A Survey on Wireless Ad Hoc Networks

Marcelo G. Rubinstein[1], Igor M. Moraes[2], Miguel Elias M. Campista[2], Luís Henrique M. K. Costa[2], and Otto Carlos M. B. Duarte[2]*

[1] PEL/DETEL/FEN – Universidade do Estado do Rio de Janeiro
R. São Fco. Xavier, 524 - 20550-013 - Rio de Janeiro - RJ - Brazil
[2] GTA/COPPE/Poli – Universidade Federal do Rio de Janeiro
P.O. Box 68504 - 21945-970 - Rio de Janeiro - RJ - Brazil

Abstract. A wireless ad hoc network is a collection of wireless nodes that can dynamically self-organize into an arbitrary and temporary topology to form a network without necessarily using any pre-existing infrastructure. These characteristics make ad hoc networks well suited for military activities, emergency operations, and disaster recoveries. Nevertheless, as electronic devices are getting smaller, cheaper, and more powerful, the mobile market is rapidly growing and, as a consequence, the need of seamlessly internetworking people and devices becomes mandatory. New wireless technologies enable easy deployment of commercial applications for ad hoc networks. The design of an ad hoc network has to take into account several interesting and difficult problems due to noisy, limited-range, and insecure wireless transmissions added to mobility and energy constraints. This paper presents an overview of issues related to medium access control (MAC), routing, and transport in wireless ad hoc networks and techniques proposed to improve the performance of protocols. Research activities and problems requiring further work are also presented. Finally, the paper presents a project concerning an ad hoc network to easily deploy Internet services on low-income habitations fostering digital inclusion.

1 Introduction

Wireless networks are being increasingly used in the communication among devices of the most varied types and sizes. Personal computers, handhelds, telephones, appliances, industrial machines, sensors, and others are being used in several environments, such as residences, buildings, cities, forests, and battlefields. Different wireless network standards and technologies have appeared in the last years to enable easy deployment of applications.

The deployment of wireless networks where there is no infrastructure or the local infrastructure is not reliable can be difficult. Ad hoc networks have been proposed in order to solve such problems. A wireless ad hoc network is a collection of wireless nodes that can dynamically self-organize into an arbitrary and temporary topology to form a network without necessarily using any

* Supported by CNPq, CAPES, FAPERJ, UOL, FUJB, FINEP, and FUNTTEL.

pre-existing infrastructure. In ad hoc networks, each node may communicate directly to each other. Nodes that are not directly connected communicate by forwarding their traffic through intermediate nodes. Every ad hoc node acts as a router.

The main advantages of ad hoc networks are flexibility, low cost, and robustness. Ad hoc networks can be easily set up, even in desert places and can endure to natural catastrophes and war. These characteristics make ad hoc networks well suited for military activities, emergency operations, disaster recovery, large scale community networks, and small networks for interaction between meeting attendees or students in a lecture room.

The design of a wireless ad hoc network has to take into account several interesting and difficult problems. Traditional wireless communication problems related to the physical medium, such as low transmission rate, high bit error rates, noise, limited range, and significant variation in physical medium conditions, must be overcomed. In the MAC sublayer, the difficulty of collision detection and the hidden and the exposed terminal problems demand new medium access algorithms. Moreover, as wireless ad hoc nodes may move arbitrarily and the status of the communication links between the nodes may vary, routing protocols proposed for wired networks are not suited for operation in wireless ad hoc networks. Several routing protocols have been proposed to cope with the various challenges of ad hoc networks. At the transport layer, TCP-like transport protocols also present several problems when used on wireless networks. High bit-error rates and frequent route failures reduce TCP performance, demanding modifications to TCP or the design of new transport protocols.

Other issues are also important when designing a wireless ad hoc network. The uncontained shared medium creates difficult challenges for securing the wireless network. On the other hand, the use of mobile devices equipped with radio interfaces turns energy conservation an important issue. Additionally, peculiarities of the wireless technology used, such as multiple channels and directional antennas, may improve the performance of the network but have to be carefulley taken into account in redesigning some of the protocol layers.

This paper presents an overview of issues related to MAC, routing, and transport in wireless ad hoc networks and techniques proposed to improve the performance of protocols. Research activities and problems requiring further work are also presented. Finally, the paper presents a project concerning an ad hoc network to easily deploy Internet services on low-income habitations fostering digital inclusion.

This paper is organized as follows. Section 2 presents different MAC protocols designed for wireless ad hoc networks. Section 3 describes Bluetooth and IEEE 802.11, the most widespread technologies for wireless ad hoc networks. Section 4 compares the main routing protocols for ad hoc networks. In Section 5, we present protocol proposals to solve the TCP performance issues related to wireless networks. Section 6 presents the issues related to directional antennas and security and gives an overview of a project that investigates a community ad hoc network for underserved populations.

2 Medium Access Control Protocols

The design of a suitable Medium Access Control (MAC) protocol is an important issue for an ad hoc network. The protocol must deal with channel constraints, attenuation, and noise, whereas provide an efficient medium access considering requirements, such as quality of service (QoS), low energy consumption, fairness, and scalability.

MAC protocols for wireless networks can be classified as contention-free or contention-based, depending on the medium access strategy [1]. The contention-free schemes pre-define assignments to allow stations to transmit without contending for the medium, e.g., TDMA, CDMA, FDMA, polling, and token-based. Contention-free mechanisms are normally employed to provide bounded end-to-end delay and minimum bandwidth, privileging delay sensitive applications such as audio and video streams. Bluetooth personal area networks employ a master-slave MAC mechanism. On the other hand, contention-based schemes are more appropriate for sporadic data transfer on mobile networks due to the random and temporary nature of the topologies. Wi-Fi local area networks in their ad hoc mode employ contention-based MAC protocols.

ALOHA and Slotted-ALOHA are the pioneers contention-based schemes for medium access. In ALOHA, a station accesses the medium as soon as it has a frame to send. If two or more stations send data at the same time collisions occur. To decrease the collision probability, in the Slotted-ALOHA access scheme, a station must wait for the beginning of a pre-defined interval of time to start its transmission. Slotted-ALOHA doubled the efficiency of ALOHA, however, it introduced the necessity of synchronization. CSMA (Carrier Sense Multiple Access) is another access scheme that added carrier sensing before transmitting a frame to minimize the number of collisions. In CSMA, a station that has data to send becomes aware of current transmissions sensing the medium. If a carrier is sensed, the medium is considered busy and the station postpones its medium access. Nevertheless, if the medium is idle, the station transmits its data frame immediately. CSMA can be non-persistent or p-persistent depending on the scheme deployed to attempt a transmission after sensing the medium busy. The non-persistent CSMA sets a random period of time to perform another medium access. In the p-persistent CSMA the station transmits with a probability p as soon as the medium gets idle. The most famous access scheme for wired networks is a variation of CSMA persistent that detects collisions. This scheme is employed by Ethernet and is called Carrier Sense Multiple Access with Collision Detection. Unfortunately, in free space collision detection is not possible. Thus, a successful reception is not guaranteed because stations may not sense a collision at the receiver. The phenomenon known as the hidden terminal problem is depicted in Figure 1. In this figure, each station centers a dotted circle that represents its own transmission range. In the example of Figure 1, the station A is transmitting to B. As station C cannot sense the ongoing transmission, it may also transmit to B, resulting in a collision at B.

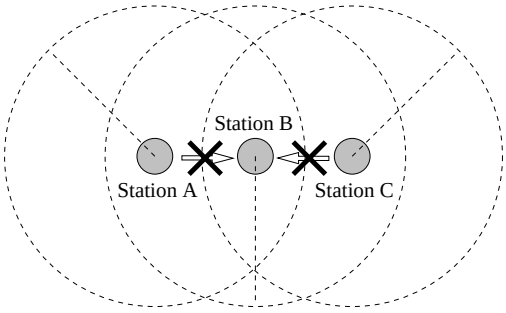


Fig. 1. The hidden terminal problem.

Unlike CSMA, the MACA (Multiple Access with Collision Avoidance) protocol [2] does not perform carrier sensing. MACA assumes that performing carrier sense before transmitting is not an efficient approach because it reduces collisions but does not completely eliminate them. To cope with the hidden terminal problem, MACA introduced a three-way handshake for data transmissions. A station that wants to transmit must immediately send a RTS (Request-To-Send) frame containing the length of the following transmission. The stations within the transmission range of the sender will defer for the time announced in RTS. Upon receiving the RTS, the destination will send a CTS (Clear-To-Send) packet to the transmitter. The stations within the transmission range of the destination will defer as well for the time announced in CTS, which corresponds to the length of the data frame. Thus, the medium will be reserved for the transmission of the upcoming frame, avoiding collisions. If the CTS is not received after a RTS transmission, a collision is inferred and the stations enter into a collision resolution phase. To resolve collisions, the stations perform a binary exponential backoff. The MACAW (MACA for Wireless LANs) protocol [3] extends MACA by adding link level acknowledgment (ACK) for data frames. The data acknowledgment at link layer is an important improvement because it accelerates the loss frame recovery, which were only initiated at transport level. MACAW also altered the backoff scheme to improve fairness.

Although the RTS/CTS mechanism avoids the hidden terminal problem, it may accentuate another typical problem of ad hoc networks, the exposed terminal. Every station that is within the transmission range of a communicating node does not send frames. This happens even if the other potential destination is out of the former receiver range. In Figure 2, station C does not transmit to D even if its transmission will not interfere at destination A.

