Recent developments in wireless communications have made it possible to provide multimedia services for mobile users through wireless devices. Multimedia applications over wireless links require that the underlying wireless network supports the Quality of Service concept.

**Abstract**

Wireless networks come in force into the market of computer communications. Unfortunately, several standards coexist (e.g., IEEE 802.11, Bluetooth, HomeRF, HIPERLAN), leading to various types of products. The purpose of this article is to present an overview of those standards and to establish a comparative evaluation. We mainly focus on the medium access control protocols and their ability to support the quality of service required by multimedia applications. Those protocols generally support two modes of operation, a random access mode for asynchronous traffic and a polling mode for real-time synchronous traffic. This article analyzes each protocol’s ability to support user QoS requirements.

**Introduction**

Recent developments in wireless communications have made it possible to provide multimedia services for mobile users through wireless devices. Multimedia applications over wireless links require that the underlying wireless network support quality of service (QoS). Current wireless standards such as IEEE 802.11, Bluetooth, HomeRF, and HIPERLAN 1 and 2 try to support multimedia services in the most appropriate way.

This article is organized as follows. Before describing these five wireless protocols, we establish several comparative criteria in the next section. We consider the traffic submitted by an application to a wireless network and express how the application’s requirements are taken into account by the wireless network. Different traffic classes can be distinguished (e.g., audio/video streaming, bulk transfer, Web traffic); each class is defined by specific features (e.g. bandwidth, transmission delay, and bounded jitter). Each class of traffic requires a certain level of QoS affecting the quality of transmission perceived by the user. The QoS can be examined from two perspectives: user and network. From the user perspective, QoS requirements are based on user perception of the level of service delivered. User QoS must be translated into network QoS according to a mapping function. The network’s role is to ensure that the desired QoS is met by means of management and control functions. In the third section we describe the medium access control (MAC) protocols for the five wireless standards, focusing on mechanisms that support QoS requirements according to the user point of view. We describe how user-level QoS requirements can be mapped to the low-level network. In the fourth section, a table summarizes these protocols according to the criteria given in the second section. We then study the adequacy of these five wireless standards with respect to different application constraints. Finally, we discuss some open issues for future work.

**Comparative Criteria**

We now focus on any application running on a wireless network. This application has constraints with respect to the network supporting it. We can distinguish three types of constraints: global, MAC-related, and traffic-related.

The first constraints are global, which are based on general technical considerations related to wireless networks. They essentially concern the deployment of such a network and its ability to be interconnected. Among the global constraints are:

**Nomadity of devices:** Some or all devices can change their location and want to keep the same virtual environment (e.g., services offered to the user); the mapping of the virtual environment to the real one depends on the physical location of the device. Such a device must be connected regardless of location.

**Mobility of devices:** Some or all devices can move while they are communicating. Service continuity must be provided.

**Power management:** Battery-operated devices must be able to save power when they are inactive. This constraint has a strong impact on protocol design.

**Number of interconnected devices:** This defines the maximum number of devices that...
can be managed in the same area under the control of a central station (if used).

Global throughput: This characterizes the maximum throughput supported by a wireless network

Frequency band: This is the range of radio frequencies used for transmission and reception, generally restricted by a country's regulations

Confidentiality: A minimum requirement is given by Wired Equivalent Privacy (WEP), where a wired LAN equivalent data confidentiality is provided to users of wireless networks.

Easy installation and maintenance

Cost effectiveness: Networking cost must be low for three reasons: first, low-cost devices; second, a high number of interconnected devices; third, the application lifetime is short.

Ability to interconnect with other networks (wired or not)

Wireless transmission provides undeniable advantages for a communication network. However, such a physical medium introduces some unique problems. A wireless MAC protocol needs to support some specific mechanisms in order to solve these problems. These include:

The need for a wired infrastructure topology: Wireless LANs (WLANs) can be built with or without an infrastructure, leading to either an infrastructure or ad hoc topology (Fig. 1). In an infrastructure topology, there is a specific device called an access point (AP). An AP not only controls the communication of devices within its radio range, but also provides access to a wired network.

