HØGSKOLEN I AGDER

Agder University College

Postgraduate thesis
Information and Communication Technology

Modelling of coverage in WLAN

Stig Erik Arnesen & Kjell Åge Håland

Grimstad, Norway
May 2001

Abstract

The freedom of being connected to the Internet everywhere without any wires has been a dream for people many years. Now there seems to be an opening for this dream. While waiting for the UMTS technology IP-Zones are now being build. An IP-Zone is a public place where Wireless Local Area Network (WLAN) offers you a connection to the Internet. The WLAN technology has finally arrived with decent transmission speeds; with the introduction of IEEE 802.11b with transmission speeds up to11 Mbps. Subsequently we decided to take a closer look on this technology.

This thesis presents an introduction to several WLAN technologies. We have taken a closer look at IEEE 802.11, 802.11b, 802.11a and the ETSI/BRAN standard HiperLAN type 2.

We have been working on a general model of coverage within a room for WLAN. As a base model we had an indoor office path loss model intended for UMTS. The background of the model was unknown and had to be explored. We examined other free space models designed for indoor environments.

We ended up with the Log-distance path loss model. Measurements were performed and used to adjust the model to fit the actual environments.

We have also created a site survey on HiA 3rd floor in the old building in Grimstad, and proposed a way to cover the Master of Science room and the north-west wing of the building.

Preface

This postgraduate thesis is a part of the master of engineering degree in Information and Communication Technology (ICT) at the Agder University College. Stig Erik Arnesen and Kjell Åge Håland have made this report during spring semester 2001. This last assignment is a closure on the education that lead to the title Master of Engineering.

This assignment was given by Agder University College in Grimstad and gives an introduction to WLAN technologies. It also describes the work of creating a model of coverage for WLAN.

We would like to thank Magne Arild Haglund for guiding us through this project.

We would also like to thank Stian Andresen from Siemens for helping us get technical information on the Siemens WLAN equipment.

Grimstad, 28 May 2001

Stig Erik Arnesen
Kjell Åge Håland

Index

LIST OF FIGURES AND TABLES

1 Introduction

1.1 Background for the Postgraduate thesis

Wireless LAN is starting to become a popular alternative to wired networks both at work and at home. The increase in popularity is partly due to the speed is now acceptable. The price of the equipment has also reached acceptable levels. Since we were curious on this technology we wanted to take a closer look. We wanted the assignment to be of importance for the school and others, who could have an interest in how to predict the coverage and understand the WLAN technologies. Models prediction the coverage in a WLAN is important. Not only to find when a user will loose connection, it can also be used to plan how multiple access point can placed in the same building without causing interference with each other.

We ended up creating an assignment together with Magne Arild Haglund from HiA and Thomas Haslestad from Telenor FoU. During this project we have learned much about WLAN technology, data communications and radio wave theory.

1.2 The Postgraduate thesis definition

Title: Modelling of coverage in WLAN.

Create a general overview over the WLAN technologies.

Based on a cell within a room, a mathematical model that simulates the radio coverage of the room will be created, using fading algorithms from ETSI TR-101-112 ch. B 1.8. Measurements of the coverage in the room will be performed, and the results will be used to adjust the parameters in the model in order to fit the simulation model to the actual environments.

If possible, simulate the capacity of the WLAN as a function of users and field power within a room with one cell, or within a room with several cells with or without overlapping. Construct a site survey for HiA 3rd floor (that includes coverage, channel use and throughput). How to construct the WLAN most efficient based on the site survey.

1.3 Limitations of the assignment

We have not described and considered all possible coverage models or fading theories, but have concentrated most of our work on empirical models and the factors affecting it.

The application measuring the signal strength was using a percentage scale and forced us to take assumptions in order to get the measured values connected to the model. We have not received any conversion tables from Siemens that say exactly what the percent values are measuring. Because of this we cant guarantee the correctness of our model.

We didn’t have enough time or sufficient equipment to perform the throughput test in our assignment.

1.4 Method

In the start-up phase we decided that this project should consist of one theoretical part and one practical part. We used most of the time to study the theory regarding WLAN technologies and radio fading algorithms in general.

In the second part we used a lot of time finding a suitable indoor model of coverage in WLAN.

We had meetings with our supervisor every 14 days to discuss progress we had done, and to consider what we to be done the next 14 days. We thought this was a god way to manage our further work and get the best progress in our assignment.

1.6 Structure of the Postgraduate thesis

This thesis is organized in four main parts:

- We started with the part describing the **WLAN technologies** in general.
- The second part describes **phenomena's and other factors** that affect the model of coverage.
- In the third part we described some of the **models** we found in our search of a suitable model for coverage in WLAN. The measurements we performed to fit our model to the real world environments are also described in this part.
- The fourth part is a **site survey** suggestion of how to implement the WLAN using the model from part three.

2 General overview over WLAN technologies

Making the general overview a part of the assignment was more of our own interest in order to find the different aspects of wireless local area networks. We find this relatively new technology interesting and know for sure it will influence the development of people's workplace in the years to come. According to "ukeavisen Telecom" this marked is growing 30 percent a year.

2.1.1 Wireless Local Area Network (WLAN)

Wireless local area network (WLAN) uses radio frequency technology to receive and transmit data over the air. It can be implemented as an extension to, or as an alternative for, a wired LAN. It minimizes the need for wired connections and offers both data connectivity and user mobility.

Typical wireless LAN configurations consist of a transmitter/receiver device, called an access point, which connects to the wired network from a fixed point using standard cabling. A single access point can support a small group of users and normally function within a range of 60 to 100 meters as shown at figure 1. The access point is usually mounted high but may be mounted anywhere as long as the desired radio coverage is obtained.

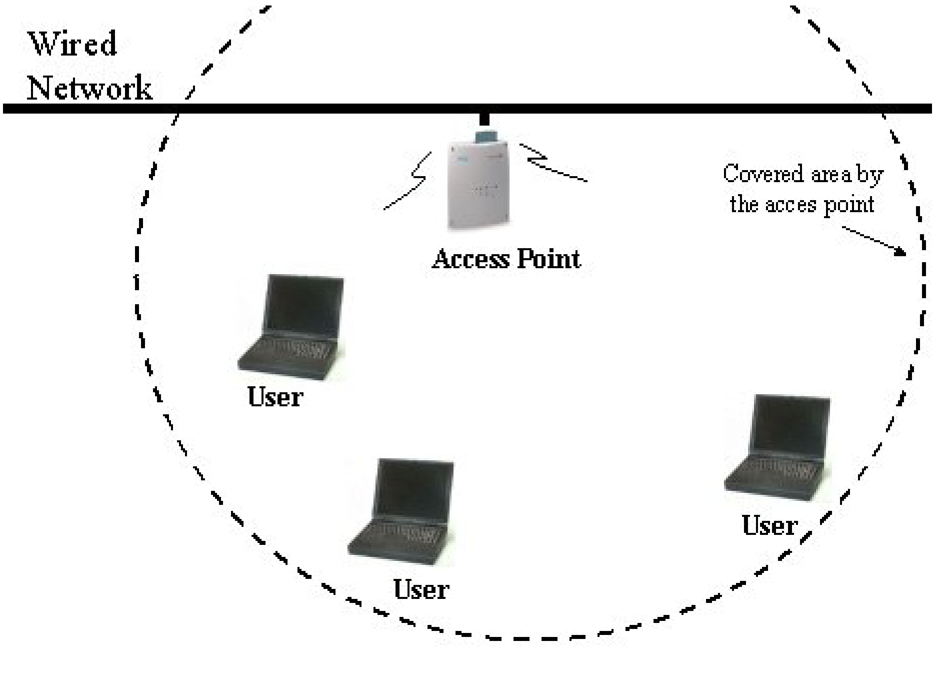


Figure 1 Wireless LAN adapters

End users access the wireless LAN through wireless-LAN adapters, which are implemented as PC cards in notebook or palmtop computers, as cards in desktop computers, or integrated within hand-held computers.

