10 Wireless Local Access to the Mobile Internet

José Antonio García-Macías and Leyla Toumi

CONTENTS

10.1	Introduction	227
10.2	Local Access Technologies	228
10.2.1	The 802.11 Standard	228
10.2.2	802.11 Architecture	229
10.2.3	The Physical Layer	230
10.2.4	The Data Link Layer	231
10.2.5	Other Related Standards	232
10.2.5.1	HiperLAN	232
10.2.5.2	Bluetooth	234
10.2.6	WLAN Interoperability	235
10.3	Mobility and the Internet Protocols	236
10.3.1	The Problem of IP-Based Mobility	236
10.3.2	Mobile IP	238
10.3.4	Mobile IP problems	239
10.3.5	Micro-Mobility	240
10.4	Perspectives and Conclusions	242
	References	242

10.1 INTRODUCTION

The Internet has been around for more than three decades now. A key factor for its longevity is its flexibility to incorporate new technologies. However, this is not always a seamless process, as some of these new technologies break the basic assumptions under which the Internet works. For instance, the Internet was born at a time when all nodes in a network were fixed devices. Therefore, all the basic protocols were designed assuming that the end-points would stay fixed. Obviously, with the recent arrival of mobile networking devices (PDAs, laptops, 3G phones, etc.), these assumptions no longer hold.

We will discuss the problem of mobility in IP networks, making a special emphasis on the case of mobility within a restricted geographical span, also called

TABLE 10.1
Activities of the Task Groups Working on the 802.11 Standard

Task Group	Activities
802.11	Initial standard, 2.4-GHz band, 2 Mbps
802.11a	High speed PHY layer in the 5-GHz band, up to 24 or 54 Mbps
802.11b	High speed PHY layer in the 2.4-GHz band, up to 11 Mbps
802.11d	New regulatory domains (countries)
802.11e	Medium access control (MAC) enhancements: Multimedia, QoS, enhanced security
802.11f	Interaccess point protocol for AP interoperability
802.11g	Higher data rate extension in the 2.4-GHz band, up to 22 Mbps
802.11h	Extensions for the 5-GHz band support in Europe

micro-mobility. Before addressing the problem of local IP mobility, we will examine the technologies that allow local connectivity, so-called “last-meter” technologies such as 802.11 (WiFi), Bluetooth, and HiperLan.

10.2 LOCAL ACCESS TECHNOLOGIES

Among the different technologies available for wireless local networks, the most popular without a doubt is IEEE 802.11. Such popularity is evidenced by the number of products based on this standard that are commercially available. We will describe technologies used for access networks, with a particular emphasis on the 802.11 standard; also, we will discuss other technologies such as Bluetooth and HiperLAN.

It is also worth noting that some companies (e.g., Airify) have announced products to support multiple wireless standards using the same network interface; this way, the same device could be used to take advantage of WLAN technologies such as 802.11 or Bluetooth, or wide area wireless, such as GSM or GPRS. However, these types of products have yet to be commercially available.

10.2.1 THE 802.11 STANDARD

The Institute of Electrical and Electronic Engineers (IEEE) ratified the original 802.11 specification in 1997 as the standard for wireless LANs (WLANs). That version of 802.11 provides for 1 and 2 Mbps data rates and a set of fundamental signaling methods and other services. Some disadvantages with the original 802.11 standard are the data rates that are too slow to support most general business requirements. Recognizing the critical need to support higher data transmission rates, the IEEE ratified the 802.11b standard for transmissions of up to 11 Mbps. With 802.11b (also known as WiFi), WLANs are able to achieve wireless performance and throughput comparable to wired 10-Mbps Ethernet. 802.11a offers speeds of up to 54 Mbps, but runs in the 5-GHz band, so products based on this standard are not compatible with those based on 802.11b.¹ Several task groups are working on further developments for the 802.11 standard, as shown in Table 10.1.

FIGURE 10.1 The 802.11 standard and the ISO model.

Like all 802.x standards, 802.11 focuses on the bottom two layers of the OSI Reference Model, the physical and the data link layers. In fact, the standard covers three physical layer implementations: direct-sequence (DS) spread spectrum, frequency hopping (FH) spread spectrum, and infrared (IR). A single medium access control (MAC) layer supports all three physical layer implementations, as shown in Figure 10.1. We will further discuss the two ISO layers that the 802.11 standard deals with.