Centralized/decentralized medium access: In a centralized medium access topology (Fig. 2), a central entity controls the medium among the devices in its radio range (e.g., by means of a polling scheme). In this case, it ensures that all transmissions between devices under its control are contention-free. Generally, this access type is used for synchronous traffic. Moreover, with this access type, it is easier to implement the power saving mode, since the polling scheme can account for the sleeping period of battery-operated devices. In a decentralized medium access, each device is independent and competes for medium access. Random access schemes are generally used. In a wireless environment, a device cannot detect a collision while transmitting; the transmitting power is much greater than the receiving power. This is why a collision avoidance scheme is used. Examples include carrier sense multiple access with collision avoidance (CSMA/CA) and elimination yield-non-preemptive priority multiple access (EYNPMA). An infrastructure topology may use decentralized medium access, where the control entity is the AP. An ad hoc infrastructure generally uses a decentralized medium access; however, it can also use a centralized one, where a central entity is elected.

Centralized communication: If the medium access scheme needs a centralized communication, all traffic must be transmitted through a central entity. Each transmission is performed twice: from (or toward) the central entity in downlink direction (or uplink direction).

Communication with out-of-range devices: Since radio coverage is limited, routing solutions may need to be implemented in a WLAN. In an infrastructure topology, the wired network performs routing between devices using different APs. In an ad hoc topology, routing can be done in the WLAN itself without resorting to a wired network.

The hidden node problem: This problem (Fig. 3) occurs when two devices, A and B, that cannot hear each other transmit simultaneously to a third device, C, hearing both A and B. This generic problem in radio transmission induces loss of efficiency in terms of delay and bandwidth.

All these constraints have a major impact on MAC protocol design.

An application generates different types of traffic on the network and expresses constraints with regard to this traffic. Among these constraints, we can cite:

Coexistence of different types of traffic: An application can be characterized from a network point of view as a set of weighted elementary traffic. The weight and services offered to each traffic type depends on the application.

Dynamics of the traffic distribution: A wireless environment is subject to frequent changes. Consequently, the way the traffic is distributed over the devices changes in space and time: for
instance, devices previously in communication can become inactive. In such versatile environments, the latency to adapt to a time or space variation of the traffic distribution is an important parameter to consider.

The traffic produced by an application can be decomposed into elementary traffic types. Each elementary traffic type can be characterized by technical parameters determining system performance. They are:

- Throughput
- Message size
- User-level priority
- Time constraints: can be expressed by the maximum end-to-end delay, maximum tolerated jitter, or maximum time to establish or release a connection
- Dependability: defines the network’s behavior when communication fails (message or connection loss, device failure, etc.)
- Type of communication: unicast, multicast, broadcast
- Message arrival law: periodic (with constant interarrival time), sporadic (with interarrival time greater than or equal to the minimum interarrival time), aperiodic (with only one arrival), bursty (with the duration and period of the burst), and so on

**Wireless Standards and Protocols**

We now introduce five wireless standards that are studied according to some constraints presented in the previous section. For global constraints, we focus on the topology used. For MAC-related constraints, the wireless standards are presented according to services provided for data transmission. In order to support traffic-related constraints, each wireless standard has to support the mapping functions of QoS requirements and mechanisms to support these QoS requirements.

**IEEE 802.11**

The IEEE 802.11 [1] protocol defines an ad hoc network architecture for devices within mutual communication range. When communicating devices belong to different coverage areas, distribution services are needed to communicate through a wired network. APs are used for bridging with wired networks and forming a WLAN.

IEEE 802.11 MAC can provide users two service types for data transmission: asynchronous transmission within a contention period, as provided by the distributed coordination function (DCF), and synchronous transmission within a contention-free period (CFP) as provided by the point coordination function (PCF). Integration of the two access methods is achieved using a superframe (Fig. 4), which includes two successive periods: a contention-free period and a contention one. In the situation illustrated in Fig. 4, the medium is busy when a new CFP starts. This period is therefore foreshortened.

For both services, the MAC protocol supports mechanisms such as the acknowledgment of unicast transmission and the handshaking control frames to reduce the hidden node problem. This mechanism, called virtual sensing, is based on the exchange of short control frames: a Request To Send (RTS) frame sent by a potential transmitter to the receiver and a Clear To Send (CTS) frame sent from the intended receiver in response to the received RTS frame. Any other node having received either this RTS or CTS frame delays its transmission. The effectiveness of the RTS/CTS mechanism depends on the length of the packet to be protected [2]. An RTS_threshold fixed by the user could be applied to disable the mechanism for shortest frames.

