WLAN Standards:

Jui-Hung Yeh, Jyh-Cheng Chen and Chi-Chen Lee

in particular, the IEEE 802.11 family

Wireless communications are breaking the bonds Internet users have had to wired connections. *Mobility* while accessing the Internet and increased *flexibility* are motivating the wireless network technology push. Also, Wireless Local Area Networks (WLANs) can even (at times) be more economical and efficient than installing wired networks throughout a building. With the market promotion of wireless network technologies, services and applications are increasing everyday.

However, the growth of the WLAN market and services also relies on the policy and regulation of each country. A loose regulation may accelerate the expansion of WLAN market but also creates interference problems. By contrast, strict regulations could allocate the spectrum well but might impede market development.

This article introduces various modern WLAN standards with a focus on the IEEE 802.11 family. Moreover, influences of policy and regulation in the WLAN market are discussed. Public access WLAN services are introduced with service types. Finally, we conclude with future expectations.

The IEEE 802.11 family

Wireless network technologies were uninteresting (and immature) for years until 1985 when the Federal Communications Commission (FCC) of the United States authorized the Industrial, Scientific and Medical (ISM) frequency bands. These three ISM bands accelerated the development of WLANs because vendors no longer needed to apply for licenses to operate their products. In 1989, the IEEE 802.11 Working Group began elaborating on the Wireless LAN Medium Access Control and Physical Layer specifications. The final draft was ratified on 26 June 1997.

The IEEE 802.11 standard defines what comprises a Basic Service Set (BSS). That is, the set has two or more fixed, portable, and/or moving nodes or stations that can communicate with each other over the air in a geographically limited area. Two configurations are specified in the standard: ad-hoc and infrastructure.

The ad-hoc mode is also referred to as the peer-to-peer mode or an Independent Basic Service Set (IBSS) as illustrated in Fig. 1(a). This ad-hoc mode enables mobile stations to interconnect with each other directly without the use of an access point. All stations are usually independent and equivalent in the ad-hoc network. Stations may broadcast and flood packets in the wireless coverage area without accessing the Internet. The ad-hoc configuration can be deployed easily and promptly when the users involved cannot access or do not need a network infrastructure. For instance, participants of a conference can configure their laptops as a wireless ad-hoc network and exchange data without much effort.

However, in many instances, the infrastructure network configuration is adopted. As indicated in Fig. 1 (b), in the infrastructure mode there are access points which bridge mobile stations and the wired network. BSSs can be connected by a distributed system that normally is a LAN. The coverage areas of BSSs usually overlap. Handoff will happen when a station moves from the coverage area of one access point to another access point. Although the radio range of a BSS limits the movement of wireless stations, seamless roaming among BSSs can construct a campus-wide wireless network service.

Medium Access Control (MAC) layer

The IEEE 802.11 standard specifies the physical layer and the medium access control (MAC) sublayer of a WLAN. Although several physical techniques are specified, only one MAC is defined in the standard. In the MAC layer, the Distributed Coordination Function (DCF) is known as the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. This protocol is specified in all the stations of both the ad-hoc and the infrastructure configurations.

By physically sensing the carrier, a backlogged station may immediately transmit packets when it detects free medium for greater than or equal to a DIFS (DCF Interframe Space) period. If the carrier is busy, the station defers transmission and enters a back off state. The time period following the DIFS is called a contention window and consists of a pre-determined number of slots. The station, which has entered the back off state, randomly selects a slot in the contention window and continuously senses the medium up to its selected contention slot. If it detects transmission from other nodes during this time period, it enters the back off state again. If no transmission is detected, the station captures the medium and transmits its frame. The operation of a DCF is illustrated in Fig. 2.

In addition to the physical carrier-sensing mechanism just described, the DCF supports virtual carrier sensing by the exchange of RTS (Request-to-Send) and CTS (Clear-to-Send) frames. It can also distribute the Duration/ID field that sets the medium holding time within the RTS and the CTS frames. Before transmitting any data, the sender transmits a RTS frame to the receiver. The receiver must reply with a CTS frame if the transmission is permitted. Other nodes sensing the CTS frame cannot transmit during the holding time set in the Duration/ID field because they are close to the receiver. On the other hand, any node that only sees the RTS frame but not the CTS frame is free to transmit. This is because these nodes will not cause interference with the receiver. The mechanism can also solve the *hidden node* and *exposed node problems* as illustrated in Fig. 3.