10.2.2 802.11 ARCHITECTURE

Each computer (mobile, portable, or fixed) is referred to as a station in 802.11. Mobile stations access the LAN during movement. The 802.11 standard defines two modes: infrastructure mode and *ad hoc* mode. In infrastructure mode (Figure 10.2), the wireless network consists of at least one access point (AP) connected to the wired network infrastructure and a set of wireless end stations.

This configuration is called a basic service set (BSS). An extended service set (ESS) is a set of two or more basic service sets forming a single subnetwork. Two or more ESSs are interconnected using a distribution system (DS). In an extended service set, the entire network looks like an independent BSS to the logical link control (LLC) layer; this means that stations within the extended service set can communicate or even move between basic service sets transparently to the logical link control. The distribution system can be thought of as a backbone network that is responsible for MAC-level transport of MAC service data units (MSDUs). The distribution system, as specified by 802.11, is implementation independent; therefore, the distribution system could be a wired 802.3 Ethernet LAN, an 802.4 token bus LAN, an 802.5 token ring LAN, a fiber distributed data interface (FDDI) metropolitan area network (MAN), or another 802.11 wireless medium. Note that while the distribution system could physically be the same transmission medium as the basic service set, they are logically different because the distribution system is solely used as a transport backbone to transfer packets between different basic service

FIGURE 10.2 Infrastructure mode.

sets in the extended service set. An extended service set can provide gateway access for wireless users into a wired network such as the Internet. This is accomplished via a device known as a portal. The portal is a logical entity that specifies the integration point on the distribution system where the 802.11 network integrates with a non-802.11 network. If the network is an 802.x, the portal incorporates functions that are analogous to a bridge, i.e., it provides range extension and the translation between different frame formats.

The *ad hoc* mode (also called peer-to-peer mode or an independent basic service set, or IBSS) is simply a set of 802.11 stations that communicate directly with one another without using an access point or any connection to a wired network (Figure 10.3). In *ad hoc* networks, there is no base and no one gives permission to talk; these networks are spontaneous and can be set up rapidly, but are limited both temporally and spatially.

10.2.3 THE PHYSICAL LAYER

The three physical layers originally defined in the 802.11 standard included two spread spectrum radio techniques and a diffuse infrared specification. The radio-based standards operate within the 2.4-GHz ISM (industrial, scientific, and medical) band. These frequency bands are recognized by international regulatory agencies, such as the FCC (United States), ETSI (Europe) and the MKK (Japan) for unlicensed radio operations. As such, 802.11-based products do not require user licensing or special training. Spread spectrum techniques, in addition to satisfying regulatory requirements, boost throughput and allow many unrelated products to share the spectrum without explicit cooperation and with minimal interference.

FIGURE 10.3 *Ad hoc* mode.

The original 802.11 wireless standard defines data rates of 1 and 2 Mbps via radio waves using frequency hopping (FH) spread spectrum or direct sequence (DS) spread spectrum. It is important to note that these are fundamentally different transmission mechanisms and will not interoperate with each other. Direct sequence has a more-robust modulation and a larger coverage range than FH, even when FH uses twice the transmitter power output level. Frequency hopping gives a large number of hop frequencies, but the adjacent channel interference behavior limits the number of independently operating collocated systems. Hop time and a smaller packet size introduce more transmission time overhead into FH, which affects the maximum throughput. Although FH is less robust, it gives a more-graceful degradation in throughput and connectivity.

Under poor channel and interference conditions, FH will continue to work over a few hop channels a little longer than over the other hop channels.

Direct sequence, however, still gives reliable links for a distance at which very few FH hop channels still work. For collocated networks (access points), DS gives a higher potential throughput with fewer access points than FH, which has more access points. The smaller number of access points used by DS lowers the infrastructure cost.

10.2.4 THE DATA LINK LAYER

The data link layer within 802.11 consists of two sublayers: logical link control (LLC) and media access control (MAC). 802.11 uses the same 802.2 LLC and 48-bit addressing as other 802.x LANs, allowing for very simple bridging from wireless to wired networks, but the MAC is unique to WLANs.

