BLUETOOTH AND WI-FI WIRELESS PROTOCOLS: A SURVEY AND A COMPARISON(*)

ERINA FERRO, FRANCESCO POTORTÌ

ISTI - CNR (Institute of the National Research Council)
via Moruzzi 1, 56124 Pisa, Italy
{Erina.Ferro,Potorti}@isti.cnr.it

Abstract. Bluetooth and IEEE 802.11 (Wi-Fi) are two communication protocol standards which define a physical layer and a MAC layer for wireless communications within a short range (from a few meters up to 100 meters) with low power consumption (from less than 1 mW up to 100 mW). Bluetooth is oriented to connecting close devices, serving as a substitute for cables, while Wi-Fi is oriented towards computer-to-computer connections, as an extension of or substitution for cabled LANs. In this paper we offer an overview of these popular wireless communication standards, comparing their main features and behaviors in terms of various metrics, including capacity, network topology, security, quality of service support, and power consumption.

1 INTRODUCTION

Wireless communications is a fast-growing technology that enables people to access networks and services without cables. Deployment can be envisaged in various scenarios: different devices belonging to a single user, such as a mobile telephone, a portable computer, a personal digital assistant (PDA) and others, which need to interact in order to share documents; a user who receives emails on the PDA; a shopping mall where customers display special offers on their PDA; car drivers loading maps and other tourist information while driving on the motorway. All of these scenarios have become a reality from a technological point of view and successful experiments are being carried out around the world.

The wireless approach shows many advantages but also has some disadvantages with respect to cabled networks. Mobility is clearly one of the major advantages of wireless with respect to cabled devices, which require plugging. Another advantage lies in the way new wireless users can dynamically join or leave the network, move among different environments, create ad hoc networks for a limited time and then leave. Wireless networks are simple to deploy, and in some cases, they cost less than wired LANs. Nevertheless, the technological challenges involved in wireless networks are not trivial, leading to disadvantages with respect to cabled networks, such as lower reliability due to interference, higher power consumption, data security threats due to the inherent broadcast properties of the radio medium, worries about user safety due to continued exposition to radio frequency, and lower data rates.

(*) Work funded by the Italian Ministry of Instruction, University and Research (MIUR) within the framework of the "IS-MANET" project (Infrastrutture Software per Mobile Ad hoc NETworks) and by SatNEx (Satellite Communications Network of Excellence) in the VI Research Framework Programme of the European Commission.

Currently the wireless scene is held by two standards, namely the *Bluetooth* and the *IEEE 802.11* protocols, which define the physical layer and the medium access control (MAC) for wireless communications over a short action range (from a few up to several hundred meters) and with low power consumption (from less than 1 mW up to hundreds of mW). Bluetooth is mainly oriented towards connections between close-connected devices, as a substitute for data transfer cables; IEEE 802.11 is devoted to connections among computers, as an extension or substitute for cabled LANs. The standards cover different techniques at the physical layer: *infrared* communications, which are rarely used in commercial products and are not treated in this work, and different radio signal multiplexing techniques: *frequency hopping spread spectrum* (FHSS), used by Bluetooth devices, *direct sequence spread spectrum* (DSSS), *complementary code keying* (CCK), and *orthogonal frequency division multiplexing* (OFDM), used in IEEE 802.11 commercial devices.
Both Bluetooth and IEEE 802.11 systems are evolving towards more powerful multiplexing technologies, namely *ultra wide band* (UWM) and *multiple input - multiple output* (MIMO), respectively.

The material presented here is widely available in the literature; therefore the main purpose of this paper is not to contribute to research in the area of wireless standards, but to present a comparison of the major characteristics of the two main protocols for short-range terrestrial communications.

2 A SURVEY OF BLUETOOTH AND IEEE 802.11

2.1 BLUETOOTH

Bluetooth [1] is a standard for wireless communications based on a radio system designed for short-range, cheap communications devices suitable for substituting cables for printers, faxes, joysticks, mice, keyboards, etc. The devices could also be used for communications between portable computers, act as bridges between other networks, or serve as nodes of ad hoc networks. This range of applications is known as WPAN (*Wireless Personal Area Network*).

2.1.1 History, current status and prospective developments

The original idea behind Bluetooth technology was conceived in 1994, when Ericsson Mobile Communications began to study a low-power-consumption system for substituting the cables in the short-range area of its mobile phones and relevant accessories. In 1998 Ericsson, Nokia, IBM, Toshiba, and Intel formed the Bluetooth SIG (Special Interest Group). Subsequently, 1999 was the year of the first release of the Bluetooth protocol; the next year, four other companies joined the SIG group: 3COM, Agere (Lucent Technologies), Microsoft and Motorola. In that year, the first Bluetooth headset, from Ericsson, appeared on the market.
Bluetooth is currently at version 1.2. Since March 2002, the IEEE 802.15 working group has adopted the work done for Bluetooth (without any major changes) and made it an IEEE standard, namely IEEE 802.15.1 (Figure 1).
The future of Bluetooth may be based on ultra-wide band (UWB) [2]. UWB systems use very high-speed, precisely timed impulses for transmitting information over a very wide spectrum; this is very different from most other transmission schemes, which modulate a sine wave.

UWB pulses require precise synchronization between transmitter and receiver, but in return, they are able to traverse common obstacles, such as walls, even at low emission power. Among the many proposed applications for this technology are high-speed, low-range, low-power communications, making it a natural candidate for WPANs. The WPAN (wireless personal area networks) working group at IEEE is considering adopting UWB for the physical layer of the 802.15.3a standard, capable of rates in the hundreds of Mb/s.

2.1.2 Basic operation

When a Bluetooth device is powered on, it may try to operate as one of the slave devices of an already running master device. It then starts listening for a master's inquiry for new devices and responds to it. The inquiry phase lets the master know the address of the slave; this phase is not necessary for very simple paired devices that are granted to know each other's address. Once a master knows the address of a slave, it may open a connection towards it, provided the slave is listening for paging requests. If this is the case, the slave responds to the master's page request and the two devices synchronize over the frequency hopping sequence, which is unique to each piconet and is decided by the master. Bluetooth predefines several types of connection, each with a different combination of available bandwidth, error protection and quality of service. Once a connection is established, the devices can optionally authenticate each other and then communicate. Devices not engaged in transmissions can enter one of several power- and bandwidth-saving modes or tear down the connection. Master and slave can switch roles, which may be necessary when a device wants to participate in more than one piconet.

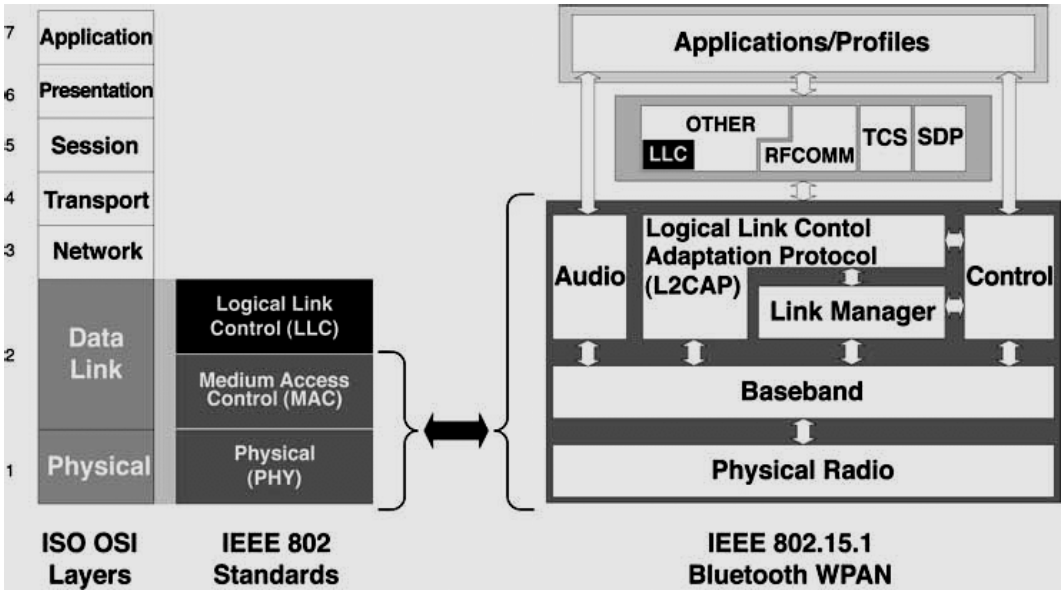

Figure 1. The Bluetooth stack[1].

2.1.3 Protocol overview

Bluetooth defines not only a radio interface, but a whole communication stack that allows the devices to find each other and advertise the services they offer. In Figure 1, the *Link Manager* layer handles the type of link configuration, authentication, security, quality of

[1] Reproduced from the IEEE 802.15.1 standard, page 22.

service (QoS), power consumption and transmission scheduling. The *Control* supplies a command interface to the Link Manager and Baseband levels, thus providing a coherent interface to hardware developed by different manufacturers. The *L2CAP* (Logical Link Control Adaptation Protocol) layer supplies connection-oriented and connectionless services to the upper levels. Its functions include: i) protocol multiplexing, which is necessary because the Baseband protocol does not include a "type" field identifying the origin of the packet from the upper levels; ii) segmentation and reassembly of the protocol data units coming from the upper levels; and iii) QoS support. It is possible to implement IP directly on L2CAP, but Bluetooth 1.1 does not define a profile implementing this facility. Thus, IP is typically implemented by using PPP over RFCOMM, a profile that emulates a serial port. RFCOMM is useful because many existing applications are based on serial communications. Up to 60 connections can be simultaneously active between two Bluetooth devices. The other acronyms in Figure 1 are TCS (Telephony Control Specifications) and SDP (Service Discovery Protocol).

