WI-FI$_{\text{TM}}$, BLUETOOTH$_{\text{TM}}$, ZIGBEE$_{\text{TM}}$ AND WIMAX$_{\text{TM}}$

WI-FI$_{\text{TM}}$, BLUETOOTH$_{\text{TM}}$, ZIGBEE$_{\text{TM}}$ AND WIMAX$_{\text{TM}}$

by

H. LABIOD

ENST, Paris, France

H. AFIFI

INT, Evry, France

C. DE SANTIS

INT, Evry, France

Springer

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN 978-1-4020-5396-2 (HB)
ISBN 978-1-4020-5397-9 (e-book)

Published by Springer,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

www.springer.com

Printed on acid-free paper

I dedicate this book to my husband, my parents and my sister and brothers

Houda Laboid

Contents

Preface

The advent of ubiquitous computing and the proliferation of portable computing devices have raised the importance of mobile and wireless networking. Recently, there has been a tremendous interest in broadband wireless access systems, including wireless local area networks (WLANs), broadband wireless access, and wireless personal area networks (WPANs). This domain is a subject of huge research and many standardization activities are undertaken throughout the world.

Based on the most recent developments in the field of wireless technologies related to WLAN, WPAN, wireless sensor networks (WSN) and wireless metropolitan area network (WMAN), this book gives a detailed description of the widespread or recently used standards like Wi-Fi, Bluetooth, ZigBee, and WiMAX. Our book aims at regrouping in a single volume up-to-date information related to these different technologies, which can be used separately or combined to provide specific applications. The emergence of these very promising systems is mainly due to great technological progress in the field of wireless communication protocols; they will also make it possible to offer a broad range of new applications in both civilian and military domains. The inherent characteristics of these systems imply new challenges. Our book deals with several relevant topics related to the evolution of these spontaneous, self-organized, or cellular-based networks. Through its seven chapters, we tackle critical problems such as the design of medium access control (MAC) and routing protocols, the support of the quality of service, the security mechanisms, the mobility/roaming aspects, etc. We preferred to follow an analysis-oriented approach which aims at drawing up complete states of the art on both technology and standards. We also present some practical aspects and highlight some trends as a stake for future standards. This book is intended for readers with knowledge of networking and protocols. The audience includes network engineers, designers, implementers, undergraduate/graduate/postgraduate students, and information systems managers.

The standards that we present are definitely based strongly on the knowledge of modulation and coding though we try, in this book, to pass over this domain which is widely tackled in many specialized books. Hence, we try to attract readers who are new to these technologies and make them aware of the challenges in the different layers. As standards are made by those who have the interest and patience to participate, discuss, and reach consensus, we also hope to create a new interest in participation so as to open and improve the technical levels of our future standards.

Wireless technology remains the most exciting area in telecommunications and networking, thanks to its continuous and very fast evolution. The book thus invites the reader for an exploring travel in order to understand the genesis of the most important and interesting systems, which will certainly change the landscape of future communications.

Houda Labiod
Hossam Afifi
Costantino De Santis

Foreword

It is a great honour for me to write the foreword for this book. The development of wireless communication applications and services has been incredibly boosted to the point that the ubiquitous communication concept has found many concrete expressions.

The Ethernet networks available in all offices since the 1980s allowed a comfortable computer resources usage thanks to their high bandwidth. But soon the laptop became the principal office equipment, and the Ethernet suffered from the necessity to connect physically, impeding employee mobility and the frequent need to move from offices to meeting rooms. While on the move, employees could not modify or consult data bases, email, etc. Ten years ago "Allways on" (always online) was an essential request of Internet users. Mobile communication networks such as GPRS, CDMA, and UMTS offered insufficient bandwidth for comfortable usage. The arrival of the wireless local area networks (WLANs) has made "Allways on" a reality in companies, public places, streets, hotels, supermarkets, and private residences.

Korea pioneered in the venture, and at the end of 2003, 16,000 WLANs were available for public use. Korean customers could pay a fixed price for subscription to high-speed network access, which included access to their residence by Ethernet or ADSL and connectivity through WLAN to the whole territory when on the move. In Europe hotel chains, airports, museums, metros, etc., equipped themselves to offer this service to their customers. High bandwidth access anywhere anytime is perceived today as a natural convenience associated with many service benefits (e.g. housing, travel, lecture, tourism).

The development of PDAs, game consoles, smart phones, household appliances, and cars with digital services additionally creates the need for local communication between these objects in order to allow them to cooperate. A good example is ADSL home gateways that integrate wireless access (Wi-Fi, Bluetooth, etc.) to provide easily installable triple-play services (telephony, Internet, and television) in the home. Furthermore, an accepted phone call on your mobile can pause the program on the nearest television set, use its loudspeakers, and perhaps use the television screen for a video call or a video clip received in an MMS.

Most of these objects will have access to several interfaces of communications (GPRS, Wi-Fi, Bluetooth) in order to be able to combine the services offered on every domain. The next step is the “always best connected” concept, assuming that a single object could discover the most favourable network and use it transparently for the service required at any time and in any location. This is also becoming a commercially available service in Korea and France. For instance, the telecom operator Orange has recently put on the market its “Unik” facility, which allows mobile phone users Wi-Fi access without service disruption whenever available, with associated low fares, instead of UMTS or GSM used outdoors.