2.1.2 Application

There are many possible uses for WLAN technology with only our fantasy as the limitation. We will give you a brief overview over some applications of wireless LANs:

- **Inventory Control**
  Employees in stores may scan information from items in the shelves into a data-collection terminal device, which may transmit scanned information to an access point on the stores LAN. This means inventory information are transmitted to the stores existing communication system and can be sent to the home office of the company.

- **Hospital**
  There is a wide range of applications suitable for wireless LANs within a hospital. One example is PDAs or notebooks with wireless communication possibilities used by doctors or nurses to obtain and update patient information.

- **Hotel**
  Computer terminals in the kiosk can be connected to the hotel's wired LAN, without having to string wires through the lobby when using wireless communication.

- **Training**
  Private organizations, colleges and universities may use wireless LANs for training. Wireless LANs may easily be set up when all wired networks are used or reserved. Thus wireless LANs adds both flexibility and responsiveness to the networking requirements of different applications.

- **Trade shows**
  Employees in the different booths use their laptops or notebook computers to access their email, checking their delivery schedule, or perform other functions. Each computer uses wireless communication to connect to a wired LAN in the building housing the trade show, which has an Internet connection.

- **New wireless tool helps police fight crime**
  In the city of Oakland, California police force has announced it will deploy a new wireless tool from Padcom. Officers on the prowl for suspects soon will have more information at their fingertips, thanks to the new system that is designed to give officers high-speed wireless access to large data files from their squad cars. The new system can transmit mug shots and detailed crime reports wirelessly. It will allow 220 squad-car computers to receive large files though a wireless LAN available in parking lots citywide. Without intervention by officers, spread-spectrum capabilities are activated automatically when officers enter the 300- to 500-foot service radius of parking-lot access points, and all data is routed through the wireless LAN.

- **IP Zones**
  While waiting for UMTS technology there have been build IP-Zones. An IP-Zone is a public place where Wireless Local Area Network offers you a connection to the

Internet. Places that are of interest of making IP-Zones are airports, railway stations, congress locations, hotels and other public places.

2.1.3 What WLAN offers as an advantage over traditional wired networks

- **Mobility**
  WLAN system can provide users with access to real-time information anywhere in their organization. This means WLAN have the possibility to support productivity and service in a way that is not possible in wired LANs.

- **Installation speed, simplicity and flexibility**
  It is fast an easy and you don't need to pull cables through walls and ceilings. It is also flexible since it can be places where wires can't be.

- **Reduced cost**
  While the initial investment required for WLAN hardware may be more expensive than the cost of wired LAN, overall investment and long–term cost may be significantly lower. This is especially true in dynamic environments where WLAN is much more flexible. The growing popularity of wireless LANs makes it now possible that is even less expensive for the initial investment.

- **Scalability**
  WLAN can be configured in a variety of topologies. Configurations are easily changed and range from peer-to-peer networks to full infrastructure networks with thousands of users.

2.2 Technology used in WLAN

Wireless LANs use electromagnetic airwaves to send information from one point to another without any physical connection. There are several methods used in WLAN to do this. First is the possibility to use IR, but this is limited to line of sight or small distances. Consequently the best technology for use indoor is the use of radio waves. Radio waves can penetrate trough more objects than IR. There are several methods of modulating the radio waves; the ones used in WLAN is Frequency hopping and direct sequence. Frequency hopping is used for systems up to 3 Mbps and direct sequence systems achieve speeds up to 11 Mbps.

2.2.1 Spread Spectrum Technology

Most wireless LAN systems use the spread spectrum technology. This technology is a wideband radio frequency technique developed by the military during the late 1940s as a mechanism to provide a reliable and secure communication method for the military under battlefield conditions. More bandwidth is consumed with this technology than with narrowband technology, but it produces a signal that in effect is louder and easier to detect. The receiver must know the parameters of the spread-spectrum being broadcast. If a receiver is not tuned to the right frequency, a spread spectrum signal looks like background noise. There are two types of spread spectrum radio used in wireless LANs defined under the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard: frequency hopping and direct sequence.

Frequency hopping Spread Spectrum

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that shift frequency in a pattern, which must be known, to both transmitter and receiver. This means that the frequency shifting spreads the transmission over a wide frequency band. When it is properly synchronized it function as a single logical channel. To a receiver that doesn't know the hopping pattern it appears to be a short-duration impulse noise. When frequency hopping occurs at a rate that is faster than the message bit rate, it is a fast hopping system, when it is slower it is a slow-hop system.

Direct-Sequence Spread Spectrum

In direct-sequence spread-spectrum a carrier is modulated by a digital signal.
Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip or chipping code. The longer the chip is the greater the probability that the original data can be recovered. The disadvantage is that it requires more bandwidth. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as a lowpower wideband noise and is rejected (ignored) by most narrowband receivers.

2.2.2 Infrared

Infrared technology is little used in commercial wireless LANs. Infrared (IR) communication systems use very high frequencies that are just below visible light in the electromagnetic spectrum. IR cannot penetrate opaque objects just as light. This limits its transmission capability to a direct line of sight or diffuses method of communications.
Diffuse communications alleviate the need for line of sight path, but transmission distance is limited in comparison with frequency-hopping- or direct sequence spread-spectrum communications. Although a few vendors developed IR wireless LANs, their capability to support communications typically is limited to a small area within a room or using diffuse or reflective technology to an individual portion of a room.

2.3 Network Architecture

There are different possibilities of network architecture when setting up a wireless LAN. We divide Wireless LANs networks into two architectures possibilities: Peer-to-peer or access point-based architecture.

2.3.1 Peer-to-peer

In the peer-to-peer architecture the wireless devices create a LAN by communicating directly with each other as shown at figure 2. This network is easy to install but is limited because all stations must be within airwave distance to each other when communicating. Peer-to-peer architecture is typically used for small temporary networking requirements between a few computers or devices.

Figure 2 Peer-to-peer architecture

2.3.2 Access point based

The access point based architecture is more commonly used than the peer-to-peer topology. An access point functions as a bridge that connects wireless clients to the wired network The WLANs don't necessary replace wired LANs, but often extend the connectivity to mobile devices. An access point may also function as a radio relay to the mobile stations located within a geographic area. Then the stations won't have to communicate directly to each other, but via the access point. Although this increases the use of bandwidth, it reduces the requirements to power need and right antenna position from stations that must reach all other stations within a geographic area. Instead they only communicate with the access point. Since the access point is connected to the wired LAN it allows each wireless client to obtain access to all wired LAN resources. Most access points cant range more then about 60-100 meters and if you need to extend the coverage area you can use an extra access point that works as an extension point. An access point based architecture is shown at figure 3.