A Bluetooth device may operate either in *master mode* or in *slave mode*; a maximum of eight devices — seven active slaves plus one master — working together form a *Piconet* (Figure 2), which is the simplest configuration of a Bluetooth network. Piconets may be connected together, thus forming a *Scatternet*.

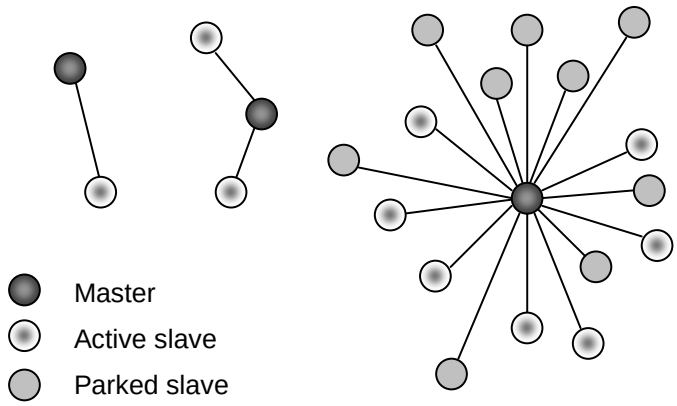

Figure 2. Piconet configurations.

A Scatternet (Figure 3) is a topology over which a *multihop* wireless network can be built. A wireless network is said to be *multihop* when two nodes can communicate with each other even if there is no direct connection between them, by using other nodes as relays. Two Piconets can communicate by means of a common node belonging to both of them. A node can be master in one Piconet at most and slave in several others.

Bluetooth devices use the 2.4 GHz band, which is unlicensed in most countries (in the USA it is known as ISM band). In most European countries and the USA, 79 1 MHz-wide channels are allocated, while only 23 channels are allocated in France, Spain and Japan. The channels are accessed using a FHSS (Frequency Hopping Spread Spectrum) technique, with a signal rate of 1 Mb/s, using a GFSK (Gaussian shaped Frequency Shift Keying) modulation. Frequency hopping consists in accessing the different radio channels according to an extremely long pseudo-random sequence that is generated from the address and clock of the master station in the Piconet. Using this method, different Piconets use different hop sequences. When entering a Piconet, a slave waits for an *Inquiry* message from the master to learn the master's address and clock phase, which it then uses to compute the hopping sequence. The transmission channel changes 1600 times per second; this means that the

transmission frequency remains unchanged for 625 μs long *slots*, which are identified by a sequence number. The master station starts its transmissions in the even slots, the slaves in the odd ones. A message may last for 1, 3, or 5 consecutive slots. The channel used to transmit *multislot* messages is the same one used for the first slot of the message: this means that the hopping sequence does not advance when transmitting multislot messages.

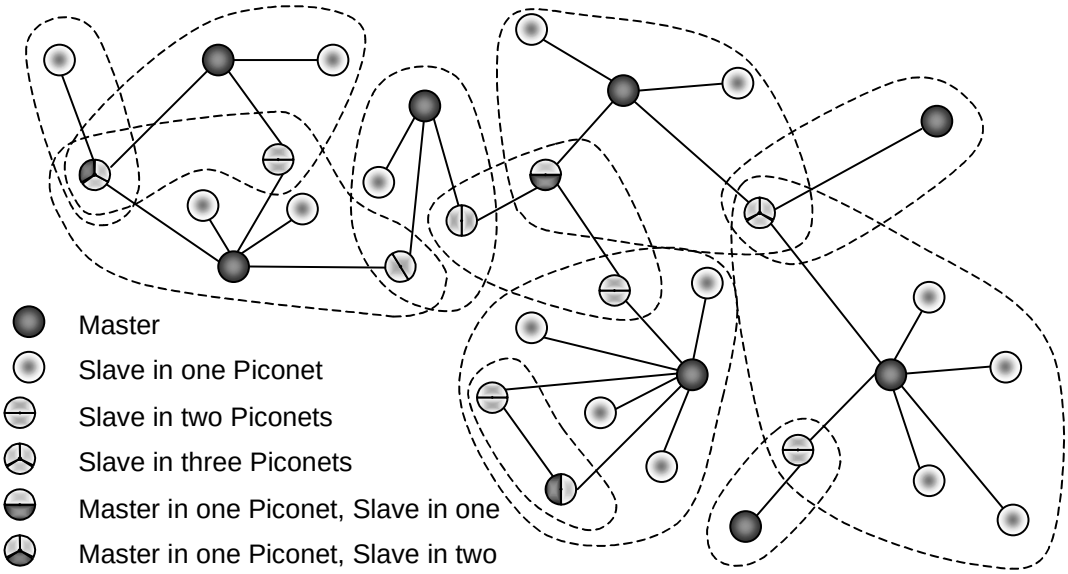

Figure 3. A complex scatternet configuration.

Two different link types are defined in Bluetooth, namely *Asynchronous ConnectionLess* links (ACL), and *Synchronous Connection-Oriented* links (SCO).
A SCO link provides guaranteed delay and bandwidth, apart from possible interruptions caused by the LMP (Link Manager Protocol) messages, which have higher priority. A slave can open up to three SCO links with the same master, or two SCO links with different masters, while a master can open up to three SCO links with up to three different slaves. SCO links provide constant bit rate, symmetric channels, which makes them suitable for streaming applications which require fixed, symmetric bandwidth. They provide limited reliability: no retransmission is ever performed, and no CRC (Cyclic Redundancy Check) is applied to the payload, though they are optionally protected with a 1/3 or 2/3 FEC (forward error correction) convolutional code. The data rate is 64 kb/s in both directions; an asymmetric connection is also defined, with only the forward guaranteed rate of 64 kb/s and 2/3 FEC.

Table I. Data transfer speeds needed by some audio systems.

Audio system	Quality	Data rate (kb/s)
CD audio	16 bit stereo 44.1 kHz sampling	1411.2
MP3 audio	Close to CD audio	128
POTS (telephone)	8 bit mono 8 kHz sampling	64
GSM audio	Close to POTS (telephone)	13.42

SCO links are suitable for transmitting average-quality voice and music. As an example, Table I reports the data transfer speeds required by some audio systems. Figure 4 illustrates the packet exchange sequence in a SCO link.

ACL links are appropriate for non-real-time (datagram) traffic. A slave can exchange one packet at a time with the master according to a schedule between slaves, which is computed by the master. Only a single ACL link can exist between a given slave and the master, which means that applications requiring different QoS parameters should use different links. ACL links exist in both symmetric and asymmetric flavours, with different preset bandwidths, error protection by means of a 16-bit CRC applied to the payload, optional 2/3 FEC convolutional code, and optional ARQ (automatic repeat request, i.e., packet retransmission on error).

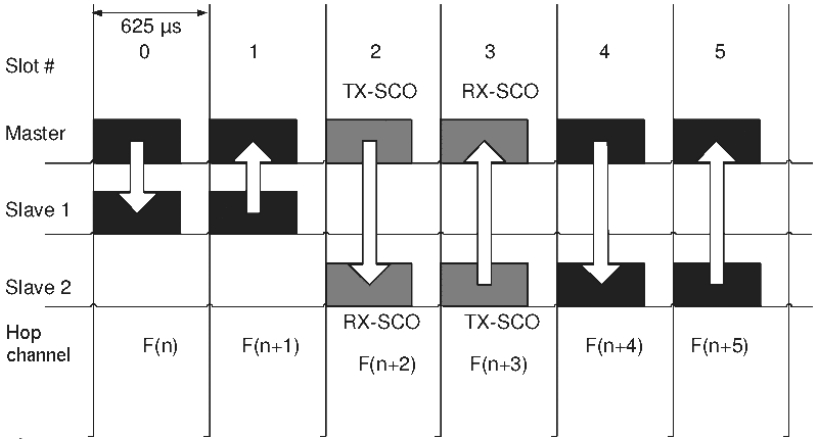

Figure 4. An example of packet exchange: dark packets belong to ACL links.

The configuration of the ACL links, from the point of view of bandwidth and quality of service, is done by means of an interface offered by the Link Manager. The configurable parameters are: *type of QoS* (none, best effort, and guaranteed best effort, the latter being the default), *token rate* (the data transfer rate guaranteed on that link; no default), *token rate bucket size* (the buffer size for the received data, default is zero), *peak bandwidth* (default is not specified), *latency* (default is not specified) the *delay variation* (the maximum allowable difference between packet delays, default is not specified). The use of these parameters is implemented by means of primitives that make a request to the admission control function implemented by the master's Link Manager. If the master accepts the QoS request, it configures the link with the slave by setting two parameters: the *poll interval* (the maximum time interval between two consecutive transmissions), and N_{BC}, that is, the number of retransmissions for broadcast packets. The latter are not acknowledged by slaves, so they can be transmitted with a given number of retransmissions to increase their reliability. The Link Manager may communicate any violation of the requested QoS parameters to the upper levels of the Bluetooth stack. The set of configurable parameters provides the basis for implementing a complete QoS policy by using a Bluetooth stack.

Bluetooth security is divided into three modes:

- Mode 1: non-secure
- Mode 2: Service Level enforced security (after channel establishment)
- Mode 3: Link Level enforced security (before channel establishment).