Moreover, different interframe spaces (IFS) have been introduced (Fig. 5): shortest for control frames such as acknowledgment and RTS/CTS frames, medium for synchronous traffic, and longest for asynchronous traffic. These IFS of different duration are a way to implement prioritized accesses. Lower-priority packets can be delayed with larger IFS [3].

The DCF implements the basic access method CSMA/CA. Collisions are avoided by means of a random backoff counter. The backoff period is bounded by two configurable parameters: the lower bound is Short Retry Limit (SRL) and the upper bound is Long Retry Limit (LRL), which control the latency and reliability of pending messages [4]. Moreover, the size of the backoff period and its offset can be made shorter to implement priority between different traffic types.
Higher-priority packets will use a smaller backoff period, and the offset can be calculated such that there is no overlap in contention periods.

The PCF, which implements a polling access method, is available only in an infrastructured topology where an AP is used. The PCF relies on the service provided by the DCF, because devices requesting for synchronous communication have to use DCF rules to notify the AP. The AP periodically polls devices, giving them the opportunity to transmit. The maximum duration of CFP (CFP_Max_Duration) and its repetition rate (CFP_Rate), defined as a number of superframes, should be determined according to the characteristics of traffic that has to be conveyed by the AP. Other polling-based MAC mechanisms, more efficient than round-robin, can be implemented to support real-time communications (see, e.g., [5]). Proposals for a QoS enhanced PCF have been presented as part of the 802.11e Working Group.

### Bluetooth

Bluetooth devices [6] use fast frequency hopping for data transmissions. Any two Bluetooth devices within range of each other can set up an ad hoc connection, establishing a small network called a piconet. Each piconet consists of a unique master that selects a frequency hopping sequence for the piconet and controls the access to the medium. Other participants of the piconet, called slave units, are synchronized to the hopping sequence of the piconet master. Up to seven active slave units may form a piconet. Multiple overlapping piconets can coexist because each piconet uses a different hopping sequence. Piconets can be interconnected via bridges to form a bigger network called a scatternet. Therefore, to support forwarding data between devices from different piconets, a routing mechanism must be implemented at upper layers [7]. To deal with the hidden node problem, Bluetooth devices use fast frequency hopping.

To communicate, Bluetooth MAC implements a time-division duplex (TDD) scheme, splitting the channel into slots alternately used for transmission and reception between the piconet master and its slaves (Fig. 6). The slots for any master-to-slave communication are immediately followed by slots for slave-to-master communication. A slave is only allowed to transmit in a given slot if the master has polled it in a preceding slot. Moreover, any direct communication between slaves is impossible. The piconet master has to manage a polling scheme between slaves using a round-robin scheme or a more efficient scheme based on delay and throughput, as studied in [8].

Two types of service for data communications are provided to the users: asynchronous, called asynchronous connectionless (ACL), and synchronous, named synchronous connection-oriented (SCO). ACL service is used for the transmission of data bursts. The master entirely manages the ACL connection bandwidth: a master polls a slave, which may answer during following slot(s). The master defines the maximum packet length granted to the slave; this length is based on criteria such as the quantity of data to be transmitted or the number of successive slots available in the presence of SCO traffic. A maximum poll interval can be negotiated as the maximum time between subsequent transmissions between the master and a particular slave. It is used to support bandwidth allocation and latency control. The SCO service supports time-constrained point-to-point connections. The length of an SCO packet cannot exceed one time slot. This service allows the negotiation of repetition rate and latency.

Best-effort QoS is generally applied to communications. A user can request a QoS guarantee for traffic defined by its flow spec parameters such as token rate and peak bandwidth. All these options have to be negotiated during connection establishment.

### HomeRF

Based on the Shared Wireless Access Protocol (SWAP) 1.0 [9], HomeRF architecture is a combination of a managed network for synchronous and centralized services and an ad hoc network that provides asynchronous service. A unique AP, generally a gateway to a wired network, manages centralized services, and synchronizes and controls communications on the medium according to MAC rules. In a certain way, a unique AP prevents the hidden node problem. If the AP is not available, the devices may create an ad hoc network where the control of the network is distributed between all the devices.