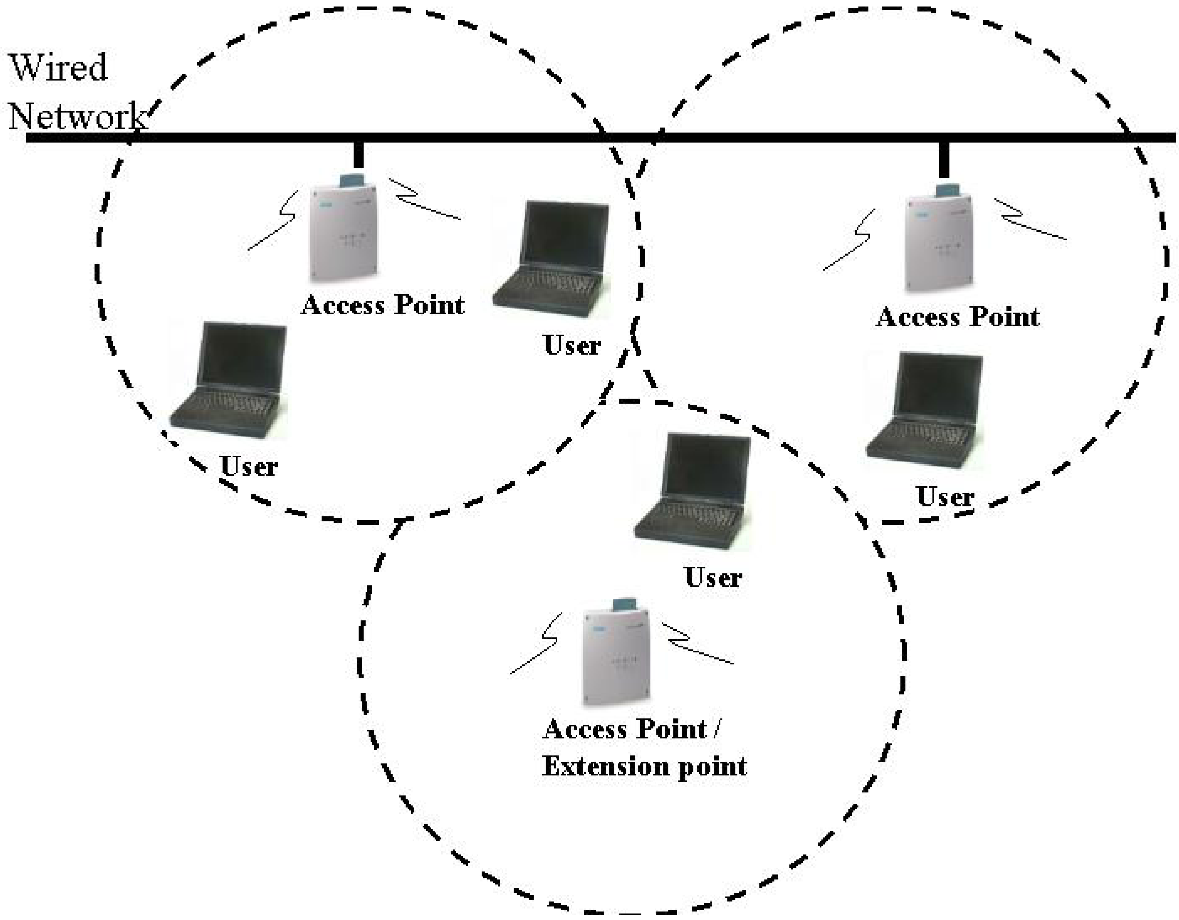


Figure 3 Access point based architecture

2.4 Security

There are three basic methods to secure access to an Access Point that are built into 802.11 networks:

- Service set identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

One or more set of these methods can be implemented. However best security will be accomplished when all three methods are implemented.

2.4.1 SSID

Network access control can be implemented using an SSID associated with an AP or a group of APs. The SSID provides a mechanism to "segment" a wireless network into multiple networks service by one or more APs. Each AP is programmed with a SSID corresponding to a specific wireless network. To access this network, client computers must be configured with the correct SSID.

Because a client computer must present the correct SSID to access the AP, the SSID acts as a simple password and this provides a measure of security. However, this minimal security is compromised if the AP is configured to “broadcast” its SSID.

2.4.2 MAC Address Filtering

While an AP or group of APs can be identified by a SSID, a client computer can be identified by the unique MAC address of its 802.11 network card. To increase the security of an 802.11 network, each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client’s MAC is not in this list, the client will not be allowed to associate with the AP.

MAC address security provides good security, but it is best suited for small networks. Each AP must be manually programmed with a list of MAC addresses, and the list must be kept up to date. The administrative overhead limits the scalability of this approach.

2.4.3 WEP Based Security

WEP provides encrypted communication using an encryption key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network.

WEP specifies the use of a 40 bit encryption key and there are also implementations of 104 bit keys. The encryption key is concentrated with a 24 bit “initialisation vector”, resulting in a 64 or 128 bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted.

WEP uses the RC4 PRNG algorithm from RSA Data Security.

The 802.11 standard does not specify a management protocol, so all WEP keys on a network must be managed manually. WEP security is not available in ad hoc (or peer-to-peer) 802.11 networks that do not use APs.

The Wired Equivalent Privacy (WEP) algorithm

The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, used to protect link layer communication from eavesdropping and other attacks. This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security we find in a wired medium.

Properties of the WEP algorithm

The WEP algorithm has following properties:

- It is *reasonable strong*: The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute force attack. This in turn is related to the length of the secret key and the frequency of changing keys.
- It is *self-synchronizing*: WEP is self-synchronizing for each message. This property is critical for a data-link level encryption algorithm, where “best effort” delivery is assumed and packet loss rates may be high.

- It is *efficient*: The WEP algorithm is efficient and may be implemented in either hardware or software.
- It is *optional*: The implementation and use of WEP is an IEEE 802.11 option

2.4.4 Authentication

Authentication services
IEEE 802.11 defines two subtypes of authentication service: Open system and shared key. The subtype invoked is indicated in the body of authentication management frames. Thus authentication frames are self-identifying with respect to authentication algorithm. All management frames of subtype Authentication shall be unicast frames as authentication is performed between pairs of stations (i.e. multicast authentication is not allowed). Management frames of subtype deauthentication are advisory, and may therefore be sent as group-addressed frames.

A mutual authentication relationship exists between two stations following a success authentication exchange as described below. Authentication shall be used between stations and the AP in an infrastructure BSS.

Open system authentication
Open system authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second step in the sequence is the authentication result. If it is “successful”, The STAs shall be mutually authenticated.

Shared key authentication
Shared key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. Shared key authentication accomplishes this with the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented.

The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11.
During the shared key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudorandom number (PRN) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames.

VPN wireless security
For business networks, a VPN solution for wireless access is currently the most suitable alternative to WEP and MAC address filtering. VPN solutions are already widely deployed to provide remote workers with secure access to the network via the Internet. In this remote user application, the VPN provides a secure, dedicated path or tunnel over an “untrusted” network. (E.g. Internet).

The same VPN technology can also be used for secure wireless access. In this application, the untrusted network is the wireless network. The APs are configured for open access with no WEP encryption, but wireless access is isolated from the enterprise network by the VPN server and a WLAN between the APs and the VPN servers. Authentication and full encryption over the wireless network is provided through the VPN servers that also act as gateways to the private network. Unlike the WEP key and MAC address filtering approaches, the VPN-based solution is scalable to a very large number of users.