Of particular interest in the specification is the support for two fundamentally different MAC schemes to transport asynchronous and time-bounded services. The first scheme, distributed coordination function (DCF), is similar to traditional legacy packet networks. The DCF is designed for asynchronous data transport, where all users with data to transmit have an equally fair chance of accessing the network. The point coordination function (PCF) is the second MAC scheme. The PCF is based on polling that is controlled by an access point.

FIGURE 10.4 Standard 802.11 frame format.

The basic access method, DCF, is drawn from the family of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocols. The collision detection (CD) mechanism as used in the CSMA/CD protocol of Ethernet cannot be used under 802.11 due to the near/far problem: to detect a collision, a station must be able to transmit and listen at the same time, but in radio systems the transmission drowns out the ability of the station to hear a collision. So, 802.11 uses CSMA/CA, under which collisions are avoided by using explicit packet acknowledgment (ACK) to confirm that the data packet arrived intact.

802.11 supports three different types of frames: management, control, and data. The management frames are used for station association and disassociation with the access point, timing and synchronization, and authentication and deauthentication. Control frames are used for handshaking during a contention period (CP), for positive acknowledgment during the CP, and to end the contention-free period (CFP). Data frames are used for the transmission of data during the CP and CFP, and can be combined with polling and acknowledgments during the CFP. Figure 10.4 shows the standard 802.11 frame format.

10.2.5 OTHER RELATED STANDARDS

There are other WLAN technologies available besides 802.11, and we will review some of the most prominent ones, namely Bluetooth and HiperLAN. It is relevant to point out that up to now the market for WLANs has been dominated by products based on the 802.11 standard. There are starting to appear some products based on Bluetooth but they have been very deceiving and many important equipment and software manufacturers have decided not to support this standard,^{2,3} at least temporarily. Although some early prototypes for HiperLAN 2 have been demonstrated,⁴ there are no commercial products available yet.

10.2.5.1 HiperLAN

Between 1990 and 1992, the European Telecommunications Standards Institute (ETSI) noticed the trend toward faster and better wireless networks and started the development of standards for this type of network. Within this framework, the

FIGURE 10.5 Overview of HiperLAN standards.

Broadband Radio Access Networks (BRAN) Project 3 of ETSI is working on a standard called High Performance Radio Local Area Network (HiperLAN). This project quickly separated into four different HiperLAN types:

1. HiperLAN 1 is a standard for ad hoc networking operating in the 5.2-GHz band with a spectrum of 100 MHz and speeds of up to 19 Mbps. It offers one-to-one communications as well as one-to-many broadcasts. Using the CSMA/CA technique for resolving contention, the scheme shares available radio capacity between active users who attempt to transmit data during an overlapping time span. Although HiperLAN 1 provides a means of transporting time-bounded services, it does not control nor guarantee QoS on the wireless link. This is what motivated ETSI to develop a new generation of standards that support asynchronous data and time-critical services bounded by specific time delays.
2. HiperLAN 2 specifies a radio-access network that can be used with a variety of core networks (e.g., IP, ATM, UMTS). HiperLAN 2 operates in the 5.2-GHz band with 100 MHz spectrum, but at speeds of up to 54 Mbps.⁵
3. HiperAccess is the next step from HiperLAN 2, providing outdoor wireless access. It gives up to 5 km coverage between wireless access points and wireless termination points and is therefore intended for stationary and semistationary applications. The original operating frequencies were in the 5-GHz band, but this is currently under discussion.
4. HiperLink is the standard meant to provide interconnecting services for high data rate sources, such as networks (e.g., HiperLANs). Therefore, HiperLink provides point-to-point interconnections at very high data rates of up to 155 Mbps over distances up to 150 meters. The operating frequency is in the 17-GHz band with 200 MHz spectrum at the moment.

The standard for HiperLAN 1 was finalized in 1996, although amendments were made to it in 1998. HiperLAN types 2 through 4 were designed to support only ATM networks, but at the moment HiperLAN 2 supports access to IP and UMTS networks. The names for types 3 and 4 were changed to HiperAccess and HiperLink, respectively. Figure 10.5 gives an overview of the different HiperLAN standards.