For communication services, a user may choose between two services types: synchronous and asynchronous. The SWAP MAC includes a time-division multiple access (TDMA) scheme to support synchronous traffic, as well as a CSMA/CA scheme derived from DCF in IEEE 802.11. This last scheme supports asynchronous traffic and control frames (e.g., request for synchronous traffic).

The MAC protocol uses a superframe incorporating two CFPs and one contention period (Fig. 7). The access mechanism used during each CFP is TDMA, while CSMA/CA is used during the contention period. The next version of HomeRF will implement a priority asynchronous data service in which selected data packets gain...
priority access to the channel by means of an offset on the contention period.

Each CFP is divided into six pairs of fixed-length slots. The first slot of each pair is used to transmit data from the AP to a device. Respectively, the second one is used for communications from a device to the AP. The second CFP, at the end of the superframe, is used for data transmission, while the first CFP at the start of the superframe is used for optional retransmission of any data not received or incorrectly received in the previous frame. To adapt the bandwidth to its requirements, a user can set the repetition rate of its allowed slots under the CFP mechanism.

**HIPERLAN/1**

The HIPERLAN/1 standard [10] works independent of any fixed infrastructure as an ad hoc network but allows access to conventional wired networks. HIPERLAN/1 supports the ad hoc topology with a multihop routing capability at the MAC layer. With this capacity, packets are forwarded from a source to a destination that cannot be reached directly. This routing protocol [11] is proactive: it maintains a route for each destination in the wireless network. It belongs to the link state family, in which the broadcast of topology information has been optimized. The multipoint relay set, a subset of one-hop neighbors of the transmitter, allows connection to all two-hop devices of the WLAN. This set has been introduced for that purpose: only the multipoint relays of the transmitter forward the packet, making this routing protocol efficient (Fig. 8).

The access scheme used in HIPERLAN/1 is called EY-NPMA, a specific implementation of the traditional CSMA with active signaling. This mechanism is a way to deal with the hidden node problem. With active signaling, a signal burst is sent by contending nodes before data transmission, and the usual carrier sensing is employed during idle time. The performance analysis given in [12] shows that active signaling has better performance than CSMA/CA with regard to the hidden node problem and unfairness in the medium access.

The MAC layer of HIPERLAN/1 uses a form of priority in granting access to the medium. Basically, when the channel is assessed to be clear, packets ready for transmission are submitted to a prioritization phase during which the packets with the highest priority are selected (Fig. 9). Packets with the same access priority are submitted to a collision avoidance phase. Each remaining device transmits a signal, the length of which is chosen in a random fashion. The device that broadcasts the longest signal gains control of the channel. Acknowledgment of unicast transmission is done after data transmission.

The two criteria used to establish the priority level of a packet are the user-level priority (as described in the traffic constraints discussion earlier) and residual packet lifetime (normalized to the number of hops to reach the final destination) deduced from the packet deadline given by the user. The mapping function of the user-level priority and normalized residual lifetime into the medium access priority is given in [8]. So HIPERLAN/1 offers prioritized access to fulfill traffic requirements for delay-sensitive applications.

**HIPERLAN/2**

The HiPERLAN/2 standard [13] is mainly defined for infrastructure-based topology where an AP manages the wireless network. The AP controls in-range devices with connection-oriented links. This centralized topology is combined with an ad hoc capability: unlike some centralized protocols where two devices attached to the same AP cannot communicate directly, HIPERLAN/2 has an option allowing a direct communication between such in-range devices.

Several logical links can be established between devices and a priority, mapped from the user-level...
priority, is attached to each link. This priority can be translated into traffic classes according to IEEE 802.1p [14]. When a device wants to transmit data, it must first send a resource request to the AP in random access slots, which grants resources in the next frames according to the traffic, other requests, and its own transmission buffers. A request contains the number of packets to be sent, transmission frequency, and link quality requested. These parameters are determined according to the application’s needs. The hidden node problem is solved by means of a centralized communication. Indeed, all communications are managed by the AP with a contention-free mechanism, even in direct communication between two devices.