As shown in Fig. 3 (a), node B can

 0278-6648/03/$17.00 © 2003 IEEE

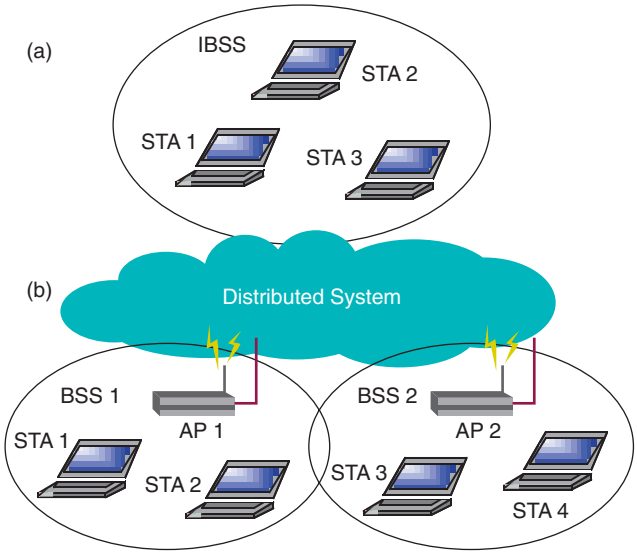


Fig. 1 (a) Ad-hoc and (b) infrastructure network architectures

reach both node A and node C, but node A and node C cannot hear each other. If node A is transmitting data to node B, node C will not detect the transmission. Thus node C might also send data to node B. Thus, a data collision will occur in node B. This is called the *hidden node problem* since node A and node C are *hidden* from each other. The exchange of RTS and CTS frames between node A and node B will prevent node C from sending data to node B. Why? Because node C will detect the CTS frame sent by node B.

In Fig. 3 (b), we assume that node B and C intend to transmit data only without receiving data. When node C is transmitting data to node D, node B is aware of the transmission. This is because node B is within the radio coverage of node C. Without exchanging RTS and CTS frames, node B will not initiate data transmission to node A because it will detect a busy medium. The transmission between node A and node B, therefore, is blocked even if both of them are idle. This is referred as the *exposed node problem*.

Also in Fig. 3(b), the RTS frame sent by node C will reach node B, but the CTS frame sent by node D will not propagate to node B because node B is not within the radio coverage of node D. Thus, node B knows that the transmission from node C to node D might not interfere with its transmission to node A. Hence, node B will try to initiate transmission by sending RTS to node A if it has data to transmit. This strategy overcomes the exposed node problem and enhances the radio efficiency.

The contrastive optional mechanism in the MAC layer is the Point Coordination Function (PCF) which is only used in infrastructure network configuration. The PCF provides contention-free transmission through a point coordinator that shall be performed by access point in the BSS. As the polling master, the point coordinator coordinates all the stations and determines which one can use the medium. If priority-polling mechanisms are followed, different QoS (quality of service) levels can be achieved in the point-coordinated BSS. To start a contention-free period (CFP), the point coordinator first broadcasts a beacon management frame. All the stations then set their network allocation vector (NAV) before the CFP. When a point coordinator polls a station, it replies with an acknowledgment. The acknowledgment can also be piggybacked with other data frames. A *CF-end (Contention-Free-end)* frame sent by the point coordinator will end the CFP.