FIGURE 10.6 A Bluetooth scatternet of four piconets.

10.2.5.2 Bluetooth

Bluetooth is a protocol intended to wirelessly connect cellular phones, laptops, handheld computers, digital cameras, printers, and other devices.⁶ It operates over short distances of up to 10 meters, basically being a wireless replacement for data cables and infrared connections. There are currently some discussions underway to extend its range to 100 meters by increasing the transmit power to 100 mW. Although Bluetooth was initially developed by Ericsson in the late 1990s, it is currently led by the Bluetooth SIG 4, including members such as Nokia, IBM, Toshiba, Intel, 3Com, Motorola, Lucent Technologies, and Microsoft. It is, then, not a technology backed by an standards body, but instead backed by an industry consortium.

The Bluetooth system supports point-to-point or point-to-multipoint connections. In point-to-multipoint, the channel is shared among several Bluetooth units. Two or more units sharing the same channel form a piconet. There is one master unit and up to seven active slave units in a piconet. These devices can be in any of the following states: active, park, hold, and sniff. Multiple piconets with overlapping coverage areas form a scatternet (Figure 10.6).

The Bluetooth system consists of a radio unit, a link control unit, and a support unit for link management and host terminal interface functions.

The radio operates in the 2.4-GHz ISM band. Depending on the class of the device, a Bluetooth radio can transmit up to 100 mW (20 dBm) to a minimum of 1 mW (0 dBm) of power. It uses frequency hopping for low interference and fading, and a TDD (time-division duplex) scheme for full-duplex transmission and transmits using GFSK (Gaussian frequency shift keying) modulation.⁷

FIGURE 10.7 The Bluetooth protocol stack.

The Bluetooth protocol uses a combination of circuit and packet switching. The channel is slotted and slots can be reserved for synchronous packets. The protocol stack can support an asynchronous connectionless link (ACL) for data and up to three simultaneous synchronous connection-oriented (SCO) links for voice or a combination of asynchronous data and synchronous voice (DV packet type). Each voice channel supports a 64 kbps synchronous channel in each direction. The asynchronous channel can support a maximum of 723.2 kbps uplink and 57.6 kbps downlink (or vice versa) or 433.9 kbps symmetric links. The stack (shown in Figure 10.7) primarily contains a physical level protocol (baseband) and a link level protocol (LMP) with an adaptation layer (L2CAP) for upper layer protocols to interact with lower layer ones.

It should be clear, given its distance coverage, bandwidth, and other characteristics, that Bluetooth does not really fit within the profile for supporting WLANs as their promoters portend through intense marketing campaigns. Bluetooth fits more within the profile of technologies used for wireless personal area networks (WPANs), as those studied by the 802.15 Working Group.

10.2.6 WLAN INTEROPERABILITY

Given their ease of installation, dropping prices, and increasingly higher speeds, WLANs are gradually replacing many wired LANs as the networks of choice for typical activities such as Internet access. There are currently coexistence problems between some of the technologies we mention here, namely between 802.11 and Bluetooth. A source of problems is the fact that Bluetooth has been designed to transmit blindly, whenever its timing dictates, as if there was no possibility that a

collocated system might be using the same frequency (as 802.11 does). This has earned it the reputation of a “bad neighbor” in the 2.4-GHz band. There are also other common sources of interference in this unregulated band, including microwave ovens and newer generations of cordless phones. Historically, microwave ovens are by far the most-significant source of interference in residential and office environments, but with the impending avalanche of new communications devices with embedded Bluetooth radios, serious questions have been raised about their interference on wireless LANs. The 802.15 WPAN Task Group 2 is developing recommended practices and mechanisms to facilitate coexistence between WLANs (such as 802.11) and WPANs (such as Bluetooth).

10.3 MOBILITY AND THE INTERNET PROTOCOLS

The Internet was born in an era when no mobile networking equipment was available. Therefore, all the basic protocols were designed under the tacit assumption that the end-points of a communication would stay fixed all along a session. With the arrival of modern communications equipment that allows these end-points to change their position, new protocols for handling mobility have been proposed.

Mobile IP allows mobility of devices, potentially around the world; this is why the type of mobility support it provides is sometimes referred to as global mobility. However, as we will see, mobility within a limited geographical area (called micro-mobility), has different characteristics and requirements that pose the need for specialized support.