Future services that will be available are body area networks (BANs), in which sensors and actuators need to communicate to send their information and to adapt their behaviour to the physical environment. Context-specific applications, such as handicapped persons’ services, for instance, require new LANs that use energy sparingly, and can efficiently discover and communicate with transient neighbours such as RFID, biosensors, and biochips. New, currently designed services will need such properties. Billions of such sensors, captors, and activators will surround us and our personal assistants should be able to get the information across in time to provide us with useful enhanced services. Many of those tiny objects will have at their disposal very low energy capacity, and the choice for the optimal system design is still an open issue.

This book provides a comprehensive description of IEEE802.11, also called Wi-Fi, Bluetooth, WiMAX, or ZigBee. In-depth descriptions of the protocols are provided. The authors possess a solid practical experience of these networks that appears clearly in the explanations and numerous outlines in the text. Security, service discovery, and operating system integration are critical issues discussed in this book.

The authors have developed the important points of wireless networks describing the profits and technical elements of each approach, and explaining the integration of the WLAN in the context of the Internet.

Professors Hossam Afifi and Houda Labiod should be congratulated for their synthetic and very complete work.

Pierre Rolin
Dean of Telecom INT
Evry, France

Chapter 1

Introduction

Today wireless is becoming the leader in communication choices among users. It is not anymore a backup solution for nomadic travellers but really a new mood naturally used everywhere even when the wired communications are possible. Many technologies evolve then continuously, changing the telecommunication world. We talk about wireless local area networks (WLANs), wireless personal area networks (WPANs), wireless metropolitan area networks (WMANs), wireless wide area networks (WWANs), mobile ad hoc networks (MANETs), wireless sensor networks (WSNs) and mesh networks. Since we can find today a multitude of wireless technologies we decided to group a number of complementary technologies into one document to make it easier for a reader to understand some of the technical details of each media. Our attention has hence gone towards the most popular wireless techniques nowadays used at different scales. The first scale is the new defined "human body" scale where we envision to have many wireless devices not necessarily powered by anything, but just with ambient noise or with human heat and radiating digital information proper to ones very intimate life such as medical care.

A slightly larger scale of use cases, considered to be very important, addresses personal communications. Here, we talk about a personal "bubble" where everything belongs to a user with constraints on bandwidth and security.

In these two situations we consider in this book the available standards that fit to the usage, i.e. Bluetooth and ZigBee. Note that ZigBee is normally known under the name of Institute of Electrical and Electronics Engineers (IEEE) 802.15.4, whereas ZigBee is more targeted to design a related architecture for upper layers. In both standards a special care has been taken with power consumption. Of course with time, one can conclude that still an effort can be made over these solutions to save more energy, but every standard is related to a period where research advances are not yet mature enough to propose them as technical solutions. Even more, it may happen that a theoretical solution is not feasible with today's state-of-the-art integration and silicon technologies.

When we expand the "bubble" to larger scales with interpersonal collaborations, small office and home applications, we cannot neglect the wireless fidelity (Wi-Fi) standard of course. The larger part of this book is dedicated to that huge group of standards. Wi-Fi is going through the same growth as the Internet Protocol (IP), that makes it a great success and that takes it away from its original purpose to what people want to do effectively with it. Wi-Fi or IEEE 802.11 for technical people is an always evolving standard. We see that engineers still show an increasing interest in proposing new ideas that make better solutions. The group that meets every two months all over the world in a pseudorandom walk, is composed of a few hundreds of engineers and researchers, considered as experts in wireless and mobile communications. Contrarily to other standard bodies, that are more driven by business, there is still room in IEEE 802.11, for research studies and the pseudo-democratic procedure that is used in this area to select proposals still leaves the space for new ideas to come up. Of course, contributing to that group is still not easy as one could imagine, as one must physically follow all meetings and compete with large industrial well-known groups that control the floor.

The Wi-Fi group as we show in the book consists of a few tens of working groups each dedicated to a specific problem. The groups consider very diverse problems such as increasing the bandwidth or range, securing connections, mesh networking, vehicular communications, cooperative transmission and so on.

The last area that we consider in this book is about metropolitan radio transmission. We focus of course on IEEE 802.16 or what is commercially called worldwide interoperability for microwave access (WiMAX) as it seems to be the leading choice in this area.

IEEE 802.16 is also a very dynamic group that is competing with different bodies such as the Third Generation Partnership Project (3GPP) and even with Wi-Fi when it is deregulated in terms of transmission power.

We consider in this book two additional aspects: security and practical deployment because we believe that they are necessary to have a better view of how things are used and are put together in a real environment.

We do not consider, however, regulatory problems although it is *in se* a group in the IEEE 802 since it is strictly a per country political issue too complex to treat in a technical book. We need, however, to raise the reader's attention to the fact that regulatory wireless aspects do influence both the technique and the future.

A regulation can, for example, prevent a standard from being deployed in whole continent such as North America or Europe by disabling some frequency bands or by reducing the authorized power or channel width.

