AD HOC NETWORKS – AN OVERVIEW

Michel Daoud Yacoub, Paulo Cardieri, Élvio João Leonardo, Álvaro Augusto Machado Medeiros, and David Muñoz Gallego

Resumo - Este artigo introduz os conceitos relativos às redes ad hoc e aborda quatro tópicos principais: roteamento, acesso ao meio, TCP/IP e capacidade. Em roteamento, são descritos os principais algoritmos de roteamento. Em acesso ao meio, os principais protocolos de acesso ao meio são apresentados. Em TCP/IP, os aspectos relacionados ao desempenho do protocolo TCP/IP em uma rede ad hoc são discutidos. Em capacidade, alguma formulação a respeito da capacidade da rede é delineada. O objetivo deste artigo é dar uma visão geral das redes ad hoc, servindo como um tutorial sobre o assunto.

Palavras Chaves: Redes ad hoc, algoritmos de roteamento, protocolos de acesso ao meio, TCP/IP, capacidade.

Abstract - This paper introduces the very general concepts of ad hoc networks. It addresses the subject in four principle topics: routing, medium access, TCP/IP issues, and capacity. In routing, the main routing algorithms are illustrated. In medium access, the main medium access protocols are described. In TCP/IP issues, the aspects concerning the performance of TCP/IP in an ad hoc network are discussed. In capacity, some formulation concerning the capacity of the network is tackled. The aim of this article is to give an overview of ad hoc networks serving as a tutorial on the subject.

Keywords: Ad hoc networks, routing algorithms, medium access protocols, TCP/IP, capacity.

1. INTRODUCTION

An ad hoc network is a wireless network that is established without the aid of infrastructure or centralized administration. It is formed by a group of wireless terminals (nodes) such that a communication between any two terminals is carried out by means of a store-and-relay mechanism. A terminal wishing to transmit accesses the medium and sends its information to a nearby terminal. Upon receiving such information this terminal determines that this is not addressed to it. It then stores the information in order to relay it to another terminal at an appropriate time, and this process continues until the destination is reached. Note that in ad hoc networks there are no fixed routers. Nodes may be mobile and can be connected dynamically in an arbitrary manner. Nodes function as routers, which discover and maintain routes to other nodes in the network. Ad hoc networks find applications in emergency-and-rescue operations, meeting or conventions, data acquisition operations in inhospitable terrain, sensor networks, and home and office networks. Cheaper hardware, smaller transceivers, and faster processors fuel the increased interest in wireless ad hoc networks. This paper addresses the ad hoc networks from four main aspects: routing, medium access, TCP/IP issues, and capacity. In routing, the main routing algorithms are illustrated. In medium access, the main medium access protocols are described. In TCP/IP issues, the aspects concerning the performance of TCP/IP in an ad hoc network is discussed. In capacity, some formulation concerning the capacity of the network is tackled.

Michel Daoud Yacoub, Paulo Cardieri, Álvaro Augusto Machado de Medeiros, and David Muñoz Gallego are with DECOM/FEEC/UNICAMP, Campinas SP, Brazil, PO Box 6101, 13081-970, Phone: +55 19 378-83812, FAX: +55 19 3289-1395. E-mails: {michel, cardieri, alvaro, dmunoz}@decom.fee.unicamp.br. Élvio João Leonardo is with UEL, Rod. Celso Garcia Cid km 380, 86055-900 Londrina PR, Brazil. E-mail: elvio@uel.br.

2. ROUTING ALGORITHMS

The design of routing algorithms in ad hoc networks is a challenging task. Algorithms must provide for a high degree of sophistication and intelligence so that the limited resources inherent to the wireless systems can be dealt with efficiently. They must be robust in order to cope with the unkind wireless environment. At the same time they must be flexible in order to adapt to the changing network conditions such as network size, traffic distribution, and mobility. Routing algorithms have long been used in wired systems and they are usually classified into two categories: Distant Vector (DV) and Link-State (LS). DV algorithms provide each node with a vector containing the hop distance and the next hop to all the destinations. LS algorithms provide each node with an updated view of the network topology by periodical flooding of link information about its neighbors. A direct application of these algorithms in a wireless and mobile environment may be cumbersome. DV protocols suffer from slow route convergence and may create loops. LS protocols require the frequent use of the resources, thence large bandwidth, in order to maintain the nodes updated.

With the increasing interest in wireless networks, a variety of routing algorithms overcoming the limitations of the DV and LS protocols have been proposed. They are usually classified into three categories: proactive or table-driven; reactive or on-demand; and hybrid. The proactive protocols require the nodes to keep tables with routing information. Updates occur on a periodical basis or as soon changes in the network topology are perceived. The algorithms differ basically in the type of information is kept and in the way updates occur. The reactive protocols create routes on demand. This is accomplished by means of a route discovery process, which is completed once a route has been found or all possible route permutations have been examined. The discovery process occurs by flooding route request packets through the network. After establishing a route, it is maintained by a route maintenance procedure

until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. The hybrid protocols are both proactive and reactive. Nodes with close proximity form a backbone within which proactive protocols are applied. Routes to faraway nodes are found through reactive protocols.

2.1 PROACTIVE ALGORITHMS

CGSR – Clusterhead-Gateway Switch Routing [1]. In CGSR, the whole network is partitioned into clusters of nodes. Within each cluster a *clusterhead* is elected among the nodes. A node may belong to one cluster only, in which case it is an internal node, or to more than one cluster, in which case it becomes a *gateway*. Packets are transmitted from the node to the clusterhead and from the clusterhead to the node. Routing within such a network occurs as follows. Assume source and destination belonging to different clusters. The source sends its packets to the clusterhead, which relays these packets to a gateway, which relays them to another clusterhead, and this process continues until the destination is reached.

DREAM – Distance Routing Effect Algorithm for Mobility [2]. In DREAM, GPS is used so that each node can maintain a location table with records of locations of all the nodes. The nodes broadcast control packets for location updating purposes. A source having packets to send calculates the direction towards the destination. It then selects a set of one-hop neighbors in the respective direction. (If the set is empty, the data is flooded to the whole network.) The data header encloses the respective set and is sent. Those nodes specified in the header are entitled to receive and process the data. All the nodes of the paths repeat this process until the destination is reached. Upon receiving the packets, the destination issues an ACK, which is transmitted to the source using the same algorithm.

DSDV – Destination-Sequential Distance-Vector Routing [3]. In DSDV, each node keeps a routing table containing all of the possible destinations within the network in conjunction with the number of hops to each destination. The entries are marked with a sequence number assigned by the destination node so that mobile nodes can distinguish stable routes from the new ones in order to avoid routing loops. Table consistency is kept by periodical updates transmitted throughout the network.

FSLS – Fuzzy Sighted Link State [4]. In FSLS, an optimal link state update algorithm (Hazy Sighted Link State) is used. Updates occur every $2^k T$, in which k is the hop distance, T is the minimum link state update transmission period, and 2^k is the number of nodes to be updated. FSLS operates in a way very similar to FSR, as described below.

FSR – Fisheye State Routing [5, 6]. In FSR, each node maintains a topology map, and link state information is exchanged with neighbors periodically. The frequency with which it occurs depends on the hop distance to the current node. Nearby destinations are updated more frequently whereas for the faraway ones the updates are less frequent. Therefore, FSR produces accurate distance and path information about immediate neighborhood, and imprecise information about the best path to a distant node. On the other hand, such an imprecision is compensated for as the packet approaches its destination.

GSR – Global State Routing [7]. In GSR, a link state table based on the update messages from neighboring nodes is kept and periodical exchanges of link state information are carried out. The size of update messages increases with the increase of the size of the network, and a considerable amount of bandwidth is required in this case.

HSR – Hierarchical State Routing [8]. In HSR, the link state algorithm principle is used in conjunction with a hierarchical addressing and topology map. Clustering algorithms may also be used so as to organize the nodes with close proximity into clusters. Each node has a unique identity, which are typically a MAC address and a hierarchical address. A communication between any two nodes occurs by means of physical and logical links. The physical links support the true communication between nodes whereas the logical links are used for the purposes of the hierarchical structure of the communication. This way, several levels in the hierarchy may be built. The lowest level is always the physical level whereas the higher levels constitute the logical levels. Communications then occur starting from the lowest level up to the higher levels and down again to the lowest level.

MMWN – Multimedia support in Mobile Wireless Networks [9]. In MMWN, a clustering hierarchy is used, each cluster having two types of nodes: switch and endpoint. Endpoints do not communicate with each other but with switches only. Within a cluster, one of the switches is chosen as a location manager, which performs location updating and location finding. This means that routing overhead is drastically reduced as compared to the traditional table-driven algorithms. This way, information in MMWN is stored in a dynamically distributed database.

OLSR – Optimized Link State Routing [10]. In OLSR, each node keeps topology information on the network by periodically exchanging link state messages. OLSR uses the multipoint replaying strategy (MPR) in order to minimize the size of the control messages and the number of re-broadcasting nodes. To this end, each node selects a set of neighboring nodes (multipoint relays – MPRs) to retransmit its packets. Those not in the selected set may read and process each packet but not retransmit. The selection of the appropriate set is carried out as follows. Each node periodically broadcasts a list of its one-hop neighbors. From the lists the nodes are able to choose a subset of one-hop neighbors that cover all of its two-hop neighbors. An optimal route to every destination is constructed and stored in a routing table.

STAR – Source-Tree Adaptive Routing [11]. In STAR, each node keeps a source tree with the preferred paths to destinations. It uses the least overhead routing approach (LORA) to reduce the amount of routing overhead disseminated into the network. The reduction in the amount of messages is achieved by making update dissemination conditional to the occurrence of certain events.

TBRPF – Topology Broadcast Based on Reverse Path Forwarding [12, 13]. In TBRPF, two separate modules are implemented: neighbor discovery module and the routing module. The first module performs a differential HELLO messages that reports only the changes (up or lost) of neighbors. The second module operates based on partial

topology information. The information is obtained through periodic and differential topology updates. If a node n is to send an update message, then every node in the network selects its next hop (parent) node towards that node. Link state updates are propagated in the reverse direction on the spanning tree formed by the minimum-hop paths from all nodes to the sending node. This means that updates originated at n are only accepted if these updates arrive from the respective parent node. They are then propagated towards the children nodes pertaining to n.

WRP – Wireless Routing Protocol [14]. In WRP, each node maintains a set of tables as follows: Distance Table, Routing Table, Link-cost Table, Message Retransmission List (MRL) table. Each entry of the MRL table contains a sequence number of the update message, a retransmission counter, an acknowledgement required flag vector with one entry per neighbor, and a list of updates sent in the update message. It records which updates need to be retransmitted and which neighbors should acknowledge the retransmission. Update messages are sent only between neighboring nodes and they occur after processing updates or detecting a change in the link to the neighbor. Nodes learn of the existence of their neighbors from the receipt of ACK and other messages. In case a node is not sending messages of any kind, then a HELLO message is sent within a specified period of time to ensure connectivity.