10.3.1 THE PROBLEM OF IP-BASED MOBILITY

Although networking-enabled mobile devices are becoming more common everyday, most networking protocols — including the TCP/IP protocol suite — have been designed assuming that hosts are always attached to the network at a single physical location. Therefore, host mobility is seen as a rarely occurring fact that can be handled manually. Consider for instance the following scenario: a business executive is usually connected to the network in the office, but occasionally needs to use a laptop computer for meetings; the meeting facilities may be elsewhere in the building or perhaps in a different building or city. If the executive’s desk and the meeting room have direct access to the same IP subnet, then the mobility process is trivial. In situations where this is not the case, the only solution is for the user to acquire a new IP address from the appropriate local authority. Then, several configuration files on the moving machine, on various name servers, and on other machines that use the original IP address to identify the moving machine need to be modified. Thus, moving the computer from one place to another involves a slow, error-prone, manual procedure that a typical user does not have the skills or the inclination to deal with. Moreover, even if the process is successfully performed, the mobile host will lose its former identity and will usually need rebooting.

The situation is that, given TCP/IP’s early design assumptions that end systems are stationary, if during an active connection one end system moves, then the whole connection breaks, obviously disrupting all networking services layered on top of

TCP/IP. Evidence has been given⁸ that in order to retain transport layer connections, a mobile host's address must be preserved regardless of its point of attachment to the network. The problem with a transport layer protocol such as TCP is that a TCP connection is identified by a 4-tuple:

```
<src IP address, src TCP port, dest IP address, dest  
TCP port>
```

So, if neither host moves, all elements of the tuple remain fixed and the TCP connection can be preserved. However, if either end of the connection moves, the following problem will take place:

- If the mobile host acquires a new IP address, then its associated TCP connection identifier also changes. This causes all TCP connections involving the mobile host to break.
- If the mobile retains its address, then the routing system cannot forward packets to its new location.

These problems come from the very design of IP which, in addition to fragmentation and reassembly, is responsible for “providing the functions necessary to deliver a package of bits (an Internet datagram) from a source to a destination over an interconnected system of networks.”⁹ So, this definition designates responsibility to IP for routing datagrams to and from mobile hosts transparently to higher layers. The problem is that IP addresses serve a dual purpose, as they are not only used by higher layers to identify source and destination hosts, but also by their division into network and host parts which contain location information. Therefore, in its role as an identifier, an IP address must be constant during mobility to avoid affecting higher layers.

Research studies on IP mobility have suggested that mobility is essentially an address translation problem and is best resolved at the network layer.⁸ As Figure 10.8 shows, a mobile host *MH* can move away from its home network and attach to the Internet through a foreign network. While away, *MH* obtains a forwarding address derived from the address space of the foreign network. However, if another host *S* tries to send packets to *MH*, it will do so using *MH*'s home address. The problem is resolved by the use of an address translation agent (ATA) at the home network, and a forwarding agent (FA) at the foreign network. These agents perform functions *f* and *g*, respectively, which are defined as follows:

- *f*: home address $\rightarrow$ forwarding address
- *g*: forwarding address $\rightarrow$ home address

This way, when *S* sends packets to *MH*, they first pass through ATA. This agent performs mapping *f* to send the packets to the address that *MH* acquired in the foreign network. At the foreign network, *FA* intercepts all packets containing *MH*'s forwarding address. It then proceeds to apply the function *g* to map from this forwarding address to *MH*'s original home address and effectively forward the packets.

FIGURE 10.8 Mobility as an address translation problem.

10.3.2 MOBILE IP

In order to react to the new challenges posed to the Internet architecture by the arrival of mobile networking devices, the IETF created the Mobile IP Working Group. The basic Mobile IP standard¹⁰ specifies a mobility management architecture for the Internet. In principle, both local-area and wide-area mobility across wired and wireless networks can be handled, although certain inefficiencies have been detected. Later, we will see extensions to Mobile IP proposed to overcome such inefficiencies.