Note also that all these standards are dealt with in the IEEE 802 group that means that they are compatible with the general two layers architecture defined there. This also means that addressing, bridging and interface with upper layers are somehow the same in all these technologies.

An additional effort is done to be able to switch from one technology to the other in a seamless way. Although the group is not detailed in the book we have to present it in the introduction as a global virtual layer that enables the handover from a technology to the other without a service interruption. This effort is jointly led in IEEE 802.21 (media independent handover [MIH]) and in the Internet Engineering Task Force (IETF), where an orthogonal layer is designed to be able to extract radio information from the physical layer and to send it to an appropriate decision entity in the terminal, in the network or both to decide whether it is appropriate to change the connection from one wireless technology to the other. In the book we start with the IEEE 802.11 standard and all of its variants.

We continue with IEEE 802.16 group of standards with its different physical layers. The Bluetooth technology is described afterwards and we finish with the ZigBee standard. As explained before, two additional chapters describe the security issues in these different standards and some practical experiments that we led to provide a practical and critical view of potential usage of these technologies.

Organization. After the introduction (chapter 1), chapter 2 briefly gives a general description of WLANs. It starts by describing the context of this new type of networks within the framework of mobile networks. It then provides a rather broad outline on the particular characteristics of fourth-generation WLANs, their uses, the elements which constitute the architecture and the supported applications by quoting various types of current market segments covered by this technology. The second part of this chapter is dedicated to IEEE 802.11/802.11b (Wi-Fi) standards, which describes in an exhaustive way the mechanisms developed, with a special focus on access protocols. Standardization activities for the IEEE 802.11 family specifications are given in order to show the rapid evolution of the technical enhancements related to this technology.

Following the same clear and descriptive approach, the specification of the Bluetooth standard is detailed in chapter 3, while reviewing its major characteristics for lower and higher layers.

Chapter 4 covers IEEE 802.15.4 and ZigBee which are concerned with wireless sensor networks. ZigBee technology enables the coordination of communication among thousands of tiny sensors, which are very low cost, with lower power consumption and low data rate.

In chapter 5, we provide an overview of the IEEE 802.16 architecture and services and then look in more detail at the IEEE 802.16 specification.

Chapter 6 is devoted to security, which represents one of the major issues when deploying a wireless network. It comprises four parts. The first part includes an exhaustive state of the art of security for Wi-Fi systems, with an approach that consists in reviewing the developed mechanisms for authentification and encryption. Then we analyze thoroughly security flaws, showing an up-to-date classification of attacks. A report on standardization efforts, as well as short-term and medium-term solutions, is explicitly examined by highlighting still unsolved problems. In a similar way, the second part comprises a security study of Bluetooth systems. The third and fourth parts address, respectively, the security mechanisms related to WiMAX and ZigBee systems. A general conclusion ends this chapter by giving hot lines to set up short- and long-term security solutions.

The goal of chapter 7 is to illustrate by practical examples and experiments real WSN setups and WiMAX fresh equipment. The material is organized giving first a brief overview of TinyOS, an open source project devoted to network embedded technology and devices. Then some experiments and results are presented in a step-by-step fashion, to provide suggestions and feeling with WSNs. With reference to WMANs, the main focus is on configuration and testing of a complete wireless system composed of a base station and a couple of subscriber units using certified WiMAX equipment. A lab set-up for basic network performance measurements is showed, together with results attained by using popular tools.

The reader will find at the end of the book two appendices, which will provide him specific details concerning some important elements. Appendix A describes the structure of packets transmitted, according to the selected IEEE 802.11 physical layer. Appendix B contains a detailed description of the structure of IEEE 802.11 medium access control (MAC) frames.

Given the vast amount of information and the diversity of concepts, we preferred, in order to facilitate the reading of the book, to develop an extended glossary, which expands acronyms and provide a concise explanation of technical terms. A great number of figures are also included to provide an easy illustration of the various developed schemes as well as protocols and structures. A variety of useful documents and relevant websites are given to provide information related to the topics of this book.

This book, through its synthesis-based approach, can thus constitute an invaluable help for a broad range of readers who will benefit from an understanding of wireless communications and the associated technologies. This includes students, professionals, designers, implementers and managers.

Chapter 2

Wi-Fi$_{\mathrm{TM}}$: Architecture and Functions

In just the past few years, WLANs have gained a tremendous place in the local area network (LAN) market. Today, WLANs based on the IEEE 802.11 standard constitute a practical and interesting solution of network connection offering mobility, flexibility, low cost of deployment and use. The purpose of this chapter is to describe in a detailed way the concepts, principles of operation and rationales behind some of the features and/or components of the standard which was originally started in 1997. We chose a clear and concise style of writing to facilitate the understanding of the inherent concepts in this technology, which sometimes require knowledge from several disciplines. Different aspects are covered throughout the chapter. Section 1 is devoted to a brief description of the main characteristics of WLANs. Then a detailed analysis of the IEEE 802.11 standard is given, including the physical transmission layer (section 3), the access to the medium (section 5) and the management functions such as addressing, association/disassociation, roaming and energy-conserving (section 6). In this chapter we focus particularly on the IEEE 802.11 and 802.11b (labelled Wi-Fi) standards, nonetheless an overview of several derivative standards and working groups is shown in section 9.