The MAC protocol in the HIPERLAN/2 standard is based on TDMA. The basic frame structure has a fixed duration and incorporates several communications slots: one for broadcast and frame control, one for retransmission, two for data transmission (downlink and uplink directions), possibly one for direct mode transmission, and the last one for random access (Fig. 10). The AP can adapt the frame composition to traffic variation and adjust access delay. The scheduling policy, performed at the MAC level of the AP, is not specified. To support QoS requirements, additional mechanisms such as admission control and congestion control have to be implemented.

The connection-oriented nature of HIPERLAN/2 makes it straightforward to implement support for QoS. To adapt the quality and reliability of the link as a function of the environment, HIPERLAN/2 provides a set of internal functionalities such as dynamic frequency and data rate selection, and link adaptation. Depending on the performance and the reliability requested for transmission, the user can choose for each connection whether to use these previous mechanisms.

**ADEQUACY BETWEEN STUDIED WIRELESS PROTOCOLS AND APPLICATION CONSTRAINTS**

**RECAPITULATIVE TABLE**

Table 1 shows how the studied wireless standards account for the previous application constraints: global, MAC-related, and traffic-related.

**ADEQUACY ANALYSIS**

We summarize the main results described in Table 1.

If the application is such that all communicating devices are in range, any studied standard is possible. However, if the communication is not central-
enabling the message with the highest priority to be transmitted. The coexistence of both access schemes is made possible by the following rule: synchronous traffic is served first, whereas asynchronous traffic is served only if there is enough bandwidth left over by synchronous traffic. This rule is acceptable by an application only if this application has no real-time constraint attached to asynchronous traffic. Indeed, this traffic can suffer long queuing delays, increasing the jitter and end-to-end transmission delay.

Synchronous traffic can easily be differentiated from asynchronous traffic in almost all standards. Except for HIPERLAN/1 and 2, no mechanism

<table>
<thead>
<tr>
<th>Global constraints</th>
<th>IEEE 802.11</th>
<th>HomeRF</th>
<th>Bluetooth</th>
<th>HIPERLAN1</th>
<th>HIPERLAN2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nomadicty</td>
<td>Partially achieved by the AP</td>
<td>Only within the AP coverage</td>
<td>Partially achieved by the AP</td>
<td>Achieved by the MAC routing protocol</td>
<td>Partially achieved by the AP</td>
</tr>
<tr>
<td>Mobility</td>
<td>Yes, if managed by upper layers</td>
<td>No</td>
<td>Master mobility affects piconet configuration Must be managed by upper layer</td>
<td>Yes (for slow, medium speed)</td>
<td>Yes, if roaming by the fixed LAN</td>
</tr>
<tr>
<td>Power management</td>
<td>With awake patterns and AP buffers messages during sleeping period</td>
<td>With awake patterns and AP buffers messages during sleeping period</td>
<td>With awake patterns</td>
<td>With awake patterns and buffering devices</td>
<td>With awake patterns and AP buffers messages during sleeping period</td>
</tr>
<tr>
<td>Number of interconnected devices</td>
<td>127</td>
<td>127</td>
<td>7 slaves per master</td>
<td>(--)</td>
<td>256</td>
</tr>
<tr>
<td>Global throughput</td>
<td>1, 2 Mb/s for 802.11 11 Mb/s for 802.11b 54 Mb/s for 802.11g 54 Mb/s for 802.11a</td>
<td>1.6 Mb/s</td>
<td>1 Mb/s</td>
<td>23.5 Mb/s</td>
<td>54 Mb/s</td>
</tr>
<tr>
<td>Frequency band</td>
<td>5 GHz for 802.11a 2.4 GHz for the others</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>5 GHz</td>
<td>5 GHz</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Authentication + WEP</td>
<td>Authentication + encryption</td>
<td>Key sharing + encryption</td>
<td>Encryption</td>
<td>Key sharing + encryption</td>
</tr>
<tr>
<td>Easy installation</td>
<td>Immediate for ad hoc</td>
<td>Immediate for ad hoc</td>
<td>Yes</td>
<td>Immediate for ad hoc</td>
<td>Immediate for ad hoc</td>
</tr>
<tr>
<td>Easy maintenance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cost effectiveness</td>
<td>Medium $150</td>
<td>Low-medium $10 to $100</td>
<td>Low $5 to $50</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Ability to interconnect with other networks</td>
<td>With bridge for IEEE802 LAN, with router otherwise</td>
<td>With bridge for IEEE802 LAN, with router otherwise</td>
<td>With PPP protocols or with bridge for IEEE802 LAN</td>
<td>With bridge for IEEE802 LAN, with router otherwise</td>
<td>With internal functionalities to support packet- and cell-based traffic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC constraints</th>
<th>IEEE 802.11</th>
<th>HomeRF</th>
<th>Bluetooth</th>
<th>HIPERLAN1</th>
<th>HIPERLAN2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless topology</td>
<td>Ad hoc or infrastructure</td>
<td>Ad hoc or infrastructure</td>
<td>Infrastructure</td>
<td>Ad hoc</td>
<td>Ad hoc or infrastructure</td>
</tr>
<tr>
<td>Medium access type for infrastructure topology</td>
<td>Decentralized for asynchronous traffic Centralized otherwise</td>
<td>Decentralized for asynchronous traffic Centralized otherwise</td>
<td>Centralized</td>
<td>Decentralized</td>
<td>Centralized</td>
</tr>
<tr>
<td>Medium access type for ad hoc topology</td>
<td>Decentralized for asynchronous traffic only</td>
<td>Decentralized for asynchronous traffic only</td>
<td>Centralized</td>
<td>Decentralized</td>
<td>Centralized with election of an AP for the control of the medium</td>
</tr>
<tr>
<td>Centralized communication</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No if optional direct communication</td>
</tr>
<tr>
<td>Communication with out-of-range devices</td>
<td>Yes if upper layer routing is employed</td>
<td>Yes if upper layer routing is employed</td>
<td>Yes if upper layer routing is employed</td>
<td>Yes</td>
<td>Yes if upper layer routing is employed</td>
</tr>
<tr>
<td>Solution for hidden node problem</td>
<td>RTS and CTS frames</td>
<td>Only one AP used</td>
<td>Frequency hopping</td>
<td>Active signaling</td>
<td>Each neighbor uses a different channel frequency</td>
</tr>
</tbody>
</table>