Physical layers

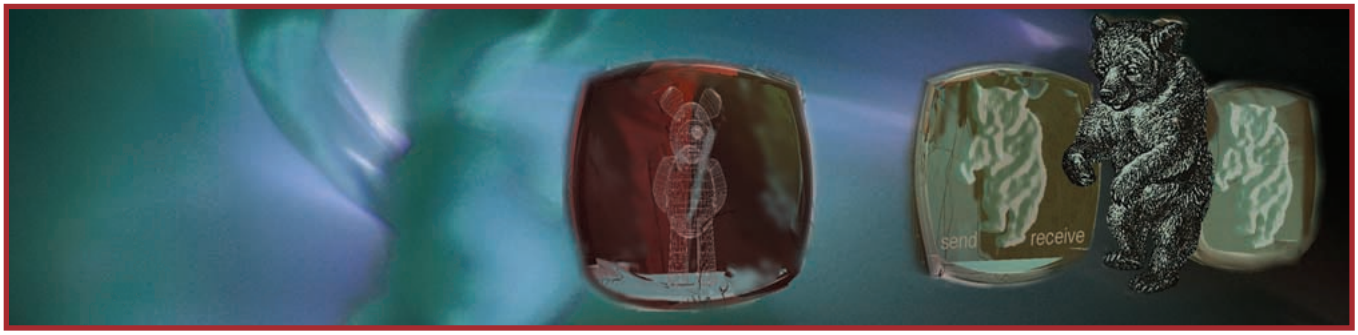
The IEEE 802.11 standard specifies different radio frequency (RF) physical layers primarily operating at the 2.4 GHz ISM band: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). The DSSS physical layer provides 2 Mbps of peak rate and optional 1 Mbps in extremely noisy environments. On the other hand, the FHSS physical layer operates at 1 Mbps with optional 2 Mbps in very clean environments.

In addition to the RF physical layer, an infrared (IR) physical layer is also specified. The IR physical layer supports both 1 Mbps and 2 Mbps for receiving, and 1 Mbps with an optional 2 Mbps bit rate for transmitting. The IR physical layer uses the reflected infrared energy for communications, which is called *diffuse infrared* transmission, such that the transmission is not directed. The typical range of 10 m extremely limits IR wireless systems. The communication quality is also sensitive to the environment (e.g. the number of reflecting surfaces and line-of-sight paths). Therefore, vendors usually adopt the RF techniques rather than the IR system.

802.11b/a/g

The IEEE 802.11 standard proposed in 1997 was a milestone for WLANs. But two years later on 16 September 1999, the IEEE 802.11 standard was officially revised. The new standard, still operating on the 2.4 GHz frequency band, is called 802.11b or 802.11 High Rate. The 802.11b standard provides a data rate up to 11 Mbps, which is comparable to a fixed Ethernet. It is a more robust system but still accommodates the same 802.11 protocols. Moreover, this revision promises interoperability among products of different vendors and compatibility with legacy 802.11 products. This promise not only encouraged the manufacturing of 802.11b products but also stimulated competition among WLAN vendors.

The IEEE 802.11b physical layer adopts Complementary Code Keying (CCK) technology such that upgrading can be done easily. While the data rate goes to 11 Mbps, it has fallback rates of 5 Mbps, 2 Mbps, and 1 Mbps. The 802.11b uses the same bandwidth as the original 802.11 DSSS physical layer. Backward compatibility thus can be ensured. Besides, the coexistence of the 11 Mbps 802.11b system and



the 2 Mbps 802.11 system permits a smooth transition to a faster WLAN system.

Although 802.11b products have successfully conquered the WLAN market, the resulting interference within the 2.4GHz ISM band is a major issue. Not only Bluetooth devices, but also many medical equipment and household appliances (e.g. microwave ovens and cordless telephones) use the 2.4 GHz frequency band. Therefore, the IEEE 802.11a standard was approved in September 1999 that instead uses the 5 GHz frequency band. This band change implicitly implies that 802.11a and 802.11b are not compatible. Furthermore, the 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM), a new coding scheme that provides a significantly higher data rates up to 54 Mbps and beyond. The required speeds defined in 802.11a are 6, 12 and 24 Mbps with optional speeds up to 54 Mbps.

As mentioned in the 802.11 specification: *well-defined wireless coverage areas simply do not exist because of dynamic and unpredictable propagation characteristics*. However, based on performance measurements in Chen and Gilbert's work, the comparison of data rate versus radio coverage range is shown in Fig. 4. It indicates that the data rate slows down substantially the greater the distance between the access point and the client. However, at any range, the 802.11a data rate is still higher than for 802.11b.

What hinders the progress of 802.11a is not only the incompatibility with today's 802.11b products, but that the 5 GHz spectrum is not license-free in every country. Therefore, the IEEE proposed the 802.11g standard in November 2001 to enhance the 2.4 GHz 802.11b technology.

802.11g defines two optional modulations. The Packet Binary Convolution Code (PBCC) modulation optionally supports 22Mbps and 33Mbps for payload data rate. Another optional modulation, OFDM, supports at most 54Mbps payload data rate. In addition, compatibility with 802.11b products is promised. The 802.11g standard was ratified on 13 June 2003. Products based on its early drafts are available on the market already.