1. WLAN Roadmap via IEEE 802.11 Family Evolution

Wi-Fi standard has gained some age and hence some maturity. It is still a very active group of standardization and one can see that new working or study groups are created to explore new directions. Note also that different national regulatory boards strongly influence the standard. We can see, for example, that in Europe, after the liberation of some frequencies in the 5 GHz band with good output power (1 W) makes the Wi-Fi a challenger to other long-range technologies such as WiMAX that is explained later in chapter 5.

1.1 Panorama of Standards

A WLAN is a data transmission system designed to ensure a connection that does not depend on the location of peripherals using wireless links rather than a cabled, fixed infrastructure. In companies, WLANs are generally deployed as the final link between the existing wired network and a group of customers' computers, offering a wireless access to the whole of the resources and services of the corporate network, in one or more buildings (sites).

In these last years WLANs are also getting their way into university campuses and public zones such as railway stations and airports, allowing any individual equipped with a portable computer to reach public information services or to connect itself to the Internet through the wireless infrastructure.

The widespread of WLANs depends closely on the developed standards. Indeed, the standardization ensures the reliability and the compatibility of products from different equipment suppliers. The IEEE 802 Committee, acknowledged as the world authority for LANs, defined several LAN standards during last 20 years, including the IEEE 802.3 Ethernet, the IEEE 802.5 Token Ring and the IEEE 802.3u 100BASE-T Fast-Ethernet. In 1990, the IEEE 802 Committee formed a new working group, the IEEE 802.11, specifically devoted to WLANs, with a charter to develop a physical medium specification and a MAC protocol. The Institute of Electrical and Electronics Engineers (IEEE) ratified the 802.11 specification in 1997. This standard, in its first version, featured data rates of 1 and 2 Mbps and defines the fundamental rules for signalling and wireless services. The major problem, which limited the initial industrial development of WLANs, was then the limited throughput, too low to really meet the various enterprises needs. Conscious of the need for increasing this rate, the IEEE defined the 802.11HR specification (also named IEEE 802.11 high rate or 802.11b) with speeds of 5.5 and 11 Mbps. The IEEE also worked out the specifications of the 802.11a version in the 5 GHz band.

The statutory organizations and suppliers' alliances adopted this new high data rate standard, and many market sectors appeared (Small Office Home Office [SOHO], as well as public/governmental and private/corporate related).

Apart from the standard bodies, the main players of the wireless industry met within the Wi-Fi Alliance, previously called Wireless Ethernet Compatibility Alliance (WECA). The mission of the Wi-Fi alliance is to certify the interworking and the compatibility between IEEE 802.11HR network equipments and also to promote this standard.

The Wi-Fi alliance regroups manufacturers of semiconductors for WLANs, hardware suppliers and software providers. Among them we can find companies like 3Com, Cisco-Aironet, APPLE, Breezecom, Cabletron, Compaq, Dell, Fujitsu, IBM, Intersil, Lucent Technologies, No Wires Needed, Nokia, Samsung, Symbol Technologies, Wayport and Zoom.

Up to now, the IEEE 802.11 family of standards did not cease to continuously come up with new proposals of standards. Right below we provide a list of IEEE Standards and Task Groups (TGs) that exist within the IEEE 802.11 working group. The Official 802.11 WG Project Timelines can be found at http://www.ieee802.org/11/802.11_Timelines.htm.

As it can be seen from the IEEE 802.11 home page, it is very easy to become an active member in the group where a minimum of three physical meetings are required for a person to become a voting member and hence influence the decisions taken there.

The most prevalent WLAN protocols are those related to the IEEE 802.11, IEEE 802.11b (Wi-Fi) and IEEE 802.11g standards. This family of standards deals with the physical and data link layers as defined by the OSI basic reference model (ISO/IEC 7498-1:1994). Today we see that the IEEE 802.11n is slowly taking over them.

The term used for IEEE 802.11b-certified products is Wi-Fi. Wi-Fi certification is provided by Wi-Fi alliance; notice that at present it has been extended to include IEEE 802.11g products as well. Wi-Fi alliance has also developed a certification procedure for IEEE 802.11a products called Wi-Fi5.

The list of standards and those derived from Wi-Fi are quoted below:

- IEEE 802.11: the original 1 and 2 Mbps, in the 2.4 GHz industrial, scientific and medical (ISM) band, and infrared (IR) standard (1999).
- IEEE 802.11b: enhancements to IEEE 802.11 to support 5.5 and 11 Mbps (1999).
- IEEE 802.11a: the IEEE 802.11a standard operates in the 5 GHz band and allows throughputs from 6 to 54 Mbps.
- IEEE 802.11g: allows to reach higher data rates (54 Mbps, identical to IEEE 802.11a) in the 2.4 GHz band. The orthogonal frequency-division multiplexing (OFDM) modulation is used. It provides backwards compatibility with 802.11b (2003).
- IEEE 802.11d: international (country-to-country) roaming extensions (2001), access points (APs) communicate information on available radio channels and acceptable power levels, according to countries' lawful restrictions.
- IEEE 802.11c: bridge operation procedures, included in the IEEE 802.1D standard (2003).