Authentication and encryption at the link level are handled by means of four basic entities: i) the Bluetooth device address, which is a 48-bit unique identifier assigned to each device; ii) a private authentication key (random number); iii) a private encryption key (random number); and iv) a 128-bit frequently-changing random number, dynamically generated by each device

[3]. There are two security levels for devices: *trusted* and *untrusted*, and three levels defined for services: open services, services requiring authentication and services requiring authentication and authorization.
The same PIN code, of length comprised between 1 and 16 octets, must be entered for each communicating Bluetooth device at initialization; alternatively, the PIN code can be hardwired in all or some of the devices.

2.2 IEEE 802.11 (WI-FI)

The aim of the IEEE 802.11 standard [4][5][6][7] is to provide wireless connectivity to devices that require a quick installation, such as portable computers, PDAs, or generally mobile devices inside a WLAN (Wireless Local Area Network). It defines the MAC procedures for accessing the physical medium, which can be infrared or radio frequency. Mobility is handled at the MAC layer, so handoff between adjacent cells is transparent to layers built on top of an IEEE 802.11 device.

2.2.1 History, current status and prospective developments

In 1997 the IEEE (Institute for Electric and Electronic Engineering) approved a standard for wireless LAN called 802.11, which specified the characteristics of devices with a signal rate of 1 and 2 Mb/s. The standard specifies the MAC and the physical layers for transmissions in the 2.4 GHz band. The spectrum used ranges from 2.4 to 2.4835 GHz in the USA and Europe, while in Japan it ranges from 2.471 to 2.497 GHz. After the good results obtained by companies such as Lucent Technologies and Harris Semiconductors, the IEEE ratified a new amendment, with better performance, called IEEE 802.11.b, which works at additional signal rates of 5.5 and 11 Mb/s: most devices currently on the market are based on this technology. 802.11b specifies some coding modifications, leaving the lower-layer radio characteristics unmodified, and making very small changes to the upper MAC layers, thus facilitating the compatibility with 802.11 devices. Hereinafter, conveniently but somewhat inaccurately, to the IEEE 802.11 standard as *Wi-Fi* (Wireless-Fidelity), which is in fact a trademark certifying device interoperability relative to a set of tests defined by the Wi-Fi Alliance.
In the same year, 1997, the IEEE published the specifications of a new amendment of the 802.11 family, the 802.11a. The specifications still refer to the MAC and the physical layers, and the band used is the 5 GHz, which is unlicensed in the USA but not in most other countries. The signal rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mb/s. Devices following this standard should be usable in those parts of Europe where Dynamic Frequency Selection (DFS) and Adaptive Power Control (APC), as specified in the 802.11h amendment, are used; however, six months after the amendment approval (end of 2003), manufacturers do not actively promote any 802.11h devices, though many of them are announcing devices compliant with ETSI regulations in some European countries.
In 2003, the IEEE approved 802.11g as a further evolution of the 802.11 standard. 802.11g provides the same performance as 802.11a, while working in the 2.4 GHz band, which makes it deployable in Europe. Compatibility with 802.11b devices is guaranteed.
The future for Wi-Fi will likely be multiple input – multiple output (MIMO) [8]. MIMO systems use multiple transmit and multiple receiving antennas. In a scattering-rich environment, each receiving antenna is able to compute a signature of each of the transmitting antennas, and thus distinguish their transmissions. In principle, such a system has an overall capacity proportional to the number of antennas used, at the price of increased complexity. In August 2003 Airgo announced a Wi-Fi MIMO chipset available for sampling,

capable of rates up to 108 Mb/s per channel, while remaining compatible with current Wi-Fi standards. The 802.11n task group is working towards definition of a MIMO physical layer.
Table II summarizes the status of the IEEE 802.11 standards family, including the draft versions and those that are still at task group development status.

Table II. IEEE 802.11 standards family.

Standard	Description	Status
IEEE 802.11	WLAN; up to 2 Mb/s; 2.4 GHz	Approved 1997
IEEE 802.11a	WLAN; up to 54 Mb/s; 5 GHz	Approved 1999
IEEE 802.11b	WLAN; up to 11 Mb/s; 2.4 GHz	Approved 1999
IEEE 802.11g	WLAN; up to 54 Mb/s; 2.4 GHz	Approved 2003
IEEE 802.11e	New coordination functions for QoS	Task group development
IEEE 802.11f	IAPP (Inter-AP Protocol)	Approved 2003
IEEE 802.11h	Use of the 5 GHz band in Europe	Approved 2003
IEEE 802.11i	New encryption standards	Approved 2004
IEEE 802.11n	MIMO physical layer	Task group development

2.2.2 Basic operation

When powered on, a Wi-Fi station will scan the available channels to discover active networks where beacons are being transmitted. It then selects a network, be it in ad hoc mode or infrastructured. In the latter case, it authenticates itself with the access point and then associates with it. If WPA security is implemented, a further authentication step is done, after which the station can participate in the network. Wi-Fi provides for different degrees of quality of service, ranging from best effort to prioritised and, in infrastructured networks, guaranteed services. While being part of a network, stations can keep discovering new networks and may disassociate from the current one in order to associate with a new one, e.g. because it has a stronger signal. Stations can roam this way between networks that share a common distribution system, in which case a seamless transition is possible. A station can sleep to save power, and when it finishes infrastructured mode operation it can deauthenticate and disassociate from the access point.

2.2.3 Protocol overview

A Wi-Fi WLAN (Wireless LAN) is based on a cellular architecture; each cell is called a *Basic Service Set* (BSS). A BSS is a set of mobile or fixed Wi-Fi stations. Access to the transmission medium is controlled by means of a set of rules called a *coordination function*. Wi-Fi defines a *Distributed Coordination Function* (DCF) and a *Point Coordination Function* (PCF), the latter being optional.
The simplest network configuration is the *IBSS* (Independent BSS), which implements an ad hoc network topology comprising at least two stations: no structure exists, so creating a multihop network requires higher-level protocols. Alternatively, an infrastructured BSS may be part of a wider network, the so-called *extended service set* (ESS). An ESS is a set of one or more infrastructured BSSes connected via a *Distribution System*, whose nature is not specified by the standard: it could be a cabled network, or some other type of wireless network; 802.11f will specify the Inter-AP Protocol. The stations connected to the Distribution System are called *Access Points* (AP). Services offered by the stations fall into two classes: *station services* and *distribution system services*. The latter are offered by the APs, and allow data transfer between stations belonging to different BSSes. The standard also defines the functions of the *Portal*, which is a bridge for interconnecting a Wi-Fi WLAN

with a generic IEEE 802.x LAN. Figure 5 illustrates all the typical components of a Wi-Fi network.

The available bandwidth is divided into 14 partially overlapping channels, each 22 MHz wide. Only 11 of these channels are available in the US, 13 in Europe, and just 1 in Japan. All the devices in the same BSS (either infrastructured or ad hoc) use the same channel. One of three techniques is used for multiplexing: a) the *Direct Sequence Spread Spectrum (DSSS*), which uses a Barker sequence, is adopted for the 1 and 2 Mb/s signal rates; b) the *Complementary Code Keying (CCK*), defined in 802.11b, is used for the 5.5 and 11 Mb/s signal rates; and c) the *Orthogonal Frequency Division Multiplexing (OFDM)*, defined in 802.11a and also used in 802.11g, which is used for 6, 9, 12, 18, 24, 36, 48 and 54 Mb/s. Other optional multiplexing schemes are defined in the standard, but we will not mention them here.

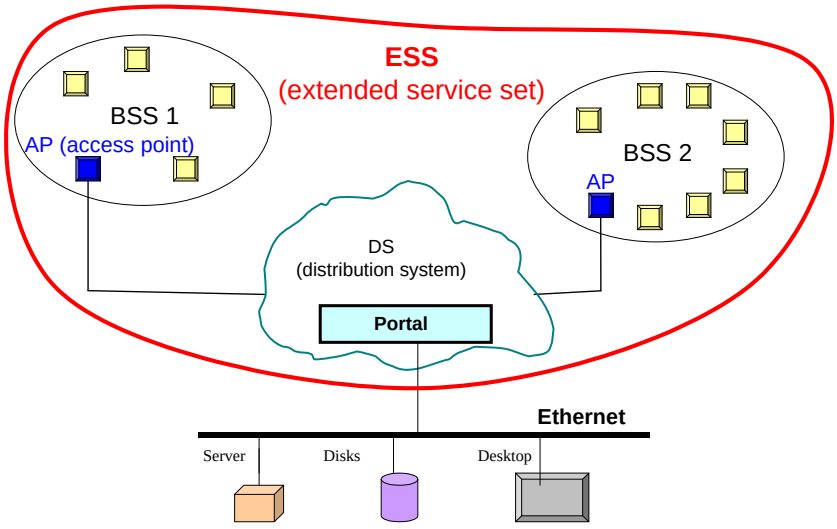

Figure 5. Typical components of a Wi-Fi network.