2.2 REACTIVE ALGORITHMS

ABR – Associativity-Based Routing (ABR) [15]. In ABR, a query-reply technique is used to determine routes to the required destination. Stable routes are chosen based on an associativity tick that each node maintains with its neighbors, with the links with the higher associativity tick being selected. This may not lead to the shortest paths but rather to paths that last longer. In such a case, fewer route reconstructions are needed thence more bandwidth is available. ABR requires periodical beaconing so as to determine the degree of associativity of the links which requires all nodes to remain active at all time, which result in additional power consumption.

AODV – Ad Hoc on Demand Distance Vector [16]. In AODV, periodic beaconing and sequence numbering procedure are used. The packets convey the destination address rather than the full routing information, this also occurring in the route replies. The advantage of AODV is its adaptability to highly dynamic networks. On the other hand, the nodes may experience large delays in route construction.

ARA – Ant-colony-based Routing Algorithm [17]. In ARA, the food searching behavior of ants is used in order to reduce routing overheads. When searching for food, ants leave a trail behind (pheromone) that is followed by the other ants until it vanishes. In the route discovery procedure, ARA propagates a Forwarding ANT (FANT) through the network until it reaches the destination. Then a Backward ANT (BANT) is returned, a path is created, and data packet dissemination starts. The route is maintained by means of increasing or decreasing the pheromone value at each node. The pheromone at a given node is increased each time a packet travels through it, and it is decreased overtime until it expires. As can be inferred, the size of FANT and BANT is small; therefore the amount of overhead per control packet is minimized.

CBRP – Cluster-Based Routing Protocol [18]. In CBRP, the nodes are grouped into clusters, a cluster presenting a clusterhead. The advantage of using the hierarchical approach is the decrease in the number of control overhead through the network as compared with the traditional flooding methods. Of course, there are overheads associated with the formation and maintenance of the clusters. The long propagation delay due to the hierarchical structure may render the nodes bearing inconsistent topology information, which may lead to temporary routing loops.

DSR – Dynamic Source Routing [19]. In DSR, there is no periodic beaconing (HELLO message), an important feature that can be used for battery saving purposes, in which the node may enter the sleep mode. Each packet in DSR conveys the full address of the route, and this is a disadvantage for large or highly dynamic networks. On the other hand, the nodes can store multiple routes in their route cache. The advantage of this is that the node can check its route cache for a valid route before initiating route discovery. A valid route found avoids the need for route discovery. And this is an advantageous feature for low mobility networks.

FORP – Flow Oriented Routing Protocol [20]. In FORP, routing failure due to mobility is minimized by means of the following algorithm. A Flow-REQ message is disseminated through the network. A node receiving such a message, and based on GPS information, estimates a Link Expiration Time (LET) with the previous hop and append this into its Flow-REQ packet, which is re-transmitted. Upon arrival at the destination, a Route Expiration Time (RET) is estimated using the minimum of all LETs for each node. A Flow-SETUP message is sent back towards the source. Therefore, the destination is able to predict when a link failure may occur. In such a case, a Flow-HANDOFF message is generated and propagated in a similar manner.

LAR – Location Aided Routing [21]. In LAR, using location information routing overhead is minimized, which is commonly present in the traditional flooding algorithms. Assuming each node provided with a GPS, the packets travel in the direction where the relative distance to the destination becomes smaller as they travel from one hop to another.

LMR – Light-weight Mobile Routing [22]. In LMR, the flooding technique is used in order to determine the required routes. Multiple routes are kept at the nodes, the multiplicity being used for reliability purposes as well as to avoid the re-initiation of a route discovery procedure. In addition, the route information concerns the neighborhood only and not the complete route.

RDMAR – Relative Distance Micro-discovery Ad hoc Routing [23]. In RDMAR, a relative-distance micro-discovery procedure is used in order to minimize routing overheads. This is carried out by means of calculating the distance between source and destination, thence limiting each route request packet to a certain number of hops (i.e., the route discovery procedure becomes confined to localized regions). In fact, this is only feasible if previous communications between source and destination has been established. Otherwise, a flooding procedure is applied.

ROAM – Routing on-Demand Acyclic Multi-path [24]. In ROAM, inter-nodal coordination and directed acyclic sub-graphs, derived from the distance of the router to the destination, are used. In case the required destination is no longer reachable multiple flood searches stop. In addition, each time the distance of a router to a destination changes by more than a given threshold, the router broadcasts update messages to its neighboring nodes. This increases the network connectivity at the expense of preventing the nodes entering the sleep mode to save battery.

SSA – Signal Stability Adaptive [25]. In SSA, route selection is carried out based on signal strength and location stability, and not on associativity tick. In addition, route requests sent toward a destination cannot be replied by intermediate nodes, which may cause delays before a route is effectively discovered. This is due to the fact that the destination is responsible for selecting the route for data transfer.

TORA – Temporarily Ordered Routing Algorithm [26]. In TORA, the key design concept is the localization of control messages to a very small set of nodes near the occurrence of a topological change. The nodes maintain routing information about one-hop nodes. Route creation and route maintenance phases use a height metric to establish a directed acyclic graph rooted at the destination. Then, links are assigned as upstream or downstream based on the relative height metric to neighboring nodes. Route's erasure phase involves flooding a broadcast clear packet throughout the network in order to erase invalid routes.

2.3 HYBRID ALGORITHMS

DDR – Distributed Dynamic Routing [27]. In DDR, a tree-based routing protocol is used but a root node is not required. The trees are set up by means of periodic beaconing messages, exchanged by neighboring nodes only. Different trees, composing a forest, are connected via gateways nodes. Each tree constitutes a zone, which is assigned a zone ID. The routes are determined by hybrid ad hoc protocols.

DST – Distributed Spanning Trees Based Routing Protocol [28]. In DST, all nodes are grouped into trees, within which a node becomes a routing node or an internal node. The root, which is also a node, controls the structure of the tree. This may become a disadvantage of DST for the root node creates a single point of failure.

SLURP – Scalable Location Update Routing Protocol [29]. In SLURB, the nodes are organized into non-overlapping zones and a home region for each node in the network is assigned. The home region for each node is determined by means of a static mapping function known to all nodes whose inputs are the node ID and the number of nodes. Thus, all nodes are able to determine the home region for each node. The current location of the node within its home region is maintained by unicasting a location update packet towards its region. Once it reaches its home region, it is broadcast to all nodes within its home.

ZHLS – Zone-Based Hierarchical Link State [30]. In ZHLS, hierarchical topology is used such that two levels are established: node level and zone level, for which the use of GPS is required. Each node then has a node ID and a zone ID. In case a route to a node within another zone is required, the source node broadcasts a zone-level location request to all of the other zones. This generates lower overhead as compared to the flooding approach in reactive protocols. Mobility within its own zone maintains the topology of the network such that no further location search is required. In ZHLS, all nodes are supposed to have a pre-programmed static zone map for initial operation.

ZRP – Zone Routing Protocol [31]. In ZRP, a routing zone is established that defines a range in hops within which network connectivity is proactively maintained. This way, nodes within such a zone have the routes available immediately. Outside the zone, routes are determined reactively (on demand) and any reactive algorithm may be used.

3. MEDIUM ACCESS PROTOCOLS

Medium Access Control (MAC) for wireless ad hoc networks is currently a very active research topic. The characteristics of the network, the diverse physical-layer technologies available, and the range of services envisioned render a difficult task the design of an algorithm to discipline the access to the shared medium that results efficient, fair, power consumption sensitive, and delay bound. A number of issues distinguish wireless MAC protocols from those used in wireline networks [32], as quoted next.

Half-Duplex Operation. Due to self-interference (i.e., the energy from the transmitter that leaks into the receiver), it is difficult to construct terminals able to receive while transmitting. Therefore collision detection while sending data is not possible and Ethernet-like protocols cannot be used. Since collisions cannot be detected, wireless MAC protocols use collision avoidance mechanisms to minimize the probability of collision.

Time Varying Channel. In multipath fading channels, the received signal is the sum of time-shifted and attenuated copies of the transmitted signal. With the change of the channel characteristics as well as in the relative position of terminals, the signal envelope varies as a function of time. The signal experiences fading that may be severe. The nodes establishing a wireless link need to sense the channel so as to assess the communication link conditions.

Burst Channel Errors. Wireless channels experience higher bit error rate than wireline transmissions. Besides, errors occur in bursts as the signal fades, resulting in high probability of packet loss. Therefore, an acknowledgement mechanism must be implemented so that the packet retransmission may be possible in case of packet loss.

Location-Dependent Carrier Sensing. Because the signal strength decays with distance according to a power law, only nodes within a specific range are able to communicate. This gives rise to the hidden and exposed terminals and the capture effect, as described next.

Hidden Terminal. Refer to Figure 1 where the relative positions of terminals A, B, and C are shown. B is within range of both A and C but A and C are out of range of each other. If terminal A is transmitting to B and terminal C wishes to transmit to B, it incorrectly senses that the channel is free because it is out of range of A, the current transmitter. If C starts transmitting it interferes with the

reception at B. In this case C is termed the hidden terminal to A. The hidden terminal problem can be minimized with the use of the Request-to-Sent/Clear-to-Send (RTS/CTS) handshake protocol (to be explained later) before the data transmission starts.

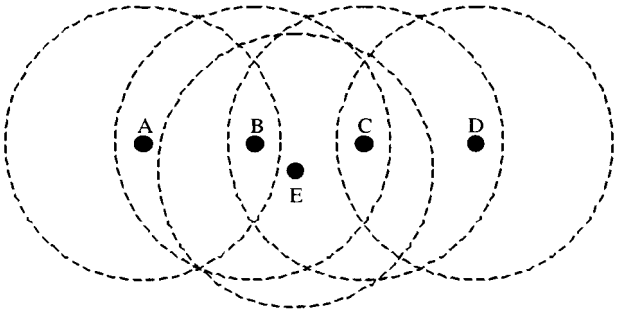

Figure 1. Hidden-exposed terminal problem

Exposed Terminal. An exposed terminal is one that is within range of the transmitter but out of range of the receiver. In Figure 1, if terminal B is transmitting to A and terminal C senses the channel it perceives it as busy. However, since it is out of range of terminal A it cannot interfere with the current conversation. Therefore it can utilize the channel to establish a parallel link with another terminal that is out of range of B, for instance, terminal D. In this case C is termed the exposed terminal to B. Exposed terminals may result in under-usage of the channel. As in the hidden terminal problem, this also can be minimized with the use of the RTS/CTS handshake protocol.