More Privacy and Security Issues

WLAN is based on the absence of privacy. The Access point based in the 802.11 network acts as a Bridge. The nature of a bridge is to relay all traffic to the nodes that is registered to the access point. If the access point receives a data packet for a station that is not logged into it, it forwards the packet to the Ethernet; in the other direction it continuously monitors the Ethernet for data directed to stations logged on to it and forwards the packets to the radio cell. As all mobile stations must log onto the access point, the access point always knows which stations are on the wireless side. All the traffic on the wireless side is sent to every other device on the Ethernet, including every wireless device.

If you put a wireless card into your laptop and connect to a network, you do not immediately see all this traffic from the other wireless users. You have to run a program to make it visible. Such programs are available for free for Windows and Mac machines, and are provided as a part of UNIX operating systems

A user would have to pass network authentication to access resources off the wireless LAN, but not just to monitor the LAN. In fact, a sophisticated hacker could monitor the LAN traffic without actually connecting to the access point, just by listening to the radio broadcast, but this is more complex than simple interception program.

To prevent eavesdropping, the WEP algorithm is used. WEP is a optional part of 802.11, and is therefore not implemented by all vendors. Without WEP, all traffic on the wireless network is broadcasted in the clear, and is available for monitoring by any hacker. With a directional antenna and a scanner, 802.11 networks are detectable at surprising distances. There is one major drawback with WEP that is that the privacy protection is not fully automatic, like a digital cell phone, so that the user isn't required to take any action to enable it.

Problems with WEP

Scientists with the computer science division at the university of California, Berkley has grouped together ISAAC (internet Security, Applications, Authentications and Cryptography) to work with central security issues related to Internet. They have discovered a number of flaws in the WEP algorithm, which seriously undermine the security claims of the system. In particular, they found the following types of attacks:

- Passive attacks to decrypt traffic based on statically analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

In passive attacks you only listen and analyse the traffic. The scientists show you how to accomplish statically analyses to decrypt messages that is sent with WEP-protection trough a wireless network. They also show how to, after a about 24 hours how to build up a catalogue that makes it possible to decrypt all traffic in real-time.

Active attacks means that the attacker must have physical access to the equipment to change or reprogram the components, The scientists shows you how this can be done with material that is easy available on the open marked, and with knowledge that is within reach for special interested people. With active attacks you can not only break the encryption, but also change the contents on the traffic that is on the wireless network.

Note that the attacks apply both on 40-bit and the so-called 128 bit versions of WEP equally well.

The scientists conclude that WEP isn't protecting good enough. They say that the protocol problems are a result of misunderstanding of some cryptographic primitives and therefore combining them in insecure ways. These attacks point to the importance of inviting public review from people with expertise in cryptographic design; had this been done, the problems would be avoided, they claim.

2.5 Mobility support

Mobile IP has been under development for many years. The technology is a part of UMTS, but also works between different types of networks and to connect IP-Zones. With the use of an agent technology IP-addresses may be switched seamless so you may move freely from a net to another without loosing connection. This is essential for seamless roaming between different networks, and it will of course make the WLAN technology even more interesting when you can move freely between different WLANs without loosing connection. This makes the "coverage" area much larger. There is work going on to make it possible for mobile IP to perform a vertical roaming between WLAN and GPRS. This is called vertical roaming, because you are switching between two different communications systems. In this case a telecommunication system and a data-networking system. With this phrase "Internet anywhere, any time on any device" [Bill Gates], states the vision from a leader in software innovation. This phrase states that wireless products will try to dominate the future and mobility support will be of essence.

Mobile IP can be thought of as the cooperation of three major subsystems. First, there is a discovery mechanism defined so that mobile computers can determine their new attachment points (new IP addresses) as they move from place to place within the Internet. Second, once the mobile computer knows the IP address at its new attachment point, it registers with an agent representing it at its home network. Lastly, mobile IP defines simple mechanisms to deliver data grams. We think that mobile IP is an important mechanism for mobility support in WLAN so we will take a closer look on it.

Characteristics of mobile IP

IP uniquely identifies the node's point of attachment to the Internet. Therefore, a node must be located on the network indicated by its IP address to receive data grams destined to it; otherwise, data grams destined to the node would be undeliverable. Without Mobile IP, one of the two following mechanisms typically must be employed for a node to change its point of attachment without losing its ability to communicate:

1. The node must change its IP address whenever it changes its point of attachment
2. Host-specific routes must be propagated throughout the relevant portion of the Internet routing infrastructure.

Both of these alternatives are plainly unacceptable in the general case. The first makes it impossible for a node to maintain transport and higher layer connections when the node changes location. The second has severe scaling problems that are especially relevant considering the explosive growth in sales of mobile computers.

Mobile IP was devised to meet the following goals for mobile nodes that do not move more frequently than once per second. Even so, the protocol is likely to work quite well until the frequency of movement of the mobile node begins to approach the round-trip-time for mobile IP protocol control messages. The following five characteristics should be considered baseline requirements to be satisfied by any candidate for a Mobile IP protocol:

1. A mobile node must be able to communicate with other nodes after changing its link-layer point of attachment to the Internet, yet without changing its IP address.
2. A mobile node must be able to communicate with other nodes that do not implement Mobile IP. No protocol enhancements are required in hosts or routers unless they are performing the functions of one or more of the new architectural entities introduced in section 1.
3. All messages used to transmit information to another node about the location of a mobile node must be authenticated to protect against remote redirection attacks.
4. The link by which a mobile node is directly attached to the Internet may often be a wireless link. This link may thus have a substantially lower bandwidth and higher error rate than traditional wired networks. Moreover, mobile nodes are likely to be battery powered, and minimizing power consumption is important. Therefore, the number of administrative messages sent over the link by which a mobile node is directly attached to the Internet should be minimized, and the size of these messages should be kept as small as possible.
5. Mobile IP must place no additional constraints on the assignment of IP addresses. That is, a mobile node can be assigned an IP address by the organization that owns the machine, as is done with any other protocol engine administered by that organization. In particular, the address does not have to belong to any globally constrained range of addresses.

Mobile IP is intended to enable nodes to move from one IP subnet to another. It is just as suitable for mobility across heterogeneous media as it is for mobility across homogeneous media.

Mobile IP introduces the following functional entities:

Mobile Node
A host or router that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (Constant) IP address, assuming link layer connectivity to a point of attachment is available.

Home Agent
A router on a mobile node's home network, which tunnels data grams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.

Foreign Agent
A router on a mobile node's visited network that provides routing services to mobile node while registered. The foreign agent detunnels and delivers data grams to the mobile node that were tunnelled by the mobile node's home agent. For data grams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

Care of Address
The Care of address is an address that identifies the mobile node's current location. It can be viewed as the end of a tunnel directed towards a mobile node. It can be either assigned dynamically or associated with its foreign agent.

Correspondent Host
This node sends the packets that are addressed to the mobile node.

Mobile IP support these services
Mobile is in essence, a way of doing three relatively separate functions.

Agent Discovery
Home Agents foreign agents broadcast their availability on each link to where they can provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present.

Registration
When the mobile node is away from home, it registers its Care-of-address with its home agent; it registers its care-of-address with its home agent so that the home agent knows where to forward its packets. Depending on the network configuration, the mobile node could either register directly with its home agent, or indirectly via the help of its foreign agent.

Tunnelling
In order for data grams to be delivered to the mobile node when it is away from home, the agent has to tunnel the data grams to the care-of-address. Figure 4 shows tunnelling.