In opposition to MACA and its derivatives, the FAMA (Floor Acquisition Multiple Access) protocol [4] shows that carrier sensing must be used along with the RTS/CTS mechanism to improve medium access. Without carrier sensing, MACA behaves essentially as ALOHA, dropping down its overall performance when the medium is high loaded. It is also shown that MACA does not completely solve the hidden terminal problem and collisions may occur between

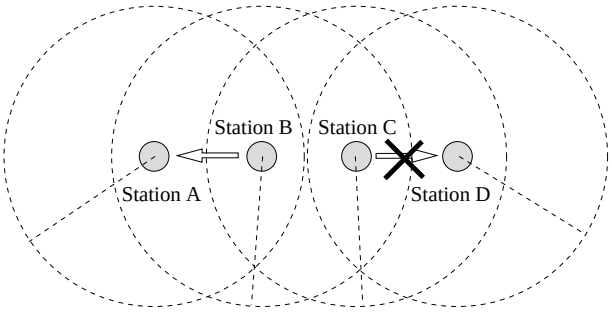


Fig. 2. The exposed terminal problem.

control and data frames. In Figure 1, depending on the propagation delays, a CTS from B to A may have already been received at A, but not at C. When A starts sending its data frame, C has not yet received the CTS, hence, it will simultaneously send a RTS to B. FAMA addresses this problem introducing intervals of time between a reception and a following transmission. These intervals, also known inter-frame spaces, must take into account the maximum propagation and processing delay of all stations within the network. This amount of time is enough to assure that the entire network is aware of the state of the current transmission. In the example above, if station B had waited some time before responding with the CTS, the RTS from C would have arrived. Thus, a collision would have been inferred between control frames, which is less harmful then a collision involving a data frame.

The CSMA/CA (CSMA with Collision Avoidance) combines characteristics of CSMA, MACA/MACAW, and FAMA. CSMA/CA senses the medium before transmissions, deploys RTS/CTS, acknowledges data frames, and uses inter-frame spaces to compensate propagation delays. Besides, CSMA/CA adds a random interval of time before transmissions to further avoid collisions from stations that were simultaneously contending for the medium. The concept of NAV (Network Allocation Vector) is also introduced in CSMA/CA. NAV is a timer maintained by each station that contains the interval of time which the medium is expected to be busy. Thus, the stations can only transmit after the expiration of the NAV. As CSMA/CA is used in the IEEE 802.11 standard, it will be examined in more details in Section 3.

Depending on the deployment of the ad hoc network, the design of the MAC protocol focus on a specific desirable characteristic. These characteristics are related to higher throughput, lower delay, lower power consumption, etc [1, 5, 6]. Next sections summarizes some existing protocols that use multiple channels, power-aware schemes, and QoS-aware schemes to achieve these goals.

2.1 Multiple Channel Protocols

The deployment of a single channel for the transmission of data and control frames increases the collision probability when a high number of nodes is ac-

tively accessing the medium. Using multiple channels, the overall performance of the network can be improved because each channel is a different collision domain and the available bandwidth increases with the number of channels. Additionally, differentiation among channels to support QoS is possible.

MAC protocols for multiple channels can be classified considering whether there is a dedicated control channel. When a dedicated control channel is used, the remaining channels are exclusive for data transmissions. In RI-BTMA (Receiver Initiated Busy Tone Multiple Access) [7] the transmitter sends a preamble to the intended destination. After receiving the preamble, the destination sets up an out-of-band busy tone to reserve the medium for the data frame. In the DBTMA (Dual Busy Tone Multiple Access) protocol [8] the transmitter emits a transmit-busy tone in the control channel after sending a RTS frame. Upon receiving an RTS frame, the receiver emits a receiver-busy tone to reserve the medium. When a dedicated control channel is not used, all traffic is shared among the multiple channels. In the Multi-Channel CSMA protocol [9] the total available bandwidth is divided by N distinct channels. Every station senses the last used channel before attempting a transmission. If the last channel used is idle, the station sends its frame. Otherwise, the station randomly chooses another channel to transmit. The Hop-Reservation Multiple Access (HRMA) protocol [10] employs frequency hopping to send data frames.

Multiple channel protocols must deal with distributed mechanisms to manage channel assignments. This requirement represents the major drawback of this approach. Contention-free schemes can also be used, however, these schemes introduce synchronization requirements and, as consequence, complexity and cost that are not desirable in ad hoc networks.

Currently, the deployment of multiple channels along with multiple interfaces is receiving especial attention in Wireless Mesh Networks (WMN) [11, 12]. Mesh Networks are a special case of hybrid ad hoc network, where fixed nodes are used to guarantee connectivity and interconnection to isolated nodes. The fixed nodes can be considered an infrastructure.

2.2 Power-aware Protocols

Mobile wireless devices are battery powered, therefore, energy constraints must be taken into account. In mobile ad hoc networks, stations must be able to save energy to extend their battery lifetimes. Power-aware protocols use three basic techniques: active and standby modes switching, power setting, and retransmissions avoidance. Switching between active and standby modes avoids wasting energy during idle periods. In addition, power must be set, during transmissions, to the minimum necessary for the receiver correctly receive the data frames. Finally, retransmissions are also power consuming due to successive transmissions of a single frame.

Currently, the power-aware proposals implement power management or power control mechanisms [13, 1]. In power management mechanisms, the stations must alternate between “wake” and “sleep” periods. In the PAMAS

(Power Aware Medium Access Control with Signaling) protocol [14] the destination sends a busy tone in the out-of-band channel when receiving a data frame to signalize that the medium is busy. The neighbors decide, upon listening to the busy tone, whether it is worth to power down their transceivers since they cannot transmit. The Dynamic Power Saving Mechanism (DPSM) protocol [15] uses beacons to divide the time in intervals. The beacons announce the status of the frame to be sent in the following interval. After participating on a communication in the prior interval, the transmitter and the destination may decide to sleep. In power management mechanisms, it is important to define when to sleep and when to be awake so as not to loose availability.

The control mechanisms adapt the transmission power according to the minimum necessary for a correct reception at the destination. In the Power Control MAC (PCM) protocol [16], besides avoiding the hidden terminal problem, the RTS/CTS mechanism is used to negotiate the transmission power of the data and the ACK frames. In the Power Controlled Multiple Access (PCMA) protocol [17] the power to send data and ACK frames is set similarly to PCM. Power control mechanisms face problems regarding accurate power measurements and the variability of medium conditions concerning noise and attenuation.

2.3 QoS-aware Protocols

Providing QoS in ad hoc networks means guarantee limited end-to-end delay and minimum bandwidth to specific flows. These requirements arise with delay sensitive applications such as video and audio streams. In a wireless environment, however, it is difficult to guarantee QoS given the medium unpredictability. Moreover, it is a major challenge to distinguish between frame losses due to collisions and congestions, or erroneous receptions because of high bit error rate. The distributed scheme and the dependency on other stations to forward data frames in multihop communications further aggravate the problem.

To guarantee QoS constraints, the whole protocol stack must be aware of the QoS requirements. There are some frameworks that aim to define guidelines to assure QoS in ad hoc networks using cross-layer models [18, 19, 20]. At the MAC layer, one possible approach involves synchronous schemes that are not suitable for distributed networks [21, 22, 23]. The asynchronous proposals can guarantee QoS by avoiding collisions and useless retransmissions or by adjusting inter-frame spaces and backoff periods according to the priority of the frame. In Real Time MAC (RT-MAC) protocol [24], the stations set a deadline to each frame. Upon reaching the deadline, the frame is discarded because it has become useless for the real-time application. RT-MAC avoids collisions by recording the next backoff value in the header of the frame. Thus, the neighbors will be able to choose a different backoff value for their own transmissions. In DCF with Priority Classes (DCF-PC) [25] the differentiation is done by setting different inter-frame spaces and backoff periods depending on the priority of the frames. Thus, using lower inter-frame spaces and backoff periods guarantee priority

during medium access. The same idea is used in the IEEE 802.11 standard with QoS, which is presented in Section 3.

3 Enabling Technologies

Bluetooth and IEEE 802.11 are the main technologies for implementing wireless ad hoc networks [26]. In the following subsections, we give a brief overview of the MAC sub-layer and some physical layer characteristics of Bluetooth and IEEE 802.11.

3.1 Bluetooth

Bluetooth is a wireless technology that is being used to deploy personal area networks and adopted as IEEE 802.15.1 standard [27]. Most Bluetooth products are compliant with the 1.1 specification [28].

The Bluetooth architecture consists of a basic unit called piconet and of scatternets. A piconet is an ad hoc network formed by a master and slaves devices. A device can be a master or a slave, but not both at the same time. The master is the device that establishes the piconet and the slaves are the other devices that belong to the piconet. The master informs the slaves the logical addresses to be used, when the slaves can transmit and for how long and what frequencies must be used in transmission. Communication is always between a master and one or more slaves (point-to-point or point-to-multipoint). There is no direct communication between slaves.

A piconet is composed of a master and up to seven active slaves. Moreover, there may be up to 255 inactive devices in the network, in a low-power state.

The maximum number of active devices could limit the applicability of Bluetooth, but a Bluetooth network can be extended by the interconnection of piconets. In this case, the network is called a scatternet and the piconets are interconnected by bridge nodes. The bridge between the piconets can have the role of slave in all piconets to which they belong or of master in one piconet and slave on the others. A bridge cannot be master in more than one piconet, because the master is the unit that establishes the frequencies to be used in communication. Figure 3 shows an scatternet example in which the bridge node is a master in one piconet and a slave in the other piconet.

In order to separate master and slave transmissions, Bluetooth uses a Time Division Duplexing (TDD) scheme, with a 625 μs slot time. The master begins its transmission in even slots and slaves transmit in odd slots. Frames can be one, three or five slots long, depending on the frame type.

Frames are transmitted over links called logical channels between the master and one or more slaves. There are two kinds of links: ACL (Asynchronous Connectionless) and SCO (Synchronous Connection-Oriented). The ACL is a point-to-multipoint link between the master and all active slaves of the piconet. There is only one ACL link per piconet. Polling is used for medium access. A

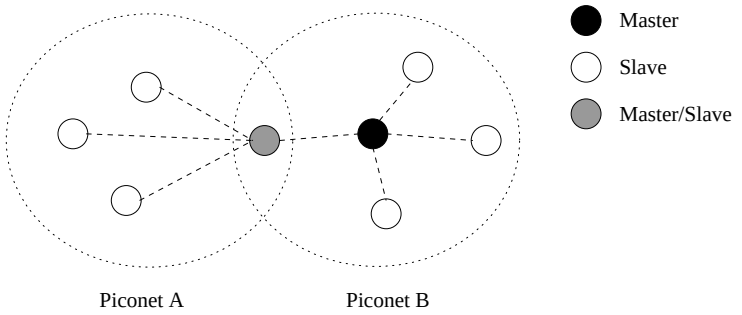


Fig. 3. Scatternet example.

slave can transmit data to the master only if the slave has been addressed in the previous master-slave slot. ACL frames not addressed to a specific slave are considered broadcast frames and are read by all slaves. In ACL, a best effort service is provided. This link is used to send asynchronous data. The maximum data rate to the master is 723.2 kbps. In symmetric links, the maximum data rate is 433.9 kbps. The SCO is a point-to-point link between the master and a slave. SCO uses slots reservation at regular intervals. This link is mainly used to transmit real-time data. SCO does not use retransmission but can use Forward Error Correction (FEC). A master can have up to three SCO links to the same slave or to different slaves. A slave can have up to three SCO links to the master or up to two SCO links to different masters. In each link, the data rate is 64 kbps. Figure 4 shows an example of an SCO link between the master and the slave 1 and the ACL link.