Continued on next page
supports differentiation among asynchronous traffic. However, this differentiation is generally requested by multimedia applications. Additional mechanisms have to be implemented to support differentiation between asynchronous traffic.

HIPERLAN/2 and IEEE 802.11a are based on similar technology, operating in the 5 GHz band. HIPERLAN/2 has technical advantages, such as the inclusion of QoS mechanisms that allow it to handle voice and streaming media, and technology to prevent interference with other 5 GHz radio equipment; however, 802.11a arrived first on the U.S. market.

**OPEN ISSUES**

At the end of this study, we can point out some open issues. We can distinguish three major technical issues related to the MAC access scheme, routing and mobility, and the end-to-end QoS in multihop wireless networks:

**The MAC access scheme and QoS requirements in a one-hop network:**

- **Hidden node.** How can we find an efficient solution to this problem, inherent to wireless networks?

- **Mapping of user priority and real-time constraints.** The real-time constraints can be attached to synchronous and asynchronous traffic. In all studied standards but HIPERLAN/1, asynchronous traffic is transmitted only if synchronous traffic has left enough bandwidth. How can it be improved? How can we differentiate asynchronous traffic with different real-time constraints?

**Expression of real-time guarantees.** In all studied standards but HIPERLAN/1, we notice no real-time guarantees on delay and jitter for asynchronous traffic. How can we express bounded delays for such traffic? On the other hand, delay and bounded jitter are guaranteed only for already established synchronous traffic. Indeed, for submitting new synchronous traffic, an admission request, treated as asynchronous traffic, is used. How can we decrease the latency to establish new synchronous traffic?

**Routing and mobility in multihop wireless networks:**

- **Efficiency of routing done at the MAC level vs. at the IP level:** Implementing routing at layer 2 spares processing time in layer 3. However, it supposes that routing algorithms are implemented in the network controller firmware. This is a more expensive solution than a layer 3 solution, generally implemented in software.

- **QoS routing in multihop wireless networks.** This is needed in order to ensure end-to-end QoS in such networks. QoS routing must select a route that offers the features (e.g., bandwidth, delay) required by the requested QoS.

- **Mobility in multihop wireless networks.** How can we guarantee that the QoS is ensured while...
In a hierarchical approach, more intelligence is put in the AP, less complexity in the other devices. As the number of APs is small with regard to the number of other devices, such an approach makes it possible to reduce the networking cost of the application.

the device is moving? Mobility and real-time constraints are difficult to reconcile.