Figure 10.9 shows the basic operation of Mobile IP. A mobile node is normally attached to its home network using a static home address. When the mobile node moves to a foreign network, it makes its presence known by registering with a foreign agent (FA). The mobile node then communicates with a home agent (HA) in its home network, giving it the care-of address (COA), which identifies the foreign agent's location. Typically, routers in a network will implement the roles of home and foreign agents. When IP datagrams are exchanged over a connection between the mobile node A and a correspondent host B, the following operations occur:¹¹

1. Host B transmits an IP datagram destined for mobile node A, with A's home address in the IP header. The IP datagram is routed to A's home network.
2. At the home network, the incoming IP datagram is intercepted by the home agent. The home agent encapsulates the entire datagram inside a new IP datagram, which has A's care-of address in the header, and retransmits the datagram. The use of an outer IP datagram with a different destination IP address is known as tunneling.
3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a MAC-level PDU (for example, an Ethernet frame), and delivers the original datagram to A across the foreign network.

FIGURE 10.9 Basic mobile IP scenario.

4. When *A* sends IP traffic to *B*, it uses *B*'s IP address. In our example, this is a fixed address; i.e., *B* is not a mobile node. Each IP datagram is sent by *A* to a router on the foreign network for routing to *B*.
5. The IP datagram from *A* to *B* travels directly across the Internet to *B*, using *B*'s IP address.

10.3.4 MOBILE IP PROBLEMS

There are currently several outstanding problems facing Mobile IP, posing technical as well as practical obstacles for its deployment.¹² One of the most notable problems is due to routing inefficiencies. In the basic Mobile IP protocol, IP packets destined to a MN that is outside its home network are routed through the home agent. However, packets from the MN to the corresponding nodes are routed directly. This is known as triangle routing (see Figure 10.10).

This method may be inefficient when the correspondent host and the MN are in the same network, but not in the same home network of the MN. In such a case, the messages will experience unnecessary delay because they have to be routed first to the HA that resides in the home network. In order to alleviate this, a technique known as route optimization has been proposed.¹³ However, implementing it requires changes in the correspondent nodes that will take a long time to deploy in IPv4.

Some other problems are related to performance and scaling issues. Studies have shown that Mobile IP can suffer from unacceptably long handoff latencies when the mobile host is far from its home network.¹⁴ Scalability can be a problem as the number of mobile hosts grow, but in this case the network is the bottleneck, as mobility agents (i.e., HAs, FAs) can easily service at least a few hundred hosts. Suggestions have been made that using a hierarchical model to manage mobility

FIGURE 10.10 Triangular routing.

could reduce or eliminate these performance and scaling problems.^{15,16} Security is also a particular area of attention in Mobile IP.

A lot of the problems of Mobile IP are related to the lack of features for streamlining mobility support in IPv4.¹⁷ Some of these problems may be solved by IPv6. While Mobile IP was originally designed for IPv4, IPv6¹⁸ incorporates features that support mobility much more easily; several mechanisms that had to be specified separately now come integrated with IPv6. Some of these IPv6 features include stateless address autoconfiguration¹⁹ and neighbor discovery.²⁰ IPv6 also attempts to drastically simplify the process of renumbering, which may be critical to the future of routability of the Internet.²¹ Security is a required feature for all IPv6 nodes.

10.3.5 MICRO-MOBILITY

As several studies indicate,^{22,23} users' mobility patterns are highly localized. For instance, business professionals may spend a considerable amount of time away from their desks, but once away, most of their mobility will take place within the same building. While the mobile user is at the foreign administrative domain, there is no need to expose motion within that domain to the home agent or to correspondent hosts in other domains. Therefore, mobility management within an administrative domain should be separate from global mobility management.

In principle, Mobile IP can handle both global and local mobility. However, it requires that the mobile's home network is notified of every change in location. Moreover, route optimization extensions¹³ further require that every new location is registered with hosts that are actively communicating with the mobile node. All

these location updates incur communications latency and also add traffic to the wide-area portion of the internetwork. Therefore, Mobile IP does not extend well to large numbers of portable devices moving frequently between small cells. It also has been demonstrated that, when used for micro-mobility support, Mobile IP incurs disruption to user traffic during handoff, and high control overhead due to frequent notifications to the home agent.¹⁵ Another type of protocol, a micro-mobility protocol,²⁴ is then needed for local environments where mobile hosts change their point of attachment to the network so frequently that the basic Mobile IP tunneling mechanism introduces network overhead in terms of increased delay, packet loss, and signaling.