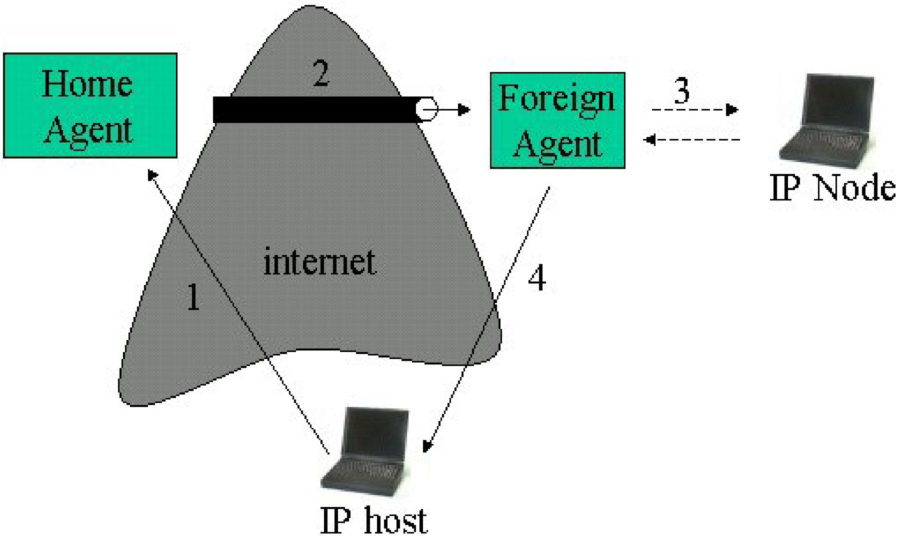


Figure 4 Mobile IP Datagram Flow

1. A datagram to the mobile node arrives on the on the home network via standard IP routing.
2. The datagram is intercepted by the home agent and tunneled to the care-of-address.
3. The datagram is detunneled and delivered to the mobile node.
4. For datagrams sent by the mobile node, standard IP routing delivers each datagram to its destination. In figure 1 the foreign agent is the mobile nodes default router.

When away from home, Mobile IP uses protocol tunnelling to hide mobile nodes home address from intervening between its home network and its current location. The tunnel terminates at the mobile nodes care-of-address. The care-of-address must be an address to which datagrams can be delivered via conventional IP routing. At the care-of-address, the original datagram is removed from the tunnel and delivered to the mobile node.

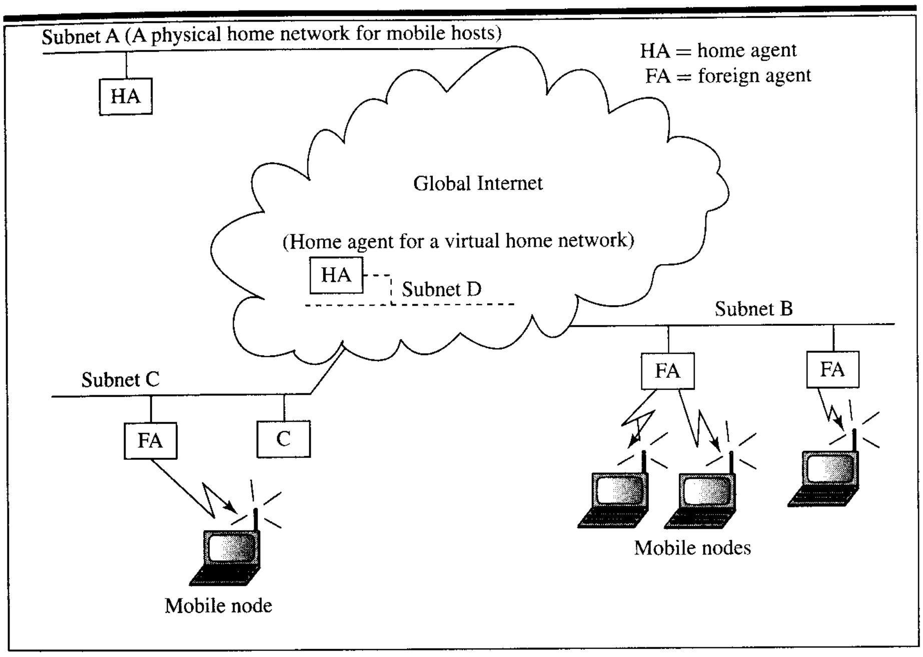


Figure 5 Mobile IP

An overall illustration of the entities of Mobile IP and home and foreign networks is shown in figure 5 In the diagram there are two foreign networks, B and C, with foreign agents; Two home networks, A and D, with home agents; and mobile nodes that are attached to the various foreign networks by way of radio and infrared attachments. The tunnels go from the home agents, across the global Internet, and finally arrive at the foreign agents for final delivery.

2.6 IEEE 802.11 and 802.11b specifications

The institute of Electrical and Electronics Engineers (IEEE) ratified the original 802.11 specifications in 1997 as the standard for Wireless LANs. That version of 802.11 provides for 1 mbps and 2 mbps data rates and a set of fundamental signalling methods and other services. The disadvantage with the original 802.11 standard is the slow data rates that are too slow to support most general business requirements. Recognizing the critical need to support higher data-transmissions rates, the IEEE in 1999 ratified the 802.11b standard for transmissions of up to 11 Mbps. With 802.11b WLANs are able to achieve wireless performance and throughput comparable to wired Ethernet.

Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels of the ISO model, the physical layer and data link layer. Any LAN application, network operating system, or protocol, including TCP/IP and Novell Netware, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

The original 802.11 standard defines the basic architecture, features, and services of 802.11b. The 802.11b specification affects only the physical layer, adding higher data rates and more robust connectivity.

Basic Configuration

The IEEE 802.11 standard defines two configurations for stations. One is the point-to-point configuration described earlier and is referred to as an *independent configuration* in 802.11. The second is called *infrastructure configuration*. Under this method stations communicate with one or more access points, which are connected to a wired LAN, described earlier as access point based configuration.

Frequency Selection

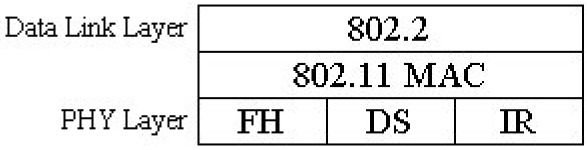
The 2.4 GHz band is used in the 802.11 standard. This is an unlicensed frequency band reserved for industrial, scientific, and medical (ISM) use on a global basis. By supporting operations in the band consistent with the power levels allowed by different countries, it became possible to develop a wireless LAN standard that could be used on a global basis, which was the most important reason for choosing this band.

Architecture Components

The 802.11 standard is based on a cellular architecture where the system is divided into cells. Each cell is referred to as a Basic Service Set (BSS) and is controlled by a base station called Access Point (AP). Most installations consist of several cells that form a network and where the access points connect to a backbone. This is called a Distribution System (DS). The backbone may be a wired LAN or even a wireless. The whole interconnected wireless LAN, including the cells, their Aps and the DS is viewed as a single IEEE 802 network to upper layers of the OSI Reference model and is known in the standard as Extended Service Set (ESS). There is also a component defined as a portal in the standard. The portal is a device that interconnects the 802.11 LAN and another 802 LAN. It may be considered as a translation bridge. Most vendors include the access point and portal as a single physical entity.

2.6.1 IEEE 802.11 Layers

As all 802.x standards, the 802.11 protocol covers the MAC and physical layer. The standard in fact covers three physical layers. These are direct-sequence spread spectrum, frequency-hopping spread spectrum and infrared. A single MAC layer supports all the three physical layers, provides a interface to upper layers and performs certain functions normally related to upper-layer protocols. MAC supports functions like Fragmentation, Packet Retransmissions and Acknowledges.



