

# WLAN Radio and Networks

Timo Hänninen  
Helsinki University of Technology

## Abstract

This paper introduces the wireless network standards and concentrates on the IEEE 802.11 standards. In addition, this paper introduces the outlines of frequency allocation, network ranges and basics of radio communication. Some problems of WLANs are also pointed out and possible solutions are presented.

## 1 Introduction

Wireless local area networks (WLAN), especially the IEEE 802.11b based WLANs, have become very common. Wireless networks utilize license-free frequency bands. WLANs normally offer a transmit rate of 11 Mb/s and cover a range of tens of meters. There are many WLAN standards, of which the IEEE 802.11 standards are the most popular. The physical layer specifications are evolving fast, but on the other hand the link layer specifications are pretty stable.

Section 2 describes the frequencies and radio of WLAN. Section 3 addresses the different wireless network standards. In Section 4, the physical layer of WLAN is described. Section 5 describes and analyzes the link layer of WLAN, and Section 6 concludes the paper and proposes future work.

## 2 Frequencies for Wireless Techniques

The two primary methods for wireless signal transmission are light, particularly infrared, and radio waves. Light transmission is normally used within a short range, such as between mobile phone and laptop computer. Radio waves are versatile: the connection can be as short as the connection between a keyboard and a computer or as long as the distance between a satellite and a satellite dish. [3]

### 2.1 Frequency Allocation

A specialized agency of the United Nations (UN), the International Telecommunications Union - Radiocommunications Sector (ITU-R), coordinates international standards, regulations, and promotes the efficient use of the radio spectrum. The ITU spectrum plan divides the world into three regions [10]:

1. Europe, Africa, Middle East, Russia
2. South, and North America
3. China, Japan, Southeast Asia, and South Pacific

Within each region, regional and national agencies deal with the detailed spectrum planning and management. In Finland, the Finnish Communications Regulatory Authority (FICORA, in Finnish “Viestintävirasto”) oversees the use of radio frequencies. [1]

## 2.2 ISM Band

There are also license-free radio bands for industrial, scientific and medical (ISM) purposes. The ISM band is defined by the telecom standardization organization of the ITU (ITU-T). The ISM band includes several frequency ranges [15]:

- 902–928 MHz
- 2.4–2.483 GHz
- 5.15–5.35 GHz
- 5.725–5.875 GHz

In addition to wireless network equipments, video cameras, microwave ovens and Bluetooth equipments use the 2.4–2.483 GHz frequency range. The utilization of the ISM band is often difficult, because all devices use the same frequency band and different devices can interfere with each others.

## 2.3 WLAN Coverage

Cabling specifications consistently provide a maximum channel length for a given type of cable. In contrast, the coverage of a wireless system depends on the characteristics of the site where the system is to be installed. Naturally, the transmit power and sensitivity of the receiver also affect the coverage. In Finland, the maximum effective isotropically radiated power (EIRP) of a 2.4 GHz signal is 100 mW (20dBm). In the USA, the coverage of 2.4 GHz WLAN system is larger, because the maximum EIRP is 1000 mW (30 dBm). The FICORA has also allocated other frequency ranges within the ISM band, where EIRP of 200 mW can be used indoor and EIRP of 1000 mW can be used outdoors. [9, 8]

The coverage of a WLAN system depends highly on the environment. A reliable estimate for a point-to-point distance of a 2.4 GHz signal in an open environment is a minimum of 120 m, but could be as high as 200 m. In an obstructed environment an estimate for point-to-point distance is 10 m. The coverage area provided by WLAN equipment may also vary significantly from one manufacturer to another. [7]

## 2.4 Antennas and Propagation

In addition to power output and sensitivity of WLAN card, cables, connectors, antennas, intervening clutter, noise, and even weather affect the range of a signal. The propagation of radio signal divides into free space, reflection, diffraction and scattering mechanisms. At first, I figure out how much a signal attenuates between two sites. It is called the path loss:

$$L = 10 \log \left( \frac{\lambda}{4\pi d} \right)^2 \text{ dB}, \quad (1)$$

where  $\lambda$  is the wavelength, and  $d$  is the distance between antennas. The equation (1) is valid, when both antennas radiate and receive equally in all directions. That kind of isotropic antenna is hypothetical, but it represents convenient reference antenna. [16]