DSSS uses an 11-bit Barker sequence, so each sequence of 11 chips codifies a single information bit. The modulation rate is 1 Msymbol/s using either BPSK (Binary Phase Shift Keying) or QPSK (Quadrature Phase Shift Keying), for transmission rates of 1 or 2 Mb/s, respectively. With CCK, a 16-bit sequence transmitted on the channel codifies either 4 or 8 information bits. The modulation is QPSK at 1.375 Msymbol/s, for signal rates of either 5.5 or 11 Mb/s. Note that in both DSSS and CCK cases the chip rate is 11 Mchip/s, which means that the lowest layer of the radio section is the same; the difference lies in the modulation and multiplexing. OFDM uses a comb of 52 sub-carriers (48 for data) with a spacing of 0.3125 MHz and a symbol duration of 4 μs, for a total of 12 Msymbol/s. Each symbol is protected with a convolutional code of either 3/4, 2/3 or 1/2 rate, using MQAM modulation (M-ary Quadrature Amplitude Modulation) with M being 2, 4, 16 or 64. The resulting combinations provide signal rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mb/s.

The fundamental Wi-Fi MAC protocol, which must be implemented by every station, is called Distributed Coordination Function (DCF). DCF is a CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) channel access method, used in both ad hoc and infrastructured networks. Once a station senses that no other station has transmitted for a short time, called Inter Frame Space (IFS), it transmits a frame. For unicast transmissions, the

receiving station replies with an ack; if the transmitter does not hear the ack, it will retransmit the frame up to a maximum number of times before giving up: this is a standard ARQ mechanism. When a station must send a new frame just after having sent one, it first waits for an IFS, then it initializes a *random backoff interval counter* and starts decrementing it at a fixed rate while listening to the channel. If it detects that another station is transmitting, it stops decrementing the counter, waits for the end of the current transmission, waits for one IFS time, and starts decrementing the counter from where it had left: this is called a *backoff* procedure. A backoff procedure ends when the backoff counter reaches zero, at which point a frame is sent. A station enters a backoff procedure even when it wants to transmit a frame, but detects that the channel is busy.

As a variation in the basic DCF access method, stations may optionally use an RTS/CTS (request to send/clear to send) mechanism, which is useful for reducing the number of collisions where hidden terminals are present. To understand that, let's suppose that stations A and C are both in view of station B, but they do not see each other, either because they are too far apart, or because there is an obstacle between them. In this case, when both A and C transmit data to B, they will often collide, because neither will sense the transmission of the other, and neither will back off. To reduce the chance of collision, the transmitting station (say A) first sends an RTS, a very short frame asking permission to transmit, and the receiving station (say B) responds with a CTS, meaning it is ready to listen. Station C does not hear the RTS, but it hears the CTS, so it defers transmission. Since an RTS is shorter than a data frame, chances of a collision are reduced.

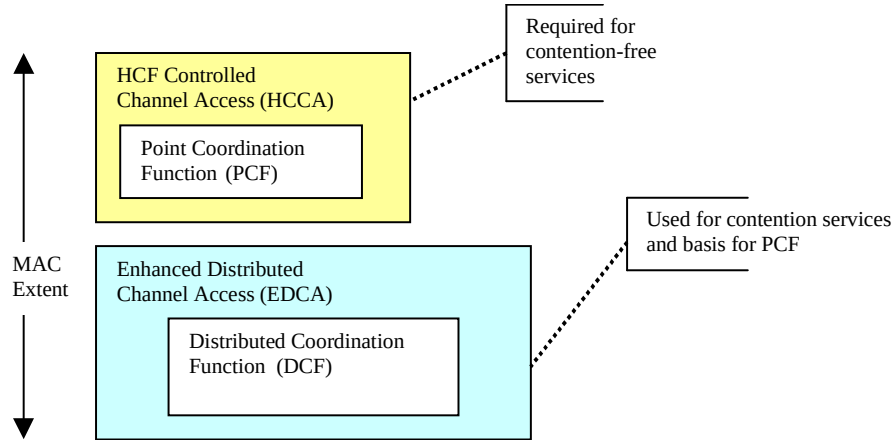

Figure 6: Wi-Fi MAC access modes (Coordination Function).

Wi-Fi defines an *optional* medium access protocol called *Point Coordination Function* (PCF), which can be used in an infrastructured topology only. Figure 6 depicts the roles of DCF and PCF in the Wi-Fi MAC, together with the new EDCA and HCCA coordination functions described below.

The *Point Coordinator* (PC), a function normally performed by the AP, uses a round-robin policy to poll each station for data to be transmitted. PCF can be used to implement a contention-free (CF) access mechanism, in the sense that the PC controls the access of the stations, thus avoiding any contention. The Wi-Fi standard states that the two methods (DCF and PCF) must coexist: when in a BSS a PC is present, PCF and DCF alternate, thus creating a contention-free period (CFP) followed by a contention period (CP). It is optional for an AP to act as a PC, and it is optional for a station to implement the possibility of replying to the PC's requests during the CFP. The stations that implement this facility are referred to as *CF-*

pollable stations. The standard requires that a CP must always be present, lasting sufficiently to transmit at least a complete frame sequence, in order to allow the transmission of management frames. Figure 7 shows how the DCF and PCF methods alternate: B indicates the reference *beacon* sent by the PC, at the start of each CFP, for synchronization purposes, which contains important information relevant to the CFP; NAV (*network allocation vector*) is a counter set by the station to compute the expected end of the current transmission.

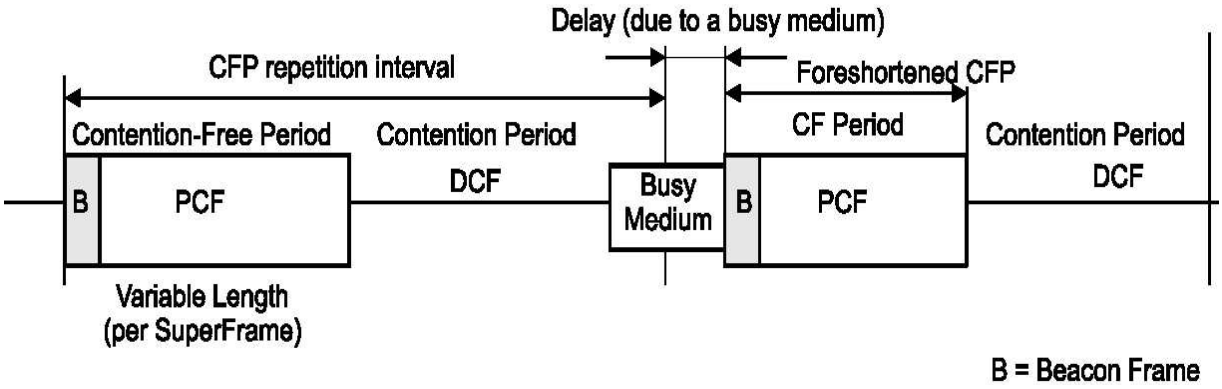

Figure 7: How PCF and DCF alternate[2].

The PCF, as described in the standard, has many drawbacks [9]; in fact, it is not implemented in any commercial device. The IEEE 802.11e amendment corrects this situation by redefining the QoS aspects of the multiple access protocol. The new coordination functions are called EDCA (*enhanced distributed channel access*) and HCCA (*HCF controlled channel access*), which together constitute the new HCF (*hybrid coordination function*). The new mechanisms can interoperate with the old ones.
EDCA provides 8 different priority levels for data. Each station keeps different queues, and the priority on the channel is implemented via different IFS (interframe space) values: higher priority queues use a shorter IFS, thus gaining preferential access to the channel. In addition, backoff times are shorter for higher priority traffic, and collisions result in preemption of the channel by the highest-priority colliding transmitter.
In HCCA, one of the stations has the role of Hybrid Coordinator (HC). Thanks to centralized control, EPCF provides hard guarantees expressed in terms of service rate, delay and jitter [10].

The Wi-Fi specification security framework is called *wireless equivalent privacy* (WEP) protocol. An important component of WEP is the use of the stream cipher RC4, which is well known and widely used; unfortunately, its implementation in Wi-Fi is of questionable quality [11]. Because of the nature of a wireless packet network, which will frequently drop packets, it is not easy to maintain synchronization between the encryptor and the decryptor for any length of time. To overcome this limitation, WEP uses a 24-bit initialisation vector to generate the cipher key stream on each packet. Since the initialisation vector is so short, eavesdropping on a busy network makes it possible to break the cipher in a reasonable length of time [12].
In late 2002 the Wi-Fi Alliance defined WPA (Wireless Protected Access), a notable improvement over WEP intended as an intermediate step while the 802.11i specifications

[2] Reproduced from the IEEE 802.11 standard, page 87.

were being worked out. WPA uses the 802.1X/EAP framework with TKIP (Temporal Key Integrity Protocol) for the cipher suite and an EAP (Extensible Authentication Protocol) method for authentication or alternatively preshared keys for implicit authentication; it is widely implemented in currently marketed devices.
In mid-2004 the 802.11i working group finalized an amendment providing a comprehensive authentication framework based upon 802.1X and EAP methods, also known as WPA2. Different EAP methods can be used for authentication and key material generation based upon different application needs, ranging from user names and passwords to certificates and smart cards. The 802.11i amendment also defines two cipher suites, TKIP, which can be implemented as a software upgrade on existing equipment, and CCMP (based upon AES), which requires new equipment to support the computationally complex AES encryption algorithm. TKIP uses a key mixing function to generate per-frame WEP keys and a 48-bit initialisation vector, rather than the 24-bit vector used by WEP.