Capture. Capture at a given terminal occurs in case among several simultaneous signals arriving at it the signal strength of one of them prevails over all of the others combined. In Figure 1, terminals C and E are both within range of terminal B. If C and E are transmitting the interference may result in a collision at B. However B may be able to receive successfully if one of the signals is much higher than the other, for instance, the signal from E. Capture can improve throughput because it results in less collisions. However it favors senders that are closer to the intended destination, which may cause unfair allocation of the channel.

From the above considerations, it is promptly inferred that, the design of a MAC protocol for ad hoc networks requires a different set of parameters must be considered as compared with those of the wireline systems.

3.1 PROTOCOLS CATEGORIES

Jurdak et al. [33], after conducting a survey and analysis of a number of current MAC protocol proposals, offer a set of key features that may be used in order to classify MAC protocols for ad hoc networks.

Channel Separation and Access. The way the medium is organized is an important issue in the protocol design. For instance, all stations may share a single channel, which they use for control and data transmissions. On the other hand, the medium may be divided into multiple channels, in general one for control and the others for data. The single channel approach was favored in earlier MAC designs because of its simplicity. However, it is intrinsically subject to collisions and it does not perform well in medium to heavy traffic conditions. Particularly at heavy loads, simulations show that single channel protocols are prone to increased number of collisions of control packets, for example, RTS and CTS, which cause increased back off delays while the medium is idle [34]. The choice for multiple channels brings the issue of how to separate these channels. The most common ways of separating channels make use of FDMA, TDMA, and CDMA technologies. *Frequency Division Multiple Access* (FDMA) uses multiple carriers to divide the medium into several frequency slots. It allows multiple transmissions to occur simultaneously although each sender can use only the bandwidth of its assigned frequency slot. *Time Division Multiple Access* (TDMA) divides the medium into fixed length time slots. A group of slots forms a time frame and defines the slot repetition rate. Because of its periodic nature, TDMA protocols are suitable to delay sensitive traffic. In TDMA, a sender uses the whole available bandwidth for the duration of a slot assigned to it. In addition, to access the medium terminals need to keep track of frames and slots and, as a result, TDMA protocols require synchronization among terminals. *Code Division Multiple Access* (CDMA) allows senders to use the whole available bandwidth all the time. Each sender is assigned one of several orthogonal codes and simultaneous transmissions are possible for users are identified by their unique code. A general requirement in CDMA is for power control. The reason behind it is that an unwanted signal that is stronger than the desired signal may overwhelm it at the receiver's antenna. This is known as the near-far effect. *Space Division Multiple Access* (SDMA), similarly to CDMA, aims at allowing senders to use the whole available bandwidth all the time. However the terminals use directional antennas and are allowed to start transmission only if the desired transmission's direction does not interfere with an ongoing conversation.

RTS/CTS handshake. Many MAC protocols for ad hoc networks use variants of the RTS/CTS handshake. The original three-way handshake minimizes both the hidden and exposed terminal problems. A terminal wishing to send data first senses the channel. If the channel is idle for the appropriate amount of time, the terminal sends a short Request-to-Send (RTS) packet. All terminals on hearing the RTS defer their transmissions. The destination responds with a Clear-to-Send (CTS) packet. All terminals on hearing the CTS also defer their transmissions. The sender, on receiving the CTS assumes the channel is acquired and initiates the data transmission.

Topology. Ad hoc networks have a large degree of flexibility and uncertainty. Terminals may be mobile and have distinct capabilities and resources. The network must take this into account and adapt dynamically while optimizing performance and minimizing power consumption [33]. A network topology can be centralized, clustered, or flat. *Centralized topologies* have a single terminal or base station that controls and manages the network. The central terminal may be responsible for broadcasting information relevant to the operation of the network. In addition, terminals may only communicate through the central terminal. *Clustered topologies* create a local version of a centralized network where one terminal

assumes some or all of the duties expected from the central terminal. *Flat topologies* implement a fully distributed approach where all terminals are at the same level, and central control is not used. Flat topologies are further divided into single-hop and multiple-hop. *Single-hop* assumes that the destination node is within range of the sender. *Multiple-hop* assumes that the destination node may be beyond the sender's reachable neighbors. In this case, intermediate terminals are responsible for relaying the packets until they reach the intended destination. Single-hop protocols are simpler but pose limitations on the size of the network. Multiple-hop adds scalability to the network at the expense of higher complexity.

Power. Power consumption is a relevant issue for all wireless networks. Power conservation is particularly influential for the mobile terminals because of the limited battery power available. An efficient power conservation strategy involves several aspects. The energy used to transmit the signal represents a large share of the power consumption. Ideally the transmit power used should be just enough to reach the intended destination. Another source of wasted energy is the long periods of time terminals need to spend sensing the channel or overhearing irrelevant conversation. If terminals are able to learn in advance about when the medium will be unavailable they may decide to go into a sleep mode for that period of time in order to save energy. The network behavior may be influenced by the terminals' battery power level, for instance, in the selection of a cluster head or in assigning transmission priorities. Terminals aware of their battery level may adjust their behavior accordingly. The exchange of control messages before the data transmission phase also represents power wastage. Reduced control overhead should therefore be pursued for the sake of power efficiency.

Transmission Initiation. Intuitively, it is expected that a terminal wishing to start a conversation must initiate the transmission. And in fact most of the protocols are organized this way. However, a receiver-initiated protocol may be more suitable to some specialized networks, for instance, a sensor network. In receiver-initiated protocols the receiver polls its neighbors by sending a Ready-to-Receive (RTR) packet, which indicates its readiness to receive data. If the receiver is able to know or successfully predict when a neighbor wishes to send its data, this class of protocols actually produces better performance. However for generalized networks and unpredictable traffic, sender-initiated protocols are still a better choice.

Traffic Load and Scalability. Protocols are usually optimized for the worst expected scenario. Sparse node distribution and light traffic conditions do not pose a challenge for the implementation of ad hoc networks. The protocols are optimized for high traffic load, high node density and/or real-time traffic, depending on the intended use. Protocols that offer the possibility of channel reservation are those with best performance on both high load and real-traffic situations. Receiver-initiated approaches also tend to work well in high load conditions because there is a high probability that RTR packets reach terminals wishing to send data. If the network ranks terminals and traffic, then it is able to assign priorities based on the traffic nature. Therefore, it can offer favored handling of real-time traffic. Dense networks tend to suffer from higher interference because of the proximity of transmitting nodes. For this reason the use of power control makes a significant difference in the performance of the network.

Range. Transmission range is the distance from the transmitter's antenna that the radio signal strength still remains above the minimum usable level. Protocols can be classified [33] as very short-range (range up to 10 m), short-range (from 10 up to 100 m), medium-range (from 100 up to 1000 m), and long-range (from 1000 m). There is a trade-off between increasing the transmission range and achieving high spatial capacity that needs to be negotiated during the protocol design.

3.2 INDUSTRY STANDARD PROTOCOLS

3.2.1 IEEE 802.11

The family of IEEE 802.11 standards [35, 36, 37] can be viewed as a wireless version of the Local Area Network (LAN) protocol Ethernet. The 802.11a standard operates in the unlicensed 5 GHz band and offers data rates up to 54 Mb/s. The commercially popular 802.11b operates in the industrial, scientific, and medical (ISM) band at 2.4 GHz and offers data rates up to 11 Mb/s. The current activity of the 802.11-working group is towards quality of service (QoS) (802.11e, described later) and security (802.11i). The 802.11 standards focus on the specification of the MAC and physical (PHY) layers. While their PHY layers differ, existing 802.11 standards rely on the same medium access mechanisms. The basic (and mandatory) access mechanism is referred to as Distributed Coordination Function (DCF). The optional Point Coordination Function (PCF) is an access mechanism in which a central node (the access point) polls terminals according to a list. DCF is available for both flat ad hoc and centralized topologies whereas PCF is only available in centralized configurations. MAC offers two types of traffic services. The mandatory asynchronous data service is based on the best effort and is suited to delay insensitive data. The optional time-bound service is implemented using PCF.

DCF uses the listen-before-talk scheme based on Carrier Sense Multiple Access (CSMA). A terminal wishing to transmit a data packet first monitors the medium activity. If the channel is detected idle the terminal waits for a DCF interframe space (DIFS) time interval (34 us in 802.11a). If the channel remains idle during the DIFS period, the terminal starts transmitting its packet immediately after DIFS has expired. The transmission is successfully completed when the sender receives an acknowledgement (ACK) packet from the destination. However, if the channel is sensed busy a Collision Avoidance procedure is used. In this procedure, after sensing the channel idle again for a DIFS period, the terminal wishing to transmit waits an additional random backoff time. The terminal then initiates its transmission if the channel remains idle during this additional time. The backoff time is a multiple of the slot time (9 us in 802.11a) and it is determined individually and independently by each station. A random number between zero and contention window (CW) is selected for any new transmission attempt. The back off time is decremented

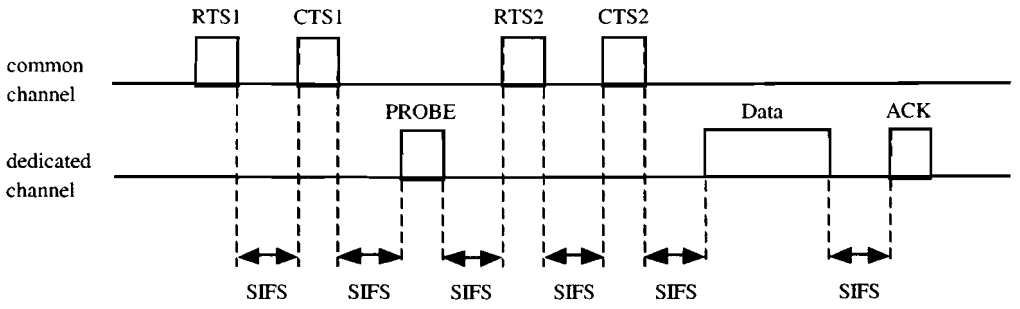

Figure 2. IEEE 802.11 backoff timing

while the medium is in contention phase and frozen otherwise. Thus the backoff time may be carried over for several busy cycles of the medium before it expires. Refer to Figure 2 for an example of the backoff procedure. The initial value for CW is CWmin (15 for 802.11a) and since all terminals operate with the same CWmin value they all have the same initial medium access priority. After any failed transmission, i.e., when the transmitted packet is not acknowledged, the sender doubles its CW up to a maximum defined by CWmax (1023 in 802.11a). A now larger CW decreases the probability of collisions if multiple terminals are trying to access the medium. To reduce the hidden terminal problem, 802.11 optionally uses the RTS/CTS handshake. Both RTS and CTS packets include information on how long the data frame transmission is going to last, including the corresponding ACK. Terminals receiving either the RTS or CTS use this information to start a timer, called network allocation vector (NAV), which informs the period of time the medium is unavailable. Between consecutive frames RTS and CTS, and a data frame and its ACK, the short interframe space (SIFS) (16 us in 802.11) is used. SIFS is shorter than DIFS and therefore gives the terminals sending these frames priority to access the medium.

