consequently reducing the overall system performance. The second strategy uses a protocol stack such that the TCP keeps its original behavior whereas the underlying protocols incorporate the required mechanisms to mask out the negative effects of mobility on TCP. Notice that these protocols need to be designed to adjust to the principles of TCP. Atra [34] is a framework that aims to minimize the probability of a route failure, predict route failures in advance so the source node can recompute an alternate route before the existing one fails, and minimize the latency in conveying route failure information to the source node, when a prediction was not successfully predicted.

A third strategy is to design a new transport protocol for the mobile ad hoc network. The expected advantage of this approach is to have a protocol that fits better the ad hoc environment. On the other hand, its integration to an existing protocol stack may be more difficult. The ATP (Ad-Hoc Transport Protocol) [35] is a protocol designed to cope with the problems present in TCP arising from mobility. It is a rate-based transport protocol. ATP defines three entities: ATP sender, intermediate node, and ATP receiver. The ATP sender is responsible for connection management, reliability, congestion control, and initial rate estimation. The intermediate nodes help the ATP sender in its operations by providing network information regarding congestion control and initial rate estimation. The ATP receiver is responsible for collating the information provided by the intermediate nodes before sending the final feedback to the ATP sender for reliability, rate, and flow control.

1.3.6 Energy Conservation

Mobile devices in a MANET must operate under energy constraints since they typically rely on a battery, which has a finite capacity. For these mobile nodes, the most important system design criteria for optimization may be energy conservation [36].

Thus energy represents one of the greater constraints in designing algorithms for mobile devices [37]. It is interesting to notice that energy conservation is related to all network layers [38, 39], including MAC [40], routing [41], and application [42] protocols for MANETs.

Power-aware protocols are often based on the following techniques: active and standby modes switching, power setting, and retransmission avoidance. Mode switching between active and standby aims to avoid spending energy during system idle periods. Furthermore, power transmission must be set to the minimum level for the correct message reception at the destination. Retransmissions should be avoided since they waste energy by sending messages that will not be processed by the destination nodes. Power awareness is achieved using power management or power control mechanisms [40]. A power management mechanism alternates the state of a mobile device *wake* and *sleep* periods. Furthermore, the wireless data interface consumes nearly the same amount of energy in the receive, transmit, and idle states, whereas in the sleep state, a data interface cannot transmit or receive, and thus its power consumption is highly reduced [43]. However, it is not possible to have a mobile device most of the time in power-saving mode (sleep state), which will extend its battery lifetime but comprise the network lifetime, because ad hoc networks rely on cooperative efforts among participating nodes to deliver messages.

A possible strategy is to allow the network data interface to enter a power-saving mode while trying to achieve a minimum impact to the process of sending and receiving messages. In general, these algorithms depend on data collected from the physical and MAC layers. For instance, an algorithm can monitor the transmission error rates to avoid useless transmissions when the channel noise reduces the probability of a successful transmission [44, 45]. At the MAC layer, an algorithm can save energy by determining intervals during which the network data interface does not need to be listening [46]. This is the case, for instance, whenever a node transmits a message and the other nodes within the same interference and carrier sensing range must remain silent. During this period, these nodes can sleep with little or no impact on system behavior. Related to this strategy is to have a density control algorithm controlling the operational mode of mobile devices so only those needed to forward the data traffic are awake and the overall network lifetime is optimized [47]. The strategies of controlling the transmission power and the node density in a MANET must be performed very carefully. Reducing the transmission power and keeping the node density to a minimum level may lead to a smaller number of available data communication links among nodes and, hence, a lower connectivity that can increase the number of messages not transmitted.

1.3.7 Network Security

Mobile ad hoc networks are generally more prone to physical security threats than are fixed-wired networks [48, 49]. The broadcast nature of the wireless channels, the absence of a fixed infrastructure, the dynamic network topology, the collaborative multihop communication among nodes, and the self-organizing characteristic of the network increase the vulnerabilities of a mobile ad hoc network.