Thus, I can calculate, if it is possible to set up a WLAN system with a one-kilometer range. Using equation (1), the signal loss for a 2.45 GHz signal is  $-100.2$  dB. The transmitter output power of a Orinoco card is 15 dB, and losses are approximately 4 dB. I suppose that signal has the maximum amplification on site A, so the EIRP of site A is 20 dBm. On site B, the antenna gains 5 dBi. The total gain of site B is  $15 - 4 + 5 = 16$ . [11]

Now, I subtract the path loss from the total gain:

$$20 + 16 - 100.2 = -64.2$$

The sensitivity of a receiver depends on the data transfer rate. For example, the receiver sensitivity specifications for the Orinoco PC Card (Silver/Gold) are shown in Table 1.

11 Mb/s	5.5 Mb/s	2 Mb/s	1 Mb/s
-82 dBm	-87 dBm	-91 dBm	-94 dBm

Table 1: Receiver sensitivity for Orinoco Silver/Gold cards [11, 14].

We are generating a signal of  $-64.2$  dBm. If the transmit rate is 11 Mbps, there is a margin of error of 17.8 dB. Typically, a margin of error of 20 dB is enough to ensure normal operation despite weather conditions or interference. The range can be extended by lowering the transmit rate, amplifying the signal, or using beam antennas. For example, the margin of error would be 22.8 dB, if transmit rate of 5.5 Mb/s was used. When amplification is designed, the regulations discussed in Section 2.3 must be followed. [11]

## 3 WLAN Standards

The 802.11 Working Group was formed in September of 1990. Their original goal was to create a wireless LAN specification that will operate in one of the ISM ranges. The first 802.11 standard was released in 1997 by IEEE.

The IEEE 802 standards address the lower levels of the OSI model. However, the 802 model splits the data link layer into two parts: Logical Link Control (LLC) and Media Access Control (MAC). The 802.2 standard defines a common LLC layer that is used by other 802 MAC and Physical Layer (PHY) standards. Figure 1 shows the lower layers of the 802 series of protocols. [3, 12]

802 LCC			
802.11 MAC			
802.11	802.11b	802.11a	802.11g

Figure 1: The layers of the IEEE 802 series of protocols [12].

The original IEEE 802.11 specification documented three different physical layers: Infrared, 2.4 GHz Frequency Hopping Spread Spectrum (FHSS), and 2.4 GHz Direct Sequence Spread Spectrum (DSSS). 802.11b was released in 1999, and it provides a higher bit rate using DSSS in the 2.4 GHz range. The newest physical layer standards of IEEE, 802.11a and 802.11g, use Orthogonal Frequency Division Multiplexing (OFDM) modulation and operate at very high bit rates. IEEE 802.11g is expected to be published in mid-June 2003. It provides backward compatibility with existing 802.11b standard and offers 54 Mb/s transfer rate. [3, 6]

HiperLAN/2 is specified by European Telecommunications Standards Institute (ETSI). Both HiperLAN/2 and 802.11a operate at a maximum of 54 Mb/s using frequencies in the unlicensed 5 GHz band. The HomeRF was developed by the HomeRF Working Group, which disbanded in January of 2003. Table 2 shows the specifications of physical layer standards. [13]

Standard	Max Data Rate	Frequency	Modulation
802.11	2 Mb/s	2.4 GHz (and IR)	FHSS and DSSS
802.11b	11 Mb/s	2.4 GHz	DSSS
802.11g	54 Mb/s	2.4 GHz	OFDM
802.11a	54 Mb/s	5 GHz	OFDM
HiperLAN/2	54 Mb/s	5 GHz	OFDM
HomeRF 2.0	10 Mb/s	2.4 GHz	WBFH

Table 2: WLAN Standards [3, 5, 4, 6, 13, 2].