3.2.2 HIPERLAN 1

High Performance LAN type 1 (HIPERLAN 1) is a wireless LAN standard operating in the 5 GHz band, which offers data rate up to 23.5 Mb/s to mobile users in either clustered ad hoc or centralized topology. HIPERLAN 1 offers asynchronous best effort and time-bound services with hierarchical priorities. There are five priority values defined, from zero (highest) to four (lowest). Each individual MAC protocol data unit (PDU) is assigned a priority that is closely related to its normalized residual lifetime (NRL) value. The NRL is an estimation of the time-to-live the PDU has considering the number of hops it still has to travel. A PDU is discarded if its NRL value reaches zero. In addition, some terminals are designed forwarders and are responsible to relay data to distant nodes in a multi-hop fashion. HIPERLAN 1 allows terminals to go into sleep mode in order to save energy. These terminals, called p-savers, inform support terminals, called p-supporters, of their sleep/wake-up patterns. p-supporters then buffer packets directed to p-savers terminals, as required. Although it has some interesting features, HIPERLAN 1 has not been a commercial success. The channel access mechanism used in HIPERLAN 1 is the Elimination-Yield Non-Preemptive Priority Access (EY-NPMA). It comprises three phases: prioritization (determine the highest priority data packets to be sent); contention (eliminate all contenders except one); and transmission. During the prioritization phase, time is divided in five minislots, numbered sequentially from zero to four. A terminal wishing to transmit has to send a burst during the minislot corresponding to its MAC PDU priority. For example, a terminal with a priority two PDU monitors the medium during minislots zero and one before it can assert its intention by transmitting a burst during minislot two. If the medium becomes busy during either minislot zero or one this terminal defers its transmission. Once a burst is transmitted, the prioritization phase ends and only terminals having PDUs at the same priority level remains in the dispute. The contention phase follows. It starts with the contending terminals transmitting an elimination burst. The individual terminals select the burst length, varying from 0 to 12 minislots, at random and independently. After transmitting the burst the terminals sense the medium. If it is busy they defer their transmissions. Otherwise, the remaining terminals enter the yield listening period. They select at random and independently a value between 0 and 9 and start monitoring the medium. If at the end of this period the medium is still idle the terminal assumes it has won the contention and is allowed to transmit its data. Otherwise, it defers its transmission. It is clear that the mechanism does not allow any lower priority packet to be sent if another with higher priority packet is waiting. At the same time the mechanism does not totally eliminate the possibility of collision but reduces it considerably. Similarly to IEEE 802.11, if the medium has been idle for a time longer than the interframe period a terminal wishing to transmit can bypass the EY-NPMA and transmit immediately.

3.2.3 BLUETOOTH

Bluetooth [38] is a wireless protocol using the license-free ISM band to connect mobile and desktop devices such as computers and computers peripherals, handheld devices, cell phones, etc. The aim is to produce low-cost, low-power and very-short range devices able to convey voice and data transmissions at a maximum gross rate of 1 Mb/s. Bluetooth uses frequency hopping spread spectrum (FHSS) with 1600 hops/s. For voice, a 64 kb/s full-duplex link called

synchronous connection oriented (SCO) is used. SCO assigns a periodic single slot to a point-to-point conversation. Data communication uses the best effort asynchronous connectionless (ACL) link in which up to five slots can be assigned. Terminals in Bluetooth are organized in piconets. A piconet contains one terminal identified as the master and up to seven other active slaves. The master determines the hopping pattern and the other terminals need to synchronize to the piconet master. When it joins a piconet, an active terminal is assigned a unique 3-bit long active member address (AMA) It then stays in either transmit state, when it is engaged in a conversation, or connected state. Bluetooth supports three low-power states: park, hold, and sniff. A parked terminal releases its AMA and is assigned one of the 8-bit long parked member address (PMA). Terminals in the hold and sniff states keep their AMA but have limited participation in the piconet. For instance, a terminal in the hold state is unable to communicate using ACL. A terminal not participating in any piconet is in stand-by state. Bluetooth piconets can co-exist in space and time and a terminal may belong to several piconets. A piconet is formed when its future master starts an inquiry process, i.e., inquiry messages are broadcast in order to find other terminals in the vicinity. After receiving inquiry responses the master may explicitly page terminals to join the piconet. If a master knows already another terminal's identity it may skip the inquiry phase and page the terminal directly. Bluetooth uses time division duplex (TDD) in which master and slave alternate the opportunity to transmit. A slave can only transmit if the master has just transmitted to it, i.e., slaves transmit if polled by the master. Transmissions may last one, three, or five slots although only single-slot transmission is a mandatory feature.

3.2.4 IEEE 802.11E

The IEEE 802.11e is an emerging MAC protocol, which defines a set of QoS features to be added to the 802.11 family of wireless LAN standards. Currently there is a draft version of the specifications [39]. The aim is to better serve delay-sensitive applications, such as voice and multi-media. In 802.11e, the contention-based medium access is referred to as Enhanced Distributed Channel Access (EDCA). In order to accommodate different traffic priorities, four access categories (AC) have been introduced. To each AC corresponds a backoff entity. The four distinct parallel backoff entities present in each 802.11e terminal are called (from highest to lowest priority): voice, video, best effort, and background. For the sake of comparison, existing 802.11/a/b standards define only one backoff entity per terminal. Each backoff entity has a distinct set of parameters, such as CWmin, Cwmax, and the Arbitration Interframe Space (AIFS). AIFS is at least equal to DIFS and can be enlarged if desired. Another feature added to 802.11e is referred to as transmission opportunity (TxOP). A TxOP defines a time interval, which a back off entity can use to transmit data. It is specified by its starting time and duration, and the maximum length is AC dependent. The protocol also defines the maximum lifetime of each MAC Service Data Unit (MSDU), which is also AC dependent. Once the maximum lifetime has elapsed, the MSDU is discarded. Finally, the protocol allows for the optional block acknowledgement in which a number of consecutive MSDUs are acknowledged with a single ACK frame.

3.3 OTHER PROTOCOLS

PRMA – Packet Reservation Multiple Access [40]. In PRMA, the medium is divided into slots and a group of N slots forms a frame. Slots are either reserved or available. The access to the medium is provided by means of the slotted-ALOHA protocol. Data may be either periodic or sporadic, and this is informed in the header of the packet. Terminals are allowed to reserve a slot when they have periodic data to transmit. Once the central node successfully acknowledges the periodic packet, the terminal assumes the slot is reserved and uses it without contention. When the terminal stops sending periodic information then the reserved slot is released. PRMA assumes the existence of a central node but the mechanism can be adapted to other topologies [41].

MACA-BI – Multiple Access with Collision Avoidance by Invitation [42]. In MACA-BI, the receiver polls a prospective sender by transmitting a Ready-to-Receive (RTR) packet. (This is an example of a receiver-initiated protocol.) In order to perform the polling in a timely fashion the receiver is required to correctly predict the traffic originated by the sender. Periodic traffic makes this task easier. In case either the data buffer or the delay at the terminal increases above a certain threshold this terminal may trigger a conversation by transmitting an RTS packet. Improvements to MACA-BI are proposed in [43], in which RIMA-SP – Receiver Initiated Multiple Access with Simple Polling –, and RIMA-DP – Receiver Initiated Multiple Access with Dual-purpose Polling – are introduced. Both protocols render the RTR-data handshake collision free. RIMA-DP gives an additional purpose to the RTR packet: a request for transmission from the polling terminal. After a reservation phase both terminals can exchange data between them.

DBTMA – Dual Busy Tone Multiple Access [44]. In DBTMA, the RTS/CTS handshake is replaced by two out-of-band busy tones, namely: BTt (transmit busy tone) and BTr (receive busy tone). When a terminal has data to transmit, it first senses the presence of the BTt and BTr tones. If the medium is free (no busy tone detected), the terminal turns on the BTt, sends an RTS packet, and turns off the BTt. As in other protocols, there is a random backoff time if the medium is busy. The destination terminal, upon receipt of an RTS addressed to it, turns on the BTr and waits for the data. Once the BTr tone is sensed, the sender assumes it has successfully acquired the medium. After waiting a short time (for the BTr to propagate) it transmits the data packet. On successful reception of the data packet the destination terminal turns off the BTr tone, completing the conversation. If no data is received, the BTr tone is turned off after a timer expires at the destination terminal.

Fitzek et al. [45] proposes a multi-hop MAC protocol based on the IEEE 802.11. A common channel conveys signaling and dedicated channels carry the data traffic and the ACK packets. Figure 3 presents the proposed MAC handshake. The first RTS packet is used to contact the destination and assess its willingness to receive data. The sender includes a list of idle dedicated channels, which is

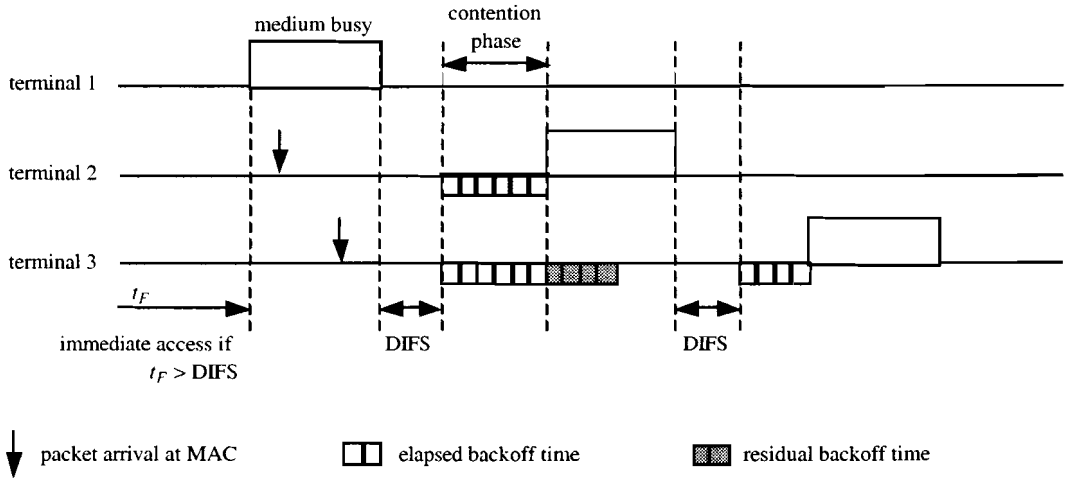

Figure 3. MAC handshake [45]

used by the destination terminal to select the dedicated channel. It then transmits this information to the sender in a CTS packet. If no suitable dedicated channel is available the handshake ends. After receiving the CTS packet, the sender transmits a PROBE packet on the dedicated channel. The destination terminal uses this packet to test the channel conditions. It then sends a second CTS packet on the common channel informing about the chosen coding/modulation scheme. The sender to confirm the parameters chosen transmits a second RTS packet. Although at a higher complexity cost, the authors claim that the proposed scheme outperforms the original 802.11.