Security (WEP and 802.11i)

Like other wireless standards, security is one of the most critical problems. In the original IEEE 802.11 standard, a Wired Equivalent Privacy (WEP) algorithm was adopted to encrypt messages. WEP uses a RC4 (Rivest Cipher 4) pseudo-random number generator (PRNG) algorithm with two key structures of 40 and 128 bits. However, claims of cracking the WEP algorithm have been made recently. Several network security research groups have discovered and successfully attacked the weakness of WEP. Borisov, Goldberg, and D. Wagner's paper, for instance, demonstrates the vulnerability of WEP. Today, one can easily download a WEP cracking tool from the Internet and crack the 802.11 WEP secret key. Thus, the IEEE 802.11i committee is developing two new encryption algorithms. WEP2 is an enhanced version of WEP. The Advanced Encryption standard (AES) provides another stronger encryption alternative.

In addition to encrypting messages over the air, the IEEE 802.11i committee is working on the enhanced security and authentication mechanisms for IEEE 802.11 systems. The committee has adopted IEEE 802.1x, a Port Based Network Access Control standard, to authenticate wireless users. The IEEE 802.1x standard leverages an existing authentication protocol called EAP (Extensible Authentication Protocol, IETF RFC 2284). Three main components are defined in the IEEE 802.1x WLAN authentication: 1) the supplicant (usually the client agent), 2) the authenticator (usually the access point), and 3) the authentication server (usually a RADIUS server).

Before an 802.11 client is authenticated, the access point blocks all traffic except 802.1x messages. The user's authentication data, which are transported by EAP, are encapsulated in 802.1x messages. The access point then relays EAP messages to the RADIUS server, which is the central authority containing user authentication information. If the user is authenticated successfully, the RADIUS server replies with a RADIUS accept packet, in which the EAP success packet is encapsulated. In addition to relaying the EAP success packet to the user, the access point also unblocks traffic from the user. The 802.11i is still a draft specification. The completed standard should be ratified by the end of 2003.

Glossary

AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
BSS	Basic Service Set
CCK	Complementary Code Keying
CF-Poll	Contention Free Poll
CF-end	Contention Free End
CFP	Contention Free Period
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear-To-Send
DCF	Distributed Coordination Function
DFS	Dynamic Frequency Selection
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EDCF	Enhanced DCF
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HCF	Hybrid Coordination Function
HIPERLAN	High Performance Radio Local Area Network
HiSWAN	High Speed Wireless Access Network
IAPP	Inter Access Point Protocol
IBSS	Independent Basic Service Set
IR	Infrared
ISM	Industrial, Scientific and Medical
MAC	Medium Access Control
MMAC	Multimedia Mobile Access Communication
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
PBCC	Packet Binary Convolution Code
PCF	Point Coordination Function
PIFS	PCF Interframe Space
PRNG	Pseudo-Random Number Generator
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RC4	Rivest Cipher 4
RF	Radio Frequency
RTS	Request-To-Send
TDD	Time-Division Duplex
TDMA	Time-Division Multiple Access
W-ISP	Wireless Internet Service Providers
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WLL	Wireless Local Loop
WPA	Wi-Fi Protected Access

MAC enhancements (802.11e) and multi-vendor access point interoperability (802.11f)

The IEEE 802.11e committee aims to enhance the IEEE 802.11 MAC for QoS support, with the classification of services, and to improve efficiency of the protocol. The work being done is compatible with all the existing IEEE 802.11 WLAN standards, including IEEE 802.11b, a and g. The IEEE 802.11e draft standard specifies Enhanced DCF

(EDCF) from the original DCF defined in the 802.11 MAC layer.

Each station supports up to eight independent multiple back off instances to transfer data. Each back off instance has its traffic category that contains several QoS parameters corresponding to the priority. A back off instance must start a back off period after the Arbitration Interframe Space (AIFS). The AIFS can be equal to or larger than the DIFS depending on the QoS parameter. A high priority instance has a smaller AIFS than a low priority instance. Thus, a high priority instance will enter the contention window period earlier than a low priority instance. Also, the contention window size relies on the parameters within the traffic category. A high priority instance gets a smaller contention window to increase the transmission probability. Since there are up to eight transmission queues within one station, a scheduler can coordinate instances to avoid the *virtual collision* inside the station.