<table>
<tr><td>Data Link Layer</td><td colspan="3">802.2</td></tr>
<tr><td></td><td colspan="3">802.11 MAC</td></tr>
<tr><td>PHY Layer</td><td>FH</td><td>DS</td><td>IR</td></tr>
</table>

Figure 6 IEEE 802.11 Layers

2.6.2 IEEE 802.11 Physical layer

The RF methods operate as mentioned earlier in the 2.4 GHz frequency band, typically occupying 83 MHz of bandwidth from 2,400 to 2,483 GHZ. The permissible power when selecting this frequency may vary between different countries. Federal Communication Commission (FCC) in the United States limits radiated antenna power to 1 W. In Japan it is limited to 10 mW per 1 MHz and in Europe it is limited to 100 mW.

Frequency-Hopping Spread Spectrum

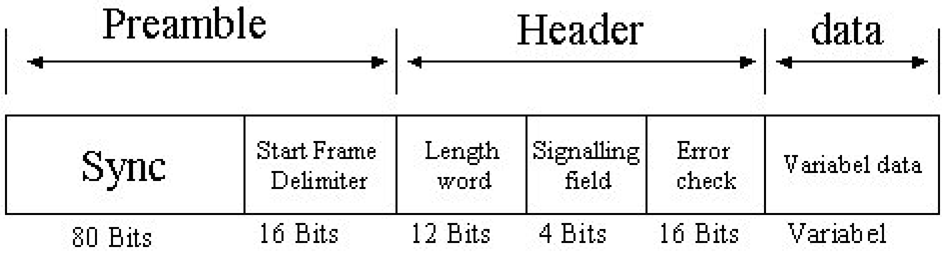
This technique represents one of the possible physical layers of the 802.11 standard. It uses 79 nonoverlapping frequency channels where each channel has 1 MHz channel space. This allows 26 networks to be located in the same area, which make the aggregated throughput more reasonable. Although the standard specifies 79 channels, the actual number of channels that are used depend on the regulatory authority assignment of frequency usage in a particular country. There are also different regulatory bodies that restrict the number of hopping channels that can be used in other locations of the world. The number of hops defined for IEEE 802.11 standard operation in each country, is referred to as a *hopping set.*

FHSS Modulation

Frequency-shift keying (FSK) is used for FHSS because of its low cost and easy operation. There are two versions of FSK that are specified, more formally referred to as gaussian-shaped FSK (GFSK). This is because data is filtered by a low-pass gaussian filter, before it is frequency modulated onto a carrier. It operates at 1 Msymbol/s with non-return to zero (NRZ) data. Mandatory a two-level GFSK method is used, with binary 1's and 0's modulated into one of two different frequencies. Optional a 2 Mbps data rate may be supported, using a four-level GFSK modulation method. This method has pairs of bits being modulated into one of four different frequencies.

FHSS Frame Format

Figure 7 shows the IEEE 802.11 FHSS frame format



Preamble		Header			data
Sync	Start Frame Delimiter	Length word	Signalling field	Error check	Variabel data
80 Bits	16 Bits	12 Bits	4 Bits	16 Bits	Variabel

Figure 7 FHSS frame format

Preamble

The FHSS preamble contains two separate subfields: the Preamble Synchronization (SYNC) field and the Start Frame Delimiter (SFD).

Sync field

The sync field is an 80-bit field containing an alternating zero-one pattern, starting with zero and ending with one when transmitted. The field is used to detect a potentially receivable signal, select an antenna if diversity is supported and acquire symbol timing.

Start Frame Delimiter (SFD) field

The SFD consists of the 16-bit binary pattern 0000 1100 1011 1101 and with this defines the frame timing.

Header

The Header contains three separate subfields: a 12-bit Length field, a 4-bit Signalling field and a 16-bit Header Error Check (HEC) field.

Length word field

This field indicates the length of the payload field that may be up to 4095 octets.

Signalling field

This 4-bits field indicates the data rates from 1 Mbit/s to 4.5 Mbit/s in 0.5 Mbit/s increments.

Header Error Check (HEC) field

The HEC field is a 16-bit error detection field and uses the CCITT CRC-16 generator polynomial $G(X) = X^{16} + X^{12} + X^{5} + 1$.

The preamble and header are always transmitted at 1 Mbit/s. The rest of the frame is transmitted at the rate indicated by the signalling field. To minimize the effect of multipath reflection the FHSS has a minimum hop distance between frequencies. This is because the reflections from the next hop have minimal effect on the next hop since it takes time for the reflection to arrive at the receiver, which then probably will waiting for information at different frequency.

Direct-sequence spread spectrum

The direct-sequence spread spectrum is a second physical layer supported by 802.11. DSSS is also the only specified physical layer for the 802.11b standard, which supports data rates of 5.5 and 11Mbps. In Europe (ETSI) it is 13 channels that are supported. According to 802.11 it must be 30 MHz distance between the centre frequencies if the cells are overlapping and/or adjacent to not cause interference. In 802.11b it must 25 MHz distance. This means that there may be 3 cells that are adjacent and/or overlapping without causing interference to each other in the 802.11b standard (channel 1, 7 and 13 in Europe).

As mentioned earlier the 802.11b standard uses DSSS, with the same 2.46-GHz bandwidth and channelization design as the 802.11 standard. The main difference in the two standards is that 802.11b uses Complimentary code keying (CCK) to support operating rates of both 5.5 Mbps and 11 Mbps. CCK uses and eight-chip code-spreading sequence, The 802.11b supports also both 1 Mbps and 2 Mbps, which means it is also backward compatible with 802.11 devices.

DSSS Modulation for 802.11

There is two DSSS modulation methods supported by the 802.11 standard. Differential binary phase-shift keying (DBPSK) is used when having a data rate at 1 Mbps. DBPSK have each bit represented by one of two possible phases. Differential quadrature phase-shift keying (DQPSK) is used to support 2 Mbps. DQPSK have pairs of bit represented by one four possible phases.

Barker Code

Barker Code has been basic signals for BPSK and QPSK communication due to their low power and relatively high energy (due to long symbol duration) resulting in relatively low

power spectral density. Barker Codes are members of direct sequence class of spread spectrum signals.
The use of Barker codes for basic data-carrying signals enables the transmission of 1 or 2 bits of data per pulse-use under the binary or quaternary phase shift keying formats, respectively. Upon correlation with a filter matched to the Barker code, the received codeword has a main lobe, which is one chip wide for the 11-chip Barker code. The following 11-chip Barker sequence shall be used as the PN code sequence for the 1 and 2 Mbit/s modulation:
+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1
The leftmost chip shall be output first in time. The first chip shall be aligned at the start of a transmitted symbol. The symbol duration shall be exactly 11 chips long. [25]

Complementary Code Keying (CCK)
The CCK modulation is used at 5.5 Mbit/s and 11 Mbit/s. the spreading code length is 8 and is based on complementary codes. The chipping rate is 11 Mchip/s. The symbol duration shall be exactly 8 complex chips long.[25]

CCK codes perform well when used with a RAKE receiver in an indoor multipath environment and can be efficiently demodulated.

Properties of CCK

Let the kth code word given by $\mathbf{s}^k = [s^k_1, s^k_2, \ldots s^k_N]^T$ where N is the length of the codeword, and k = [1,2,…K].