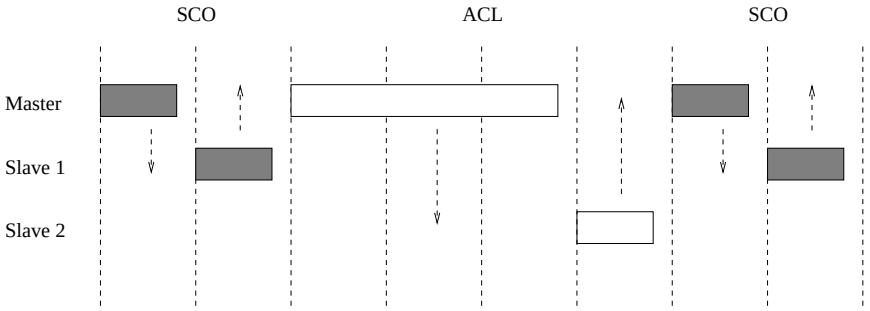


Fig. 4. SCO and ACL links example.

Bluetooth uses FHSS (Frequency Hopping Spread Spectrum) in the 2.4 GHz band and supports 1 Mbps physical data rate.

3.2 IEEE 802.11

IEEE 802.11 [29], also know by Wi-Fi (Wireless Fidelity), is the most widespread wireless technology. The 802.11 family includes several standards, e.g., IEEE 802.11b, IEEE 802.11a, and IEEE 802.11g, which differ in the physical layer.

The IEEE 802.11 MAC protocol specifies two medium access algorithms: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is a distributed mechanism in which each node senses the medium and transmits if the medium is idle. On the other hand, PCF is a centralized mechanism where an access point controls medium access. Therefore, this mechanism is designed for infrastructured networks.

The DCF function uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to control medium access (Figure 5). A station that wants to transmit first senses the medium. If the medium is idle for at least a time called Distributed Inter-Frame Space (DIFS), the station transmits. Otherwise, if the medium is busy, the transmission is postponed until a DIFS period after the end of the current transmission. After deferral, a backoff process is initiated. A station chooses a random number between zero and the Contention Window (CW) size and starts a backoff timer. This timer is periodically decremented by a slot time after the medium is sensed idle for more than DIFS. The backoff timer is paused when a transmission is detected. If the medium gets idle for DIFS again, the station resumes its backoff timer. When the timer expires, the station sends its frame.

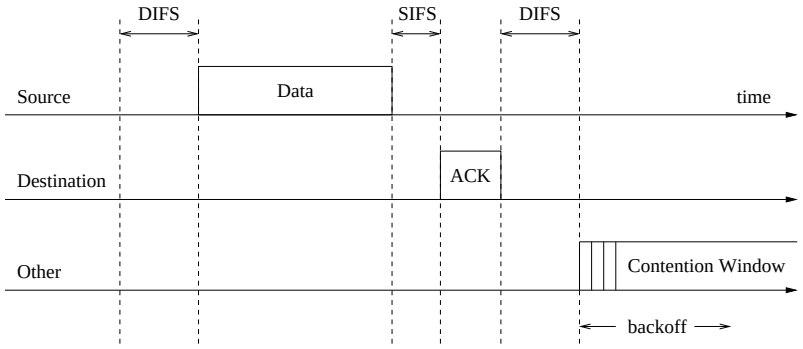


Fig. 5. Transmission of a data frame using the IEEE 802.11 protocol.

A Cyclic Redundancy Check (CRC) is used for error detection. If the frame seems to be correct, the receiver sends an acknowledgment frame (ACK) after sensing the medium idle for a period of time called Short Inter-Frame Space (SIFS). By definition, SIFS is smaller than DIFS to prioritize the access and reception of acknowledgment frames over data frames. If the sender does not receive the ACK frame, it schedules a retransmission and enters the backoff

process since a collision is assumed. Hence, to reduce collision probability, the contention window starts with a minimum value given by CW_{min}. After each unsuccessful transmission, the contention window increases to the next power of 2 minus 1, until reaching a maximum predefined value called CW_{max}. CW_{min} and CW_{max} values depend on the physical layer used. Moreover, if a maximum number of retransmissions is reached, the frame is dropped. To avoid medium capture, prior to transmitting another frame the sending station will wait for DIFS and then enter the backoff phase.

The DCF method optionally uses Request to Send (RTS) and Clear to Send (CTS) frames to avoid the hidden terminal problem [29].

The original IEEE 802.11 uses the 2.4 GHz band and supports 1 and 2 Mbps physical data rates. IEEE 802.11b also uses the 2.4 GHz band and supports up to 11 Mbps using DSSS (Direct Sequence Spread Spectrum). IEEE 802.11a uses the 5 GHz band and defines up to 54 Mbps physical data rates using OFDM (Orthogonal Frequency Division Multiplexing). As the standards a and b use different frequency ranges, they are incompatible. To attain the same 54 Mbps physical data rate of IEEE 802.11a at the 2.4 GHz band of IEEE 802.11b, the standard IEEE 802.11g has been proposed.

IEEE 802.11e The original IEEE 802.11 does not support QoS. A best effort service is provided for all kinds of data traffic. Moreover, a great part of the medium access time is "wasted" by fragmentation, inter-frame spacing, and acknowledgments [30]. In order to deal with these problems, a new standard, called IEEE 802.11e [31], was published in 2005. This standard modifies IEEE 802.11 and its extensions.

IEEE 802.11e defines a Transmission Opportunity (TxOP) as a limited time interval in which a station is allowed to transmit a series of frames [32]. A TxOP is defined by the start time and a maximum duration, in order to avoid a large delay to the other stations.

IEEE 802.11e defines two access algorithms: Enhanced Distributed Channel Access (EDCA) and Hybrid Coordination Function Controlled Channel Access (HCCA). HCCA is a centralized mechanism that demands an infrastructured mode. EDCA provides QoS based on the medium access priority. Differentiation using different priorities is obtained by: varying the amount of time a station listens to the medium before backoff or transmission, the size of the contention window to be used during backoff, and the transmission duration of a station after obtaining the medium. The mechanism uses eight frame priorities assigned according to IEEE 802.1D [33], but there are four instances of the coordination functions that are executed in parallel in a station, as virtual MACs. These instances are associated to Access Categories (ACs) that identify the following traffic types: background, best effort, voice, and video. Differentiation between the ACs is performed by setting different values for ACs parameters. Each AC has an specific transmission queue, in which are used different values for AIFS (Arbitration Inter-Frame Space), CW_{min}, CW_{max}, and TxOP limit. AIFS corresponds to the smaller time interval between the time the medium gets idle

and the start of a frame transmission, i.e., AIFS is analogous to DIFS for DCF. The TxOP has a maximum duration limit. ACs contend for TxOPs and perform the backoff procedure independently. An internal contention algorithm calculates the backoff based on AIFS, CW_{min}, CW_{max}, and random numbers. Backoff is similar to the one used on DCF, i.e., the AC with the smaller backoff wins the internal contention. Two or more ACs may have their timers expired at the same time. Station internally solves these conflicts between categories, offering the TxOP to the category of higher priority and forcing the categories with lower priorities to execute the backoff procedure. Then the winner AC contends externally for the medium.

4 Routing Protocols

A major challenge of wireless ad hoc networks is the design of efficient routing protocols that dynamically find routes between two communicating nodes [34, 35, 36, 37, 38]. In a mobile ad hoc network, nodes may move arbitrarily and the status of the communication links between the nodes is a function of several factors such as the position of the nodes, the transmission power level, and the interference between neighbor nodes. Therefore, the mobility of the nodes and the variability of the state of the links result in a network with fast and unpredictable topology changes. Due to this characteristic, protocols proposed for wired networks are not suited for operation in wireless ad hoc networks. These protocols are designed for operation in *quasi*-static networks with wired links and are based on periodical updates. Then, if the rate of topological changes in the network is high, the frequency of periodical updates must be fast enough to maintain the routing information consistent. Nevertheless, the action of only increasing the frequency of routing updates is prohibitive due to the limited energy of the nodes and the reduced capacity of the wireless links [39, 40].

According to the routing strategy, ad hoc routing protocols fall into two categories: topology-based and position-based protocols. Topology-based routing protocols find a route from a source to a destination according to the metrics of the network links. Networks that employ topology-based protocols forward packets based on the address of the destination node. On the other hand, position-based routing protocols do not require the establishment or maintenance of routes. Here, the idea is to obtain the information about the geographical position of the destination and find the best way to forward packets to this position.

4.1 Topology-Based Routing

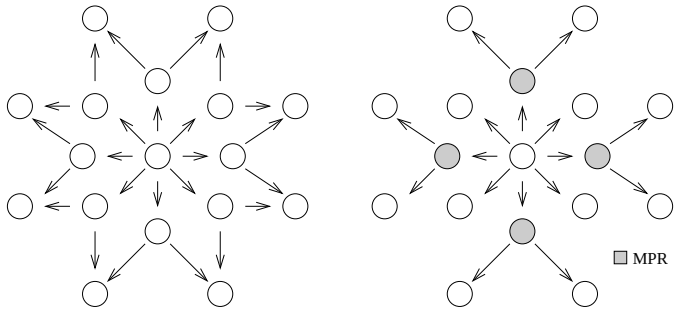
Topology-based routing protocols rely on the status of the network links to compute a route from a source to a destination. Thus, every node of the network has to exchange routing information to maintain routing tables up to date. Topology-based protocols can be further divided into proactive and reactive protocols.