The starting point to provide a proper security solution for a mobile ad hoc network is to understand the possible forms an attack can happen. In a MANET, a security problem may happen at any network layer and include: data integrity attacks, by accessing, modifying, or injecting traffic; denial-of-service attacks; flow-disruption attacks, by delaying, dropping, or corrupting data passing through, but leaving routing traffic unmodified; passive eavesdropping; resource depletion attacks, by sending data with the objective of congesting a network or draining batteries; signaling attacks, by injecting erroneous routing information to divert network traffic, or making routing inefficient; and stolen device attacks.

Given the variety of possible attacks to a mobile ad hoc network, different solutions have been proposed to address them [49]. The first step is to protect the wireless network infrastructure against malicious attacks. Digital signatures can be used to authenticate a message and prevent attackers from injecting erroneous routing information and data traffic inside the network [50]. This scheme requires a certification authority function to manage the private–public keys and to distribute keys via certificates, which needs to be distributed over multiple nodes in the MANET [51]. A strategy is to use a threshold cryptographic model to distribute trust among the MANET nodes [52, 53]. This model tolerates a threshold t of corruptions/collusions in the network, whereas it allows any set of $t + 1$ nodes to make distributed decisions such as regarding admission of new nodes to the network. These proposals require that each node must receive a certificate and a secret share in a distributed manner. However, as long as each node is able to obtain an updated VSS information (Feldman's Verifiable Secret Sharing mechanism [54]), there is no need for node-specific certificates, and it is possible to create new secret shares in a distributed manner [55].

In many mobile ad hoc network applications, such as emergency disaster relief and information sharing in a meeting, it is important to guard against attacks such as malicious routing misdirection [56]. The problem is that ad hoc routing protocols were designed to trust all participants, are cooperative by nature, and depend on neighboring nodes to route packets. This naive trust model allows malicious nodes to attack a MANET by inserting erroneous routing updates, replaying old messages, changing routing updates, or advertising incorrect routing information. Furthermore, a mobile ad hoc environment makes the detection of these problems more difficult [57]. Some of the proposed solutions to the problem of secure routing in a MANET involve the use of a pre-deployed security infrastructure [58], concealing the network topology or structure as in the Zone Routing Protocol [59], and introducing mechanisms in the network to mitigate routing misbehavior such as the SAR (Security-Aware Ad Hoc Routing) technique [60] to add security attributes to the route discovery [61].

1.4 APPLICATIONS

Mobile ad hoc networks have been employed in scenarios where an infrastructure is unavailable, the cost to deploy a wired networking is not worth it, or there is no time to set up a fixed infrastructure. In all these cases, there is often a need for collaborative computing and communication among the mobile users who typically work as teams—for instance, medical personnel in a search and rescue mission, firefighters facing a hazardous emergency, policemen conducting surveillance of suspects, and soldiers engaging in a fight. When we consider all these usual driving applications managed by specialized people, we understand why there is a slow progress in deploying commercial ad hoc applications to ordinary people.

This situation may change with the deployment of opportunistic ad hoc networks [62]. These networks aim to enable user communication in an environment where disconnection and reconnection are common activities and link performance is dynamic. They are very suitable to support the situation where a network infrastructure has limited coverage and users have "islands of connectivity." By taking advantage of device mobility, information can be stored and forwarded over a wireless link when a connection "opportunity" arises, such as an appropriate network contact happens. In this view, the traditional MANET incorporates the special feature of connection opportunity.

A MANET can be used to provide access to crisis management applications, such as in a disaster recovery, where the entire communication infrastructure is destroyed and establishing communication quickly is crucial [63]. By using a mobile ad hoc network, an infrastructure could be set up in hours rather than days or weeks, as in the case of a wired networking.

One of many possible uses of a mobile ad hoc network is in noncritical and collaborative applications. One example is a business environment where the need for collaborative computing might be more important outside the office, such as in a business meeting at the client's office to discuss a project. Another viable example is to use a mobile ad hoc network for a radio dispatch system [64]. This system can be used, for instance, in a taxi dispatch system based on MANET.

When a user wants to use an existing application on the Internet in a mobile ad hoc network, it is important to investigate its performance. This is the case, for instance, of Gnutella, one of the most widely used peer-to-peer systems, which needs to be evaluated before putting it through typical ad hoc conditions such as node mobility and frequent network partitioning [65].