End-to-end QoS in multihop wireless networks and traffic differentiation: How do we account for the distance a message has to cross to reach the final destination? Can it be mapped into a medium access priority? How do we extend QoS properties obtained locally to a multihop network? How can we keep determinism when an AP to a wired network is used? Furthermore, asynchronous traffic with real-time constraints or different priorities cannot be differentiated. How should we implement differentiation mechanisms in a current standard without drastic modification of the protocol stack?

From a more general point of view, two additional issues can be highlighted. They concern the design approaches in wireless networks and the compatibility of existing solutions:

Design approaches in wireless networks: In a hierarchical approach, more intelligence is put in the AP, less complexity in the other devices. Since the number of APs is small with regard to the number of other devices, such an approach makes it possible to reduce the networking cost of the application.

In a fully decentralized approach, all devices have the same intelligence. In order to reduce the amount of control traffic, they can elect a device among them to achieve particular centralized functions.

Compatibility of different solutions: A problem to be discussed concerns the compatibility of different products. It can be discussed at two levels:

• Coexistence and interference of different wireless networks in the same environment

• Interconnection of different heterogeneous networks

CONCLUSION AND PERSPECTIVES

Wireless networks are now easy to deploy, and the available bandwidth becomes acceptable for most applications. Moreover, with wireless networks, mobility has become a reality. At the same time, the need for wireless products is increasing, based on different wireless protocols. Standardization is evolving quickly (e.g., HomeRF v.2.0, Bluetooth as discussed in the IEEE 802.15 Personal Area Network Working Group, IEEE 802.11a). This article provides a comparison of these wireless protocols. We have focused on the first two layers of wireless standards: IEEE 802.11, HomeRF, Bluetooth, and HIPERLAN/1 and 2.

An important open issue deals with the coexistence of different traffic types. For instance, all studied protocols except HIPERLAN/1 favor synchronous traffic over asynchronous traffic, which is transmitted only if there is sufficient bandwidth left over by synchronous traffic. In order to support multimedia applications, service differentiation and traffic classes have to be provided by the underlying wireless network. To achieve that, priority-based medium access and efficient management of the waiting queues are needed. Some other technical issues require further study, concerning routing and mobility in multihop wireless networks. Furthermore, the design approaches in wireless networks and the compatibility of different existing solutions are still open issues.

REFERENCES


BIOGRAPHIES

ANTOINE MERCIER (mercier@ece.fr) graduated as an engineer of ENSEA in 2000 from the Computer and Telecommunication Sciences School, France. He is preparing a Ph.D. of sciences on quality of service in wireless network protocols at the Univ. of Paris 12, France. He is now teaching as an assistant professor of network communication at ECE, Computer and Telecommunication Sciences School, France.

PASCALE MINET (pascale.minet@inria.fr) graduated with a Ph.D. in 1982 from the Univ. of Toulouse and as an engineer in computer science in 1978. She is a research engineer with project Reflexes at INRIA, Rocquencourt, France. Her major research area is fault tolerance, real-time communication protocols, and concurrency control in distributed real-time systems. She is interested in the design methodology of real-time applications. She has been a member of the ETSI RES10 committee for the HIPERLAN standard which specifies a high-speed wireless LAN.

LAURENT GEORGE (george@univ-paris12.fr) prepared his Ph.D. thesis at INRIA. He obtained his thesis in January 1998 from the University of Versailles. The subjects of his thesis were online distributed real-time scheduling with consistency constraints and reliable/atomic multicast with real-time constraints. He is now teaching network communication at the University of Paris 12 as an assistant professor. His research activity concerns QoS for real-time distributed systems. He studies the problem of multimedia communication (over the Internet) and wireless communication with end-to-end real-time constraints.

GILLES MERCIER (mercier@univ-paris12.fr) has a 23-year career in computer and engineering systems, and since 1995 has been a professor at the University of Paris 12, mainly in sciences and computers, and real-time processes. He is a graduate engineer in electronics since 1978 and has a Ph.D. of sciences in real-time neural networks. His research topics focus on real-time industrial processes based on short distance wireless LAN communications for embedded systems.