- IEEE 802.11e: enhancements (2005), standard for the quality of service (QoS), which defines the specifications of the QoS mechanisms to support multimedia applications. Apply to IEEE 802.11b/a/g. It introduces the hybrid coordination function (HCF). HCF uses both a contention-based channel access method, called the enhanced distributed channel access (EDCA) and a contention-free channel access method, called HCF-controlled channel access (HCCA) which have been derived from their earlier versions enhanced distributed channel function (EDCF) and HCF.

- IEEE 802.11F: deals with the standardization of protocols between APs to allow the use of a multivendor infrastructure avoiding proprietary standards. The Inter-Access Point Protocol (IAPP) offers this interworking feature.

- IEEE 802.11h: spectrum managed IEEE 802.91a (5 GHz) for European compatibility (2004). Mechanisms of frequency dynamic selection and transmit power control (TPC) are considered.

- IEEE 802.11i: enhanced security (2004). Apply to standards IEEE 802.11 b/a/g.

- IEEE 802.1X standard: provides security mechanisms for various media including wireless links by the means of strong authentication procedures with dynamic key distribution.

- IEEE 802.11j: convergence of the American (IEEE 802.11) and Japanese standards (it is the adaptation of the former to the Japanese legislation).

- IEEE 802.11k: radio resource measurement (RRM) enhancements; it defines methods and measuring criteria needed by higher layer protocols to fulfill management and maintenance functions.

- IEEE 802.11n: higher throughput improvements; it offers higher data rates (108–600 Mbps) in the 2.4 and 5 GHz bands.

- IEEE 802.11p: wireless access for the vehicular environment (WAVE).

- IEEE 802.11r: fast roaming.

- IEEE 802.11s: mesh networking.

- IEEE 802.11T: wireless performance prediction (WPP) – test methods and metrics.

- IEEE 802.11u: interworking with non-802 networks (e.g. cellular).

- IEEE 802.11v: wireless network management.
- IEEE 802.11w: protected management frames.
- IEEE 802.11y: 3650–3700 operation in the United States.

Note – there is no standard or task group named “802.11x”. Rather, this term is used informally to denote any current or future IEEE 802.11 standard, in cases where further precision is not necessary. (The IEEE 802.1X standard for port-based network access control, is often mistakenly called “802.11x” when used in the context of wireless networks.)

The evolution of IEEE 802.11 standards is illustrated in Figure 2.1 which includes two types of systems: those operative in the band of 2.4 GHz and those operative in the band of 5 GHz.

FH: frequency hopping spread spectrum (FHSS) technique; DS: direct-sequence spread-spectrum technique; HR: high rate; BRAN: European project (Broadband Radio Area Network); H1: Hiperlan 1 European standard specified by the European standardization organization ETSI;

H2: Hiperlan 2 European standard specified by the European standardization organization ETSI. H2 has similar physical layer properties as IEEE 802.11a because it uses OFDM in the 5 GHz band. The MAC layer is different since it is based on a TDMA approach.

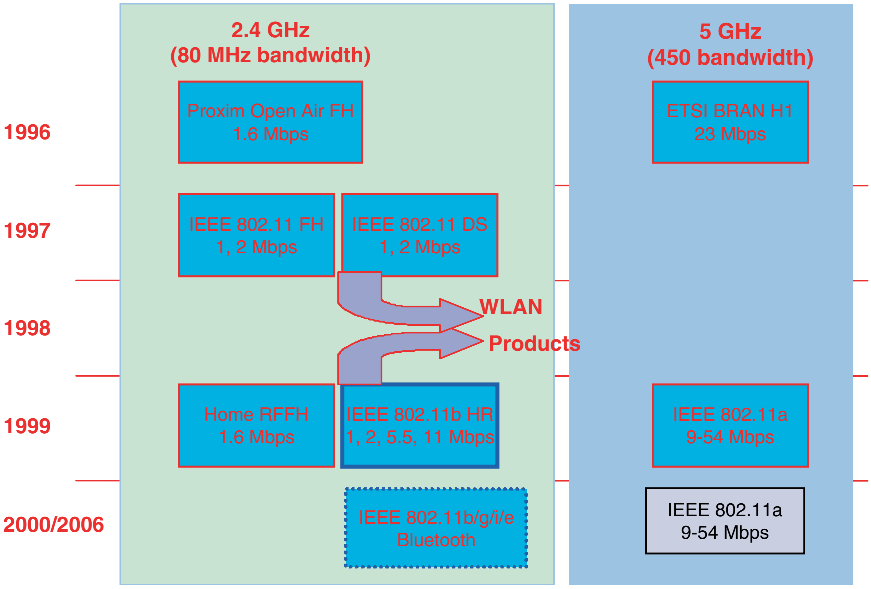

Fig. 2.1. Evolution of WLAN standards

1.2 Features of the Different WLAN Generations

A WLAN is an interesting technology because it offers a vast range of applications, thanks to its several advantageous characteristics including high capacity, short-distance coverage, full connectivity and broadcast capability. The following are the main features of WLANs.

