

ASSESSMENT OF RADIO FREQUENCY EXPOSURE FROM WLAN

Yngve Hamnerius⁽¹⁾

⁽¹⁾*Signals and Systems, Chalmers University of Technology, SE-41296 Göteborg, Sweden,
yngve@elmagn.chalmers.se*

Computers can be connected to each other; this connection is called a local area network (LAN). A wireless LAN (WLAN) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure. A typical WLAN consists of *wireless stations*, which usually is a PC, equipped with a wireless network interface card, and *access points*, which acts as a bridge between the wireless and wired networks. An access point usually consists of a radio, a wired network interface, and bridging software.

To be able to assess the human exposure correctly, accurate measurement methods are necessary. Measurement methods for other communication systems such as GSM and to some extent UMTS exists today. By combining existing measurement methods from other communication systems with knowledge of the physical layers of WLAN-systems a spectral measurement method can be developed. In the far field traditional RF equipment such as a measurement antenna and a spectrum analyzer or a measurement receiver can be used. In the case that the exposure from the wireless station shall be assessed in the near field, *i.e.* if a laptop is used in the lap or a wireless IP-phone close to the head, SAR is the most relevant measure of exposure. The same type of equipment as used for measuring the SAR values for mobile phones can be used.

Measurements shows that the exposure from access points is generally low compared to ICNIRP's reference levels. This is also true for the exposure from most wireless stations, however if the wireless station is used in contact with the body, exposure up to the range of the ICNIRP basic restrictions for general public has been measured.

INTRODUCTION

Computers at a company are usually connected to each other; this connection is called a local area network (LAN). The LAN can be connected to other networks, for example the internet. The computers in a LAN are connected via cables. A wireless LAN, WLAN, is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure. In the corporate enterprise, WLAN are usually implemented as the final link between the existing wired network and a group of client computers, giving these users wireless access to the full resources and services of the corporate network. The first WLAN came in the eighties, at that time they were called radiolan.

Both LAN and WLAN are standardised by IEEE. Ethernet is, today, the de-facto hardware standard for LAN. For WLAN, IEEE defines two important pieces of equipment; a *wireless station* (a wireless client), which usually is a PC equipped with a wireless network interface card, and an *access point*, which acts as a bridge between the wireless and wired networks. An access point usually consists of a radio, a wired network interface, and bridging software. The access point acts as the base station for the wireless network, aggregating access for multiple wireless stations onto the wired network. Other examples of wireless stations are personal digital assistants (PDA) and wireless IP-phones. In 1997 the IEEE first WLAN standard 802.11 was published. After this start new standards have been and still are developing. Currently the standards IEEE 802.11a, 802.11b and 802.11g are most used [1 - 3]. The IEEE 802.11a is working in the 5.1 – 5.7 GHz band with a bandwidth of 22 MHz while IEEE 802.11b and 802.11g are working in the 2.41 – 2.47 GHz band with up to 14 partly overlapping channels with a bandwidth of 22 MHz. The exact frequency band allocation varies in different countries.

WLAN SYSTEM PROPERTIES

The IEEE standard defines two operation modes: infrastructure mode and ad hoc mode. *In infrastructure mode*, the wireless network consists of at least one access point, connected to the wired network infrastructure and a set of wireless stations. This configuration is called a *Basic Service Set (BSS)*.

An *Extended Service Set (ESS)* is a set of two or more BSSs forming a single subnetwork. ESS networks use roaming, which means that the mobile unit can change from one access point to another, without interruption of the data connection. *Ad hoc mode* (also called Independent Basic Service Set, or IBSS) is simply a set of wireless stations, that communicate directly with one another, without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network where a wireless infrastructure does not exist.

As many PC:s etc. can use the same network, there must be procedures to handle data collisions. Ethernet LANs uses *carrier sense multiple access/collision detection (CSMA/CD)*. In CSMA/CD LANs, all stations can access the network at any time. Before sending data, each station must "listen" to the network to see if it is already in use. Data is sent only if the station doesn't "hear" any data being sent. *Collision* is a situation where two stations detect silence on the network and send data at the same time. To overcome collision problems, Ethernet hardware is equipped with collision detection sensors. Whenever a collision is detected, the colliding data is ignored, at the stations that originally sent the data, will resend it.

To avoid collisions in a WLAN a similar solution is used. The data are transmitted in packets. When a packet is to be transmitted, the transmitting node first sends out a short ready-to-send packet containing information on the length of the packet. If the receiving node hears the ready-to-send, it responds with a short clear-to-send packet. After this exchange, the transmitting node sends its packet. When the packet is received successfully, as determined by a cyclic redundancy check, the receiving node transmits an acknowledgment packet. Due to this extra communication, the useful data speed will always be lower than the specified maximum data transfer rate.