LA-MAC – Load Awareness MAC [46]. In LA-MAC, the protocol switches between contention-based and contention-free mechanisms depending on the traffic volume. Contention-based mechanisms are best suited to light traffic conditions in which the probability of collision while attempting to gain the medium is small. For heavy traffic a contention-free mechanism allows higher and more evenly distributed throughput. In [46], the IEEE 802.11 DCF is adopted during contention-based periods while contention-free periods use a token passing protocol. The traffic load is measured by the delay packets are experiencing. Each terminal for the packets it has to transmit computes such delay. During a contention-based period, before a terminal transmits its data packet, it checks the packet's current delay. If the delay is greater than a pre-defined threshold A the terminal creates a token and transmits it attached to the data packet. This indicates to all terminals the start of a contention-free period. Once the delay has fallen below another pre-defined threshold B, the terminal about to transmit removes the token. This indicates the end of the contention-free period and the start of a contention-based period. Threshold A is chosen to be greater than B to give the switching decision some hysteresis.

PCDC – Power Controlled Dual Channel [47]. In PCDC, the objective is to maintain network connectivity at the lowest possible transmit power. PCDC is a multi-hop protocol that uses the RTS/CTS handshake found in IEEE 802.11 with some modifications. Each terminal is required to keep a list of neighboring terminals and the transmit power needed to reach them. When a packet is received, the list needs to be visited. If the sender is not known an entry is added. Otherwise, the existing entry is updated. In any case, the receiver needs to re-evaluate its connectivity information and confirm that it knows the cheapest way (in a transmit power sense) to reach all terminals that appears in its neighbor list. For instance, for some terminals it might be cheaper to use an intermediate terminal instead of the direct route. At heavy traffic loads there exist enough packets transiting to keep terminals well informed of their neighborhood. For long idle periods terminals are required to broadcast a "hello" packet periodically for this purpose. PCDC achieves space efficiency and simulations carried by the authors indicate an increase in the network's throughput.

MAC ReSerVation – MAC-RSV [48]. In MAC-RSV, a reservation-based multi-hop MAC scheme is proposed. The TDMA frame consists of data and signaling slots. Data slots are marked as follows: reserved for transmission (RT), reserved for reception (RR), free for transmission (FT), free for reception (FR), or free for transmission and reception (FTR). The signaling slot is divided in minislots with each minislot further divided in three parts: request, reply, and confirm. A terminal wishing to transmit sends an RTS packet. In the RTS, the sender informs its own identity, the intended receiver's identity, and the data slots it wishes to reserve. The intended receiver replies with a CTS if any of the requested slots is among its FR or FTR slots. Otherwise, it remains silent. It is possible that the CTS packet accepts reservation of only a subset of the requested slots. Terminals other than the intended receiver replies with a Not CTS (NCTS) if any of the requested slots is among its RR. Any terminal that detects an RTS collision also replies by sending an NCTS. Otherwise, it remains silent. Finally if the sender successfully receives a CTS it confirms the reservation by sending a confirm packet (CONF). Otherwise, it remains silent. RTS packets are transmitted in the request part of the minislot; CTS and NCTS use the reply part; and CONF packets use the confirm part. Data slots are divided in three parts: receiver beacon (RB), data and acknowledgement (ACK). A terminal that has a data slot marked RR transmits an RB with the identity of the active data transmitter. In addition, the receiver

acknowledges the correct data reception by transmitting an ACK at the end of the data slot. Simulations carried out by the authors indicate that the proposed protocol outperforms the IEEE 802.11 at moderate to heavy traffic loads.

3.4 COMMENTS

In [33] a set of guidelines is provided that a suitable general-purpose MAC protocol should follow. In particular, it is mentioned that the use of multiple channels to separate control and data is desirable in order to reduce the probability of collisions. The need of flexible channel bandwidth, multiple channels, and the high bandwidth efficiency suggests that CDMA is the optimal choice for channel partition. Multi-hop support is recommended to ensure scalability with flat or clustered topologies depending on the application. In order to favor power efficient terminals, protocols need to be power aware, must control transmission power, and allow for sleep mode. To complete the set of recommendations, the authors include, for the sake of flexibility, short to medium range networks and a sender-initiated approach.

4. TCP OVER AD HOC NETWORKS

TCP is the prevalent transport protocol in the Internet today and its use over ad hoc networks is a certainty. This has motivated a great deal of research efforts aiming not only at evaluating TCP performance over ad hoc networks, but also at proposing appropriate TCP schemes for this kind of networks. TCP was originally designed for wired network, based on the following assumptions, typical of such an environment: packet losses are mainly caused by congestion, links are reliable (very low bit error rate), round-trip times are stable and bandwidth is constant [49, 50]. Based on these assumptions, TCP flow control employs a window-based technique, in which the key idea is to probe the network to determine the available resources. The window is adjusted according to an additive-increase/multiplicative-decrease strategy. When packet loss is detected, the TCP sender retransmits the lost packets and the congestion control mechanisms are invoked, which include exponential backoff of the retransmission timers and reduction of the transmission rate by shrinking the window size. Packet losses are therefore interpreted by TCP as a symptom of congestion [51]. Previous studies on the use of TCP over cellular wireless networks have shown that this protocol suffers from poor performance mainly because the principal cause of packet loss in wireless networks is no longer congestion, but the error-prone wireless medium [52, 53]. In addition, multiple users in a wireless network may share the same medium, rendering the transmission delay time-variant. Therefore, packet loss due to transmission error or a delayed packet can be interpreted by TCP as being caused by congestion. When TCP is used over ad hoc networks, additional problems arise. Unlike cellular networks, where only the last hop is wireless, in ad hoc networks the entire path between the TCP sender and the TCP destination may be made up of wireless hops (multihop). Therefore, as discussed earlier in this paper, appropriate routing protocols and medium access control mechanisms (at the link control layer) are required to establish a path connecting the sender and the destination. The interaction between TCP and the protocols at the physical, link, and network layers can cause serious performance degradation, as discussed in the following.

4.1 PHYSICAL LAYER IMPACT

Interference and propagation channel effects are the main causes of high bit error rate in wireless networks. Channel induced errors can corrupt TCP data packets or acknowledgement packets (ACK), resulting in packet losses. If an ACK is not received within the Retransmit Timeout (RTO) interval, the lost packets may be mistakenly interpreted as a symptom of congestion, causing the invocation of TCP congestion control mechanisms. As a consequence, the TCP transmission rate is drastically reduced, degrading the overall performance. Therefore, the reaction of TCP to packet losses due to errors is clearly inappropriate. One approach to avoid this TCP behavior is to make the wireless channel more reliable by employing appropriate forward error correction coding (FEC), at the expense of a reduction of the effective bandwidth (due to the addition of redundancy) and an increase in the transmission delay [54]. In addition to FEC, link layer automatic repeat request (ARQ) schemes can be used to provide faster retransmission than that provided at upper layers. ARQ schemes may increase the transmission delay, leading TCP to assume a large round-trip time or to trigger its own retransmission procedure at the same time [50].

4.2 MAC LAYER IMPACT

It is well known that the hidden and exposed terminals problems strongly degrade the overall performance of ad hoc networks. Several techniques for avoiding such problems have been proposed, including the RTS/CTS control packets exchange employed in the IEEE 802.11 MAC protocol. However, despite the use of such techniques, hidden and exposed terminals problems can still occur, causing anomalous TCP behavior. The inappropriate interaction between TCP and link control layer mechanisms in multihop scenarios may cause the so-called TCP instability [55]. TCP adaptively controls its transmission rate by adjusting its contention window size. The window size determines the number of packets in flight in the network (i.e., the number of packets that can be transmitted before an ACK is received by the TCP sender). Large window sizes increase the contention level at the link layer, as more packets will be trying to make their way to the destination terminal. This increased contention level leads to packet collisions and causes the exposed terminal problem, preventing intermediate nodes from reaching their adjacent terminals [55]. When a terminal cannot deliver its packets to its neighbor, it reports a route failure to the source terminal, which reacts by invoking the route reestablishment mechanisms at the routing protocol. If the route reestablishment takes longer than RTO, the TCP congestion control mechanisms are triggered, shrinking the window size and retransmitting the lost packets. The invocation of congestion control mechanisms results in momentary reduction of TCP throughput, causing the

mentioned TCP instability. It has been experimentally verified that reducing the TCP contention window size minimizes TCP instability [55]. However, reduced window size inhibits spatial channel reuse in multihop scenarios. For the case of IEEE 802.11 MAC, which uses a four-way handshake (RTS-CTS-Data-ACK), it can be shown that, in an H-hop chain configuration, a maximum of $H/4$ terminals can simultaneously transmit [56], assuming ideal scheduling and identical packet sizes. Therefore, a window size smaller than this upper limit degrades the channel utilization efficiency. Another important issue related to the interaction between TCP and the link layer protocols regards the unfairness problem when multiple TCP sessions are active. The unfairness problem [55, 57] is also rooted in the hidden (collisions) and exposed terminals problems and can completely shut down one of the TCP sessions. When a terminal is not allowed to send its data packet to its neighbor due to collisions or the exposed terminal problem, its backoff scheme is invoked at the link layer level, increasing (though randomly) its backoff time. If the backoff scheme is repeatedly triggered, the terminal will hardly win a contention, and the winner terminal will eventually capture the medium, shutting down the TCP sessions at the loser terminals.

4.3 MOBILITY IMPACT

Due to terminal mobility, route failures can frequently occur during the lifetime of a TCP session. As discussed above, when a route failure is detected, the routing protocol invokes its route reestablishment mechanisms, and if the discovery of a new route takes longer than RTO, the TCP sender will interpret the route failure as congestion. Consequently, the TCP congestion control is invoked and the lost packets are retransmitted. However, this reaction of TCP in this situation is clearly inappropriate due to several reasons [51]. Firstly, lost packets should not be retransmitted until the route is reestablished. Secondly, when the route is eventually restored, the TCP slow start strategy will force the throughput to be unnecessarily low immediately after the route reestablishment. In addition, if route failures are frequent, TCP throughput will never reach high rates.