## 4 Physical Layer of WLAN

The role of the physical layer is to handle the transmission of data between nodes. In most WLAN systems, the signal is modulated using spread spectrum (SS) modulation technique which was developed by the U.S. Army. The spread spectrum technique generates an expanded bandwidth wideband signal. Spread spectrum radio communicating resists jamming and makes difficult to intercept the transmission. In addition, other transmission and electrical noise will only interfere with a small portion of the spread spectrum signal,

which results in less interference and less errors during the demodulation. Spread spectrum technology is suitable for devices utilizing ISM bands, because there is always a lot of noise. In addition, there is no limit on the number of subscribers that are supported. As more and more users are using the same ISM band, there is a graceful degradation of the quality of communication. Thus, spread spectrum technique is ideal for the ISM band, unlike techniques following channelization principle and restricting number of simultaneous subscribers (e.g. TDMA/FDMA). [10]

#### 4.1 Spreading Techniques

In Finland, there are 13 frequencies for DSSS use. These frequencies are listed in Table 3. The DSSS supports transfer rates up to 11 Mb/s. In DSSS signaling, each bit in the data stream to be transmitted is multiplied by a pseudo-noise (PN) code sequence. The result is referred to as chipping code, which is normally 11 bits. The receiving device is synchronized to the transmitting device and listens for the presence of chipping codes, ignoring all other frequencies. However, in 5.5 Mb/s and 11 Mb/s DSSS systems, 8-chip complementary code keying (CCK) is employed as the modulation scheme. The DSSS system uses base band modulations of differential binary phase shift keying (DBPSK) and differential quadrature phase shift keying (DQPSK).

Channel	Frequency	Channel	Frequency
1	2.412 GHz	8	2.447 GHz
2	2.417 GHz	9	2.452 GHz
3	2.422 GHz	10	2.457 GHz
4	2.427 GHz	11	2.462 GHz
5	2.432 GHz	12	2.467 GHz
6	2.437 GHz	13	2.472 GHz
7	2.442 GHz		

Table 3: DSSS frequencies in Finland.

When DSSS is used and the transfer rate is 11 Mb/s, the channels need to be separated by at least 25 MHz (or 5 channels) to prevent overlap and possible interference. For example, it is possible to use channels 1, 7, and 13 on nearby access points without any frequency overlap. Therefore, frequency planning is needed, when operating frequency is selected for adjacent networks. [11]

Figure 2 shows the frame format of the physical layer convergence protocol (PLCP). The PLCP protocol data unit includes the DSSS PLCP preamble, the DSSS header, and the MAC protocol data unit (MPDU). Synchronization (SYNC) field consists of 128 bits of scrambled ones and it is used while synchronization of receivers. Start frame delimiter (SFD) indicates the start of PHY-dependent parameters. The value of the SFD field is fixed,  $F3A0$  in hexadecimal. The signal field indicates the modulation type and the data rate. The service field is reserved for future use. The length field indicates the number of microseconds required to transmit the MPDU. Finally, the CRC field is a CRC-16 frame check sequence of signal, service, and length fields. In DSSS, all bits are scrambled prior to transmission.

Sync 128 bits	SFD 16 bits	Signal 8 bits	Service 8 bits	Length 16 bits	CRC 16 bits	MPDU
PLCP Preamble		PLCP Header				

Figure 2: DSSS: the frame format of PLCP [3].

In FHSS signaling, the frequency band is divided into a large number of channels—79 channels in most countries for the 2.4 GHz band. FHSS uses a narrowband carrier that changes frequency, or hops, from a channel to another frequently. Before sending a message, the sending and receiving devices select a common hopping sequence from a set of available patterns. FHSS uses two- or four-level Gaussian Frequency Shift Key (FSK) modulation. Due to the narrow band (1 MHz), the maximum transmit rate of FHSS is only 2 Mb/s. Figure 3 shows the frame format of the FHSS physical layer convergence protocol. [3]

Sync 80 bits	SFD 16 bits	PLW 12 bits	PSF 4 bits	HEC 16 bits	PSDU
PLCP Preamble		PLCP Header			

Figure 3: FHSS: the frame format of PLCP [3].

The PLCP frame format of FHSS is simpler than the PLCP frame format of DSSS. The SYNC field is only 80 bits. The FHSS PLCP header consists of three fields: the PSDU length word (PLW), PLCP signaling field (PSF) and header error check (HEC) field. In FHSS, only the MAC PDU is scrambled prior to transmission.

OFDM provides transfer rates up to 54 Mb/s. OFDM encodes a single transmission into multiple sub-carriers. After that, all subchannels are multiplexed into one fast combined channel. The OFDM system uses 52 subcarriers that are modulated using BPSK, QPSK, or quadrature amplitude modulation (QAM/64-QAM). The maximum data rate, 54 Mb/s, is obtained by using 64-QAM modulation and inserting 216 data bits per OFDM symbol. The OFDM PLCP frame format is shown in Figure 4. [4]

12 symbols	Rate 4 bits	Res 1 bit	Length 12 bits	Parity 1 bit	Tail 6 bit	Service 16 bits	PSDU + Tail + Pad Bits
PLCP Preamble	PLCP Header						

Figure 4: OFDM: the frame format of PLCP [4].