Acknowledging the fact that Mobile IP may not be the universal end-all solution for mobility on the Internet, its performance and scalability challenges have been under discussion. Within this context, the Mobile IP working group has recently started discussing the subject of micro-mobility protocols. There are several attributes that micro-mobility protocols aim toward:

- Minimum (or zero) packet loss: Fast handoff techniques have been developed to achieve this, and they may reduce latency or delay.
- Reduced signaling: Techniques for locating mobile hosts, known as paging, have been proposed in order to reduce signaling. Reduced registration is also an outcome of these techniques.

Hawaii and Cellular IP are two prominent proposals for micro-mobility management and we give a brief presentation of both:

- HAWAII^{25,26} (Handoff-Aware Wireless Access Internet Infrastructure) is an alternative for providing domain-based mobility (i.e., micro-mobility). Under this approach, Mobile IP is used as the basis for mobility management in wide-area wireless networks, but new methods for managing mobility within an administrative domain are developed. One point worth highlighting is that mobile hosts retain their network address while moving within a domain; this way, the Home Agent (HA) — if using Mobile IP — and any corresponding hosts are not aware that the host has performed intradomain mobility. Dividing the network into hierarchies, loosely modeling the autonomous system hierarchy used in the Internet, is part of the HAWAII approach. Indeed, the gateway into each domain is called the domain root router, and each host is assumed to have an IP address and a home domain. As already stated, hosts retain their address while moving within a domain, so when packets destined to a mobile host arrive at the domain root router, they are forwarded over specially established paths to reach the mobile host. However, if the mobile host moves to a foreign domain, traditional Mobile IP mechanisms are used.
- Cellular IP^{27,28} aims to integrate cellular technology principles with the IP networking paradigm; this poses hard challenges, as there are fundamental architectural differences between cellular and IP networks. A Cellular IP node constitutes the universal component of a Cellular IP network,

because it serves as a wireless access point but at the same time routes IP packets and integrates cellular control functionality traditionally found in mobile switching centers (MSC) and base station controllers (BSC). Cellular IP nodes are modified IP nodes where standard routing is replaced by Cellular IP's own routing and location-management functions. A Cellular IP network is connected to the Internet via a gateway router. Mobility between gateways (i.e., Cellular IP access networks) is managed by Mobile IP, while mobility within access networks is handled by Cellular IP. Mobile hosts attached to the network use the IP address of the gateway as their Mobile IP care-of address.

Another important aspect that has received little attention in the design of micro-mobility protocols is that of quality of service (QoS). Triangular routing, address translation, and complex interaction between agents make Mobile IP unsuitable for QoS support in local environments.^{29–31}

10.4 PERSPECTIVES AND CONCLUSIONS

Among local wireless access technologies, WLANs have a predominant place in the market, as they are increasingly replacing wired LANs as the method of choice for accessing the Internet. By far, the most popular WLAN technology is currently 802.11 (particularly the 802.11b variation, also named Wi-Fi). Wireless technologies allow hosts to freely roam between cells, but the Internet's core protocols were not designed with mobility in mind. Even though Mobile IP has been proposed as a solution to handle IP mobility, it is not very suitable for the case of micro-mobility (i.e., mobility within a very limited geographical span). Thus, IP micro-mobility protocols have been proposed.

Recent research has addressed the problem of providing QoS guarantees in micro-mobility environments. Some have proposed RSVP-like signaling protocols to make resources reservations,³² while others have taken the differentiated services approach (proposed by the IETF), where no hard QoS guarantees are provided, but only statistical guarantees.³³ Also, work in progress within the IETF's SeaMoby Working Group is currently addressing problems related to QoS in mobile environments, although not exclusively for the case of micro-mobility.

References

1. Nobel, C., Making 802.11 standards work together, *eWeek*, July 19, 2000.
2. Staff, N., Psion backtracks on consumer plans, <http://news.cnet.com>, July 12, 2001.
3. Orłowski, A., Microsoft turns the drill on Bluetooth, August 1, 2001, available at <http://www.theregister.co.uk>.
4. Ericsson, Ericsson demonstrates HiperLAN 2 prototypes, Press release, December 11, 2000, available at <http://www.ericsson.com/press/20001211-0067.html>.
5. Khun-Jush, J. et al., HiperLAN type 2 for broadband wireless communication, *Ericsson Review*, 2, 108, 2000.