4.4 MAIN TCP SCHEMES PROPOSALS FOR AD HOC NETWORKS

4.4.1 TCP – FEEDBACK

This TCP scheme is based on explicitly informing the TCP sender of a route failure, such that it does not mistakenly invoke the congestion control [51]. When an intermediate terminal detects a route failure, it sends a Route Failure Notification (RFN) to the TCP sender terminal and records this event. Upon receiving an RFN, the TCP sender transitions to a "snooze" state and (i) stops sending packets, (ii) freezes its flow control window size, as well as all its timers, and (iii) starts a route failure timer, among other actions. When an intermediate terminal that forwarded the RFN finds out a new route, it sends a Route Reestablishment Notification (RRN) to the TCP sender, which in turn leaves the snooze state and resumes its normal operation.

4.4.2 TCP WITH EXPLICIT LINK FAILURE NOTIFICATION

Explicit Link Failure Notification (ELFN) technique is based on providing TCP sender with information about link or route failures, preventing TCP from reacting to such failures as if congestions had occurred [58]. In this approach, the ELFN message is generated by the routing protocol and a notice to TCP sender about link failure is piggybacked on it. When the TCP sender receives this notice, it disables its retransmission timers and periodically probes the network (by sending packets) to check if the route has been reestablished. When an ACK is received, the TCP sender assumes that a new route has been established and resumes its normal operation.

4.4.3 AD HOC TCP

A key feature of this approach is that the standard TCP is not modified, but an intermediate layer, called Ad Hoc TCP (ATCP), is inserted between IP and TCP (transport) layers. Therefore, ATCP is invisible to TCP and terminals with and without ATCP installed can interoperate. ATCP operates based on the network status information provided by the Internet Control Message Protocol (ICMP) and the Explicit Congestion Notification mechanism (ECN) [59]. The ECN mechanism is used to inform the TCP destination of the congestion situation in the network. An ECN bit is included in the TCP header and is set to zero by the TCP sender. Whenever an intermediate router detects congestion, it sets the ECN bit to one. When the TCP destination receives a packet with ECN bit set to one, it informs the TCP sender about the congestion situation, which in turn reduces its transmission rate. ATCP has four possible states: normal, congested, loss and disconnected. In the normal state ATCP does nothing and is invisible to TCP. In the congested, loss, and disconnected states, ATCP deals with congested network, lossy channel, and partitioned network, respectively. When ATCP sees three duplicate ACKs (likely caused by channel induced errors), ATCP transitions to the loss state and puts TCP into persist mode, ensuring that TCP does not invoke its congestion control mechanisms. In the loss state, ATCP retransmits the unacknowledged segments. When a new ACK arrives, ATCP returns to the normal state and removes TCP from the persist mode, restoring the TCP normal operation. When network congestion occurs, ATCP sees the ECN bit set to one and transitions to congested state. In this state, ATCP does not interfere with TCP congestion control mechanisms. Finally, when a route failure occurs, a Destination Unreachable message is issued by ICMP. Upon receiving this message, ATCP puts TCP into persist mode and transitions to the disconnected state. While in the persist mode, TCP periodically sends probe packets. When the route is eventually reestablished, TCP is removed from persist mode and ATCP transitions back to the normal state.

5. CAPACITY OF AD HOC NETWORKS

The classical information theory introduced by Shannon [60] presents the theoretical results on the channel capacity, i.e. how much information can be transmitted over a noisy and limited communication channel. In ad-hoc networks, this problem is led to a higher level of difficulty for the capacity now must be investigated in terms of several transmitters and several receivers. The analysis of the capacity of wireless networks has a similar objective as that of the classical information theory: to estimate the limit of how much information can be transmitted and to determine the optimal operation mode, so that this limit can be achieved. A first attempt to calculate these bounds is made by Gupta and Kumar in [61]. In this work, the authors propose a model for studying the capacity of a static ad hoc network (i.e., nodes do not move), based on the following scenario. Suppose that n nodes are located in a region of area $1\,m^2$. Each node can transmit at W bits per second over a common wireless channel. Packets are sent from node to node in a multi-hop fashion until their final destination is reached and they can be buffered at intermediate nodes while waiting for transmission. Two types of network configurations are considered: Arbitrary Networks, where the node locations, traffic destinations, rates, and power level are all arbitrary; and Random Networks, where the node locations, destinations are random, but they have the same transmit power and data rate. Two models of successful reception over one hop are also proposed:

Protocol Model – in which a transmission from node i to j, with a distance d_{ij} between them, is successful if $d_{kj} \geq (1+\Delta)d_{ij}$, i.e., if the distance between nodes i and j is smaller than that of nodes k and j with both i and k transmitting to j simultaneously over the same channel. The quantity $\Delta > 0$ models the guard zone specified by the protocol to prevent a neighboring node from simultaneous transmission.

Physical Model – in which, for a subset T of simultaneous transmitting nodes, the transmission from a node $i \in T$ is successfully received by node j if

$$\frac{P_i / d_{ij}^{\ \alpha}}{N + \sum_{\substack{k \in T \\ k \neq i}} P_k / d_{kj}^{\ \alpha}} \geq \beta \qquad (1)$$

with a minimum signal-to-interference ratio (SIR) β for successful receptions, noise power level N, transmission power level P_i for node i, and signal power decay α.

The transport capacity is so defined as the quantity of bits transported in a certain distance, measured in bit-meter. One bit-meter signifies that one bit has been transported over a distance of one meter toward its destination. With the reception models as described previously, the bounds for the transport capacity in Arbitrary Networks and the throughput per node in Random Networks were calculated. They are summarized in Table 1, where the Knuth's notation has been used[1]. These results show that, for Arbitrary Networks, if the transport capacity is divided into equal parts among all nodes, the throughput per node will be $\Theta\left(W/\sqrt{n}\right)$ bits per second. This shows that, as the number of nodes increases, the throughput capacity for each node diminishes in a square root proportion. The same type of results holds for Random Networks. These results assume a perfect scheduling algorithm which knows the locations of all nodes and all traffic demands, and which coordinates wireless transmissions temporally and spatially to avoid collisions. Without these assumptions the capacity can be even smaller.

	Protocol Model	Physical Model
Arbitrary Networks (transport capacity in bit-meters/s)	$\Theta\left(W\sqrt{n}\right)$	$\Omega\left(W\sqrt{n}\right)$ $O\left(Wn^{\left(\frac{\alpha-1}{\alpha}\right)}\right)$
Random Networks (node throughput in bits/s)	$\Theta\left(\frac{W}{\sqrt{n\log n}}\right)$	$\Omega\left(W/\sqrt{n\log n}\right)$ $O\left(W/\sqrt{n}\right)$

Table 1. Capacity bounds for Arbitrary and Random Networks.

Troumpis and Goldsmith [62] extend the analysis of upper limits of [61] to a three dimensional topology, and incorporated the channel capacity into the link model. In this work, the nodes are assumed as uniformly distributed within a cube of volume $1\,m^3$. The capacity $C(n)$ follows the inequality

$$k_1 \frac{n^{1/3}}{\log(n)} \leq C(n) \leq k_2 \log(n) n^{1/2} \qquad (2)$$

with probability approaching unity as $n \to \infty$, and k_1, k_2 some positive constants. Equation (2) also suggests that, although the capacity increases with the number of users, the available rate per user decreases.

An alternative approach on capacity of ad hoc networks, in which the influence of other factors is analyzed, is presented by Arpacioglu and Haas in this special issue.

[1] **Knuth's notation:** $f(n) = O(g(n))$ **if** $\limsup_{n\to\infty} f(n)/g(n) < +\infty$; $f(n) = \Omega(g(n))$ **if** $g(n) = O(f(n))$; $f(n) = \Theta(g(n))$ **if** $f(n) = O(g(n))$ **as well as** $f(n) = \Omega(g(n))$. **Thus, all** $O(\cdot)$ **results are upper bounds, all** $\Omega(\cdot)$ **results are lower bounds, and all** $\Theta(\cdot)$ **results are sharp order estimates for the capacity.**

5.1 CASE STUDIES ON CAPACITY OF AD HOC NETWORKS

5.1.1 IEEE802.11

Li et al [63] study the capacity of ad hoc networks through simulations and field tests. Again, the static ad hoc network is the basic scenario, which is justified by the fact that at most mobility scenarios nodes do not move significant distances during packet transmissions. The 802.11 MAC protocol is used to analyze the capacity of different configuration networks.

For the Chain of Nodes, the ideal capacity is 1/4 of the raw channel bandwidth obtainable from the radio (single-hop throughput). The simulated 802.11-based ad hoc network achieves a capacity of 1/7 of the single-hop throughput, because the 802.11 protocol fails to discover the optimum schedule of transmission and its backoff procedure performs poorly with ad hoc forwarding. The field experiment does not present different results from those obtained in the simulation. The same results are found for the Lattice Topology. For Random Networks with random traffic patterns, the 802.11 protocol is less efficient, but the theoretical maximum capacity of $O\left(1/\sqrt{n}\right)$ per node can be achieved.

It is also shown that the scalability of ad hoc networks is a function of the traffic pattern. In order for the total capacity to scale up with the network size, the average distance between source and destination nodes must remain small as the network grows. Therefore, the key factor deciding whether large networks are feasible is the traffic pattern. For networks with localized traffic the expansion is feasible whereas for networks in which the traffic must traverse it then the expansion is questionable.

5.1.2 WIRELESS MESH NETWORKS

A particular case of ad-hoc network, which is drawing significant attention, is the wireless mesh network (WMN). The main characteristic that differentiates a WMN from others ad-hoc networks is the traffic pattern: practically, all traffic is either to or from a node (gateway) that is connected to other networks (e.g. Internet). Consequently, the gateway plays a decisive role in the WMN: the greater the number of gateways the greater the capacity of this network as well as its reliability. Jun and Sichitiu [64] analyze the capacity of WMNs with stationary nodes. Their work shows that the capacity of WMNs is extremely dependent on the following aspects:

Relayed traffic and fairness – Each node in a WMN must transmit relayed traffic as well as its own. Thus, there is an inevitable contention between its own traffic and relayed traffic. In practice, as the offered load at each node increases, the nodes closest to the gateway tends to consume a larger bandwidth, even for a fair MAC layer protocol. The absolute fairness must be forced according to the offered load.

Nominal capacity of MAC layer (B) – It is defined as the maximum achievable throughput at the MAC layer in one-hop network. It can be calculated as presented in [65].

Link constraints and collision domains – In essence, all MAC protocols are designed to avoid collisions while ensuring that only one node transmits at a time in a given region. The collision domain is the set of links (including the transmitting one) that must be inactive for one link to transmit successfully.

The Chain Topology is first analyzed. It is observed that the node closer to the gateway has to forward more traffic than nodes farther away. For a n-node network and a per node generated load G, the link between the gateway and the node closer to it has to be able to forward a traffic equal to nG. The link between this node and the next node has to be able to forward traffic equal to $(n-1)G$, and so on. The collision domains are identified and the bottleneck collision domain, which has to transfer the most traffic in the network, is determined. The throughput available for each node is bounded by the nominal capacity B divided by the total traffic of the bottleneck collision domain. The Chain Topology analysis can be extended to a two-dimensional topology (Arbitrary Network). The values obtained for the throughput per node are validated with simulation results.