Another application area is communication and coordination in a battlefield using autonomous networking and computing [66]. Some military ad hoc network applications require unmanned, robotic components. Unmanned Airborne Vehicles (UAVs) can cooperate in maintaining a large ground mobile ad hoc network interconnected in spite of physical obstacles, propagation channel irregularities, and enemy jamming. The UAVs can help meet tight performance constraints on demand by proper positioning and antenna beaming.

A vehicular ad hoc network (VANET) is a mobile ad hoc network designed to provide communications among close vehicles and between vehicles and nearby fixed equipment. The main goal of a VANET is to provide safety and comfort for passengers. To this end, a special electronic device is placed inside each vehicle that will provide ad hoc network connectivity for the passengers and vehicle. Generally, applications in a VANET fall into two categories, namely safety applications and comfort applications [67, 68]. Safety applications aim to provide driver's information about future critical situations and, hence, have strict requirements on communication reliability and delay. Some of the safety applications envisioned for VANETs are intervehicle danger warning, intersection collision avoidance, and work zone safety warning. Comfort applications aim to improve the driving comfort and the efficiency of the transportation system and, hence, are more bandwidth-sensitive instead of delay-sensitive. Some of the comfort applications are on-board Internet access, high data rate content download (electronic map download/update), and driving through payment [68].

With numerous emerging applications, opportunistic ad hoc networks have the potential to allow a large number of devices to communicate end-to-end without requiring any pre-existing infrastructure and are very suitable to support pervasive networking scenarios. For instance, suppose we want to (a) communicate with a mobile user who is temporarily out of reach or (b) establish a public wireless mesh that includes not only fixed access points but also vehicles and pedestrians, or interconnect groups of roaming people in different locations via the Internet. It seems that finally mobile ad hoc networks and Internet are coming together to produce in the next few years viable commercial applications.

1.5 CONCLUDING REMARKS

A mobile ad hoc network is one of the most innovative and challenging areas of wireless networking and tends to become increasingly present in our daily life [69]. An ad hoc network is clearly a key step in the next-generation evolution of wireless data communication when we consider the different enabling networks and technologies. An ad hoc network inherits the traditional problems of wireless and mobile communications, including bandwidth optimization, power control, and transmission quality enhancement. In addition, MANETs pose new research problems due to the multihop nature and the lack of a fixed infrastructure. These problems are related to algorithms for different aspects such as network configuration, topology discovery and maintenance, and routing.

The problems in ad hoc networks face a very important and fundamental question that is the dynamic network topology. This has a serious impact on the design of algorithms for ad hoc networks since they are expected to work properly under different and unpredictable scenarios. Similar to other distributed problems, a designer can start reasoning about an algorithm for this type of network, initially considering a static version of the problem. In a static version, it is reasonable to assume that there is a global topological information of the network, the computation happens just once, and the proposed solution is a centralized algorithm. On the other hand, when we consider a dynamic solution for the same problem, it is reasonable to assume that there is only local information, the computation happens continuously along the time the network is operational, and the proposed solution is a distributed algorithm. Clearly, the dynamic solution is more useful for ad hoc networks. However, a detailed study of the static solution tends to provide valuable insight for the design of a distributed version, is useful to determine the upper bound on the performance of the algorithm, can even be applied to stationary ad hoc networks such as commercial mesh-based broadband wireless solutions, and is simple to understand.