The aperiodic autocorrelation of the code words is given by

(1)

$$R_{kk}[j] = \sum_{i=1}^{N-j} s_i^k \cdot s_{i+j}^{k\,*} .$$

A complementary pair of code words has the property

(2)

$$\sum_{k=1}^{2} R_{kk}[j] = \begin{cases} 0 & \text{for } j \neq 0. \\ 2N & \text{for } j = 0. \end{cases}$$

A set of K codes is considered complementary if and only if it satisfies the following equation:
(3)

$$\sum_{k=1}^{K} R_{kk}[j] = \begin{cases} 0 & \text{for } j \neq 0. \\ KN & \text{for } j = 0. \end{cases}$$

This far, we have only considered binary complementary codes, polyphase codes can also be complementary.[1]

CCK is defined by a set of 256 8-chip code words. They are specified by the following equation:

$$C = [e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)}, -e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j(\phi_1)}]$$

Where $\phi_i \in \{0, \pi/2, \pi, 3\pi/2\}$ for i=1,…4.

We consider this code set complementary because each code set has a complementary pair that is also a member of the set. Furthermore, they satisfy (3) for the entire set of 256 code words. The block coding system is shown at figure 8.

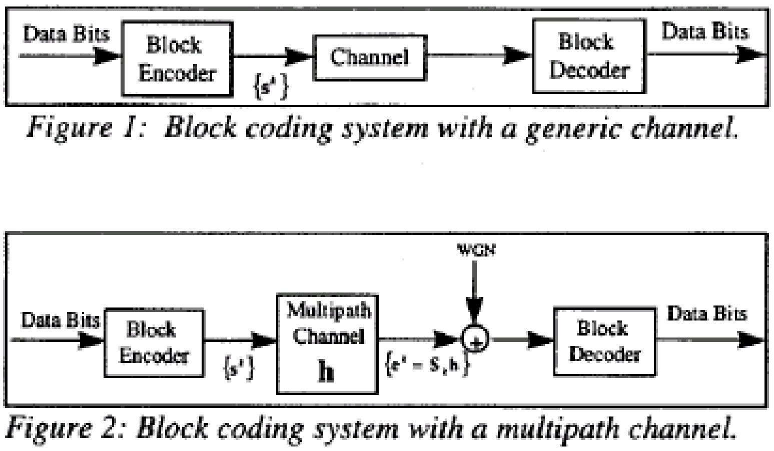


Figure 1: Block coding system with a generic channel.

Figure 2: Block coding system with a multipath channel.

Figure 8 Block coding system

DSSS Frame Format

Figure 9 shows the IEEE 802.11 DSSS frame format.

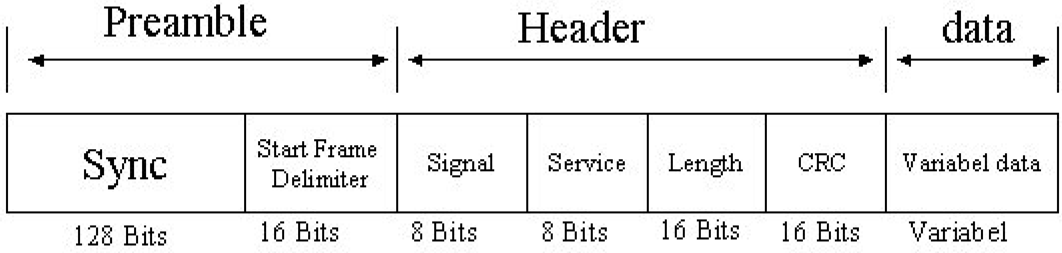


Figure 9 DSSS frame format

Like the FHSS frame the preamble and header are always transferred with 1 Mbps data rate and the Signal field indicates the data rate for the rest. In the IIIE 802.11b standard the Signal field supports higher data rates than the original 1 and 2 Mbps (11 Mbps and 5.5 Mbps).

SYNC field
The SYNC field consist of 128 bits of scrambled ones. This field makes sure the receiver can perform the necessary operations for synchronization.

Start Frame Delimiter (SFD) field
The SFD field indicates the start of the PHY-dependent parameters within the preamble.

Signal field
The signal field indicates to the PHY what modulation that shall be used for transmission. Data rate shall be equal to the signal field value multiplied by 100kbit/s.

Service field
This field is reserved for future use.

Length field
The length field is an unsigned 16-integer that indicates the number of microseconds required to transmit the payload (variable data).

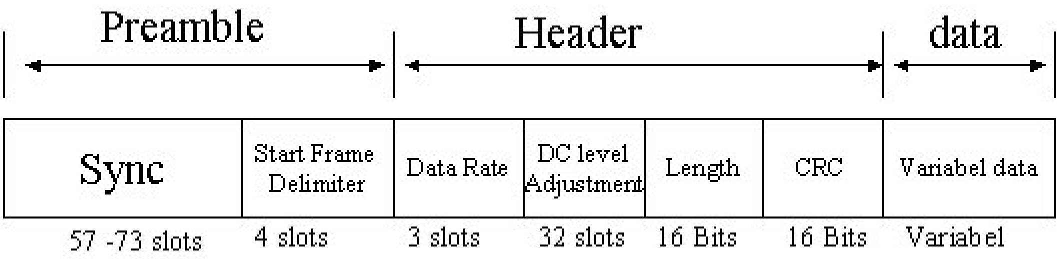
CRC field
The signal, length and service fields are protected by the CRC-16 frame check sequence.

Receiver minimum input level sensitivity
There are many physical specifications for transmitter and receiver in the 802.11b specification, but we will only mention the input level sensitivity that was needed for our assignment. According to 802.11b the frame error rate (FER) shall be less than $8*10^{-2}$ at a frame length of 1024 octets for an input level of –76dBm measured at the antenna connector. This is the FER for 11 Mbit/s CCK modulation.

For the 802.11 standard the frame error rate (FER) has the same value $8*10^{-2}$ for how much frame error that is permitted, but the input level is at –80dBm measured at the antenna connector. This is the FER for 2 Mbit/s DQPSK modulation.

Infrared
The third and last physical layer supported by the standard is infrared. It is based on the 850- to 950- nm range, which is nearly visible light. It is based on a diffuse IR transmission, which means that you don’t need a clear path between the transmitter and receiver. The transmission range is limited to 10 meters and restricted to in-building applications.

Infrared Frame Format
Figure 10 shows the IEEE 802.11 infrared frame format.



Sync	Start Frame Delimiter	Data Rate	DC level Adjustment	Length	CRC	Variabel data
57 -73 slots	4 slots	3 slots	32 slots	16 Bits	16 Bits	Variabel

Figure 10 Infrared frame format

The SYNC and SFD fields function exactly like the fields in the FHSS and DSSS frames. The Data rate field indicates the operation rates 1 Mbps referred to as “basic access rate” and the 2 Mbps referred to as “enhanced access rate”.

2.6.3 IEEE 802.11 MAC Layer

The main function for this layer is to control access to the wireless environment. It also has functions like fragmentation, encryption, power management, synchronization and roaming support where there are multiple access points.

Basic access method: CSMA/CA

The 802.11 standard use a Carrier Sense Multiple Access (CSMA) basic access method and works as follows: The station that wants to transmit senses the medium. If the medium is busy (some other station is transmitting) then the station must transfer at a later time. If the medium is free then the station is allowed to transmit.

These kinds of methods are very effective if the medium is not very heavy loaded with many stations, since it then allows stations transmit with minimum delay. Since it is possible that stations simultaneously senses the medium is free and transmits at the same time, causing a collision.