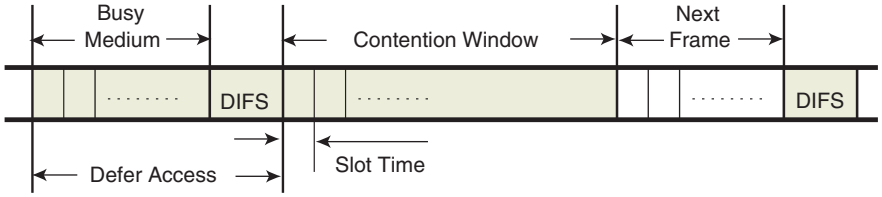


Fig. 2 Basic access method of DCF

In addition to EDCF, the Hybrid Coordination Function (HCF), extended from PCF, allows a hybrid coordinator to maintain states of stations and, thus, schedule transmission intelligently. The HCF is used not only in a contention free period (CFP) but also in a contention period. During a contention period, a station can contend the medium by itself or be polled by the QoS CF-Poll (Contention Free Poll) frame from the hybrid coordinator. The QoS CF-Poll frame is sent after the PIFS (PCF Interframe Space), which is smaller than the DIFS or the AIFS. Therefore, the hybrid coordinator can poll any stations with prioritized medium access whenever it wants. During the CFP, the hybrid coordinator schedules all stations as a point coordinator in the PCF. The major difference is the prioritized allocation by the hybrid coordinator. The IEEE 802.11e also specifies a controlled contention mechanism, which allows stations reporting the resource demands to the hybrid coordinator. The hybrid coordinator thus can dynamically assign priority.

The 802.11 standards only specify the MAC and the physical layers. They purposely do not restrict implementation techniques. This strategy has stimulated the progress of WLAN technologies. However, the interoperability of 802.11 products from different vendors has become a serious problem. To assure the interoperability of multi-vendor access points, the 802.11f committee has specified the Inter Access Point Protocol (IAPP). IAPP is a protocol for access points to communicate with each other. Most important, this protocol standardizes the handoff information of a multi-vendor WLAN network and promises the mobility among different 802.11 WLAN networks.

The work of 802.11f has been completed and is now a recommended practice part of the 802.11 standards. The 802.11e is still a draft specification. The completed standard should be ratified in late 2003.

Table 1 Comparison of various WLAN standards

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g	ETSI HIPERLAN/1	ETSI HIPERLAN/2	MMAC HiSWANa
Ratification	Jun.1997	Sept. 1999	Sept. 1999	June 2003	early 1996	Feb. 2000	April 1999
RF band	2.4GHz	2.4GHz	5GHz	2.4GHz	5GHz	5GHz	5GHz
Max. data rate	2 Mbps	11Mbps	54 Mbps	54Mbps	23.5 Mbps	54 Mbps	27 Mbps
Physical layer	FHSS, DSSS, IR	DSSS/CCK	OFDM	OFDM, PBCC	GMSK	OFDM	OFDM
Typical range	50-100m	50-100m	50-100m	50-100m	50m	50m indoor, 300m outdoor	100-150m

Wireless Fidelity (Wi-Fi) certification for interoperability

Today, most WLAN systems follow the IEEE 802.11 standards, especially 802.11b. The Wireless Ethernet Compatibility Alliance (WECA) launched in 1999 has strived for 802.11 interoperability. Its members include more than two hundred wireless networking companies worldwide. The mission of WECA is to *certify interoperability of Wi-Fi products and to promote Wi-Fi as the global wireless LAN standard across all market segments*. The wireless fidelity (Wi-Fi) compliant certification has been awarded to more than 611 products. Users may deploy these Wi-Fi products from different vendors according to their demands.

Wi-Fi certification now assures interoperability of 802.11b High Rate products. WECA also has an interoperability test for the 802.11a standard. This standard is expected to be used by most products in the future WLAN market. In addition, WECA has developed *Wi-Fi Protected Access (WPA)* as a near-term security solution before the 802.11i is ratified.