REFERENCES

1. T. Melodia, D. Pompili, and I. F. Akyildiz. On the interdependence of topology control and geographical routing in ad hoc and sensor networks. *IEEE Journal on Selected Areas in Communications*, **23**(3):520–532, 2005.
2. R. Ramanathan and R. Hain. Topology control of multihop wireless networks using transmit power adjustment. In *IEEE INFOCOM*, Tel Aviv, Israel, March 2000, pp. 404–413.
3. H. Takagi and L. Kleinrock. Optimal transmission ranges for randomly distributed packet radio terminals. *IEEE Transactions on Communications*, **32**(3):246–257, 1984.
4. T. C. Hou and V. O. K. Li. Transmission range control in multihop packet radio terminals. *IEEE Transactions on Communications*, **34**(1):38–44, 1986.
5. G. G. Finn. Routing and addressing problems in large metropolitan scale internetworks. Technical Report RR–87–180, ISI Research Report, 1987.
6. R. Nelson and L. Kleinrock. The spatial capacity of a slotted aloha multihop packet radio network with capture. *IEEE Transactions on Communications*, **32**(6):684–694, 1984.
7. L. Bao and J. J. Garcia-Luna-Aceves. Topology management in ad hoc networks. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03)*, Annapolis, MD, ACM, New York 2003, pp. 40–48.
8. Y. Xu, S. Bien, Y. Mori, J. Heidemannn, and D. Estrin. Topology control protocols to conserve energy in wireless ad hoc networks. Technical Report Center for Embedded Networked Sensing Technical Report 6, UCLA, 2003.
9. S. Guha and S. Khuller. Approximation algorithms for connected dominating sets. *Algorithmica*, **20**(4):374–387, 1998.
10. M. R. Garey and D. S. Johnson. *A Guide to Theory of NP-Completeness*. Freeman, Oxford, UK, 1979.
11. R. Sivakumar, P. Sinha, and V. Bharghavan. Cedar: A core-extraction distributed ad hoc routing algorithm. *IEEE Journal on Selected Areas in Communications*, **17**(8):1454–14655, 1999.
12. L. Jia, R. Rajaraman, and T. Suel. An efficient distributed algorithm for constructing small dominating sets. In *Proceedings of the ACM Symposium on Principles of Distributed Computing (PODS '01)*, Newport, RI, 2001.
13. P. Basu, N. Khan, and T. D. C. Little. A mobility based metric for clustering in mobile ad hoc networks. In *Proceedings of the International Workshop on Wireless Networks and Mobile Computing (WNMC '01)*, Scottsdale, AZ, 2001, pp. 72–80.
14. B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01)*, Rome, Italy, 2001, pp. 62–70.
15. E. M. Royer and C.-K. Toh. A review of current routing protocols for ad-hoc mobile wireless networks. *IEEE Personal Communications*, April 1999, pp. 40–45.
16. M. Ilyas, editor. *The Handbook of Ad Hoc Wireless Networks*. CRC Press, Boca Raton, FL, 2003.
17. J. M. McQuillan, I. Richer, and E. C. Rosen. The new routing algorithm for the ARPANet. *IEEE Transactions on Communications*, **28**(5):711–719, 1980.

18. C. Hedrick. Routing Information Protocol. Request for Comments 1058, June 1988. Available at http://www.ietf.org/rfc/rfc1058.txt.

19. C. E. Perkins and P. Bhagwat. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers. *SIGCOMM '94—Computer Communications Review*, **24**(4):234–244, 1994.

20. T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). Request for Comments 3626, October 2003. Available at http://www.ietf.org/rfc/rfc3626.txt.

21. R. Ogier, F. Templin, and M. Lewis. Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). Request for Comments 3684, February 2004. Available at http://www.ietf.org/rfc/rfc3684.txt.

22. D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. Request for Comments 4728, February 2007. Available at http://www.ietf.org/rfc/rfc4728.txt.

23. C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Request for Comments 3561, February 2007. Available at http://www.ietf.org/rfc/rfc3561.txt.

24. M. Abolhasan, T. Wysocki, and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, **2**(1):1–22, 2004. Mobile Ad-hoc Networks (MANET). IETF Working Group. http://www.ietf.org/html. charters/manet-charter.html. MANET Internet drafts available at http://www.ietf. org/ids.by.wg/manet.html.

25. J. Xie, R. R. Talpade, A. McAuley, and M. Liu. AMRoute: Ad Hoc Multicast Routing Protocol. *Mobile Networks and Applications*, **7**(6):429–439, 2002.

26. L. Ji and M. S. Corson. Differential destination multicast—A MANET multicast routing protocol for small groups. In *Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '01)*, Anchorage, AK, April 2001, pp. 1192–1202.