The PLCP preamble field constitutes of 12 “training sequences” [4]. OFDM is very sensitive to synchronization and frequency errors, so the preamble field is considerably long. Rate, reserved, length, parity, and tail fields are mapped onto a single BPSK encoded

OFDM symbol, which is denoted as the signal symbol. Service, PSDU, tail, and pad fields constitute the data part of transmission. The length of data is a variable number of OFDM symbols.

## 4.2 WLAN Topologies

The IEEE 802.11 specifies two modes of WLAN operation: ad hoc and infrastructure mode [3]. In case of IEEE 802.11b, radios participating in a wireless network must operate in one of the modes. In a wireless network, each device is referred to as a station and an access point (AP) provides wireless-to-Ethernet bridging [3, 5].

The independent basic service set (IBSS) is the most basic type of IEEE 802.11 LAN [3]. This mode is possible, when there is no access point in the network, but stations are communicating directly. That kind of network is often formed without pre-planning, and that is why it is called ad hoc network.

In infrastructure mode, the wireless network consists of a set of stations and at least one AP. This configuration is called a basic service set (BSS). When the area to be covered exceeds the range of a single BSS, multiple BSSs are linked by interconnecting APs. The architectural component used to interconnect BSSs is the distribution system (DS). An access point is station that provides access to the DS by providing DS services in addition to acting as a station. Extended service set (ESS) refers to a physical subnet that contains more than one AP [11]. Stations within an ESS may communicate and move (“roam”) from one BSS to another transparently to LLC. Figure 5 shows the components of IEEE 802.11.

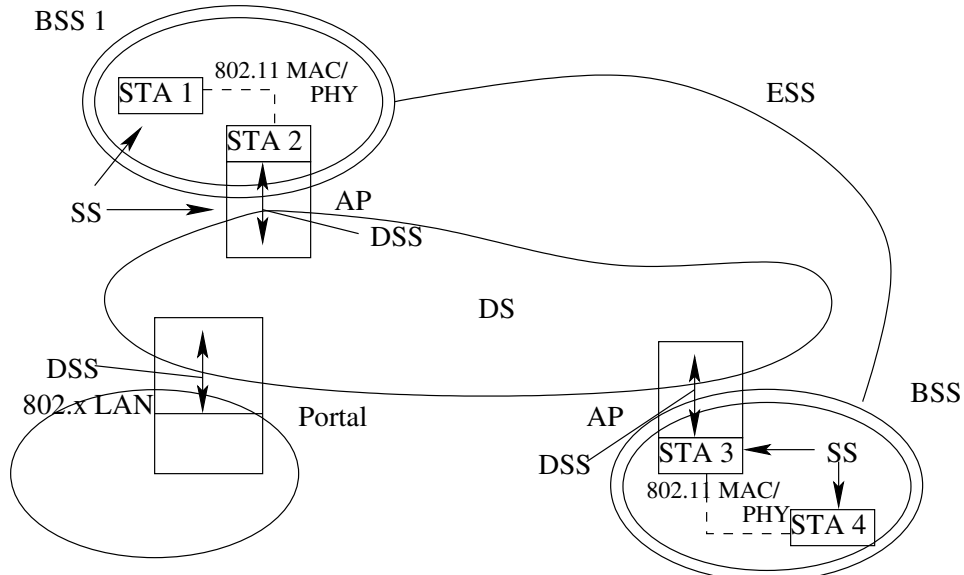


Figure 5: Complete IEEE 802.11 architecture [3].

## 5 Link Layer of WLAN

The 802.11 MAC, which is same for all currently deployed 802.11 technologies, provides several functions: access to the wireless medium, joining and leaving network, and security services. Table 4 shows the complete set of IEEE 802.11 architectural services.

Station services (SS)	Distributions system services (DSS)
Authentication	Association
Deauthentication	Disassociation
Privacy	Distribution
MSDU delivery	Integration
	Reassociation

Table 4: IEEE 802.11 architectural services [3].