Proactive Routing Proactive routing protocols work like a classical Internet routing protocol. They share routing information even if there are no specific requests for a route to maintain consistent and up-to-date routes from each node to every other node in the network. Proactive protocols require that each node stores a routing table and responds to changes in network topology by propagating update messages throughout the network in order to maintain a consistent network state. This strategy continuously produces control traffic, which should be avoided for wireless networks. On the other hand, it provides low latency route access. The existing proactive protocols differ in the number of necessary routing-related tables and the methods by which changes in network topology are broadcasted. Examples of proactive protocols are DSDV and OLSR.

The Destination-Sequenced Distance-Vector(DSDV) routing protocol [41] is a modified version of the Bellman-Ford algorithm to guarantee loop-free routes. In DSDV, every node maintains a routing table in which the next-hop to all of the possible destinations is stored. The number of hops to each destination and a sequence number assigned by the destination node are associated to each routing table entry. The sequence numbers avoid the creation of routing loops once they enable the nodes to distinguish stale routes from new ones. Update packets are periodically sent throughout the network in order to maintain up-to-date the routing tables of the nodes. In order to reduce the control overhead, two types of update packets are used: a full dump and an incremental packet. The full dump packet contains all the available information in the routing table of a node. On the other hand, the incremental packet carries only the information changed since the last full dump was transmitted. Although this mechanism reduces the routing overhead, as the topological changes increase, the number of incremental packets transmitted by DSDV also increases. In this situation, update routing packets use a large amount of network bandwidth.

The Optimized Link State Routing (OLSR) protocol [42, 43] is based on the link-state algorithm. In OLSR, each node periodically exchanges routing information with other nodes to maintain a topology map of the network. In order to reduce the flooding during the routing update process and the size of the update packets, OLSR employs multipoint relays (MPRs). The reduction of flooding provided by the MPR mechanism is illustrated in Figure 6. In this mechanism, each node in the network selects a set of neighboring nodes to retransmit its update packets. For selecting the MPRs, a node periodically broadcasts *hello* messages to all one-hop neighbors to exchange its list of neighbors. From neighbor lists, a node calculates the nodes that are two hops away and computes the MPRs set which is the minimum set of one-hop neighbors required to reach the two-hop neighbors. The optimum MPRs computation is NP-complete [44], therefore heuristics are used by the OLSR protocol to compute the MPRs set. Each node notifies its neighbors about its MPRs set in the *hello* message. When a node receives the *hello*, it records the nodes that select it as one of their MPRs. These nodes are called MPR selectors. A routing update message transmitted by a node carries only information about its MPRs selectors. Thus, the size of

a routing update message is reduced and a node can be reached only from its MPR selectors. The shortest path to a given destination is calculated using the topology map consisting of all of its neighbors and of the MPRs of all other nodes. The OLSR protocol is particularly suited for dense networks since if the network is sparse, most of the neighbors of a node becomes an MPR.



(a) Flooding. (b) MPR mechanism.

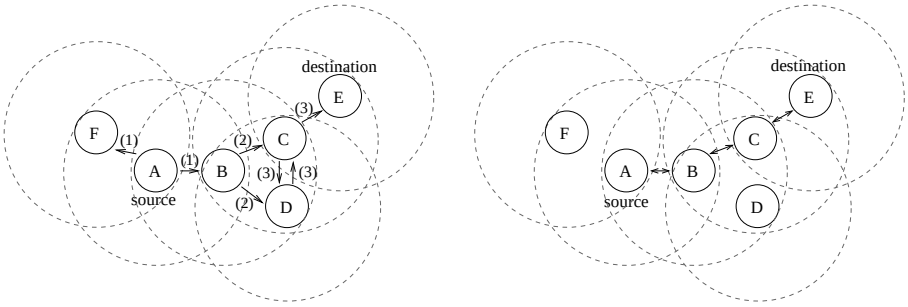
Fig. 6. The efficiency of the MPR mechanism implemented by the OLSR protocol.

Reactive Routing Reactive, or on-demand, routing protocols operate only when there is an explicit request for a route. This strategy only creates routes when desired by a source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed when a route is found or when all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible because a link rupture or until the route is no longer needed. Reactive routing significantly reduces the memory consumption in the nodes and only generates control traffic when needed, but it typically floods the network with control messages to discover routes between two communicating nodes. In spite of providing fast route discovery, flooding has several inconveniences frequently observed, such as redundancy, contention, and collision [38]. In a typical mobile ad hoc network, the resource consumption caused by control packets has a significant impact because of the low-bandwidth links and power-limited terminals.

An example of reactive protocol is the Ad Hoc On-Demand Distance Vector (AODV) [45], which is based on the Bellman-Ford algorithm. In AODV, when a source node wants to send a packet to a destination and does not already have a valid route to that destination, the source initiates a route discovery process to find a route. Then, the source broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors. This process is repeated until either the destination or an intermediate node with a valid route to the destination is found, as shown in Figure 7(a). To guarantee that routes are loop free and contain the most recent information, AODV employs destination

sequence numbers. Each node of the network maintains its own sequence number and a broadcast ID. Every time a node initiates a route discovery process, the broadcast ID is incremented. The address of the node and its broadcast ID uniquely identify an RREQ packet. The source also includes in the RREQ the most recent sequence number it has for the destination. Therefore, intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to the sequence number of the RREQ. When intermediate nodes forward RREQs, they record in their route tables the address of the neighbor from which the first copy of the RREQ packet is received, thereby establishing a reverse path. Due to the flooding process, other copies of the same RREQ can be received later and all are discarded. When the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or the intermediate node sends, in unicast, a route reply (RREP) packet back to the neighbor from which it first received the RREQ. As the RREP is routed back through the reverse path, nodes along this path set up forward route entries in their route tables. The result of this process is illustrated in Figure 7(b). There is a timer for each entry in the routing table, which limits the lifetime of unused routes. It is worth noting that AODV only supports symmetric links once the RREP is forwarded along the path previously established by the RREQ. AODV also employs a route maintenance mechanism. When a node within a route moves, its upstream neighbor notices the move and propagates a route error (RERR) message to each of its active upstream neighbors to inform them of the route rupture. These nodes in turn propagate the RERR packet to their upstream neighbors. This process is repeated until the source node is notified. Then, the source is able to initiate a new route discovery process for that destination. A link failure is detected using *hello* messages, which are periodically broadcasted to maintain the local connectivity of a node. Nodes can also detect a link failure by information from the data link layer.

The Dynamic Source Routing (DSR) [46] is another reactive protocol which is based on the strategy of source routing. In DSR, each node of the network maintains a route cache that contains the source routes of which the node knows, as Figure 8 shows. Entries in the route cache are continuously updated as the node learns new routes. DSR employs route discovery and route maintenance processes similar to AODV. When a node has to send a packet to a given destination, it first verifies its route cache to determine whether it already has a route to the destination. If it has a valid route to the destination, it will use this route to send the packet. Otherwise, if the node does not have a valid route, it initiates a route discovery process by broadcasting a route request packet. The route request contains the address of the destination, the address of the source node, and a unique identification number. Each node that receives the route request verifies if it knows a route to the destination. If it does not, it adds its own address to the route record field of the packet header and then forwards the packet to its neighbors. To limit the number of route requests propagated to its neighbors, a node only forwards the route request if the request has not



(a) Flooding of RREQs. (b) Route establishment.

Fig. 7. An example of the route discovery procedure of AODV.

yet been seen by the node and if the address of the node does not already appear in the route record. A route reply is generated when the route request reaches either the destination or an intermediate node, which contains in its route cache a valid route to the destination. When the route request reaches the destination or an intermediate node, it carries a route record containing the sequence of hops traversed. If the node that generates the route reply is the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. In order to send the route reply, the responding node must have a route to the source. If it has a route to the source in its route cache, it may use that route. Otherwise, if symmetric links are supported, the responding node may reverse the route that is in the route record. If symmetric links are not supported, the node may initiate a new route discovery process and piggyback the route reply on the new route request. The asymmetric links support is an advantage of DSR as compared to AODV. DSR employs a route maintenance process based on route error messages. These messages are generated at a node when the data link layer detects a transmission failure. When receiving a route error, a node removes the failed node from its route cache and all routes containing the failed node are truncated at that point.

4.2 Position-Based Routing

Position-based routing protocols require that information about the geographical position of the communicating nodes be available. Each node determines its own position using GPS (Global Positioning System) or some other kind of positioning system [47]. In position-based routing, nodes have neither to maintain routing tables nor to exchange routing messages since the packet forwarding is

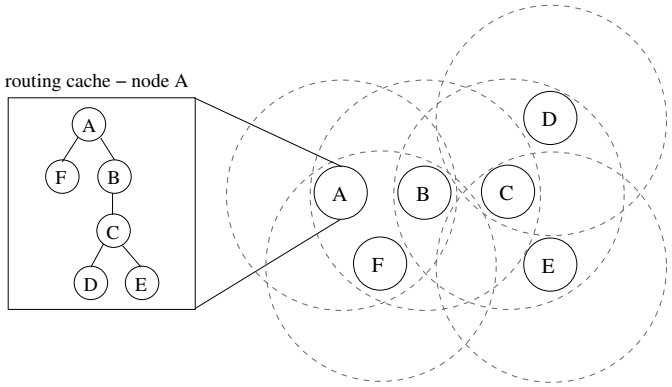


Fig. 8. An example of routing cache in DSR.

performed based on the position of the destination node, carried by each packet. Then, before sending a packet, it is necessary to determine the position of its destination. Thus, the source node needs to use a location service to determine the position of the destination node and to include it in the destination address of the packet. In the following sections, we describe two position-based protocols, DREAM and Grid.

DREAM The Distance Routing Effect Algorithm for Mobility (DREAM) protocol [48] is an example of position-based protocol that employs an all-for-all location service. In DREAM, each node stores position information concerning every node of the network in a position database. An entry of this database contains a node identifier, the direction of and distance to a node, and a time value, which indicates the age of the entry. For propagating its position, a node periodically floods the network. The advantage of exchanging position information is that it consumes significantly less bandwidth than exchanging complete routing tables even if the network is flooded. The efficacy of network flooding can be improved according to two factors. The first one is that the frequency of position updates is a function of the mobility of nodes. Thus, a node can locally control the frequency at which it sends position updates according to its own mobility rate. The higher is the mobility of a node, the higher is the frequency of position updates. The second factor is the distance separating two nodes. The greater the distance separating two nodes, the slower they appear to be moving with respect to each other. This is called the distance effect [49]. Therefore, nodes in the direct neighborhood must exchange position updates more frequently than nodes farther away. A node can employ this strategy by indicating the distance that a position update can cover before it is discarded.