6. Haarsten, J., Bluetooth – the universal radio interface for ad hoc, wireless connectivity, *Ericsson Review*, 3, 110, 1998.
7. Haarsten, J., The Bluetooth radio system, *IEEE Personal Communications Magazine*, 7, 28, 2000.
8. Bhagwat, P., Perkins, C., and Tripathi, S., Network layer mobility: an architecture and survey, *IEEE Personal Communications Magazine*, 3, 54, 1996.
9. DARPA, DARPA Internet Program Protocol Specification, Internet RFC 791, 1981.
10. Perkins, C., Mobile IP specification, Internet RFC 2002, 1996.
11. Stallings, W., Mobile IP, *The Internet Protocol Journal*, 4, 2, 2001.
12. Chesire, S. and Baker, M., Internet mobility 4x4, in *ACM SIGCOMM Computer Communications Review*, 318, 1994.
13. Johnson, D. and Perkins, C., Route optimization in mobile IP, IETF Mobile-IP draft, July 1995.
14. Mukkamalla S. and Raman, B., Latency and scaling issues in mobile IP, Iceberg Project technical report, University of California, Berkeley, 2001.
15. Caceres, R. and Padmanabhan, V., Fast and scalable handoffs for wireless internet-networks, in *ACM Mobicom* 96, 1996.
16. Soliman, H. et al., Hierarchical MIPv6 mobility management (HMIPv6), Internet draft draft-ietf-mobileip-hmipv6-04.txt, work in progress, July 2001.
17. Perkins, C., Mobile networking through mobile IP, *IEEE Internet Computing*, 2 (1), 1998.
18. Deering, S. and Hinden, R., Internet Protocol version 6 (IPv6), Internet RFC 1883, 1995.
19. Thomson, S. and Narten, T., IPv6 stateless address autoconfiguration, Internet RFC 1711, 1996.
20. Narten, T., Nordmark, E., and Simpson, W., Neighbor discovery for IP version 6 (IPv6), Internet RFC 1700, 1996.
21. Castineyra, I., Chiappa, J., and Steenstrup, M., The Nimrod routing architecture, Internet RFC 1992, 1996.
22. Kirby, G., Locating the user, *Communications International*, 1995.
23. Toh, C., The design and implementation of a hybrid handover protocol for multimedia wireless LANs, in Proc. 1st International Conference on Mobile Computing and Networking, 1995.
24. Campbell, A. and Gomez-Castellanos, J., IP micro-mobility protocols, *ACM Sigmobile Mobile Computer and Communications Review*, 2001.
25. Ramjee, R. et al., IP micro-mobility support using HAWAII, Internet draft draft-ietf-mobileip-hawaii-01.txt, work in progress, July 1999.
26. Ramjee, R. et al., HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks, in IEEE International Conference on Network Protocols, 1999.
27. Valko, A., Cellular IP — a new approach to Internet host mobility, *ACM Computer Communication Review*, 1999.
28. Campbell, A. et al., An overview of cellular IP, in IEEE Wireless Communications and Networks Conference, WCNC, 1999.
29. Chan, J. et al., The challenges of provisioning real-time services in wireless Internet, *Telecommunications Journal of Australia*, 2000.
30. Helal, A. et al., Towards integrating wireless LANs with wireless WANs using mobile IP, in IEEE Wireless Communications and Networks Conference, WCNC, 2000.
31. Mukkamalla, S. and Raman, B., Latency and scaling issues in mobile IP, ICEBERG Project technical report, University of California, Berkeley, 2001.

32. Legrand, G., Qualité de Service dans les Environnements Internet Mobile, Ph.D. thesis, Université Pierre et Marie Curie, Paris VII, July 2001.
33. García-Macías, J.A. et al., Quality of service and mobility for the wireless Internet, in ACM/IEEE Mobicom 2001, Workshop on Mobile Internet (WMI), Rome, Italy, July 2001.