### 5.1 Medium Access Control

Access to the wireless medium is controlled by distributed coordination function (DCF) known as carrier sense multiple access with collision avoidance (CSMA/CA). When using the contention-based CSMA/CA access method, any device on the WLAN being about to transmit a message must listen on the appropriate frequency to ensure that no other device is transmitting. The device can start to transmit, if the channel is clear. If the channel is busy, the device initiates a random backoff counter, which must expire before another attempt to transmit can be made. On the other hand, in Ethernet networks the signals may collide, but collisions must be detected.

In infrastructured networks, an optional access method called a PCF can be used. That access method uses a point coordinator, which operates at the access point of the BSS and determines which station has the right to transmit.

Each device on a 802.11 WLAN have a 48-bit address, which is used to uniquely identify each device or AP. The address is often referred as MAC address. There are also multi-cast and broadcast addresses, for example *FF-FF-FF-FF-FF*, which are used, when the message is intended for several devices on the same network. The format of a message is called frame. Figure 6 shows the fields of the WLAN frame.

The frame control field is used to transfer control information between devices. Its sub-fields identify such items as the protocol version, data fragment status and power management status. The duration field indicates the amount of time required for the frame to be transferred. If its value is less than 32768, the duration value is used to update the network allocation vector (NAV). The first three address fields are always used for values of the receiving AP, the sending AP, and the destination device. If the frame is transferred through many APs, the fourth address field indicates the address of the sending device. The sequence control field is used to handle fragment of an MSDU and to detect duplicate frames. The data field contains the payload. The FCS field contains a 32-bit CRC, which is calculated over all fields of the MAC header and the frame body.

Frame control	2 octets (= 2 · 8 bits)
Duration/Identification	2 octets
Address 1	6 octets
Address 2	6 octets
Address 3	6 octets
Sequence control	2 octets
Address 4	6 octets
Data	Maximum: 2312 octets
Frame check sequence (FCS)	4 octets

Figure 6: IEEE 802.11 general MAC frame format [3].

Individual types of frames are: control frames, data frames, and management frames. Control frames provide mechanisms for controlling the transmission, and the payload is transmitted using data frames. Management frames are used in many ways: for beacon, association, authentication and probe purposes. For example, a station joins a BSS in the following way [12]:

1. Station looks for available APs. APs may suppress beacons for security reasons, when the station must know the appropriate SSID.
2. Station identifies an AP it wants to join and sends an association request to the AP. A handshake will take place. Authentication may be needed in order for client to join the network.
3. Then, the station associates itself with the AP and officially joins the wireless network.
4. After using networks services, the station should disassociate from the AP. APs will also use time outs to disassociate idle connections.

The MAC also handles synchronizing and power management functions. For example, the FHSS relays on clock of each station, so the synchronizing is really important. In an infrastructured network, stations can choose power control mode and inform the AP by sending an appropriate frame. In a low power mode the station listens to beacons sent by the AP. If the station is in low power, the AP will buffer station's packets until it will send a PS-Poll message.

## 5.2 Challenges for Medium Access Control

There are some problems with carrier sensing. The first one is known as the *exposed terminal problem*: stations A and C are within the range of station B. A is transmitting to B, and C wants to transmit to D, which is not possible due to carrier sense. The second problem is called the *hidden terminal problem*: stations A and C are within the range of station B, but they know nothing about each others. If A is already transmitting to B, C cannot start to transmit, even if the medium is free.

The *hidden terminal problem* can be solved by utilizing clear to send (CTS) and request to send (RTS) messages. The transmitter sends a RTS message and the receiver sends a CTS message. If some other station listens a RTS message, it has to wait for a CTS message from the same station. If some other station listens a CTS message, it has to wait long enough to send its data. In addition, NAV maintains prediction of future traffic on the medium based on RTS/CTS frames prior to actual exchange of data. Hence, a transmission consists of 4 messages: RTS, CTS, the actual frame, and ACK. The extra messages will naturally produce some overhead.

## 6 Conclusions

In recent times, wireless local area networks are getting adopted to homes and enterprises. The advantages of WLAN are to offer wide band mobility within rather small areas and low infrastructure cost. However, wired networks provide better performance and security. Normally, the range of a single access point doesn't exceed one hundred meters. WLANs use license-free frequency bands, which means, that wireless network devices share the band with many other devices, so there is a lot of noise in the wireless medium. In addition, stations must use rather low transmission power due to regulations.