The DREAM protocol also employs a restricted directional flooding to forward packets. A source sends a packet addressed to a certain destination to all its one-hop neighbors, which are within the direction toward the destination. In order to determine this direction, called the expected region, a node calculates

the region where the destination is probably within. The expected region is a circle around the position of the destination node as it is known to the source, as shown in Figure 9. Since this position information may be outdated, the radius r of the expected region is set to $(t_1 - t_0)v_{max}$, where t_1 is the current time, t_0 is the timestamp of the position information of the destination which the source knows, and v_{max} is the maximum speed that a node can move in the network. Given the expected region, the direction toward the destination can be defined [48]. The neighboring nodes repeat this procedure using their information concerning the position of the destination. If a node does not have a one-hop neighbor in the required direction, a recovery procedure has to be initiated. This procedure is not implemented by DREAM.

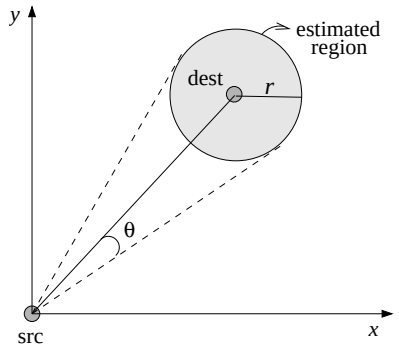


Fig. 9. The estimated region in DREAM.

Grid Grid is a routing protocol [50, 51] composed by the Grid Location Service (GLS) and a greedy strategy for forwarding packets.

The main idea of the Grid location service is to divide the area of an ad hoc network into several squares. Thus, GLS builds a hierarchy of squares where n-order squares contain four smaller $(n-1)$-order squares as shown in Figure 10. An n-order square does not overlap other square of the same order. Every node of the network knows the hierarchy of squares and its origin.

A node has a unique identification (ID) in the network defined by a hash function of one of its parameters such as the IP address or the MAC address. For identifying each node, GLS defines a circular identification space where the nearest ID of a given node is the smallest ID greater than the ID of the own node. For example, an ID space contains four IDs: 2, 12, 25, and 50. In this example, the nearest ID of 12 is 25 and the nearest ID of 50 is 2.

A node periodically broadcasts update messages that contain its position and ID. These messages are limited to the first-square where the node is. Thus, each node only knows the position and the ID of its one-hop neighbors, which are within its first-order square. For disseminating its position through the network, first, a node sends an update message toward its three adjacent first-order squares as Figure 11(a) shows. Then, the nodes within these squares,

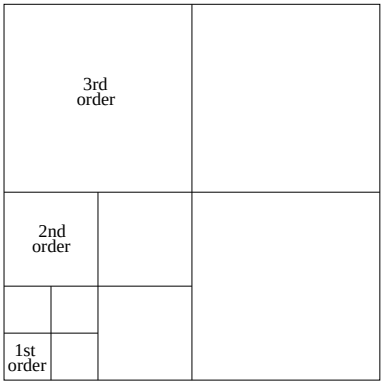
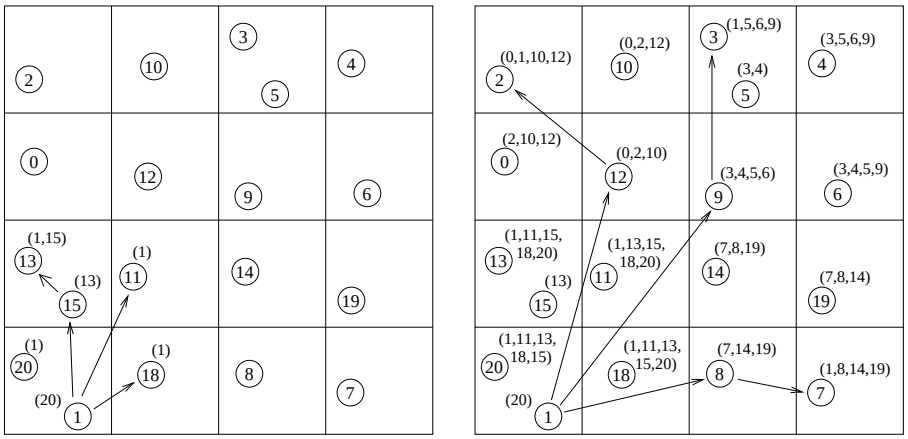


Fig. 10. Hierarchy of squares.

which have the nearest ID of the transmitting node ID, are elected to store the position information of the transmitting node. These nodes are called location servers of the transmitting node. In the example, nodes 11, 13, and 18 are elected first-order location servers of node 1. In Figure 11(a), the numbers in parenthesis are the ID of nodes that a given node knows the position. The process is repeated for all the n orders to cover the network area. Figure 11(b) illustrates the election of second-order location servers for node 1. It is worth noting that each node has only one position-server in an n-order square and, consequently, three position servers per order.



(a) First-order servers of node 1. (b) Second-order servers of node 1.

Fig. 11. Election of location servers.

Suppose that a node wants to send a packet to a destination. If the destination is not within the first-order square of the source and the source is not a location server of the destination, the source does not know the destination ID and position. Figure 12 shows an example where node 10 wants to send a packet to node 1 and it does not know the position of node 1. Then, to find the ID and the position of the destination, the source, in this case node 10, sends a request toward the node with the smallest ID of which the source knows, node 0. If this node knows the position of the destination, it responds the request toward the source. Otherwise, it forwards the request to the node with the smallest ID in its position table. The process continues until the request reaches a node that has the position of the destination. In the example, node 0 does not know the position of node 1, then it forwards the request to node 2, the node with the smallest ID which node 0 knows. When node 2 receives the request it responds to node 10 since it is a second-order location server of node 1.

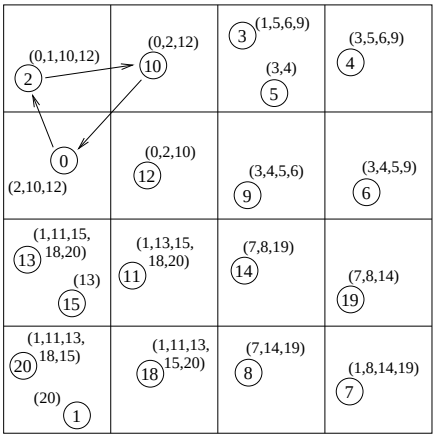


Fig. 12. Position discovery.

The Grid protocol uses the greedy strategy to forward packets. After finding the position of the destination, the source node sends a packet that ch carries this information to its closest one-hop neighbor to the destination. This process is repeated node-by-node until the destination receives the packet. Nevertheless, if there is no one-hop neighbor that is closer to the destination than the forwarding node itself, the packet forwarding fails. In this situation, an error message is returned to the source.

5 Transport Protocols

The Transmission Control Protocol (TCP) is a connection-oriented transport protocol designed to provide reliable, ordered, end-to-end delivery of data. TCP

should be independent of the underlying layers and should not care if IP is running over a wired or wireless network. Wired networks are reliable and losses are mainly due to network congestion. On the other hand, wireless networks suffer from a high bit error rate that corrupts TCP-data segments or acknowledgments, and from frequent route failures. Thus, ignoring these specific characteristics of wireless networks can lead to poor TCP performance [52, 53].

The TCP protocol was designed for wired network with low bit error rate and assumes that data loss is due to congestion. Thus, when the sender transmits a TCP-data segment, it starts a retransmission timeout (RTO), and waits for a TCP acknowledgment from the receiver. When acknowledgments do not arrive at the TCP sender before the RTO goes off, the sender retransmits the segment, exponentially backs off its retransmission timer for the next retransmission, and closes its congestion window to one segment. Therefore, the exponential backoff retransmission and the congestion window mechanism prevent the sender from generating more traffic under network congestion. Repeated errors will ensure that the congestion window at the sender remains small, resulting in low throughput. Nevertheless, because of the high bit error rate of a wireless link, TCP-data segments and acknowledgments may be lost without congestion. In this case, the retransmission of the TCP-data segment in error should be done as fast as possible, instead of backing off and closing the congestion window. For mobile wireless networks the negative aspects of these mechanisms are even worse. Mobility and fading cause link failures and, as a consequence, path disruption. While the routing protocol is finding the new path the TCP recovery mechanism continues retransmitting new copies of the TCP-data segment and exponentially increasing its retransmission timeout. Therefore, the mobile node does not begin receiving data immediately after the new path establishment.

As outlined, the main problem that affects the TCP performance is to distinguish errors due to congestion from other errors such as: corrupted data, route failures, etc. Fixed RTO [54] uses a heuristic to distinguish route failures and congestion. When two timeouts expire in sequence, the Fixed-RTO TCP sender assumes that a route failure has occurred. The unacknowledged TCP segment is retransmitted but the timer is not doubled. This proposal is restricted only to wireless networks and does not fit well for combined wired and wireless networks. TCP Detection of Out-of-Order and Response (DOOR) [55] interprets out-of-order TCP segments as route failures.

Several proposals have been made to improve the TCP performance. We classify the proposals in two types: split of transport connection and cross-layer. To ensure TCP efficiency, it is necessary to prevent the sender from reducing the congestion window when TCP-data segments are lost either due to bit errors or disconnections in the wireless environment. For scenarios composed of wired and wireless networks, this can be done introducing an intermediate host in the wired network who "spoofs" the sender into thinking that the wireless link is working well. It must be noted that the end-to-end semantics of TCP is broken with the introduction of the intermediate host. The Snoop Module creates an intermediate host near the wireless user that inspects TCP-data seg-

ments and acknowledgments and buffers copies of TCP-data segments. Therefore, the intermediate host acknowledges TCP-data segments coming from the wired network and performs local retransmissions for the wireless network. An improved version of Snoop [56] adds selective retransmissions from the intermediate host to the wireless host. The Indirect-TCP (I-TCP) [57], MTCP [58], and M-TCP [59] protocols use similar strategies.