These results lead to an asymptotic throughput per node of $O(1/n)$. This is significantly worse than the results showed in Table 1, mainly because of the presence of gateways, which are the network bottlenecks. Clearly, the available throughput improves with the increase of the number of gateways in the network.

5.2 INCREASING THE CAPACITY OF AD HOC NETWORKS

The expressions presented in Table 1 indicate the best performance achievable considering optimal scheduling, routing, and relaying of packets in the static networks. This is a bad result as far as scalability is concerned and encourages researches to pursue techniques that increase the average throughput. One approach to increase capacity is to add relay-only nodes in the network. The major disadvantage of this scheme is that it requires a large number of pure relay nodes. For Random Networks under the Protocol Model with m additional relay nodes, the throughput available per node becomes $\Theta\left(W(n+m)/n\sqrt{(n+m)\log(n+m)}\right)$ [61]. For example, in a network with 100 senders, at least 4476 relay nodes are needed to quintuplicate the capacity [61]. Another strategy is to introduce mobility into the model. Grossglauser and Tse [66] show that it is possible for each sender-receiver pair to obtain a constant fraction of the total available bandwidth, which is independent of the number of pairs, at the expense of an increasing delay in the transmission of packets and the size of the buffers needed at the intermediate relay nodes. The same results are presented by Bansal and Liu [67], but with low delay constraints and a particular mobility model similar to the random waypoint model [68]. However, mobility introduces new problems such as maintaining connectivity within the ad hoc network, distributing routing information and establishing access control. (An analysis on the connectivity of ad hoc networks

can be found at [68].) The nodes can also be grouped into small clusters, where in each cluster a specific node (clusterhead) is designated to carry all the relaying packets [69]. This can increase the capacity and reduce the impact of the transmission overhead due to routing and MAC protocols. On the other hand, the mechanisms to update the information in clusterheads generate additional transmissions, which reduces the effective node throughput.

6. CONCLUSIONS

This paper addresses essential topics of ad hoc networks, including routing algorithms, medium access protocols, TCP/IP issues, and capacity. Although these topics are reasonably well established for fixed (wired or wireless) networks or even for mobile radio with a point to multipoint architecture, they are still object for investigation in ad hoc networks. This is due to the fact that ad hoc networks have their conditions changing constantly, such as network size, traffic distribution, connectivity between terminals, and others. In this sense, the design of routing algorithms, MAC protocols, implementation of TCP, and estimation of the capacity become challenging tasks.

Routing Algorithms. A substantial number of routing algorithms have been proposed for ad hoc networks. They are classified as proactive or table-driven, reactive or on-demand, and hybrid. The proactive protocols require the nodes to keep tables with routing information. Updates occur on a periodical basis or as soon changes in the network topology are perceived. The reactive protocols create routes on demand. This is accomplished by means of a route discovery process, which is completed once a route has been found or all possible route permutations have been examined. The hybrid protocols are both mix both features. Nodes with close proximity form a backbone within which proactive protocols are applied, whereas routes to faraway nodes are found through reactive protocols.

MAC Protocols. A suitable general-purpose MAC protocol is likely to include features as follow. In order to reduce the probability of collisions it should use multiple channels to separate control and data. Channel bandwidth flexibility and high bandwidth efficiency may be achieved by using CDMA for channel partition. Multi-hop support is recommended to ensure scalability with flat or clustered topologies, depending on the application. In order to favor power efficient terminals, protocols need to be power aware, must control transmission power, and allow for sleep mode. And finally, for the sake of flexibility, short to medium range networks and a sender-initiated approach are recommended.

TCP Issues. The use of TCP over ad hoc networks is a certainty, as a manner to integrate ad hoc networks with the Internet. However, it is well accepted that TCP suffers from poor performance when operating in a wireless environment, mainly due to the inappropriate interaction between TCP and typical protocols at the physical, link and network layers employed in wireless networks. Several schemes have been proposed in the literature to appropriately address the effects on the TCP performance of typical conditions found in a mobile radio environment, such as high packet loss rate, time-variant transmission delay and user mobility.

Capacity. Unlike point to multipoint networks, ad hoc users will be not only clients sending and receiving information to and from an access point, but will act also as routers, wasting their resources sending their own data but also other nodes information. As the network grows, the quantity of other node's information that a node has to forward will be greater, and with that the transmission throughput per node will diminish. Different studies have been presented to analyze ad hoc multi-hop network capacity bounds, but a definitive analysis of their capacity remains like an open issue. There are several techniques to improve the ad hoc network capacity, including transmission power control, directional and smart antennas, and relay-only nodes.

REFERENCES

[1] Chiang, C. –C. and Gerla, M. "Routing and Multicast in Multihop, Mobile Wireless Networks," *Proc. IEEE ICUPC '97*, San Diego, CA, Oct. 1997.

[2] Basagni, S. et al., "A Distance Routing Effect Algorithm for Mobility (DREAM)," *ACM/IEEE Int'l. Conf. Mobile Comp. Net.*, 1998, pp. 76-84.

[3] Perkins, C. E. and Bhagwat, P., "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Comp. Commun. Rev.*, Oct. 1994, pp. 234-244.

[4] Santivanez, C., Ramanathan, R., and Stavrakakis, I., "Making Link-State Routing Scale for Ad Hoc Networks," *Proc. 2001 ACM Int'l. Symp. Mobile Ad Hoc Net. Comp.*, Long Beach, CA, Oct. 2001.

[5] Iwata, A. et al., "Scalable Routing Strategies for Ad-hoc Wireless Net-works," *IEEE JSAC*, Aug. 1999, pp. 1369-179.

[6] Pei, G., Gerla, M., and Chen, T.-W., "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks," *Proc. ICC 2000*, New Orleans, LA, June 2000.

[7] Chen, T. -W., Gerla, M., "Global State Routing: a New Routing Scheme for Ad-hoc Wireless Networks," *Proceedings of the IEEE ICC*, 1998.

[8] Pei, G., Gerla, M., Hong, X., Chiang, C. "A Wireless Hierarchical Routing Protocol with Group Mobility," *Proceedings of Wireless Communications and Networking*, New Orleans, 1999.

[9] Kasera, K. K., Ramanathan, R., "A Location Management Protocol for Hierarchically Organized Multihop Mobile Wireless Networks," *Proceedings of the IEEE ICUPC'97*, San Diego, CA, October 1997, pp.158-162.

[10]Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., Viennot, L., "Optimized Link State Routing Protocol for Ad Hoc Networks," *IEEE INMIC*, Pakistan, 2001.

[11]Garcia-Luna-Aceves, J. J., Marcelo Spohn, C., "Source-tree Routing in Wireless Networks," *Proceedings of the Seventh Annual International Conference on Network Protocols*, Toronto, Canada, October 1999, p.273.

[12]Bellur, B. and Ogier, R. G., "A Reliable, Efficient Topology Broadcast Protocol for Dynamic Networks," *Proc. IEEE INFOCOM '99*, New York, NY, Mar. 1999.

[13]Ogier, R. G. et al., "Topology Broadcast based on Reverse-Path Forwarding (TBRPF)," draft-ietf-manet-tbrpf-05.txt, INTERNET-DRAFT, MANET Working Group, Mar. 2002.

[14]Murthy, S. and Garcia-Lunas-Aceves, J. J., "An Efficient Routing Protocol for Wireless Networks," *ACM Mobile Networks and App. J.*, Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-197.

[15]Toh, C., "A Novel Distributed Routing Protocol to Support Ad-hoc Mobile Computing," *IEEE 15th Annual International Phoenix Conf.*, 1996, pp.480- 486.

[16]Das, S., Perkins, C., Royer, E., "Ad Hoc on Demand Distance Vector (AODV) Routing," Internet Draft, draft-ietf-manet-aodv-11.txt, 2002.

[17]Günes, M., Sorges, U., Bouazizi, I., "ARA – The Ant-colony Based Routing Algorithm for Manets," *ICPP Workshop on Ad Hoc Networks (IWAHN 2002)*, August 2002, pp.79-85.

[18]Jiang, M., Ji, J., Tay, Y. C., "Cluster based routing protocol, Internet Draft, draft-ietf-manet-cbrp-spec-01.txt, 1999.

[19]Johnson, D., Maltz, D., Jetcheva, J., "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet Draft, draft-ietf-manet-dsr-07.txt, 2002.

[20]Su, W., Gerla, M., "IPv6 Flow Handoff in Ad-hoc Wireless Networks Using Mobility Prediction," *IEEE Global Communications Conference*, Rio de Janeiro, Brazil, December 1999, pp.271 –275.

[21]Ko, Y.-B., Vaidya, N. H., "Location-aided Routing (LAR) in Mobile Ad Hoc Networks," *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom'98)*, Dallas, TX, 1998.

[22]Corson, M. S., Ephremides, A., "A Distributed Routing Algorithm for Mobile Wireless Networks," *ACM/Baltzer Wireless Networks 1*, vol 1, 1995, pp. 61-81.

[23]Aggelou, G., Tafazolli, R., "RDMAR: A Bandwidth-efficient Routing Protocol for Mobile Ad Hoc Networks," *ACM International Workshop on Wireless Mobile Multimedia (WoWMoM)*, 1999, pp. 26-33.

[24]Raju, J., Garcia-Luna-Aceves, J., "A New Approach to On-demand Loop-free Multipath Routing," *Proceedings of the 8th Annual IEEE International Conference on Computer Communications and Networks (ICCCN)*, Boston, MA, October 1999, pp. 522-527.

[25]Dube, R., Rais, C., Wang, K., Tripathi, S., "Signal Stability Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks," *IEEE Personal Communication 4*, vol 1, 1997, pp. 36-45.

[26]Park, V. D., Corson, M.S., "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proceedings of INFOCOM*, April 1997.

[27]Nikaein, N., Laboid, H., Bonnet, C., "Distributed Dynamic Routing Algorithm (DDR) for Mobile Ad Hoc Networks," *Proceedings of the MobiHOC 2000:First Annual Workshop on Mobile Ad Hoc Networking and Computing*, 2000.

[28]Radhakrishnan, S., Rao, N. S. V., Racherla, G., Sekharan, C.N., Batsell, S.G., "DST – A Routing Protocol for Ad Hoc Networks Using Distributed Spanning Trees," *IEEE Wireless Communications and Networking Conference*, New Orleans,1999.

[29]Woo, S.-C., Singh, S., "Scalable Routing Protocol for Ad Hoc Networks," *Wireless Networks 7*, vol 5, 2001, 513-529

[30]Joa-Ng, M., Lu, I.-T., "A Peer-to-peer Zone-based Two-level Link State Routing for Mobile Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications 17* vol 8, 1999, pp. 1415 –1425.