HIPERLAN

In 1992, the European Telecommunications Standards Institute (ETSI) formed a committee to establish the HIgh PErformance Radio LAN (HIPERLAN) standards. The features and capabilities of the HIPERLAN standards are similar to those for the IEEE 802.11 standards. The HIPERLAN/1 standard provides wireless communication with maximum data rate of 23.5 Mbps at the 5 GHz band. It was ratified in early 1996. HIPERLAN/1 uses Gaussian Minimum Shift Keying (GMSK) modulation which also has been adopted in the Global System for Mobile Communications (GSM) cellular system. However, owing to the complexity of implementation and the huge processing power required, HIPERLAN/1 is seldom used commercially.

Following the HIPERLAN/1 standard, HIPERLAN/2 specifications were started in mid-1998 and the first specifications were published in 2000. The ETSI HIPERLAN/2 and the IEEE 802.11a converge in many aspects. The HIPERLAN/2 operates in the same 5 GHz band as 802.11a does. The HIPERLAN/2 also provides high data rate up to 54 Mbps with OFDM technology. In contrast to the CSMA/CA of 802.11a MAC, however, the HIPERLAN/2 standard adopted a reservation-based time-division multiple access (TDMA) with time-division duplex (TDD) mechanism in the MAC.

Also, several issues relevant to 802.11a were improved by the HIPERLAN/2. The HIPERLAN/2 uses dynamic frequency selection (DFS) to reduce the interference problem and more fully utilize the available spectrum. DFS accomplishes this task by automatically allocating the carrier frequency based on the interference measured by the access point and its associated mobile terminals.

Moreover, HIPERLAN/2 is basically superior in QoS support. Different radio bearers are provided with different QoS levels by adjusting several error control settings such as automatic repeat request window size, retransmission and discarding occasions. HIPERLAN/2 aim is to work with different core networks, especially the third generation (3G) cellular systems.

MMAC – HiSWAN

Started in 1996 in Japan, Multimedia Mobile Access Communication (MMAC) System was developed to *transmit ultra high speed, high quality Multimedia Information anytime and anywhere" with seamless connections to optical fiber networks*. The MMAC-HiSWAN (High Speed Wireless Access Network) system uses two frequency bands: 5 GHz for HiSWANa and 25 GHz for HiSWANb. Here we focus on the HiSWANa using the 5 GHz license-free frequency band. The HiSWANa standard is closely aligned with the ETSI HIPERLAN/2 standard. HiSWANa adopts the OFDM physical layer providing a standard speed of 27 Mbps and 6-36 Mbps by link adaptation. However, MMAC HiSWANa differs from the ETSI HIPERLAN/2 in radio network functions owing to the differences in regional frequency planning and regulations. Instead of DFS in HIPERLAN/2, carrier sense functions of access points are mandatory in MMAC HiSWANa. Also, inter-access point synchronization is specified to avoid interference among access points and to use four available channels in Japan for wide coverage. The radio access functional specifications version 1.1 was released on 12 April 1999. (Various WLANs discussed in this article are summarized in Table 1.)

Public Wireless LAN services

In the third quarter of 2002, the hardware shipment of 802.11b grew by 24% and continues to dominate the WLAN market. On the other hand, the end-use revenues increased only eight percent because the price of WLAN products dropped drastically according to the Reed electronics Group. With the popularization of WLAN products, public access WLAN services are springing up all around the world. Numerous WLAN operators are providing diverse services in airports, hotels and cafes.

Spectrum management

At present, most WLAN products operate on the 2.4 GHz frequency band. Even though the entire 2.4 GHz band has been allocated for unlicensed use in most countries, public WLAN services still highly rely on government policy. The regulation and spectrum management by the governments directly influence services proposed by WLAN operators. In European market, France and the United Kingdom impose more restrictive regulations than those in other countries.

In France, only indoor applications with 10 mW can use the whole 2.4 GHz band (2.4 GHz - 2.4835 GHz). Indoor applications with 100 mW are allotted frequencies ranging from 2.4465 GHz to 2.4835 GHz only. For outdoor applications, the use of WLANs in public property is not permitted. Only the frequency band of 2.4465-2.4835 GHz with a maximum power of 100 mW is available on private property or the private property of public persons.