The interaction of with other layers can be useful to improve the performance of TCP. The key idea of cross-layer proposals is to provide lower-layer information to upper layers resulting in better performance of the overall system. The Explicit Link Failure Notification (ELFN) technique [60] uses a message to inform the TCP sender about a link failure. A ELFN message is piggybacked onto the route failure message sent by the routing protocol to the sender. On receiving the ELFN message, the TCP sender disables its retransmission timer and enters a standby mode. During standby, the TCP sender probes the network to verify if the route is restored. If the probe is successful, the TCP sender leaves the standby state, resumes its retransmission timers, and continues the normal operation. TCP Feedback (TCP-F) [61] similarly uses feedback messages from the network. The messages Route Failure Notification (RFN) and Route Reestablishment Notification (RRN) are used to freeze retransmission timers and congestion window size during route failures. Ad hoc TCP (ATCP) [62] also uses cross-layer information, but creates a new layer between the TCP and IP layers being compatible with other TCPs that do not implement ATCP. Another cross-layer optimization is proposed by Fu *et al.* [63], which show that there is an optimum value for the TCP congestion window size. If the congestion window is greater than this optimum value, packet losses increase and the TCP throughput decreases. Hence, the authors propose two link-level mechanisms: Link Random Early Discarding (Link RED) and adaptive spacing. Link RED tunes packet drop probability at the link layer to keep the TCP congestion window size near the optimum value. In association with Link RED, the adaptive spacing mechanism improves the spatial channel reuse through better coordination among contention for channel access. The idea is the introduction of extra backoff intervals to mitigate the exposed-terminal problem in a multihop communication.

6 Other Issues

6.1 Directional Antennas

Most of the work on ad hoc networks assume the use of omnidirectional antennas, which means that the range of a node's transmission covers a circular area around it. As a consequence, when two nodes are communicating, all nodes in the vicinity of them must remain silent for the duration of the communication. That vicinity may be defined by the union of the two transmission range circles. This assumption is made by MAC protocols such as IEEE 802.11 [29].

The advantage of directional antennas is twofold. First, the area covered by a node's transmission is no longer a circle, but may be approximated by a circular sector (Figure 13). Thus, spatial reuse may be potentially larger than with omnidirectional transmissions. Second, the transmission as well as the receiving gain are larger for directional than for omnidirectional antennas. Hence, the transmission range is larger with directional antennas.

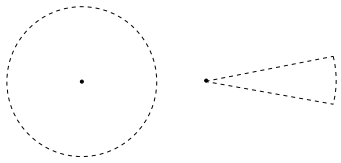


Fig. 13. Omni and directional antenna models.

The Friss Equation [64, 65] can be used to derive the maximum distance r between the communicating nodes, which is given by

$$r = \left(\frac{P_t G_t G_r}{K P_r} \right)^{1/\alpha} \tag{1}$$

where P_t and P_r are the transmitted and received powers, G_t and G_r are the transmit and receive gains, K is constant that accounts for atmospheric absorption and other losses, and α, $2 \leq \alpha \leq 4$, is the path-loss index. It is worthing note that the distance r increases with the transmit and receive gains, but in a non-linear way, because of the α parameter.

The first problem with the use of directional antennas as opposed to omni antennas in *mobile* ad hoc networks is to know where the receiver is. Depending on the antenna model, different solutions may arise. Obviously, if the locations of the stations are known or if the stations are stationary, the problem is leveraged.

The antenna model most commonly used is a system with two modes of transmission and reception, omni and directional. That system could be implemented by two antennas, an omnidirectional one and a directional one. Now, suppose a communication taking place from the viewpoint of the receiver. As the receiver does not know, *a priori*, where the communication will arrive from, the communication must start by receiving a signal in omni mode, i.e., with receive gain $G_r = g_o$. Then, if possible, the system can use the convenient directional antenna for the rest of the communication, by selecting the beam on which the incoming signal power is maximum. Then, suppose the opposite situation of a station willing to transmit a frame and not being aware of the location of the receiver. The transmitter must start the communication in omni mode, i.e. with gain $G_t = g_o$ and consequently with shorter range than with a directional transmission. Then, the communication can go on directionally. Alternately, the transmitter could try to start the communication directionally, probably by sending a starting signal in all the directional antennas in turn.

A station is said to be in either omni mode or directional mode. To be in directional mode is equivalent to say that the antenna is beamformed. When in omni mode, the station can sense signals coming from all possible directions, whereas when beamformed, the station can only send and only hears the signal coming from the sector corresponding to the chosen direction. The fact that the antenna is beamformed has two consequences: on the one hand, it reduces interference, because while being beamformed the system is not interfered by signals coming from other directions; on the other hand, the very fact that the system does not hear on the other directions produces a phenomenum called deafness, explained later.

MAC Most of the ad hoc network research and implementations are based on the IEEE 802.11 standard [29]. IEEE 802.11 is a CSMA/CA protocol which avoids collisions by physically sensing the medium before transmitting, and then by using a backoff mechanism. Additionally, IEEE 801.11 solves the hidden terminal problem by silencing all nodes in the vicinity of the sender and of the receiver [2]. The RTS/CTS control frames exchange occurs prior to the DATA communication. Both the RTS and CTS frames contain the proposed duration of the transmission. Nodes located in the vicinity of the communicating nodes can then construct a Network Allocation Vector (NAV) to implement virtual carrier sensing. As a consequence, the area covered by the transmission range of the sender and of the receiver is reserved for the duration of the transmission.

The design of IEEE 802.11 MAC assumed an omnidirectional antenna. Even if IEEE 802.11 can operate with a directional antenna at the physical layer, the potential gains of using a directional antennas may not be achieved and, actually, performance may be affected by the use of directional antennas [66].

A key advantage of using directional antennas is spatial reuse. Nevertheless, other issues arise. The first problem is, given a mobile ad hoc network where the nodes are not location-aware, how can spatial reuse be maximized. Assume the use of IEEE 802.11. If the sender does not know where the receiver is, the RTS must be sent in omni mode, hindering spatial reuse. Then, if RTS is sent omni and DATA is sent directionally, the communication ranges are different. The MAC protocol has to cope with such problems to maximize spatial reuse.

Choudhury et al. [65] summarize the main issues that arise from the use of directional antennas. The main problems are related to the phenomena called deafness and hidden terminal.

Consider two nodes, A and B, which are engaged in a communication. Suppose that A is beamformed in the direction of B, therefore, A can not be interfered by signals coming from other directions, we say that A is "deaf" in the other directions. Then, suppose that a third node, C, has a data frame to send to A. Node C then sends an RTS to A, who ignores it. As node C does not receive an CTS, it will eventually increase its backoff window. As long as A is beamformed and does not respond to C with an RTS, C will keep on backing off when it retransmits subsequent RTS frames. Suppose that B has a series of frames to be sent to A. It may actually pass a long interval before C gets access

to the medium and sends a frame to A. When it does, A may now become deaf to B's frames, causing B MAC layer to retransmit and eventually B will give up. The upper layers of B will see a packet loss. That packet loss would be interpreted as congestion by TCP, even if this is not exactly the case. Therefore, the deafness phenomenum can affect the network performance by causing multiple packet drops, without congestion or link rupture and, at the same time, cause short-term unfairness between flows that have the same receiver.

Hidden terminal problems may actually be aggravated with the use of directional antennas. Consider the example scenario of Figure 14. Suppose that nodes A and B are both beamformed in the direction of each other, and that there is an ongoing communication between A and B. Now, suppose that node C sends an RTS to node D, which is followed by a directional CTS from D to C. Thereafter, C and D start to communicate directly. The RTS issued by C, whether omni or directional, as well as the directional CTS from D were not taken into consideration by A, which was beamformed in the direction of B. Now, suppose that the conversation between A and B ends, and that A tries to start a communication with D, or any other node in the direction of D. Node A may well send an RTS in the direction of D, since it is not aware of the ongoing communication. When it does, the RTS of A will cause a collision at D. That kind of hidden terminal problem would not be possible if all control frames had been sent omni directionally.

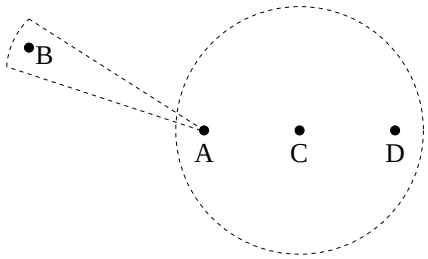


Fig. 14. RTS from C unheard by A.

The first adaptation proposed to IEEE 802.11 to support directional antennas is the use of a Directional Network Allocation Vector (DNAV) per sector, instead of a single NAV [67, 68]. The idea is to reserve a sector instead of a circular area if the reservation control frames (RTS and/or CTS) are sent directionally.

Directional MAC (DMAC) is a MAC protocol based on IEEE 802.11 with the basic modifications to support directional antennas [68]. DMAC supposes that an upper layer is capable of supplying transceiver profiles that describe the capabilities of each of the node neighbors. Basic DMAC reserves the channel using RTS/CTS frames which are both transmitted directionally. An idle node listens to the channel omnidirectionally, when it receives a signal, it beamforms

in that direction. Basic DMAC has problems with hidden terminals due to gain assimetry and unheard RTS/CTS, as explained previously.

Multihop RTS MAC (MMAC) [65] enhances basic DMAC by using RTS frames which can be retransmitted traversing multiple hops. The objective is to exploit the longer range possible with directional antennas. Assume that the idle node is in omni mode. Thus, a RTS sent directionally can only form a link whose gain is $g_d \times g_o$, that is, the receiver of the RTS will be at a distance as long as the one defined by $g_d \times g_o$. Nevertheless, if both the emitter and the receiver were beamformed, the gain would be $g_d \times g_d$ and the range would be larger. The basic idea of MMAC is to have protocol that allows the RTS to travel multiple hops and form longer links.

Ko et al. [69] investigated the use of directional RTS frames and omnidirectional CTS frames. The basic idea is that, when an idle node receives a CTS, it will block that antenna to not interfere with ongoing communications. Nevertheless, it can use the other unblocked directions to start other communications, increasing spatial reuse.