Since the computers used in WLAN systems often are portable and battery-powered, the power consumption of a WLAN client card is a critical factor. In order to minimize the power consumption the 802.11 standard defines power management protocols that can be used by the stations. Power management schemes result in up to 95 % lower consumption of battery power compared to traditional operation where a station is always monitoring the medium during idle periods. To achieve savings in power consumption, a WLAN card in a station must have a special low-power state of operation. In this state the WLAN card will not monitor the medium and will be unable to receive a packet.

In each packet transmitted by a station there is one so-called power management bit. This bit is used to indicate whether the station is in active or power saving mode. Hence, the corresponding access point will learn the state of the station, and if an incoming message is destined for a station in power saving mode the access point will put it in a buffer and wake the station up.

Access points send out beacon frames on a regular basis (e.g. every 100 ms). Every beacon include information about which stations has buffered information at the AP. Stations using the power management scheme will wake up just prior to a beacon transmission with high accuracy and via the beacon find out if there are any messages buffered. In the case that no messages are buffered the station returns to the power saving mode until the next beacon is transmitted, but when there are messages that are destined to the station buffered in the access point, the station stays in the awake state and polls the access point for transmission of the buffered messages [4] .

Thus a client station does not transmit any signals when there is no communication with it. However, this does not imply that the client only transmits when the user actively communicates. A PC has quite a lot background communication, such as checking for mails and updates.

ASSESSING EXPOSURE FROM WLAN

To be able to assess the human exposure correctly, accurate measurement methods are necessary. Measurement methods for other communication systems such as GSM and to some extent UMTS exists today, but the literature on the topic of measurements of electromagnetic fields originating from WLAN-systems are rather limited [5-8].

By combining existing measurement methods from other communication systems with knowledge of the physical layers of WLAN-systems a spectral measurement method can be developed. In the far field traditional RF equipment such as a measurement antenna and a spectrum analyzer or a measurement receiver can be used. The field shall be measured in three orthogonal directions and in several positions in space to compensate for the fast fading. The data signals are sent in packages with no RF signal between the packages, which means that full channel bandwidth might not be captured in one sweep. A way to come around this problem is to use max hold mode and measure over several sweeps, see Fig. 1. This will give a measure of the exposure during RF transmission of the data package. To assess the average exposure the zero span mode can be used to estimate the typical duty cycle, see Fig. 2.

The wide bandwidth of the signal means that ordinary spectrum analyzers do not have a resolution bandwidth, RBW, to match. The measured intensity will depend on the chosen RBW, see Fig. 3. For best result use a resolution bandwidth of 1 % to 3 % of the channel bandwidth and then assess the channel power by integration.

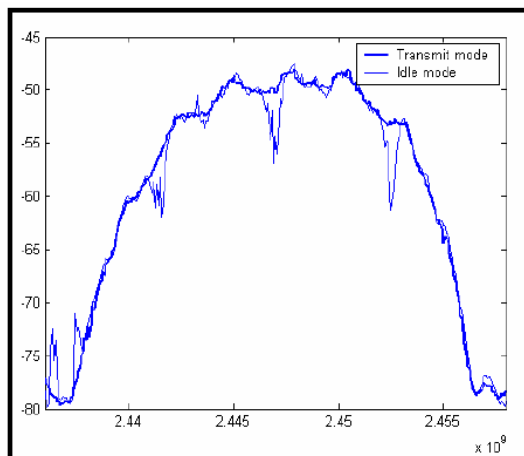


Fig. 1. Measured intensity versus frequency, close to an access point. The more solid line represents the spectrum when the access point is transferring a large file. The thinner line represent a measurement with the access point in idle mode, *i.e.* only a beacon is transmitted approximately every 100 ms. The measurements were performed in max hold mode over a five minute period [9].

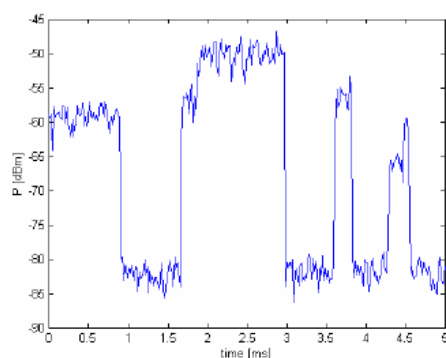


Fig. 2. Measurement of intensity in zero span mode, during data transfer from an access point to a client [9].

In the case that the exposure from the wireless station shall be assessed in the near field, *i.e.* if a laptop is used in the lap or a wireless IP-phone close to the head, SAR is the most relevant measure of exposure. The same type of equipment as used for measuring the SAR values for mobile phones can be used. There is however a need for standardized measurement positions and phantom.