Depending on the geographic location, a prior authorization procedure with the advice of the France's Ministry of Defense is essential. Due to the highly limited frequency, the growing public access WLAN market in France will soon suffer frequency saturation. Thus, the probability of interference will greatly increase. As a result, the French government has scheduled releasing the whole 2.4 GHz band in the beginning of 2004.

In the United Kingdom, only private WLAN systems in the 2.4 GHz are permitted. Public service to a third-party in the 2.4 GHz band without a license is illegal under current regulations. The Unspecified Temporary Use License issued by the Radiocommunications Agency is only available to trial commercial systems in either the 2.4 or the 5 GHz bands. Under current restrictions in the UK, wireless Internet service providers (W-ISPs) can help customers such as offices, home networks, hotels and restaurants, set up WLAN systems and provide customer support. W-ISPs however cannot charge directly for wireless access. Proposals allowing

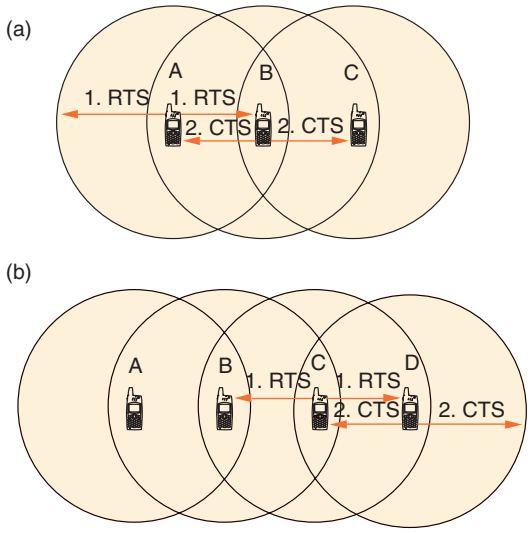


Fig. 3 (a) Hidden node and (b) exposed node

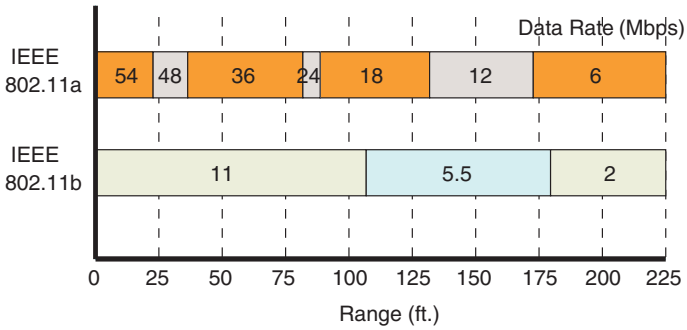


Fig. 4 Data rate vs. radio coverage range in 802.11a and 802.11b

public telecommunications without a license were set out in a National Consultation Document in late 2001. The UK government is now making decision whether or not to allow license-exempt public WLAN.

The next generation WLAN systems are expected to operate in the 5 GHz frequency band, which undoubtedly will provide a cleaner spectrum and a higher data rate for innovative wireless network applications. However the 5GHz band is still regulated in many countries. Regulators must carefully legislate the rules to ensure normal growth of the WLAN market and a smooth transition to the new technologies. At the same time, issues of interference, congestion and spectrum saturation should also be cautiously considered.

Hot spots

The liberal regulatory environment that exists in most countries allows public WLAN market to flourish. Public access WLAN services can be classified into two service types: indoor *hot spot* WLAN service and outdoor *last-mile* broadband access. Hot spot service provides indoor public wireless access to the Internet, typically in airports, coffee shops, restaurants or hotels. On the other hand, the last-mile broadband access is similar to the wireless local loop (WLL). Instead of the expensive fixed networks, W-ISPs bridge their customers through the air with a large coverage. Even so, WLAN last-mile services are still rarely deployed. Hot spot services, on contrast, have been widely commercialized.

According to the estimation by Toshiba in mid-2002, there were around 1,200 locations providing hot spot services in the United States. Hot spots usually charge customers for wireless access time. Different charging plans allow customers to choose from a monthly subscription to a metered plan, which is rated by how long customers use the service in the hot spot. Besides charging by access time, the other payment method used is charging by the volume of data transmitted. This billing strategy is often adopted in General Packet Radio Service (GPRS) connections. Compared with charging by access time, charging by volume seems to be more reasonable for users since the Internet connection is usually non-continuous.