To reduce the deafness problem caused by directional antennas, Korakis *et al.* [70] propose the use of a circular RTS, or sweeping. The main idea is that the emitter sends the RTS frame in all the directional antennas, to notify the nodes in all the possible directions about the upcoming communication.

Routing The routing layer may also be affected by the use of directional antennas. Choudhury and Vaidya [71] evaluate the impact of directional antennas over the performance of the omnidirectional routing protocol DSR and propose different strategies for directional routing. Using directional transmissions, the request message broadcast used in DSR must be implemented by sweeping at the MAC layer, i.e., retransmitting the frame for each of the directional antennas. The authors show that there is a tradeoff between the latency added by sweeping and the narrowidth of the antenna beam. Intuitively, the narrower the beam, the greater is the spatial reuse, but also the sweeping latency.

Utilizing Directional Antennas for Ad hoc Networking (UDAAN) [72] is a complete solution for wireless ad hoc networks using directional antennas. The routing protocol used by UDAAN is a link-state proactive routing protocol. UDAAN is based on the HSLS (Hazy Sighted Link-State) routing protocol. To improve scalability, the basic idea of HSLS is to reduce the amount of link-state updates as the distance from the originating node increases. This is done by setting a time-to-live of the link-state updates such that the frequency of updates with n hops is inversely proportional to n. Additionally, UDAAN routing protocol supports ToS-based routing and uses a table of radio profiles to forward packets.

Directional antennas may also be used to improve the routing protocol operation. Saha and Johnson [73] propose a modification of the DSR protocol where the larger transmission range of the directional antenna is used to find longer links and locally repair a broken route.

6.2 Security

Securing a wireless ad hoc network is a challenging task [74, 75, 76]. The broadcast nature of the radio transmission, the absence of an infrastructure, the dynamical topology, the collaborative multihop communication, and the self-organizing characteristic increase the vulnerabilities of an ad hoc network.

Free-space radio communication exposes ad hoc networks to jamming denial of service (DoS) attacks. Jamming is simple and effective in narrow-band wireless networks. Defenses against jamming involve spread spectrum communication, or detection and isolation of the affected jammed region and reroute of the traffic.

Eavesdropping in wireless communication is another threat usually impossible to detect. Hence, the use of cryptography algorithms is mandatory if privacy is required in the wireless ad hoc network.

Conventional solutions to secure communications are the use of symmetric (or secret) or asymmetric (public-private) cryptographic keys. Asymmetric algorithms require more processing than symmetric algorithms. Furthermore, asymmetric algorithms require certification, which is difficult to implement in ad networks because of the lack of infrastructure. Ad hoc nodes can easily join and leave the network. Moreover, ad hoc nodes seldom reside in safe places, and hence can fall under attackers' control. Conventional intrusion detection solutions based on certification authorities and servers are inappropriate due to the absence of infrastructure. The Techniques for Intrusion-Resistant Ad Hoc Routing Algorithm (TIARA) [77] were proposed to limit the damage caused by intrusion attacks.

Multihop ad hoc networks assume that every node is also a router that can forward messages. This makes secure routing a difficult task because a malicious node can easily join the network and modify or fabricate routing information and impersonating other nodes. Several routing attacks were identified, such as:

- Selective Forwarding - an attacker selectively drops some packets;
- Sinkhole - an attacker forges routing information claiming falsified shorter distances to attract packets and then discard some or all of them;
  - Blackhole - a variation of sinkhole where all packets are discarded;
  - Greyhole - similar to the blackhole, but selectively drops some packets but not others.
- Wormhole - a pair of attackers, nodes A and B, linked via a private network connection;
- Selfishness - a node that simply does not contribute in the network operation, not forwarding packets. A selfish node is not necessarily an attacker and do not intend to damage other nodes; it may only aim to save its battery life;
- Gratuitous Detour - an attacker forges routing information with the objective of not forwarding packets for other nodes, by adding virtual nodes and making a route through itself appear longer;
- Isolation - an attacker forges routing information to cause a node to use a route detour preventing one set of nodes from reaching another;

– Rushing - used against on-demand routing protocols that use duplicate message suppression at each node - an attacker quickly disseminates route requests throughout the network, thus causing the nodes to suppress any later legitimate route requests;
– Sibyl - an attacker presents multiple identities to other nodes.

Several secure routing protocols were proposed. The Secure Efficient Ad Hoc Distance (SEAD) [78] is a proactive secure routing protocol, based on the DSDV protocol, that avoids modification of routing-table update messages. The basic idea is to use a one-way hash function to authenticate the sequence number and the metric fields of the messages.

The Secure Routing Protocol [79] is proposed to improve the DSR reactive protocol using an extension header that is attached to the route request and the route reply messages. A node that requests a route to a destination is able to identify and discard false routing information messages. Ariadne [80] is another secure protocol based on DSR and TESLA, which is an efficient broadcast authentication scheme that requires loose time synchronization. It assumes that each pair of communicating nodes has one secret key in each direction, and no assumption is made regarding the forwarding, which may exhibit malicious behavior.

To implement security in the AODV protocol, the Secure AODV (SAODV) protocol [81] was proposed. The authors assume that there is a key management system that makes it possible for each node to obtain public keys from the other nodes of the network, and that each node is capable of verifying the association between the identity of a given node and the public key of that node. Given these assumptions, the proposal secure important fields of the AODV messages. The SAODV uses a digital signature to authenticate the fixed fields of the messages, and hash chains to secure the hop count information, which is the only changeable information in the messages.

Most of the proposals try to secure existing protocols and do not succeed against all possible attacks. Securing ad hoc networks is still an open issue. Some researchers argue that all protocols for ad hoc networks must be designed thinking in security from the beginning.

6.3 Underserved Communities

The Brazilian government intends to use the Interactive Digital TV technology as a vehicle for fostering the social inclusion of less-privileged social groups, which live on underserved communities, by using information and communication technologies as tools to encourage active citizenship. It is worth mentioning that more than 90% of the Brazilian residences have a TV set, but less than 10% have Internet access. Some initiatives promoted by non-governmental organizations show that people, when start using computers, experience a positive change in their daily lives, as returning to schools, meeting people, talking about issues regarding to their communities, such as human rights, environment, sex-

ual information, and health. Computers can also keep people away from drugs and violence.

One low-cost, scalable, and easy solution to implement the return channel is an ad hoc community network. Every set top box is a node of the community network. The set top boxes generate traffic that is routed to a gateway, which then forwards the traffic over the Internet to the TV station. Thus, the community networks have specific characteristics: the presence of a gateway and the low mobility of the nodes. Moreover, the presence of a gateway plays an important role in the return channel because all the traffic forwarded to the Internet converges to it. A node is connected only if it has a path to the gateway. Consequently, the availability of the nodes must be higher near the gateway. Campista *et al.* [82] showed that if 20% of the nodes are turned on in an ad hoc return channel, a high connectivity is already reached in typical urban scenarios.

References

1. S. Kumar, V. S. Raghavan, and J. Deng, "Medium access control protocols for ad hoc wireless networks: A survey," *Ad Hoc Networks*, vol. 4, no. 3, pp. 326–358, May 2006.
2. P. Karn, "MACA - a new channel access protocol for packet radio," in *ARRL/CRRL Amateur Radio Computer Networking Conference*, pp. 134–140, Sept. 1990.
3. V. Bharghavan, A. J. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless LAN's," in *ACM SIGCOMM*, pp. 212–225, Aug. 1994.
4. C. L. Fullmer and J. J. Garcia-Luna-Aceves, "Floor acquisition multiple access (FAMA) for packet-radio networks," in *ACM SIGCOMM*, pp. 262–273, Aug. 1995.
5. I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, Jan. 2003.
6. A. C. V. Gummalla and J. O. Limb, "Wireless medium access control protocols," *IEEE Communications Surveys and Tutorials*, pp. 2–15, Sept. 2000.
7. C. Wu and V. O. K. Li, "Receiver-initiated busy-tone multiple access in packet radio networks," in *ACM SIGCOMM*, pp. 336–342, Aug. 1987.
8. Z. J. Haas and J. Deng, "Dual busy tone multiple access (DBTMA)-A multiple access control scheme for ad hoc networks," *IEEE Transactions on Communications*, vol. 50, no. 6, pp. 975–985, June 2002.
9. A. Nasipuri, J. Zhuang, and S. R. Das, "A multichannel CSMA MAC protocol for multihop wireless networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1402–1406, Sept. 1999.
10. Z. Tang and J. J. Garcia-Luna-Aceves, "Hop reservation multiple access (HRMA) for ad-hoc networks," in *IEEE Conference on Computer Communications (INFOCOM)*, pp. 194–201, Mar. 1999.
11. I. A. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23–S30, Sept. 2005.
12. A. Raniwalaa and T.-C. Chiueh, "Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh nertwork," in *IEEE Conference on Computer Communications (INFOCOM)*, pp. 2223–2234, Mar. 2005.