The IEEE 802.11 is the most common physical layer specification for wireless networks. It offers maximum data rate of 11 Mb/s using DSSS in the 2.4 GHz range. The 802.11a is a more recent specification offering maximum data rate of 54 Mb/s using OFDM in 5 GHz range. However, the devices of different standards may not interoperate.

IEEE 802.11 standards specify the OSI physical and the bottom of the OSI data-link layer. The physical layer specifications are evolving fast, but the 802.11 MAC is stable. The MAC offers several functions, for example, access to the wireless medium and encryption. Unlike Ethernet, 802.11 tries to avoid collisions—not to detect. However, the operations of 802.11 MAC slightly reduce performance.

The main outcome of this paper is the discussion of WLAN infrastructure and standards. The discussion points out the problems of WLANs and clarifies, why building of wireless networks can be difficult. Future studies could analyze WLAN standards more specifically and study interoperability of different WLAN standards.

## References

- [1] Anonymous. FICORA - Radiocommunications. FICORA, 14 March 2003 [cited 25 March 2003]. Available from Internet: <<http://www.ficora.fi/englanti/radio/index.htm>>
- [2] Anonymous. HomeRF Specification Revision 2.01. HomeRF Working Group, Inc, 1 July 2002 [cited 23 March 2003]. Available from Internet: <<http://www.palowireless.com/homerf/docs/HomeRF-2.01-us.zip>>
- [3] Anonymous. IEEE 802.11. 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 and Physical Layer Specifications. New York: Institute of Electrical and Electronics Engineers. 528 pp, 1997.
- [4] Anonymous. IEEE 802.11a. 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 specifications High-speed Physical Layer in the 5 GHz Band New York: Institute of Electrical and Electronics Engineers, 1999.
- [5] Anonymous. IEEE 802.11b. 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 and Physical Layer specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band New York: Institute of Electrical and Electronics Engineers, 1999.
- [6] Anonymous. IEEE 802.11g. IEEE P802.11g (TM), 54Mbps Extension to 802.11b Wireless Local Area Networks, Gains Working Group Approval Final Approval Expected in June 2003 14 February 2003 [cited 13 April 2003]. Available from Internet: <<http://standards.ieee.org/announcements/80211gapp2.html>>
- [7] Anonymous Networking Technologies USA. BICSI. 308 pp, 2002.
- [8] Anonymous. The IEEE 802.11 Wireless LAN Standard. WLANA. 2001 [cited 27 March 2003]. Available from Internet: <<http://www.wlana.org/learn/tables.htm>>
- [9] Anonymous. Viestintävirasto - Langattomat lähiverkot 2,45 GHz taajuusalueella. FICORA, 28 March 2003 [cited 28 March 2003]. Available from Internet: <[http://www.ficora.fi/suomi/radio/2\\_45GHz.htm](http://www.ficora.fi/suomi/radio/2_45GHz.htm)>
- [10] Clark, M. Wireless Access Networks UK. John Wiley & Sons, Ltd. 414 pp, 2000.
- [11] Flickinger, R. Building Wireless Community Networks California. O'Reilly & Associates, Inc. 125 pp, 2002.
- [12] Garg, V.; Smolik, K.; Wilkes, J. Applications of CDMA in Wireless/Personal Communications New Jersey. Prentice Hall. 360 pp, 1997.
- [13] Johnsson, M. HiperLAN2 The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band. [cited 26 March 2003]. Available from Internet: <<http://www.hiperlan2.com/presdocs/site/whitepaper.pdf>>
- [14] Korotigin, S. Cisco and Lucent Equipment for Wireless Networks. 2002 [cited 24 March 2003]. Available from Internet: <http://www.digit-life.com/articles/wlan/index2.html>
- [15] Potter, B.; Fleck, B. 802.11 Security. California. O'Reilly & Associates, Inc. 176 pp, 2002.
- [16] Tamminen, J. 2.4 GHz WLAN Radio Interface. 19 November 2002 [cited 20 March 2003]. Available from Internet: <[http://www.radionet.fi/res/276/TUT\\_WLAN\\_Seminar.pdf](http://www.radionet.fi/res/276/TUT_WLAN_Seminar.pdf)>