[31]Haas, Z. J., Pearlman, R. "Zone Routing Protocol for Ad-hoc Networks," Internet Draft, draft-ietf-manet-zrp-02.txt,1999.

[32]Chandra, A., Gummalla, V., Limb, J.O., "Wireless Medium Access Control Protocols," *IEEE Communications Surveys and Tutorials* [online], available at: http://www.comsoc.org/pubs/surveys/, vol. 3, no. 2, 2000.

[33]Jurdak, R., Lopes, C.V., Baldi, P., "A Survey, Classification and Comparative Analysis of Medium Access Control Protocols for Ad Hoc Networks," *IEEE Communications Surveys and Tutorials* [online], available at: http://www.comsoc.org/pubs/surveys/, vol. 6, no. 1, 2004.

[34]Tseng, Y.C., Hsieh, T.Y., "Fully power-aware and location-aware protocols for wireless multi-hop ad hoc networks," *11th. International Conference on Computer Communications and Networks*, 14-16 Oct. 2002, pp. 608-613.

[35]IEEE 802.11 WG, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE/ANSI Std. 802-11, 1999 edn.

[36]IEEE 802.11 WG, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: high-speed physical layer in the 5 GHz band," IEEE Std. 802-11a.

[37]IEEE 802.11 WG, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: higher-speed physical layer extension in the 2.4 GHz band," IEEE Std. 802-11b.

[38]Bluetooth SIG, "Specification of the Bluetooth System," v. 1.0, 1999, available at: http://www.bluetooth.org.

[39]IEEE 802.11 WG, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS)," IEEE Draft Std. 802.11e/D5.0, Aug. 2003.

[40]Goodman, D.J., Valenzuela, R.A., Gayliard, K.T., Ramamurthi, B., "Packet reservation multiple access for local wireless communications," *IEEE Transactions on Communications*, vol. 37, no. 8, Aug. 1989, pp. 885-890.

[41]Jiang, S., Rao, J., He, D., Ling, X., Ko, C.C., "A simple distributed PRMA for MANETs," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 2, March 2002, pp. 293-305.

[42]Talucci, F., Gerla, M., Fratta, L., "MACA-BI (MACA By Invitation)-a receiver oriented access protocol for wireless multihop networks," *8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC'97*, vol. 2, 1-4 Sept. 1997, pp. 435-439.

[43]Garcia-Luna-Aceves, J.J., Tzamaloukas, A., "Reversing the Collision-Avoidance Handhske in Wireless Networks," *ACM/IEEE MobiCom'99*, 15-20 August 1999.

[44]Haas, Z. J., Deng, J., "Dual busy tone multiple access (DBTMA) - a multiple access control scheme for ad hoc networks," *IEEE Transactions on Communications*, vol. 50, no. 6, June 2002, pp. 975-985.

[45]Fitzek, F.H.P., Angelini, D., Mazzini, G., Zorzi, M., "Design and performance of an enhanced IEEE 802.11 MAC protocol for multihop coverage extension," *IEEE Wireless Communications*, vol. 10, no. 6, Dec. 2003, pp. 30-39.

[46]Chao, C.M., Sheu, J.P., Chou, I-C., "A load awareness medium access control protocol for wireless ad hoc network," *IEEE International Conference on Communications*, ICC'03, vol. 1, 11-15 May 2003, pp. 438-442.

[47]Muqattash, A., Krunz, M., "Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks," *22nd. Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2003*, vol. 1, 30 March-3 April 2003, pp. 470-480.

[48]Fang, J.C., Kondylis, G.D., "A synchronous, reservation based medium access control protocol for multihop wireless networks," *IEEE Wireless Communications and Networking, WCNC 2003*, vol. 2, 16-20 March 2003, pp. 994-998.

[49]Postel, J., "Transmission Control Protocol," IETF RFC 793, September 1981.

[50]Huston, G., "TCP in a Wireless World," *IEEE Internet Computing*, pp. 82-84, March-April, 2001.

[51]Chandran, K., Raghunathan, S., Venkatesan, S., Prakash, R., "A Feedback-Based Scheme for Improving TCP Performance in Ad Hoc Wireless Networks," *IEEE Personal Communications*, pp. 34 – 39, February 2001.

[52]Xylomenos, G., Polyzos, G. C., Mahonen, P., Saaranen, M., "TCP Performance Issues over Wireless Links," *IEEE Communications Magazine*, Vol. 39, No. 4, pp. 53-58, April 2001.

[53]Balakrishman, H., Padmanabhan, V. N., Seshan, S., Katz, R.H.A, "A Comparison of Mechanisms for Improving TCP

Performance over Wireless Links," *IEEE/ACM Trans. on Networking*, vol. 5, No. 6, pp. 756-769, December 1997.
[54]Shakkottai, S., Rappaport, T. S., Karlsson, P. C, "Cross-Layer Design for Wireless Networks," *IEEE Communications Magazine*, pp.74-80, October 2003.
[55]Xu, S., Saadawi, T., "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?" *IEEE Communications Magazine*, pp. 130-137, June 2001.
[56]Fu, Z., Zerfos, P., Luo, H., Lu, S., Zhang, L., Gerla, M., "The Impact of Multihop Wireless Channel on TCP Throughput and Loss", *IEEE INFOCOM*, 2003, pp. 1744-1753.
[57]Tang, K., Gerla, M., Correa, M., "Effects of Ad Hoc MAC Layer Medium Access Mechanisms under TCP," *Mobile Networks and Applications*, Kluwer Academic Publishers, vol. 6, pp. 317-329, 2001.
[58]Holland, G., Vaidya, N., "Analysis of TCP Performance over Mobile Ad Hoc Networks," *Wireless Networks*, Kluwer Academic Publishers, Vol. 8, pp. 275-288, 2002.
[59]Floyd, S., TCP and "Explicit Congestion Notification," *ACM Computer Communication Review*, vol. 24, pp. 10-23, October 1994.
[60]Shannon, C. E., "A mathematical theory of communication", *Bell System Technical Journal*, vol 79, July 1948, pp. 379-423.
[61]Gupta, P. and Kumar, P.R., "The Capacity of Wireless Networks", *IEEE Trans. Info. Theory*, vol 46, March 2000.
[62]Toumpis, S. and Goldsmith, A., "Ad Hoc Network Capacity", *Conference Record of Thirty-fourth Asilomar Conference on Signals Systems and Computers*, vol 2, 2000, pp. 1265-1269.
[63]Li, J., Blake, C., De Couto, D. S. J., Lee, H. I., and Morris, R., "Capacity of Ad Hoc Wireless Networks", *Proc. 7th ACM Int'l Conf. Mobile Comp. and Net.*, July 2001, pp.61-69.
[64]Jun, J. and Sichitiu, M. L., "The Nominal Capacity of Wireless Mesh Networks", *IEEE Wireless Communications*, October 2003.
[65]Jun, J., Peddabachagari, P., and Sichitiu, M. L., "Theoretical Maximum Throughput of IEEE 802.11 and its Applications", *Proc. 2nd IEEE Int'l Symp. Net. Comp. and Applications*, April 2003, pp.212-25.
[66]Grossglauser, M. and Tse, D., "Mobility Increases the Capacity of Ad Hoc Wireless Networks", *Proc. IEE Infocom'01*, April 2001.
[67]Bansal, N. and Liu, Z. "Capacity, Delay and Mobility in Wireless Ad-Hoc Networks", *Proc. IEE Infocom'03*, April 2003.
[68]Bettstetter, C., "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network", *Proc. ACM Intern. Symp. On Mobile Ad Hoc Networking and Computing (MobiHoc)*, June 2002.
[69]Lin, C. R. and Gerla, M., "Adaptative Clustering for Mobile Wireless Networks," *IEEE Journal on Selected Ares in Communications*, vol 15, pp. 1265-1275, September 1997.

Michel Daoud Yacoub was born in Brazil in 1955. He received the B.S.E.E. and the M.Sc. degrees from the School of Electrical and Computer Engineering of the State University of Campinas, UNICAMP, Brazil, respectively in 1978 and 1983, and the Ph.D. degree from the University of Essex, England, in 1988. From 1978 to 1985, he worked as a research specialist at the R&D Center of Telebrás, Brazil, in the development of the Tropico digital exchange family. He joined the School of Electrical and Computer Engineering, UNICAMP, in 1989, where he is presently a full professor. He consults for several operating companies and industries in the wireless communications area. He is the author of the books Foundations of Mobile Radio Engineering, CRC Press, 1993, Wireless Technology: Protocols, Standards, and Techniques, CRC Press, 2001, and the co-author of the book Telecommunications: Principles and Trends (in Portuguese), Erica Press. He holds two patents. His research interests include wireless communications in general.

Paulo Cardieri received his M.Sc. degree from the State University of Campinas - UNICAMP, Campinas – SP, Brazil, and his Ph.D. degree from Virginia Polytechnic Institute and State University, USA, both in electrical engineering. He is currently an assistant professor at the School of Electrical and Computer Engineering of UNICAMP. Prior to joining the faculty of UNICAMP, he was with the CPqD Foundation, Campinas, Brazil, where he was involved with research projects in several areas, including satellite and wireless communications. From November 1991 to August 1992 he was a visiting researcher at the Centro Studi e Laboratori Telecomunicazioni, Turin, Italy.

Élvio João Leonardo received the B.Eng. and M.Eng. degrees from the State University of Campinas, UNICAMP, Brazil, in 1984 and 1992, respectively. From 1984 to 1992 he worked at the Centro de Pesquisa e Desenvolvimento (CPqD) in Brazil with research and development of communication systems. In 1992 he moved to Australia where he spent some time as a Research Assistant at the Sydney University before joining Motorola in 1995. In both places he worked with research and development of wireless communications systems. He left Motorola to take the position of Assistant Professor at the State University of Londrina, Brazil, in 2002. His main interests include fading communication channels, mobile communications and embedded systems.

Álvaro Augusto Machado de Medeiros received his B. Eng. degree from the Federal University of Rio Grande do Norte, UFRN, Brazil in 2000. He received his M.Sc. degree from the State University of Campinas, UNICAMP, Brazil, in 2002. He is presently working towards his Ph.D. degree at UNICAMP, Brazil. He is currently working in studies on ad hoc network capacity and planning. His research interests include wireless communications and mobile networks.

David Muñoz Gallego received his degree in electronic engineering from the Javeriana University, Bogota D.C, Colombia in 2003. He is presently working towards the M.Sc. degree in electrical engineering at State University of Campinas, UNICAMP, Brazil. He is currently working in studies on ad hoc network capacity. His research interests are in the area of wireless and mobile communications.