Summary

Wireless LANs support high data rate in a mobile environment with limited radio coverage. The license-free spectrum has encouraged the growth of the WLAN market. Applications and services are thriving. In the mean time, the IEEE 802.11 committee and research community still strive to improve and innovate the wireless networking technologies.

However, the unlicensed spectrum also introduces interference. Regulators must carefully strike the balance between the market growth and the spectrum management. On the other hand, service providers must keep advancing their quality of service and providing reasonable billing strategy. Today third generation (3G) wireless telecommunication technologies are taking off. It is expected the *high data* rate of WLAN systems and the *large coverage area* of 3G systems will complement each other.

Acknowledgments

This work was sponsored in part by MOE Program for Promoting Academic Excellent of Universities under the grant number 89-E-FA04-1-4, National Science Council under the grant number 91-2213-E-007-039, and Industrial Technology Research Institute under the contract of T1-92019-3.

Read more about it

• IEEE P802.11, The Working Group for Wireless LANs." http://grouper.ieee.org/groups/802/11/index.html.

• J. C. Chen and J. M. Gilbert, "Measured performance of 5-GHz 802.11a wireless LAN systems." Atheros Communications, Inc., Aug. 2001. http://www.atheros.com/AtherosRangeCapacityPaper.pdf.

• N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. in *Proc. of ACM MOBICOM*, 2001.

• S. Kapp, "802.11: leaving the wire behind,"*IEEE Internet Computing*, vol. 6, pp. 82–85, Jan./Feb. 2002.

• S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz, and L. Stibor, "IEEE 802.11e wireless LAN for quality of service," in *Proc. of European Wireless*, (Florence, Italy), Feb. 2002.

• Wireless Ethernet Compatibility Alliance." http://www.weca.net/.

• I. R. Johnson and S. K. Barton, "Standards for wireless LANs," *Wireless Technology (Digest No. 1996/199), IEE Colloquium on*, pp. 5/1 –5/5, 1996.

• J. Khun-Jush, P. Schramm, G. Malmgren, and J. Torsner, "HiperLAN2: broadband wireless communications at 5 GHz," *IEEE Communications Magazine*, vol. 40, pp. 130–136, June 2002.

• Multimedia Mobile Access Communication Systems." http://www.arib.or.jp/mmac/e/.

• J. D. Vriendt, P. Lainé, C. Lerouge, and X. Xu, "Mobile network evolution: a revolution on the move," *IEEE Communications Magazine*, vol. 40, pp. 104–111, Apr. 2002.

• "3Q 2002 wireless LAN market analysis," Tech. Rep. IN020202WL, In-stat/MDR, Reed Electronics Group, Dec. 2002.

About the authors

Jui-Hung Yeh received his B.S. degree from the Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan in 2002. He is now a Ph.D. student in the same department.

Jyh-Cheng Chen (S'96, M'99, SM'03) is an Associate Professor in the Department of Computer Science and the Institute of Communications Engineering, National Tsing Hua University, Hsinchu, Taiwan. Prior to joining the University as an Assistant Professor, he was a Research Scientist at Telcordia Technologies (formerly Bellcore), Morristown, NJ, from August 1998 to August 2001. At Telcordia, he was one of the key architects and implementers of the ITSUMO (Internet Technologies Supporting Universal Mobile Operation) project. In Spring 2001, he was also an adjunct faculty member in the Dept. of Elect. & Comp. Engineering, New Jersey Institute of Technology, Newark, NJ. While working on his Ph.D., he worked for AT&T Labs, Whippany, NJ, and ASOMA-TCI Inc., N. Tonawanda, NY. Dr. Chen has published over three dozen papers. He holds four U.S. patents with the other 15 pending U.S. patent applications. Dr. Chen received the 2000 Telcordia CEO Award, and the 2001 SAIC ESTC (Executive Science and Technology Council) Publication Award. He received his Ph.D. degree from the State University of New York at Buffalo in 1998. Dr. Chen is an IEEE Senior member.

Chi-Chen Lee received his BS degree in Computer Science and Information Engineering from the Fu-Jen Catholic University, Hsinchuang, Taiwan in 2001, and MS degree in Communications Engineering from the National Tsing Hua University, Hsinchu, Taiwan in 2003.