MEASURED EXPOSURE LEVELS

Measurements I have performed at different work places with operating WLAN systems shows that the exposure from access points is generally low compared to the ICNIRP reference level of 10 W/m^2 [10]. The mean measured “max hold” exposure from access points was 0.10 mW/m^2 (mean value of 46 measurement positions in office environment). The duty cycles were in the range 2 – 30 % which means that the average levels were even lower.

This is also true for the exposure from most wireless stations, however if the wireless station is used in contact with the body, exposure up to the range of the basic restrictions on SAR (Specific Absorption Rate) of ICNIRP (2 W/kg averaged over 10 g) or IEEE (1.6 W/kg averaged over 1 g) for general public, is possible [10-11].

European regulation demands that the Equivalent Isotropic Radiated Power (EIRP) is maximum 100 mW for the 2.4 GHz band. For IEEE 802.11a higher power is permitted in several countries, for example Sweden allows for the frequency band 5150-5350 MHz an EIRP of 200 mW. Only indoor use is allowed in this band. In the frequency band 5470-5725 MHz, the EIRP is limited to 1 W. A SAR measurement with a dipole antenna transmitting 1 W, 5 cm from a flat phantom, at the frequency 5725 MHz, gave a maximal SAR of 2.3 W/kg when averaged over 1 g and 1.2 W/kg when averaged over 10 g [12].

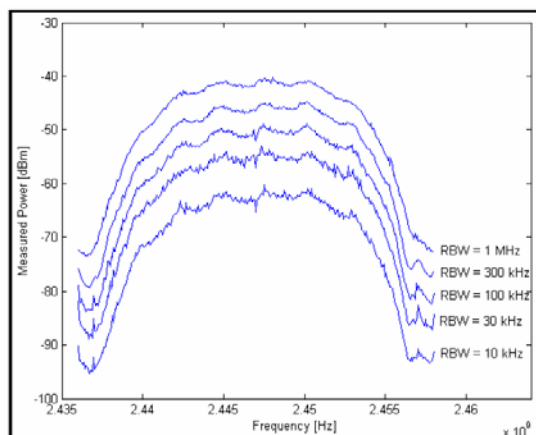


Fig. 3. Intensity from 802.11b channel measured with different resolution band width, RBW [9].

CONCLUSIONS

In the far field traditional RF equipment such as a measurement antenna and a spectrum analyzer can be used. In the case that the exposure from the wireless station shall be assessed in the near field, SAR is the most relevant measure of exposure. The far field exposure is usually well below the guidelines, however the near field exposure can be in the range of the guidelines.

ACKNOWLEDGEMENT

This work has been performed in the EUREKA project BASEXPO, with financial support from VINNOVA.

REFERENCES

1. IEEE Std 802.11a, 1999 Edition, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz band".
2. IEEE Std 802.11b, 1999 Edition, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band".
3. IEEE Std 802.11g, 2003 Edition, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band".
4. Prasad, N. and Prasad A. "WLAN Systems and Wireless IP for Next Generation Communications", Artech House 2002. Chapter 5, ISBN 158053290X.
5. CENELEC EN 50383, "Basic Standard for the calculation and measurement of electromagnetic fields related to human exposure from radio base stations and fixed terminal stations for wireless telecommunications systems (11 MHz – 40 GHz)", 2002.
6. CENELEC prEN 50400, "Basic standard to demonstrate the compliance of fixed equipment for radio transmission (110 MHz - 40 GHz) intended for use in wireless telecommunication networks with the basic restrictions or the reference levels related to general public human exposure to radio frequency electromagnetic fields, when put into service", Second draft, June 2004.
7. IEEE Std C95.3-2002. IEEE Recommended Practice for Measurements and Computations of Radio Frequency Electromagnetic Fields With Respect to Human Exposure to Such Fields, 100 kHz-300GHz.", New York, 2003.
8. Federal Communications Commission (FCC), Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Fields, OET Bullentin 65, Edition 97-01, August 1997.
9. Myhr, J "Measurement method for the exposure to electromagnetic field strength from WLAN systems" Master thesis, Chalmers University of Technology, Goteborg, Sweden 2004.
10. International Commission on Non-Ionizing Radiation Protection, ICNIRP, "Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz)". Health Physics, April 1998, Volume 74, Number 4.
11. IEEE C95.1-1991, "Safety levels with respect to human exposure to radio frequency electromagnetic fields, 3 kHz to 300 GHz", New York, 1991.
12. Lövehagen, N. "RF exposure from short-range wireless communications: A study of Bluetooth and Wireless LAN" Ericsson Thesis Report T/U 99-492, 1999.