13. D. de O. Cunha, L. H. M. K. Costa, and O. C. M. B. Duarte, "Analyzing the energy consumption of IEEE 802.11 ad hoc networks," in *IFIP/IEEE International Conference on Mobile and Wireless Communications Networks (MWCN)*, Oct. 2004.
14. S. Singh and C. S. Raghavendra, "PAMAS-power aware multi-access protocol with signaling for ad hoc networks," *ACM Computer Communications*, vol. 28, no. 3, pp. 5–26, July 1998.
15. E.-S. Jung and N. H. Vaidya, "An energy efficient MAC protocol for wireless LANs," in *IEEE Conference on Computer Communications (INFOCOM)*, pp. 1756–1764, June 2002.
16. E.-S. Jung and N. H. Vaidya, "A power control MAC protocol for ad hoc networks," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 36–47, Sept. 2002.
17. J. Monks, V. Bharghavan, and W. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *IEEE Conference on Computer Communications (INFOCOM)*, pp. 219–228, Apr. 2001.
18. H. Xiao, W. K. G. Seah, A. Lo, and K. C. Chua, "A flexible quality of service model for mobile ad hoc networks," in *IEEE VTC-Spring*, pp. 445–449, Apr. 2000.
19. G. S. Ahn, A. T. Campbell, A. Veres, and L. H. Sun, "SWAN: Service differentiation in stateless wireless ad hoc networks," in *IEEE Conference on Computer Communications (INFOCOM)*, pp. 457–466, June 2002.
20. S. B. Lee and A. T. Campbell, "INSIGNIA: In-band signaling support for QoS in mobile ad hoc networks," in *International Workshop on Mobile Multimedia Communication (MoMuc)*, pp. 12–14, Oct. 1998.
21. M. Gerla and J. T.-C. Tsai, "Multicluster, mobile, multimedia radio network," *Journal of Wireless Networks*, vol. 1, no. 3, pp. 255–265, Feb. 1995.
22. C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks," *Journal of Selected Areas in Communications*, vol. 15, no. 7, pp. 1265–1275, Sept. 1997.
23. C. W. Ahn, C. G. Kang, and Y. Z. Cho, "Soft reservation multiple access with priority assignement (SRMA/PA): A novel MAC protocol for QoS-guaranteed integrated services in mobile ad hoc networks," in *VTS-Fall IEEE VTC*, pp. 942–947, Sept. 2000.
24. R. O. Baldwin, N. J. D. IV, and S. F. Midkiff, "A real-time medium access control protocol for ad hoc wireless local area networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 3, no. 2, pp. 20–27, Apr. 1999.
25. D. J. Deng and R. S. C. and, "A priority scheme for IEEE 802.11 DCF access method," *IEICE Trans. Commun.*, vol. 82-B, no. 1, pp. 96–102, Jan. 1999.
26. D. Remondo, "Tutorial on wireless ad hoc networks," in *International Working Conference in Performance Modelling and Evaluation of Heterogeneous Networks (HET-NET)*, pp. T2/1–T2/15, July 2004.
27. IEEE, "Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)." IEEE Standard 802.15.1, 2002.
28. Bluetooth SIG, "Specification of the bluetooth system." Core Specification Version 1.1, Feb. 2001.
29. IEEE, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." IEEE Standard 802.11, 1999.
30. S. Chung and K. Piechota, "Understanding the MAC impact of 802.11e: Part 1," *Communication Systems Design Magazine*, Oct. 2003. http://www.commsdesign.com/design_corner/OEG20031029S0009.

31. IEEE, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Medium access control (MAC) quality of service enhancements." IEEE Standard 802.11e, 2005.
32. S. Chung and K. Piechota, "Understanding the MAC impact of 802.11e: Part 2," *Communication Systems Design Magazine*, Oct. 2003. http://www.commsdesign.com/design_corner/OEG20031030S0005.
33. IEEE, "Media access control (MAC) bridges." IEEE Standard 802.1D, 1998.
34. E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad-hoc mobile wireless networks," *IEEE Personal Communications Magazine*, vol. 6, no. 2, pp. 46–55, Apr. 1999.
35. X. Hong, K. Xu, and M. Gerla, "Scalable routing protocols for mobile ad hoc networks," *IEEE Network*, vol. 16, no. 4, pp. 11–21, July 2002.
36. M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad Hoc Networks*, vol. 2, no. 1, pp. 1–22, Jan. 2004.
37. M. Mauve, J. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE Network*, vol. 1, no. 6, pp. 30–39, Dec. 2001.
38. L. H. M. K. Costa, M. D. Amorim, and S. Fdida, "Reducing latency and overhead of route repair with controlled flooding," *ACM/Kluwer Wireless Networks*, vol. 10, no. 4, pp. 347–358, July 2004.
39. S.-M. Senouci and G. Pujolle, "Energy efficient routing in wireless ad hoc networks," in *IEEE International Conference on Communications (ICC)*, June 2004.
40. H. Badis, A. Munaretto, K. A. Agha, and G. Pujolle, "Qos for ad hoc networking based on multiple-metric: Bandwidth and delay," in *IFIP/IEEE International Conference on Mobile and Wireless Communications Networks (MWCN)*, Oct. 2003.
41. C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *ACM SIGCOMM*, pp. 234–244, Aug. 1994.
42. T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)." IETF Request for Comments 3626, 2003.
43. T. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The optimized link state routing protocol, evaluation through experiments and simulation," in *IEEE Symposium on Wireless Personal Mobile Communications*, Sept. 2001.
44. L. Viennot, "Complexity results on election of multipoint relays in wireless networks," tech. rep., INRIA, France, 1998.
45. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing." IETF Request for Comments 3561, 2003.
46. D. Johnson, D. Maltz, and J. Broch, *DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks*, ch. 5, pp. 139–172. Addison-Wesley, 2001.
47. J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *IEEE Computer*, vol. 34, no. 8, pp. 57–66, Aug. 2001.
48. S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (DREAM)," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, (Dallas, USA), pp. 76–84, Oct. 1998.
49. S. Basagni, I. Chlamtac, and V. R. Syrotiuk, "Geographic messaging in wireless ad hoc networks," in *Annual IEEE International Vehicular Technology Conference*, (Houston, USA), pp. 1957–1961, May 1999.

50. J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris, "A scalable location service for geographic ad-hoc routing," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, (Boston, USA), pp. 120–130, Aug. 2000.
51. R. Morris, F. Kaashoek, D. Karger, D. Aguayo, J. Bicket, S. Biswas, D. De Couto, and J. Li, "The grid ad hoc networking project." http://pdos.csail.mit.edu/grid/, 2003.
52. A. A. Hanball, E. Altman, and P. Nain, "A Survey of TCP over Ad Hoc Networks," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 3, no. 3, pp. 22–36, 2005.
53. R. Hsieh and A. Seneviratne, "A comparison of mechanisms for improving mobile IP handoff latency for end-to-end TCP," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 29–41, Sept. 2003.
54. T. D. Dyer and R. V. Boppana, "A comparison of TCP performance over three routing protocols for mobile ad hoc networks," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 56–66, Oct. 2001.
55. F. Wang and Y. Zhang, "Improving TCP performance over mobile ad-hoc networks with out-of-order detection and response," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 217–225, June 2002.
56. H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, "A comparison of mechanisms for improving TCP performance over wireless links," in *ACM SIGCOMM*, pp. 256–269, Aug. 1996.
57. A. V. Bakre and B. R. Badrinath, "Implementation and Performance Evaluation of Indirect TCP," *IEEE Transactions on Computers*, vol. 46, no. 3, pp. 260–278, Mar. 1997.
58. R. Yavatkar and N. Bhagawat, "Improving end-to-end performance of TCP over mobile internetworks," in *IEEE Workshop on Mobile Computing Systems and Applications (Mobile)*, pp. 146–152, Sept. 1994.
59. K. Brown and S. Singh, "M-TCP: TCP for mobile cellular networks," in *ACM SIGCOMM*, pp. 19–43, July 1997.
60. G. Holland and N. Vaidya, "Impact of Routing and Link Layers on TCP Performance in Mobile Ad Hoc Networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1323–1327, Sept. 1999.
61. K. Chandran, S. Raghunathan, S. Venkatesan, and R. Prakash, "A feedback-based scheme for improving TCP performance in ad hoc wireless network," *IEEE Personal Communications*, vol. 8, no. 1, pp. 34–39, Feb. 2001.
62. J. Liu and S. Singh, "ATCP: TCP for mobile ad hoc networks," *IEEE Journal on Selected Areas on Communications*, vol. 9, no. 7, pp. 1300–1315, July 2001.
63. Z. Fu, H. Luo, P. Zerfos, S. Lu, L. Zhang, and M. Gerla, "The impact of multihop wireless channel on TCP performance," *IEEE Transactions on Mobile Computing*, vol. 4, no. 2, pp. 209–221, Mar. 2005.
64. T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, 2002.
65. R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaydia, "On designing MAC protocols for wireless networks using directional antennas," *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 477–491, May 2006.
66. Z. Huang and C.-C. Shen, "A comparison study of omnidirectional and directional MAC protocols for ad hoc networks," in *IEEE GLOBECOM*, pp. 57–61, 2002.

67. M. Takai, J. Martin, A. Ren, and R. Bagrodia, "Directional virtual carrier sensing for directional antennas in mobile ad hoc networks," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 183–193, June 2002.
68. R. R. Choudhury, X. Yang, N. H. Vaydia, and R. Ramanathan, "Using directional antennas for medium access control in ad hoc networks," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 59–70, Sept. 2002.
69. Y.-B. Ko, V. Shankarkumar, and N. H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks," in *IEEE Conference on Computer Communications (INFOCOM)*, Mar. 2000.
70. T. Korakis, G. Jakllari, and L. Tassiulas, "A MAC protocol for full exploitation of directional antennas in ad-hoc wireless networks," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 98–107, June 2003.
71. R. R. Choudhury and N. H. Vaidya, "Impact of directional antennas on ad hoc routing," in *IFIP International Conference on Personal Wireless Communication*, Sept. 2003.
72. R. Ramanathan, J. Redi, C. Santivanez, D. Wiggins, and S. Polit, "Ad hoc networking with directional antennas: A complete systems solution," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, pp. 496–506, Mar. 2005.
73. A. K. Saha and D. B. Johnson, "Routing improvement using directional antennas in mobile ad hoc networks," in *IEEE GLOBECOM*, pp. 2902–2908, Dec. 2004.
74. H. Yih-Chun and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 28–39, May 2004.
75. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, Sept. 2003.
76. A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.
77. R. Ramanujan, A. Ahamad, J. Bonney, R. Hagelstrom, and K. Thurber, "Techniques for intrusion-resistant ad hoc routing algorithms (TIARA)," in *IEEE Military Communications Conference (MILCOM)*, pp. 660–664, Oct. 2000.
78. Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pp. 3–13, June 2002.
79. P. Papadimitratos and Z. Hass, "Secure routing for mobile ad hoc networks," in *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, Jan. 2002.
80. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 12–23, Sept. 2002.
81. M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *ACM Workshop on Wireless Security (WiSe)*, pp. 1–10, Sept. 2002.
82. M. E. M. Campista, I. M. Moraes, P. M. Esposito, A. A. Jr., D. de O. Cunha, L. H. M. K. Costa, and O. C. M. B. Duarte, "Wireless ad hoc network on underserved communities: An efficient solution for interactive digital TV," in *IFIP/IEEE International Conference on Mobile and Wireless Communications Networks (MWCN)*, Aug. 2006.