3 COSTS AND POWER CONSUMPTION

Bluetooth is intended for portable products, short ranges, and limited battery power. Consequently, it offers very low power consumption and, in some cases, will not measurably affect battery life. On the other hand, Wi-Fi is designed for longer-range connections and supports devices with a substantial power supply. On the average, a typical Bluetooth device absorbs from about 1 to 35 mA, while a Wi-Fi device typically requires between 100 and 350 mA. This dramatic difference makes Bluetooth the only practical choice for mobile applications with limited battery power. On the other hand, when greater ranges are needed and power consumption is less of an issue, Wi-Fi is usually the best solution.
In this section two wireless products for which detailed characteristics are publicly available, one for Bluetooth and one for Wi-Fi, are briefly presented as an example and compared in terms of power consumption and costs.

3.1 CSR BLUECORE ARCHITECTURE FOR BLUETOOTH

The CSR (Cambridge Silicon radio) designs and produces single-chip CMOS units for Bluetooth devices. Available chipsets include the Bluecore01 and Bluecore02, both of which implement the baseband and radio levels in the Bluetooth stack; their specifications are publicly available.
In Bluecore01 a flash memory may be added containing the firmware which implements the Link Controller, the Link Manager and the Host Controller Interface levels, and may optionally include the Logical Link Control level, the Adaptation Protocol, the RFCOMM protocol for the serial ports, and the Service Discovery Protocol (SDP). Bluecore02 gives some more options, such as including the flash memory in the chip, and requires about half the power.

3.1.1 Power management in Bluetooth

Two main states are defined for Bluetooth devices:
1) *Standby*: no data are exchanged, only the clock is running.
2) *Connection*: each device is connected with the master of the piconet. Four sub-states are possible:
   - *Active mode*: the device is active in the piconet.
   - *Sniff mode*: this is a low-power-consumption state as the listening activity is working during the sniff slots only.

- *Hold mode*: the ACL traffic of a device is stopped for a certain period.
- *Park mode*: the device is no longer a member of the piconet, but it remains synchronized with the master of the piconet; this is the lowest power-consuming state.

3.1.2 Power management in the Bluecore chipset

The Bluecore family chips offer two low-power modes:

- Shallow Sleep mode: the processor clock is reduced, which reduces the current absorption to 2 mA for the 01 chips, and a little less for the 02 chips.
- Deep Sleep mode: most of the chip's circuits are switched off, which reduces the current absorption to 100 μA for the 01 series and even less for the 02 family. About 10 ms are necessary to enter or exit this mode. This mode can be used only if no SCO link is active and all the ACL links are in one of the power save modes (Hold, Sniff, Park). Some other restrictions are imposed, e.g. the PCM port must be inactive, no USB connections must be active, and UART connections are forced to close.

3.1.3 Costs for the Bluecore chipset

The Bluecore02-External chipset costs 70 USD for five units. Table III shows the current absorbed by the CSR Bluecore01 chip and by the Bluecore02-External chip [13].

Table III. Power save modes in the Bluecore01 and Bluecore02-External chipsets.

Operation mode	**VDD=3.0V Temp. =20^0 C average**	**VDD=3.0V Temp. =20^0 C peak**	**VDD=1.8V Temp.=20^0 C average**
SCO connection HV3 (1 s interval sniff mode) (Slave)	41 mA		
SCO connection HV3 (1 s interval sniff mode) (Master)	42 mA		
SCO connection HV3 (40 s interval sniff mode) (Slave)			26 mA
SCO connection HV3 (40 s interval sniff mode) (Master)			26 mA
SCO connection HV1 (Slave)	78 mA		53 mA
SCO connection HV1 (Master)	77 mA		53 mA
ACL data transfer 115.2 kb/s UART (Master)	29 mA		15.5 mA
ACL data transfer 720 USB (Slave)	81 mA		53 mA
ACL data transfer 720 USB (Master)	82 mA		53 mA
Peak current during RF burst		135 mA	
ACL connection, Sniff mode 40ms interval, 38.4 kb/s UART	5.5 mA		40 mA
ACL connection, Sniff mode 1.28 ms interval, 38.4 kb/s UART	1.1 mA		0.5 mA
Parked Slave, 1.28 ms interval, 38.4 kb/s UART	1.1 mA		0.6 mA
Standby mode (connected to host, no RF activity)			0.047 mA
Deep sleep mode	0.09 mA		0.02 mA

3.2 WI-FI INTERSIL PRISM ARCHITECTURE

Intersil Corp. has been one of the major hardware producers for the development of Wi-Fi devices[3], in all its versions. Intersil is descended from Harris semiconductors which, together with Lucent Technologies, proposed the modifications to the Wi-Fi standard from which the 802.11b amendment was derived. The Intersil Wi-Fi business was sold to GlobespanVirata, which was then acquired by Conexant. We consider the Intersil Prism architecture because

[3] In 2001, Intersil controlled about 66% of the world market in the manufacture of IEEE 802.11b chipset. (http://www.intersil.com/)

data sheets for the chipsets were publicly available. Both the PHY and the MAC layers are implemented for Wi-Fi devices. The Prism 2 chipset is composed of:

- a baseband/MAC (ISL 3871) processor with the following characteristics:
  - USB 1.1 interface
  - Firmware that realizes all the functions provided by the 802.11b standard
  - Active autonomous scan
  - Base band DSSS processor
  - DBPSK and DQPSK modulations
  - CCK multiplexing and Barker sequence
  - Integrated A/D and D/A converters for AGC (automatic gain control) and transmission power adaptive control
- an RF amplifier (ISL 3984)
- a VCO (Voltage Controlled Oscillator) (ISL 3084)
- a chip to feed the radio level (ISL 3684).

The following presents an overview of the provisions of the Wi-Fi standard on the topic of power management, and a comparison of these is made with what the Prism chipset offers on this topic.

3.2.1 Wi-Fi power management

A Wi-Fi device may be in either of the *Awake* or *Doze* states. In the Doze state the station cannot either transmit or receive, which reduces the power consumption. Consequently, there are two Power management modes: *Active mode* (AM), and *Power save mode* (PS). The handling of the stations in PS mode differs according to the topology of the Wi-Fi network as follows.

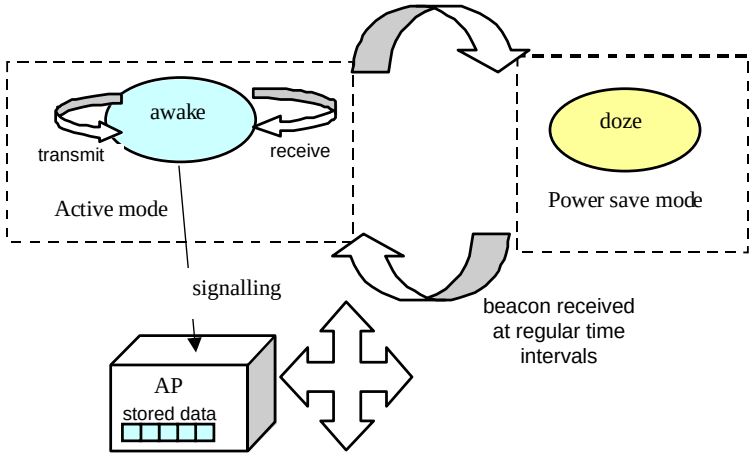

Figure 8. Power handling states in an infrastructured Wi-Fi device.

Infrastructured network: a station in AM which wants to pass in PS must signal the AP (access point) by using the power management bit in the header of its packets. The AP stores all the traffic addressed to stations that are in PS mode; when transmitting the periodic beacon, the AP sends the list of the stations in PS mode and whether it has traffic queued for them. At regular and configurable time intervals, the stations in PS switch to AM in order to

receive the beacon. If there is traffic addressed to them, the stations can receive it and then return to PS. Figure 8 illustrates this situation.

Ad hoc network: stations can use the PS mode, but the task of storing the traffic addressed to them is distributed among all the active stations, since no AP exists. All stations in PS mode switch to Awake state in a temporal window (ATIM window) during which the stations that have traffic stored for others send special frames (ATIM frames). If a station receives an ATIM frame addressed to it, it remains in Awake state in order to receive its traffic; otherwise, the station returns in PS mode until the next ATIM window is started.

Note that:

b) Due to the absence of a reference station such as the AP, the instantaneous state of a station (awake or doze) can only be estimated by all the other stations of the ad hoc network, for example according to the history of the past transmissions. In this topology, the standard does not specify any methodology for estimating the power state of the stations.

c) The transmission and reception of the ATIM frames during the ATIM window occur according to DCF rules, i.e. according to the CSMA/CA access method. It means that a station could receive an ATIM frame addressed to itself, wait for the data, and yet not receive them because of congestion on the shared channel.

In conclusion, the Wi-Fi standard specifies only one low-power state, i.e. the Doze state.

3.2.2 Power management in the Prism chipset

The chipset of the Prism family has largely been used for the development of wireless cards, available for several buses: PCI, PCMCIA, USB and CompactFlash.

The first generation Prism chipsets [14] offers several power-saving modalities, which the MAC selects on the basis of the time interval between two consecutive Awake periods. The chipsets of the Prism 2 and Prism 3 families reduce the power consumption. Table IV summarizes the publicly available data for the Prism 2 family.

Table IV. Power save modes in the Prism chipset.