- Licence-free operation; connection to backbone LAN
- World availability according to standards
- Theoretical throughputs definitely higher than those offered by 3G standards as universal mobile telecommunications system (UMTS)
- Low-cost design with equipment prices in progressive reduction (APs and wireless cards); very competitive costs compared to third-generation mobile systems (license + equipment)
- Roaming/handoff support
- Ease of deployment

The characteristics of these systems thus knew an evolution which can be summarized as follows:
* First generation (IEEE 802.11) since 1997 (WLAN/1G):

- Connectivity of PC terminals (between them or to a fixed LAN).
- Bridge-based APs.
- Roaming.
- Coexistence with other networks (e.g. WLAN and Ethernet LAN) which means bridging. Note that there is a small problem in the IEEE 802.11 in general with respect to bridging where it does not fulfill completely the bridging rules and is hence nonconformant to the 802 paradigms.

* Second generation (IEEE 802.11b) since 1998 (WLAN/2G):

- More effective management of WLAN
- Interworking and interoperability
- Migration starting from the first generation
- Conformity to the IEEE 802.11b standard

* Third generation (802.11a/g) since 2000 (WLAN/3G):

- High throughput (HT)
- Design of networks more open and integrated

- Conformity to the IEEE 802.11a/g standard
- Minimization of antenna sizes
- Improvement of receiver's sensitivities

* Fourth generation (IEEE 802.11n) (WLAN/4G):

- Very high throughput (some hundreds of Mbps)
- Long distances at high data rates (equivalent to IEEE 802.11b at 500 Mbps)
- Use of robust technologies (e.g. multiple-input multiple-output [MIMO] and space time coding).

We compared the price of an IEEE 802.11b-based solution with that of an equivalent cabled Ethernet-based solution. The IEEE 802.11b cards used are of type Cisco-Aironet. We have three APs and 50 wireless cards (25 PCMCIA and 25 PCI cards). The total price of the equipment was almost the same. Although the initial investment is important as it is shown by the carried study, it is important to point out the immediate beneficial return of the WLAN solution (Figure 2.2). Indeed, the prices are quite similar at the beginning of the installation of the two networks, but during their lifespan, and considering also the flexibility in connectivity and in configuration changes, an IEEE 802.11b WLAN-based solution will provide more advantages. It should also be mentioned that the prices of wireless equipment is continuously decreasing nowadays.

In addition, an IEEE 802.11b solution is more advantageous than a wide area network (WAN) operator solution, because there are no specialized connections. Physical limitations are also removed and the deployment is simple and fast.

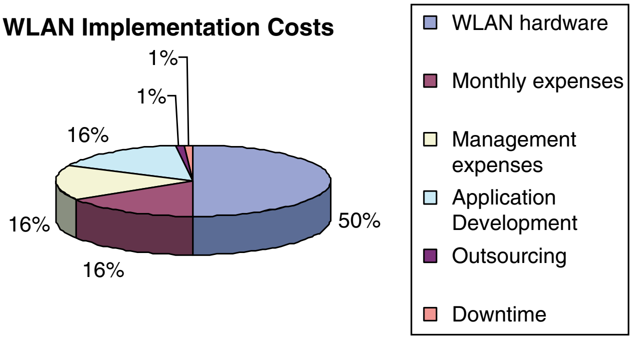

Fig. 2.2. Distribution of the costs of a WLAN solution (souce WLANA). This figure illustrates clearly that a great part of the costs relates to the used physical material (1: downtime, 2: expenses, 3: management, 4: development of applications, 5: outsourcing, 6: material)

Limitations. Independently of legal aspects, some limitations of this technology still remain such as:

- Lower data rates compared with those of high-speed fixed networks
- A limited range and influence of fixed obstacles especially metallic walls
- A shared bandwidth without a high degree of control
- Security attacks
- A quality of transmission depending on the environment (multipath propagation, path loss)
- Interworking
- Deployment
- A lack of QoS control

In order to mitigate these disadvantages, works are undertaken within several working IEEE groups. As these problems have been addressed, the popularity of WLANs has grown rapidly.

1.3 WLAN Markets

We distinguish several categories of systems where a WLAN can be used (Figure 2.3):

- Wireless personal area networks
- Wireless area networks
- Wireless metropolitan area networks

WLAN services evolve into three main categories of market segments.

Private Segment. We list three types of networks.

Enterprise networks – professional private use. WLAN solutions suitably meet a strong need for nomadism intra- and intersite for users. It remains to address two requirements: the security of access and issues related to interferences and interworking. It is a market segment which is typically filled by system integrators (deployment of WLAN networks, integration of existing systems and development of security solutions) and equipment suppliers. Many enterprise-class organizations have deployed WLAN technologies also in an attempt to increase their productivity.