27. E. M. Royer and C. E. Perkins. Multicast operation of the ad hoc on-demand distance vector routing protocol. In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99)*, Seattle, WA, August 1999, pp. 207–218.

28. K. Chen and K. Nahrstedt. Effective location-guided tree construction algorithms for small group multicast in MANET. In *Proceedings of the the ACM SIGMETRICS*, Marina del Rey, CA, June 2002, pp. 270–271.

29. E. L. Madruga and J. J. Garcia-Luna-Aceves. Scalable multicasting: The core-assisted mesh protocol. *Mobile Networks and Applications*, **6**(2):151–165, 2001.

30. C.-C. Chiang, M. Gerla, and L. Zhang. Forwarding group multicast protocol. *Journal of Cluster Computing*, **1**(2):187–196, 1998.

31. S.-J. Lee, M. Gerla, and C.-C. Chiang. On-demand multicast routing protocol. In *Proceedings of the Wireless Communications and Networking Conference (WCNC '99)*, New Orleans, LA, September 1999, pp. 1298–1302.

32. A. Al Hanbali, E. Altman, and P. Nain. A survey of TCP over ad hoc networks. *IEEE Communications Surveys & Tutorials*, **7**(3):22–36, 2005.

33. G. Holland and N. H. Vaidya. Impact of routing and link layers on TCP performance in mobile ad-hoc networks. In *Proceedings of the Wireless Communications and Networking Conference (WCNC '99)*, pages 1323–1327, New Orleans, LA, September 1999.

34. V. Anantharaman and R. Sivakumar. A microscopic analysis of TCP performance analysis over wireless ad hoc networks. In *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '02)*, New York, June 2002, pp. 1180–1189.
35. K. Sundaresan, V. Anantharaman, H.-Y. Hsieh, and R. Sivakumar. ATP: A reliable transport protocol for ad-hoc networks. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03)*, New York, Annapolis, MD, 2003, pp. 64–75.
36. A. J. Goldsmith and S. B. Wicker. Design challenges for energy-constrained ad hoc wireless networks. *Wireless Communications*, **9**(4):8–27, 2002.
37. J. R. Lorch and A. J. Smith. Software strategies for portable computer energy management. *IEEE Personal Comunications*, **5**(3):60–73, 1998.
38. C. Jones, K. Sivalingam, P. Agarwal, and J. C. Chen. A survey of energy efficient network protocols for wireless and mobile networks. *Wireless Networks*, **7**(4):343–358, July 2001.
39. V. Srivastava and M. Motani. Cross-layer design: A survey and the road ahead. *IEEE Communications Magazine*, **43**(12):112–119, 2005.
40. S. Kumar, V. S. Raghavan, and J. Deng. Medium access control protocols for ad hoc wireless networks: A survey. *Ad Hoc Networks*, **4**(3):326–358, 2006.
41. F. Xie, L. Du, Y. Bai, and L. Chen. Energy aware reliable routing protocol for mobile ad hoc networks. In *Proceedings of the Wireless Communications and Networking Conference (WCNC '07)*, Hong Kong, China, March 2007, pp. 4313–4317.
42. R. Kravets and P. Krishnan. Application-driven power management for mobile communication. *Wireless Networks*, **6**(4):263–277, 2000.
43. J. L. Sobrinho and A. S. Krishnakumar. Quality-of-service in ad hoc carrier sense multiple access wireless networks. *IEEE Journal on Selected Areas in Communications*, **17**(8): 1353–1368, 1999.
44. M. Rulnick and N. Bambos. Mobile power management for wireless communication networks. *Wireless Networks*, **3**(1):3–14, 1997.
45. M. Zorzi and R. R. Rao. Energy constrained error control for wireless channels. In *Proceedings of the Global Telecommunications Conference (GLOBECOM '96)*, London, UK, November 1996, pp. 1411–1416.
46. S. Singh and C. S. Raghavendra. PAMAS—Power Aware Multi-Access Protocol with signalling for ad hoc networks. *ACM SIGCOMM Computer Communication Review*, **28** (3):5–26, 1998.
47. L. Ma, Q. Zhang, and X. Cheng. A power controlled interference aware routing protocol for dense multi-hop wireless networks. *Wireless Networks*, **6**:50–58, 2007.
48. P. Papadimitratos and Z. J. Haas. Secure data communication in mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, **24**(2):343–356, 2006.
49. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: Challenges and solutions. *Wireless Communications*, **11**(1):38–47, 2004.
50. L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network*, **13**(6):24–30, 1999.
51. A. M. Hegland, E. Winjum, S. F. Mjølsnes, C. Rong, Ø. Kure, and P. Spilling. A survey of key management in ad hoc networks. *IEEE Communications Surveys & Tutorials*, **8**(3): 48–66, 2006.