Mode	Time spent				Power consumption
	in TX	in RX	in Power Save	to return active	
TX (continuous)	100%	-	-	-	488 mA (Prism 1) 325 mA max (Prism 2)
RX (continuous)	-	100%	-	-	287 mA (Prism 1) 215 mA max (Prism 2)
Average current consumption without Power save	2%	98%	-	-	290 mA (Prism 1) 187 mA (Prism 2)
Average current consumption with Power save	2%	8%	90% (mode 4)	-	50 mA (Prism 1) 43 mA (Prism 2)
Power Saving mode 1	-	-	100%	1 μs (Prism 1)	190 mA (Prism 1)
Power Saving mode 2	-	-	100%	25 μs (Prism 1)	70 mA (Prism 1)
Power Saving mode 3	-	-	100%	2 ms (Prism 1)	60 mA (Prism 1)
Power Saving mode 4	-	-	100%	5 ms (Prism 1)	30 mA (Prism 1) 25 mA (Prism 2)

3.2.3 Costs for the Prism chipsets

The Prism 3 kit costs about 40 USD in sets of 500 units, and includes:

- ISL3084 (SiGe VCO)
- ISL3684 (transceiver, direct Up/Down converter, single chip PHY)

- ISL3871 (integrated baseband processor/MAC for USB/PCMCIA, 11 Mb/s DS controller)
- ISL3984 (SiGe RF power amplifier, 2.4 GHz-2.5 GHz, +18 dBm with detector, MLFP package)
- ISL3872 (integrated baseband processor/MAC for mini-PC, 11 Mb/s DS controller).

4 BLUETOOTH AND WI-FI COMPARISON

In this section, we will compare the two protocols, focusing particularly on the following items:

- the spectrum used, modulation characteristics and interference problems;
- power requirements;
- characteristics of the network topology, particularly with regard to the possibility of extending the basic cells, to interconnect with other network types, and routing problems;
- the ability to create an efficient network, particularly with regard to the maximum number of terminals which can be handled in a basic cell, the creation speed of the networks, and how the networks are created and maintained;
- the characteristics of the links among the devices of a single basic cell, and the maximum attainable throughput;
- security;
- the ability to offer a given quality of service.

4.1 RADIO COMMUNICATION

At the physical level we only consider radio frequency links, and do not describe the infrared transmission methods defined for Wi-Fi, since no infrared commercial device has ever hit the market.

4.1.1 Radio bandwidth, bandwidth usage, modulation

Both protocols use a spread spectrum technique in the 2.4 GHz band, which ranges from 2.4 to 2.4835 GHz, for a total bandwidth of 83.5 MHz. Wi-Fi can also use the 5 GHz band. Bluetooth uses frequency hopping (FHSS) with 1 MHz wide channels, while Wi-Fi uses different techniques (DSSS, CCK, OFDM) with about 16 MHz wide channels. Frequency hopping is less sensitive to strong narrow band interference that only affects a few channels, while DSSS is less sensitive to wide-band noise. Both standards use ARQ at the MAC level, i.e., they retransmit the packets for which no acknowledgement is received. Since Wi-Fi always uses the same frequency, retransmitted packets only benefit from time diversity, while Bluetooth also takes advantage of frequency diversity, because of the frequency hopping. Future radio layers will likely use UWB for Bluetooth and MIMO for Wi-Fi.

4.1.2 Noise adaptation

Both protocols allow for different levels of protection from noise: Wi-Fi uses several modulation, coding and multiplexing techniques corresponding to signal rates ranging from 1 to 54 Mb/s, while Bluetooth uses a fixed signal rate of 1 Mb/s and several coding rates. Both protocols can exploit this flexibility in order to adapt to changing radio conditions, but the standards do not specify any algorithm for switching the signal and coding rates, so that implementers are free to choose their own. While the adaptation is done at the physical layer

in Wi-Fi, and as such it is transparent to higher layers, in Bluetooth this is done at the Link Layer.

4.1.3 Interference

Both technologies suffer from interference from other devices operating in the same radio bands. The 5 GHz band used by IEEE 802.11a is also used by 5 GHz cordless phones, while the 2.4 GHz band used by both Bluetooth and IEEE 802.11g is crowded with microwave ovens, HomeRF devices and 2.4 GHz cordless phones. While both standards are inherently resistant to interference, their very success is making the problem worse than it was during their emergence. The IEEE 802.11 Coexistence Task Group 2 and the Bluetooth SIG Coexistence Working Group are addressing this matter with the aim of making the Wi-Fi and the Bluetooth standards coexist peacefully. An outcome of this work is the proposed *adaptive frequency-hopping scheme* for Bluetooth, which would permit Bluetooth radios to identify and avoid the frequencies used by nearby Wi-Fi system and increase throughput while minimizing, or eliminating, interference for both systems. Another is *transmit power control*, which is being handled in IEEE 802.11h.

4.1.4 Traffic sensitivity

The aggregate throughput of a Piconet is independent of the traffic offered, because the access is centrally arbitrated. Conversely, the aggregate throughput on a BSS is dependent on the traffic offered, due to the distributed CSMA/CA technique, which uses collisions as a means of regulating access to the shared medium. Efficiency in a BSS is lower at higher load, while it is constant in a Piconet.

4.1.5 Transmission power

Both protocols define power limitations for the devices, according to the limits imposed by the various telecommunications regulator bodies.
Table V summarizes the power limitations for Bluetooth. Most devices on the market are intended to replace short cables: they have fixed output power and usually fall into Class 1. Devices intended for general communications generally fall into Class 2 or Class 3 and have variable output power.

Table V. Power classes of Bluetooth devices.

Power class	Maximum output power	Nominal output power	Minimum output power
Class 1	100 mW (20 dBm)	NA	1 mW (0 dBm)
Class 2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)
Class 3	1 mW (0 dBm)	NA	NA

The Wi-Fi standard mandates that all devices must allow for different power level settings. Most devices on the market provide an EIRP between 30 and 100 mW, that is, between 15 and 20 dBm. Many have fixed output power level, while others are able to programmatically adjust the output power.

4.2 NETWORK SIZE

The maximum number of devices belonging to the network' s building block, i.e. the Piconet for Bluetooth and the BSS for Wi-Fi, is 8 (7 slaves plus one master) for a Piconet, 2007 for a structured BSS, and unlimited for an IBSS. Up to 255 Bluetooth slaves can be put in *park*

mode, a state where they do not participate in data exchanges while keeping synchronization with the master's transmissions. Both protocols have a provision for more complex network structures, built from the respective basic blocks: the ESS for Wi-Fi and the Scatternet for Bluetooth.

4.3 SPATIAL CAPACITY

We define *spatial capacity* as the ratio between aggregated data transfer speed and transmission area used. Bluetooth, in a nominal range of 10 m, allows the allocation of 20 different Piconets, each with a maximum aggregate data transfer speed around 400 kb/s [15]. Wi-Fi allows interference-free allocation of 4 different BSSes, each with aggregate transmission speed of 910 kb/s in a nominal range of 100 m, or 31.4 Mb/s in a nominal range of 10 m. Thus, spatial capacities can be evaluated for 802.11g at roughly 0.1 kb/s·m^2 at minimum speed or 400 kb/s·m^2 at maximum speed, and 25 kb/s·m^2 for Bluetooth. It is important to notice that these numbers are intended as a guideline only, since in real cases other factors, such as receiver sensitivity and interference, play a major role in affecting the attainable data transmission speed.

4.4 PACKETIZATION, FEC AND THROUGHPUT

Bluetooth datagram payloads (ACL links) are protected by a 16-bit CRC, while stream payloads (SCO links) are not; all headers are protected by an 8-bit CRC. Different FEC types can be applied to Bluetooth packets: no FEC, a 1/3 and a 2/3 (a shortened Hamming code) FECs are available. A SCO packet has fixed length, fitting a single slot, and a fixed 64 kb/s throughput with fixed packet lengths of 10, 20 or 30 bytes. An ACL packet fits into 1, 3, or 5 slots. The payload lengths are fixed, ranging from 17 to 339 bytes, with symmetric throughput ranging from 108.8 to 433.9 kb/s, and asymmetric throughput going up to 732.2 / 57.6 kb/s.

Table VI. Maximum data transfer speeds for Wi-Fi.

Signal rate	Multiplexing	CSMA/CA	RTS/CTS
1 Mb/s	DSSS	0.91 Mb/s	0.87 Mb/s
2 Mb/s	DSSS	1.71 Mb/s	1.56 Mb/s
5.5 Mb/s	CCK	3.87 Mb/s	1.77 Mb/s
11 Mb/s	CCK	6.06 Mb/s	4.52 Mb/s
6 Mb/s	OFDM	5.40 Mb/s	5.13 Mb/s
12 Mb/s	OFDM	10.1 Mb/s	9.43 Mb/s
24 Mb/s	OFDM	17.8 Mb/s	16.1 Mb/s
54 Mb/s	OFDM	31.4 Mb/s	26.7 Mb/s

Wi-Fi packets are variable in length, with payload size ranging from 0 to 2304 bytes; they are protected by a 32-bit CRC. The maximum theoretical one-way data throughput between two hosts (no collisions) with 1500 bytes-long packets in an interference-free environment is shown in Table VI [16]. In [17] it is shown that for the average Internet mix of IP packet sizes and supposing a fixed network rate of 11 Mb/s, the expected data rate is around 3 Mb/s with CSMA/CA and 2 Mb/s with RTS/CTS.

4.5 NETWORK TOPOLOGIES

Let us consider different topology configurations. In some cases, a direct comparison is possible between the cases of Bluetooth and Wi-Fi, while other configurations have no counterpart.