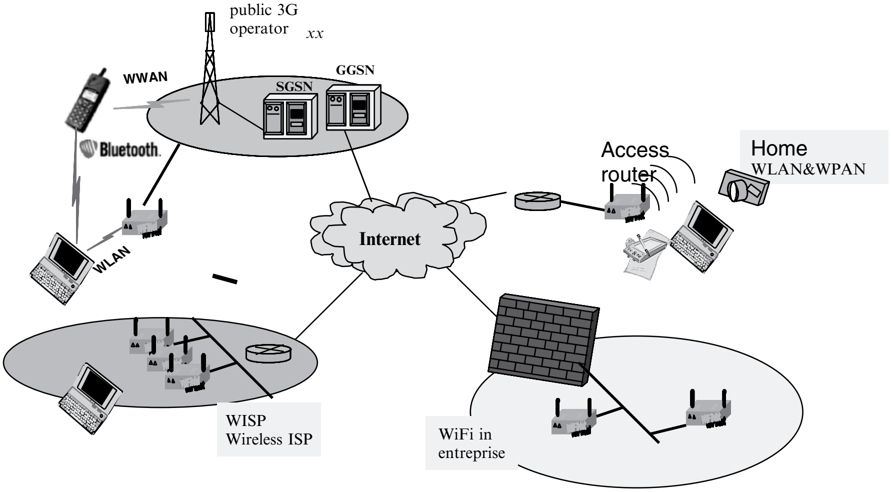

Fig. 2.3. WLAN, WPAN, WWAN: total ubiquity

Domestic wireless link – personal/home use. This kind of networks is typically deployed in a radius of a few meters around the user. The simplicity of the installation offered by a WLAN solution will probably interest, for example, a considerable part of French houses (30% of French houses are equipped with computers, 15% are multi-equipped). This solution provides free roaming inside houses, bandwidth sharing between several users, Internet access starting from an ADSL AP and it can also make radioelectric equipments communicate (house automation). Consumers of high-speed Internet access, who built their own wireless homes and small office networks, can share a fast connection among several computers.

Public private networks.

Hot Spots. Currently, it is a growing and interesting market. It concerns the high data rate access in public areas where there is an important density of users (i.e. airports, railway stations, hotels, coffee shops, libraries, subways, shopping centres, conference rooms, pirks of leisure and restaurants). A very great number of hot spots has been deployed in the United States, primarily free and cooperative (Seattle with more than 100 of relays installed to offer a free access, San Francisco, New York and Portland). In Europe, the majority of hot spots is in the Scandinavian countries and in France. The American survey firm Gartner estimated the number of hot spots in Europe to be 40,000. In the world, the annual growth is estimated, by Industrial Development Corporation (IDC), to 57%. The French operator Orange deploys 250 hot spots with approximately 1500 APs and average 200 connections per day. The directory of these hot spots is available at www.orange-wifi.com. In France, a clear tendency to the democratization of the access to the Internet appears through networks known as “libertarian” (Wi-Fi-France and Wi-Fi-Paris associations).

It is obvious that a worldwide deployment of thousands of new hot spots is well in progress and one can obtain fresher information looking for example at www.wi-fiplanet.com.

Free Networks. They are classified into two categories:

- Entirely libertarian networks which cover urban zones, although totally free, anti-terrorism laws mandate that a user still be identified for legal interception and tracking.
- Networks deployed in non-covered/non-connected rural zones.

Applications. We find several application areas for WLANs such as:

- LAN extension
- Cross-building interconnect
- Ad hoc networking
- Nomadic access
- Public hot spot access
- Data transmission within vertical markets such as:
  - LANs (offices)
  - Medical applications (real-time information transfers)
  - Retail trade, warehouse
  - Stores, shopping centres, railway stations
  - Maintenance in airports and seaports
  - Education, finance, industry
  - SOHO

Several key factors enable to foresee a rise of the WLAN market, among which we can quote:

- A progressive maturity of the standards (especially those derived from the IEEE 802.11, 802.11b Wi-Fi and 802.11a/g)
- A deployment delay of third-generation mobile systems

- A considerable investment and maturity of products (terminals, cards, adaptors, APs, etc.)
- Integration of Wi-Fi chipsets into portable laptops and tablet PCs
- Proposals for solutions of security and roaming (with certain limitations)
- An increase in the deployment of the multi-equipment in residence
- An increased mobility of users
- High throughputs of wireless systems (2G/3G/4G)
- A consequent fall in costs (Wi-Fi chips, APs, the market of PCMCIA cards disappearing)
- A frequency band usable without licence
- More widespread Wi-Fi availability
- More Wi-Fi competition
- Aggregated Wi-Fi hot spots networks (service providers wISPs, operators)
- Various markets are covered (enterprises, domestic market, telecommunication, education, health, SOHO, public sector, etc.)

We propose in section 2 a detailed technical study of the primary IEEE 802.11 standard, whose major basic mechanisms have been included in the most recent standards and more particularly Wi-Fi.

Let us note that in the continuation, the terms IEEE 802.11b and Wi-Fi will be used interchangeably.