52. K. Jiejun, Z. Petros, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for MANET. In *Proceedings of the IEEE 9th International Conference on Network Protocols (ICNP '01)*, Riverside, CA, November 2001, pp. 251–260.

53. M. Narasimha, G. Tsudik, and J. H. Yi. On the utility of distributed cryptography in P2P and MANETs. In *Proceedings of the IEEE 11th International Conference on Network Protocols (ICNP '03)*, Atlanta, GA, November 2003, pp. 336–345.

54. P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of the 28th Annual Symposium on Foundations of Computer Science (FOCS '87)*, Toronto, Canada, November 1987, pp. 427–437.

55. N. Saxena, G. Tsudik, and J.H. Yi. Efficient node admission for short-lived mobile ad hoc networks. In *Proceedings of the IEEE 13th International Conference on Network Protocols (ICNP'03)*, Boston, MA, November 2003, pp. 269–278.

56. H. Yih-Chun and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security & Privacy Magazine*, **2**(3):28–39, 2004.

57. N. Milanovic, M. Malek, A. Davidson, and V. Milutinovic. Routing and security in mobile ad hoc networks. *Computer*, **37**(2):61–65, 2004.

58. K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer. Authenticated routing for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, **23**(3):598–610, 2005.

59. Z. Haas and M. Pearlman. Zone routing protocol (ZRP): A framework for routing in hybrid ad hoc networks. In C. E. Perkins, editor, *Ad Hoc Networking*, Addison-Wesley, 2001, Reading, MA, pp. 221–253.

60. S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '01)*, Long Beach, CA, October 2001, pp. 299–302.

61. S. Gupte and M. Singhal. Secure routing in mobile wireless ad hoc networks. *Ad Hoc Networks*, **1**(1):151–174, July 2003.

62. L. Pelusi, A. Passarella, and M. Conti. Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks. *IEEE Communications Magazine*, **44**(11):134–141, 2006.

63. Y. Shibata, H. Yuze, T. Hoshikawa, K. Takahata, and N. Sawano. Large Scale Distributed disaster information system based on MANET and overlay network. In *Proceedings of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW '07)*, Toronto, Canada, June 2007, p. 7.

64. E. Huang, W. Hu, J. Crowcroft, and I. Wassell. Towards commercial mobile ad hoc network applications: A radio dispatch system. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, Urbana-Champaign, IL, May 2005, pp. 355–365.

65. M. Conti, E. Gregori, and G. Turi. A cross-layer optimization of Gnutella for mobile ad hoc networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, Urbana-Champaign, IL, May 2005, pp. 343–354.

66. D. C. Reeve, N. J. Davies, and D. F. Waldo. Constructing predictable applications for military ad-hoc wireless networks. In *Proceedings of the Military Communications Conference (MILCOM '06)*, Washington, D.C., October 2006, p. 7.

67. M. Caliskan, D. Graupner, and M. Mauve. Decentralized disovery of free parking places. In *Proceedings of the Third ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06)*, Los Angeles, CA, October 2006, pp. 30–36.

68. CAMP Vehicle Safety Communications Consortium. Vehicle Safety Communications Project: Task 3 Final Report—Identify Intelligent Vehicle Safety Applications Enabled by DSRC, March 2005. Available at http://ntlsearch.bts.gov/tris/record/tris/01002103.html.

69. I. Chlamtac, M. Conti, and J. J.-N. Liu. Mobile ad hoc networking: Imperatives and Challenges. *Ad Hoc Networks*, **1**(1):13–64, 2003.