4.5.1 Piconet versus infrastructured BSS

The Bluetooth *Piconet* and the *infrastructured BSS* topology in Wi-Fi show many analogies. In both cases, traffic is handled by a central unit, called the *master* in Bluetooth and AP in Wi-Fi, respectively. The difference is that in the Piconet the master always regulates the channel access of the slaves, while the corresponding Wi-Fi function is not currently implemented; this may change with the advent of 802.11e devices. In these topologies, the master (or the AP) is responsible for routing packets between stations. The maximum number of slave units is 7 in Bluetooth, 2007 in Wi-Fi; the nominal range is 10 m in Bluetooth, 100 m in Wi-Fi. Connection with external networks is defined for Bluetooth by the LAN Access Profile, while a Wi-Fi AP is structurally able to act as a bridge.

4.5.2 Scatternet versus IBSS

Topological analogies can also be found between the Bluetooth *Scatternet* configuration and the Wi-Fi ad hoc *IBSS*. They are both ad hoc networks, with a dynamically variable topology. One difference is that the Scatternet has substructures, called Piconets, while the IBSS has a flat structure. Both need a global addressing mechanism and a routing mechanism in order to ensure global connectivity among the stations. In Wi-Fi, a global addressing mechanism exists, since the devices are identified by a MAC 802 address. Bluetooth does not provide any global addressing, which should then be provided by upper-layer protocols, for example at the IP level. As far as packet routing is concerned, neither standard specifies any mechanism for routing the packets inside the Scatternet or the IBSS. Since these topologies are dynamic, the major problems are related to nodes joining and leaving the network and to link breaks caused by moving terminals and obstacles. In an IBSS, these events do not cause any modifications in the flat structure of the ad hoc network, while in a Scatternet both may trigger a reorganization of the underlying Piconets, and a change in the Scatternet structure.

4.5.3 ESS and LAN Access Profile

The *ESS* defined in Wi-Fi has no analogous Bluetooth concept, unless a structure is built where two or more Piconets implementing the LAN Access or PAN (personal area network) profiles are interconnected to an external network, for example to a cabled LAN.

4.6 DISCOVERY AND ASSOCIATION

Bluetooth uses an *Inquiry procedure* and a *Page scheme* for discovering new devices in the coverage area and establishing new connections. The Inquiry procedure is periodically initiated by the master device to discover the MAC addresses of other devices in its coverage area. The master device uses a Page scheme to insert a specific slave in the Piconet, by using the slave's MAC address and clock, collected during the Inquiry procedure. In order to set up a Piconet with the maximum number of active slave devices (seven), an average time of 5 s for the Inquiry phase, and 0.64 s for each Page phase ($0.64 \cdot 7 = 4.48$ s) are necessary, thus requiring a maximum of 9.48 s. We consider no external interference.

Wi-Fi uses the *Scan, Authentication,* and *Association* procedures. The *Scan* procedure (whether in active or passive mode) is used for discovering the MAC addresses and other parameters of the Wi-Fi devices in the terminal's coverage area. In passive mode, the average time of the Scan procedure is 50 ms multiplied by the number of channels to probe. In active mode, the device sends a *probe request* frame and waits for a *probe response* from the stations that received the probe request. In this case the minimum discovery time, without external interference, in a network far from saturation, is equal to the time needed to transmit a probe request plus a DCF Inter Frame Space interval, plus the transmission time of a probe response, multiplied by the number of channels to probe, that is, 3 ms at 1 Mb/s or 0.45 ms at 11 Mb/s.
In Wi-Fi ad hoc networks, the Authentication procedure is optional. In an infrastructured network, once a device has discovered the access point by means of the Scan procedure, it must perform *Authentication* with the access point and then the *Association*. Once the association with the AP is made, the station can communicate with stations in other BSSes that are known by the AP, even if these stations are not in its coverage area but are in the AP's coverage area. WEP defines two Authentication procedures, discussed in Section 4.7, which require an exchange of either two or four frames between the station and the AP. After Authentication comes the Association phase, where a station sends an *Association Request* to the AP, waiting for an *Association Response*. This operation lasts as long as it takes to send a frame and to receive the response, exactly as during the active scan phase.

4.7 AUTHENTICATION

Both protocols support authentication at the link level for granting network access to the devices; user authentication is typically carried out at a higher level.
Bluetooth provides a method for authenticating the devices by means of a shared secret, called a *link key*, between the two devices. This link key is established in a special communication session called *pairing*, during which the link key is computed starting from the address of each device, a random number, and a shared secret (PIN). If both parts must be authenticated, then the procedure is repeated in both senses. The shared secret can be manually entered the first time that the devices are used, or it can be hardwired for paired devices that are always used together. Pairing is a useful feature for devices that are usually used together.

Wi-Fi defines two authentication methods: OSA (Open System Authentication) and SKA (Shared Key Authentication), the latter being usable only if the stations implement the WEP protocol. In OSA mode, the requesting station sends a frame to the AP asking for authentication and the AP always grants authentication; two frames must be exchanged between the stations. This method provides no security and is the simplest for open Access Points.
In SKA mode, the requesting station (initiator) sends a frame to the AP asking for authentication; the AP (authenticator) sends a 128-byte clear text, which the initiator encrypts by using a shared secret and sends back to the AP. Encryption is performed by XORing the challenge with a pseudo-random string formed by the shared secret and a public initialization vector. The AP decrypts the text and confirms or denies authentications to the requester, for a total number of four exchanged frames. This is a shared-secret authentication analogous to the one used in Bluetooth.
With the 802.1X authentication scheme used by WPA, more frames are exchanged after Association, for a total of seven frames exchanged between the station and the AP, plus a

total of four packets exchanged between the AP and a RADIUS authentication server. This authentication scheme requires an external authentication server. However, with 802.11i WPA2, it promises power and flexibility: if a vulnerability is discovered in an EAP a different method can be used both in the stations and in the RADIUS server; no changes in the AP or the protocol are required.

4.8 ENCRYPTION

While wiretapping in a wired network requires physical intrusion, wireless data packets can be received by anyone nearby, with an appropriate receiver. This is why both the Bluetooth and Wi-Fi technologies use data encryption in lower network layers.
Bluetooth adopts the E0 stream cipher. For each session, a unique encryption key is generated, from which per-packet keys are derived in a way that avoids their frequent reuse. This is a superior method with respect to the WEP protocol used in Wi-Fi, even if it has its own weaknesses [18]. Recent Wi-Fi devices based on WPA encryption are much harder to break, and future devices based on the 802.1X/EAP framework (WPA2) will allow choosing among different strength algorithms.

4.9 QUALITY OF SERVICE

In Bluetooth QoS for asynchronous service (ACL links) is requested in terms of long-term data rate, bucket size (which defines the maximum size of a burst of data), peak data rate, latency and jitter; in principle these parameters allow sophisticated channel admission control and scheduling policies. Bluetooth also provides for synchronous constant bit rate services (SCO links).
The 802.11e draft standard is going to define similar provisions for QoS, by using sophisticated flow descriptions (ECDF) and guaranteed-rate services (EPCF), but the details are still being worked out.

4.10 A SIDE-BY-SIDE SUMMARY

Table VII summarizes the main differences between the two protocols. Table VIII compares power consumption for some example chipsets.

Table VII. A comparison of the Bluetooth and Wi-Fi protocols.

	Bluetooth	**Wi-Fi**
Frequency band	2.4 GHz	2.4 GHz, 5 GHz
Coexistence mechanism	Adaptive frequency hopping	Transmit power control
Multiplexing	FHSS	DSSS, CCK, OFDM
Future multiplexing	UWB	MIMO
Noise adaptation	link layer	physical layer
Typical output power	1-10 mW (1-10 dBm)	30-100 mW (15-20 dBm)
Nominal range	10 m	100 m
Max one-way data rate	732 kb/s	31.4 Mb/s
Basic cell	Piconet	BSS
Extension of the basic cell	Scatternet	ESS
Topologies	Various analogies: see Subsection 0	
Max number of devices in the basic cell	8 active devices; 255 in park mode	Unlimited in ad hoc networks (IBSS); up to 2007 devices in infrastructured networks.
Maximum signal rate	1 Mb/s	54 Mb/s
Channel access method	centralised: polling	distributed: CSMA/CA
Channel efficiency	Constant	Decreasing with offered traffic
Spatial capacity	From 0.1 to 400 kb/s·m^2	About 15 kb/s·m^2
Data protection	16-bit CRC (ACL links only)	32-bit CRC

	Bluetooth	**Wi-Fi**
Procedures used for the network setup	Inquiry, Page	ad hoc networks: Scan, Authentication infrastructured: Scan, Authentication, Association
Average speed in network setup without external interferences	5 s + n·1.28 s, where n is the number of slaves in the Piconet, ranging from 1 to 7	n·c·1.35 ms for an unsaturated network, c probed channels ($1 \le c \le 13$), n stations (excluding the AP), active scan, infrastructured topology
Authentication	Shared secret, pairing	Shared secret, challenge-response
Encryption	E0 stream cipher	RC4 stream cipher
QoS mechanism	link types	coordination functions
Typical current absorbed	1 - 35 mA	100 - 350 mA
Power save modes	Sniff, Hold, Park; Standby	Doze

4.10.1 Power needs

As shown in Table VIII, the power requirements of Bluetooth devices are significantly lower than those of Wi-Fi devices, which was to be expected. As an example, we report two possible utilization scenarios in order to compare the performance of the devices analyzed with respect to the power consumption.
Table VIII compares the currents absorbed by the different chipsets in two different cases. In the first case (continuous mode) the stations send or receive traffic at the maximum possible rate; in the second case the stations support a single 64 kb/s connection where a device spends 1% of the time transmitting, 49% of the time receiving, and the rest of the time sleeping. For Bluetooth, the appropriate SCO links are considered, while for Wi-Fi we assume 250 packets per second, each with a 256-bit payload. Since packets are received or transmitted every 4 ms, only power-save modes 1, 2, and 3 of the Prism chipset can be used.