2. IEEE 802.11 Architecture

2.1 Three Basic Operational Modes

The IEEE 802.11 standard considers two types of components: a wireless client station (in general a PC equipped with a wireless network interface card [NIC]) known as a station (STA) and an access point (AP) or sometimes called wireless relay, which functions as a bridge and a relay point between the fixed network and the wireless network. This AP is usually composed of a radio transceiver/receiver, a network card (e.g. Ethernet 802.3) and a software for layer-2 bridging in conformity with the IEEE 802.1d standard. The AP behaves like the basic station of the wireless network, aggregating the access of multiple wireless stations to the fixed network. The wireless stations include IEEE 802.11 network access cards or wireless adapters (or network interface controller). These adapters are available in many formats (PCI, PCMCIA, USB and nowadays Wi-Fi chips).

The IEEE 802.11 standard's model defines three modes: an infrastructure mode, an ad hoc mode and a mesh mode.

Infrastructure Mode. Within the infrastructure mode, the wireless network consists of at least an AP connected to the fixed network infrastructure and a set of wireless client stations. This configuration is based on a cellular architecture where the system is subdivided into cells. Each cell (called Basic Service Set[BSS], in the IEEE 802.11 is controlled by a base station (called AP).

The stations within a BSS execute the same MAC protocol and compete for access to the same shared wireless medium. We can refer to it in the following sections as a cell. Although a WLAN may be formed by a single cell (with a single AP), the maximum distance between stations is limited by many factors like RF output power and the propagation conditions of the indoor/outdoor environments. To provide for an extended coverage area, multiple BSSs are used where the APs are connected through a backbone called a distribution system (DS).

The whole interconnected WLAN including at least two different BSSs (with respect to their APs) and the DS, is seen as a single logical IEEE 802 network to the logical link control (LLC) level and is called an Extended Service Set (ESS). The majority of WLANs should be able to reach the fixed LAN services (file servers, printers and Internet access). The DS is responsible of transporting the packets between various cells within the ESS area. Data transfers occur between stations within a BSS and the DS via an AP. DS handles address mapping and interworking functions. BSSs may partially overlap. This is commonly used to cover an extended area. BSSs could be physically disjointed or colocated. To provide flexibility to the WLAN architecture, IEEE 802.11 logically separates the wireless medium from the DS medium. The DS can correspond to an Ethernet network, Token Ring, FDDI or any other communication network such as a wireless IEEE 802.11 point to point. A wide zone ESS can also provide to the various client stations an access towards a fixed network, such as Internet. Before any communication can be set within a BSS, the wireless client stations must execute an association with the AP.

Figure 2.4 shows a typical IEEE 802.11 LAN including the components described above.

The standard defines the concept of "portal or gateway", it is a device which is used to interconnect an IEEE 802.11 architecture with a traditional wired 802.x LAN. This concept is an abstract description of a part of the functionalities of a translation bridge. The portal's function is to provide a logical integration between WLAN architectures and existing wired LANs. In most hardware implementations, all the APs behave as portals. The portal logic can be implemented in a device, such as a bridge or a router or a switch, and it is a part of the WLAN and is attached to DS. In Linux, some good implementers have

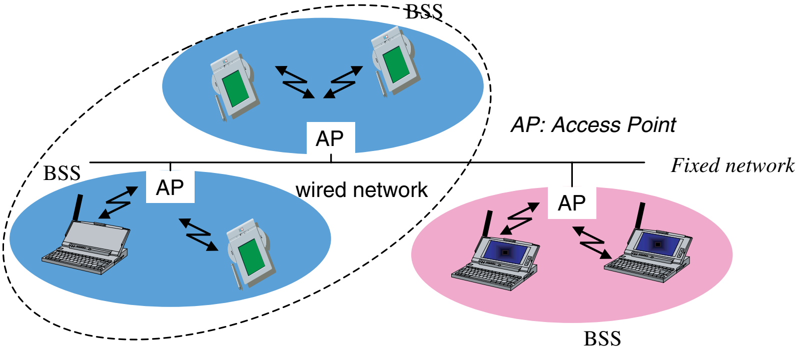

Fig. 2.4. Infrastructure mode in IEEE 802.11

provided a complete open source implementation of such a portal called *hostap*, very useful for testing any unsupported function in the current standards.

Cell identifier BSSID/ESSID and network service identifier SSID. The AP is thus the central element within a cell; since it includes the necessary functionalities to control the communications between the stations within its coverage zone with which a service zone is associated. The standard IEEE 802.11 adopts a particular addressing scheme. Each cell is identified by 6 bytes address (48 bits) called Basic Service Set Identifier (BSSID) which corresponds to the MAC address of the AP managing the cell (more details are given in the paragraph 2.6.1).

However to avoid undesirable connections, we can find an additional information called *service set identity* (SSID) that allows to identify the service network; it is a 32 bytes character string of a variable size. SSID is used in order to guarantee the authentication and the identification between an AP and a client. Any station wishing to connect itself to the extended network area must thus know as a preliminary the value of the SSID. It should be noted that this mechanism is not considered as a security protection because the identifier of the network is generally transmitted in clear through some frames (probe). So do not try to protect your network by omitting the SSID diffusion. . . .

We should note that the infrastructure mode is the most used and it offers less performance in term of bandwidth utilization.

Nomadism and Mobility. Several types of mobility can take place (Figure 2.5):

- A local mobility within the same BSS
- A mobility intra-ESS between two different BSSs
- A mobility inter-ESS between two BSSs belonging to two different ESSs.