Table VIII. Current absorbed by the Bluetooth and Wi-Fi chipsets in two operating modes.

Mode		**Bluecore01**		**Bluecore02**		**Prism II**	
		TX	**RX**	**TX**	**RX**	**TX**	**RX**
Continuos mode		135 mA	135 mA	80 mA	80 mA	325 mA	215 mA
64 kb/s	250 packet/s, 256 bit long	-		-		130 mA	
	SCO, FEC 1/3	77 mA		53 mA		-	
	SCO, no FEC (1s sniff)	40 mA		-		-	
	SCO, no FEC (40ms sniff)	-		26 mA		-	

5 CONCLUSIONS AND FUTURE DEVELOPMENTS

This paper gives a broad overview of the two most popular wireless standards, with a comparison in terms of capacity, network topology, security, quality of service support, and power consumption. Some of these characteristics, such as data link types and performance, topologies, and medium access control are stable and well defined by the standards. Others, such as power consumption, quality of service, and security are open challenges, where the technology is continuously improving, both as far as the standards and their implementations are concerned. Research areas include finding an efficient solution to the hidden terminal problem, supporting real-time transmissions in such a way that real-time traffic constraints map the user QoS requirements, developing efficient routing algorithms in mobile multihop environments, increasing data transfer security while maintaining ease of use, mitigating interference and using new multiplexing techniques such as UWB and MIMO.

Standardization is evolving quickly, with several complementary standards, among which Bluetooth and Wi-Fi dominate. Both have plenty of room for improvement, which is being explored by standardisation committees. Other actors are the HomeRF and HiperLAN, which

are not currently significant factors in the market place; others may appear in the next few years.

REFERENCES

[1] IEEE Std 802.15.1-2002 IEEE Std 802.15.1 IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs).

[2] Moe Z. Win and Robert A. Scholtz, "Impulse radio: how it works", IEEE Communications letters, vol. 2, no. 2, February 1998, pp. 36-38.

[3] Vainio, T. Juha, "Bluetooth security", Internetworking seminar, Department of Computer Science and Engineering, Helsinki University of Technology, 2000 <http://www.iki.fi/jiitv/bluesec.html>.

[4] ISO/IEC 8802-11; ANSI/IEEE Std 802.11, 1999 edn Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[5] ISO/IEC 8802-11:1999/Amd 1:2000(E); IEEE Std 802.11a-1999 Information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 1: high-speed physical layer in the 5 GHz band.

[6] IEEE Std 802.11b-1999 Supplement To IEEE Standard For Information Technology- Telecommunications And Information Exchange Between Systems- Local And Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band.

[7] IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001).

[8] H. Bölcskei and A. J. Paulraj, "Multiple-input multiple-output (MIMO) wireless systems", chapter in "The Communications Handbook", 2nd edition, J. Gibson, ed., CRC Press, pp. 90.1 - 90.14, 2002.

[9] Giuseppe Anastasi and Luciano Lenzini, "QoS provided by the IEEE 802.11 wireless LAN to advanced data applications: a simulation analysis", Wireless Networks, vol. 6, No. 99, 2000, pp. 99-108.

[10] Stefan Mangold, Sunghyun Choi, Guido R. Hiertz, Ole Klein, and Bernhard Walke, "Analysis of IEEE 802.11e for QoS Support in Wireless LANs", IEEE Wireless Communications Magazine, Special Issue on Evolution of Wireless LANs and PANs, July 2003.

[11] W. A. Arbaugh, "An inductive chosen plaintext attack against WEP and WEP2. 2001", IEEE 802.11 Working Group, task Group I (Security), 2002.

[12] J. Walker (Intel Corp), "Unsafe at any key size; an analysis of the WEP encapsulation", available from <http://md.hudora.de/archiv/wireless/unsafew.pdf>.

[13] CSR Inc., "BlueCore 01" and "BlueCore 02" data sheets, <http://www.csr.com/guide.htm>.

[14] Carl Andren, Tim Bozych, Bob Rood and Doug Schultz, "PRISM Power Management Modes", Intersil Americas Inc. application note, February 1997, AN9665.

[15] S. Souissi, E.F. Meihofer, "Performance Evaluation of a Bluetooth Network in the Presence of Adjacent and Co-channel Interference", IEEE Emerging Technologies Symposium on Broadband Wireless Internet Access, 2000, pp. 1-6.

[16] Jangeun Jun, Pushkin Peddabachagari, Mihail Sichitiu, "Theoretical maximum throughput of IEEE 802.11 and its applications", the 2nd International Symposium on Network Computing and Applications, NCA-03, 2003, USA.

[17] Muhammad Umar Ilyas, "Performance analysis of MAC layer in IEEE 802.11 networks", Fast abstracts of the International Conference on Dependable Systems and Networks (DSN 2004), Florence (IT), pp. 178-180.

[18] Markus Jakobsson and Susanne Wetzel, "Security Weaknesses in Bluetooth,", Topics in Cryptology. CT-RSA 2001: The Cryptographers' Track at RSA Conference 2001, San Francisco, Calif., 8-12 April 2001. (Lecture Notes in Computer Science, 2020). Berlin: Springer-Verlag, pp. 176-191.

ADDITIONAL READINGS

[19] J. Bray and C. Sturman, "Bluetooth: connect without cables", Prentice hall, London, UK, 2001.

[20] B.A. Miller, and C.Bisdikian, "Bluetooth revealed: the insider's guide to an open specification for global wireless specifications", Prentice Hall, 2001.

[21] Chatschik Bisdikian, "An overview of the Bluetooth wireless technology", IEEE Communication Magazine, vol. 39, no. 12, December 2001, pp. 86-94.

[22] Jaap C. Haartsen, "The Bluetooth radio system", IEEE Personal Communications, vol. 7, no. 1, February 2000, pp. 28-36.

[23] Matthew S. Gast, "802.11 networks: the definitive guide", ISBN: 0-596-00183-5, Publisher: O'Reilly.

[24] William A. Arbaugh, Narendar Shankar, and Y. C. Justin Wan, "Your 802.11 Wireless network has no clothes", IEEE Wireless Communications, December 2002, Vol. 9, No. 6, pp. 44-51.

[25] Brian P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, "IEEE 802.11 Wireless Local Area Networks", IEEE Communication Magazine, Vol. 35, N. 9, September 1997, pp. 116-126.

[26] A. Kamerman, and G, Aben, " Net throughput with IEEE 802.11 wireless LANs", Wireless Comm. Net. Conf., Chicago, IL, Sept. 2000, pp. 747-752.

[27] T. Pagtzis, P. Kirstein, and S. Hailes, "Operational and fairness issues with connection-less traffic over IEEE 802.11b", IEEE ICC, Helsinki, Finland, June 2001.

[28] Eckhard Grass et al., "On the single-chip implementation of a Hiperlan/2 and IEEE 802.11a capable modem", IEEE Personal Communications, vol. 8, no. 6, December 2001, pp. 48-57.
[29] J.C. Chen et al., "A comparison of MAC protocols for wireless local area networks based on battery power consumption", Proc. IEEE INFOCOM '98, San Francisco, CA, Mar. 29-Apr. 2, 1998, pp. 150-157.
[30] Antoine Mercier, Pascale Minet, Laurent George, and Gilles Mercier, "Adequacy between multimedia application requirements and wireless protocols features", IEEE Wireless Communications, December 2002, Vol. 9, No. 6, pp. 26-34.
[31] Jeikan Karaoguz, "High rate wireless personal area networks", IEEE Comm. Magazine, vol. 39, no. 12, December 2001, pp. 96-102.
[32] F. Bennet et al., "Piconet – embedded mobile networking", IEEE Personal Communications, vol. 4, no. 5, October 1997, pp. 8-15.
[33] P. Gupta, and P.R. Kumar, "Capacity of wireless networks", IEEE Trans. Info. Theory, March 2000, pp. 388-406.
[34] V. Rodoplu, and T. Meng, "Minimum energy mobile wireless networks", IEEE JSAC, vol. 17, no. 8, Aug. 1999, pp. 1333-1344.

AUTHORS' ADDRESSES AND BIOGRAPHIES

Erina Ferro and Francesco Potortì
ISTI - CNR
via Moruzzi, 1
I-56124 Pisa

Fax +39 050 313 8091
Erina.Ferro@isti.cnr.it Tel +39 050 315 3070
Potorti@isti.cnr.it Tel +39 050 315 3058

Erina Ferro is a senior researcher with ISTI-CNR in Pisa where she has worked since 1976. Her main interest areas are satellite access schemes for multimedia traffic transmissions with guaranteed quality of service, fade countermeasure techniques, call admission control policies, satellite systems' performance analysis, wireless LAN and their interconnection with the satellite network. She is responsible of the wireless laboratory at ISTI. She co-authored more than 80 papers published on international journals and conference proceedings.

Francesco Potortì is a full-time researcher at the ISTI-CNR institute in Pisa, Italy, where he has worked since 1989 in the fields of satellite communication protocols and fade countermeasure systems. His research interests include communications protocols and their implementation, wireless and satellite communications, internet technology with regard to integrated services, TCP congestion management and TCP over wireless channels, simulation of communications systems, free software.