While one of the most popular access methods on wired networks is CSMA/CD (Collision Detection) used by IEEE 802.3 (Ethernet), this method may not be used for wireless networks. There are two main reasons for this:

1. You need a full duplex radio capable of transmitting and receiving at once for implementing a Collision Detection method, which would increase the price on the equipment significantly.
2. In a wired network all the stations can hear each other, which is a requirement for using the collision detection method. But wireless stations that may be far from each other, in networks with many access points, may not hear all collisions.

So to overcome the problems the IEEE 802.11 standard defines a collision avoidance (CA) method together with a positive acknowledge scheme to, as follows:

1. The station that wants to transmit senses the medium. If the medium is busy (some other station is transmitting) then the station must transfer at a later time. If the

medium is free for a specified time (called Distributed Inter Frame Space (DIFS) in the standard) then the station is allowed to transmit.

2. The receiving station checks the CRC of the received packet and sends an acknowledgement packet (ACK). If the station receives an acknowledgement it indicates to the transmitter that no collision occurred. If the Transmitter does not receive the acknowledgement then it retransmits the fragment until it receives acknowledgement or is thrown away after a given number retransmissions.

Virtual Carrier Sense to avoid collisions

To reduce the probability of two stations colliding because they cannot hear each other, the standard defines a Virtual Carrier Sense mechanism:

The station that wants to transmit first have to transmit a “Request To Send” (RTS), which contains source, destination and the duration of the following transaction (i.e. the packet and the respective ACK). The destination station responds with a response control packet “Clear to Send” (CTS), which contains the same duration information.

All the stations receiving either the RTS and/or the CTS set their Vertical Carrier Sense indicator for the given duration. This indicator is called NAV “Network Allocation Vector”. The station uses this info together with Physical Carrier Sense when sensing the medium.

A station that is “hidden” from the transmitter won’t cause collision in the receiver area under the short RTS transmission, because the station hears the CTS and “reserves” the medium as busy until the end of the transaction. The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledging station).

Since RTS and CTS are short frames, the mechanism also reduces the overhead of collisions, since these are recognized faster than if the whole packet was to be transmitted. This is only true if the packet are significantly bigger than the RTS and the standard allows small packets to be transmitted without RTS and CTS transaction in the beginning. The station has a RTS threshold parameter to regulate this.

Fragmentation and Reassembly

Wireless LANs prefer smaller packets for many reasons:

1. There is a higher bit error rate of a radio link and the probability of a packet getting corrupted increases with the packet.
2. If the packet is corrupted, the smaller the packet, the less overhead to retransmit the packet.
3. In the FHSS system the medium is interrupted periodically for hopping, so the smaller the packet, the smaller the chance that the transmission will be postponed after dwell time.

Because of this the MAC layer has a fragmentation and reassembly mechanism so it can deal with packets that are long, such as Ethernet packets that may be up to 1518 bytes long. The mechanism is a Send-and-Wait algorithm, where the transmitting station is not allowed to transmit a new fragment until of the following happens:

1. It receives an ACK for the said fragment, or
2. It decides that the fragment was retransmitted too many times and drops the whole frame.

But the standard allows the station to transmit to a different address between retransmission of a given fragment. This is useful when an AP has several outstanding packets to different destinations and one of them does not respond.

Inter Frame Spaces
The Inter Frame Spaces defines priorities and the standard defines four types:

1. SIFS - Short Inter Frame Space
   Is used to separate transmissions belonging to a single dialog.
2. PIFS - Point Coordination IFS
   Is used by the access point to gain access to the medium before any other station.
3. DIFS - Distributed IFS
   Are the IFS used by a station that wants to start a new transmission.
4. EIFS – Extended IFS
   Are longer IFS used by a station that has received a station that it can’t understand.

Frame types
The MAC layer supports three main types of frames:

1. Data frames that are used to transmit information between stations.
2. Control frames that are used to control access to the medium (e. g. RTS, CTS and ACK).
3. Management frames that are used to exchange management information between stations.

Figure 11 below shows the general MAC Frame Format.

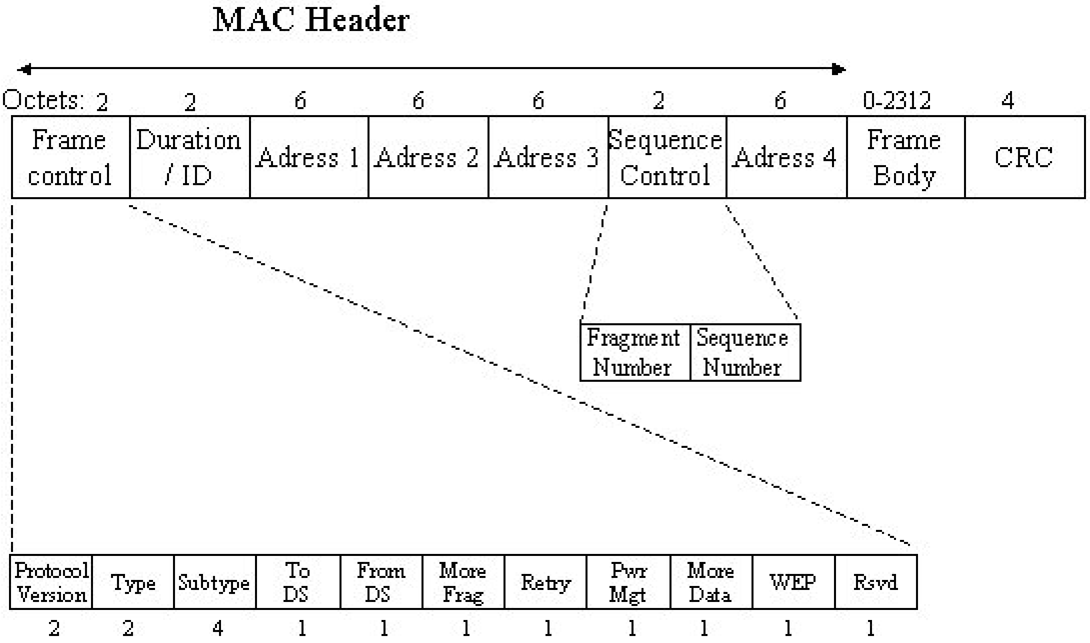


Figure 11 Frame types

Where DS = Distribution System

This format is used to transmit information between stations. Portions of this frame in the form of several fields are used in other types of frames. The frame body field can be up to a maximum of 2312 bytes that is enough to support transportation of an Ethernet frame with maximum length (1500 bytes).

Control field
The control field consists of 11 fields that we briefly will describe:

Protocol Version Subfield - This field provides a mechanism that identifies the version of the 802.11 standard.

Type Subfield – This field identifies four types of frames, which will be described later (only three presently defined).

Subtype Subfield – This field identifies a specific type of frame within the Type category.

ToDS Subfield – This field is set to the value 1 when the frame is addressed to an AP for forwarding to the distribution system, else it is set to 0.

FromDS Subfield – The value of this field is set to 1 if the frame is received from the distribution system otherwise it is 0.

More Fragments Subfield - This bit is set to 1 when there are more fragments belonging to the same frame following the current fragment.

Retry Subfield – This bit indicates that this fragment is a retransmission of a previously transmitted fragment. The receiver uses this to recognize duplicate transmissions, which may happen when Acknowledgement packets are lost.

Power Management Subfield – This bit is used to indicate the power management mode the station will be in after the transmission of the frame, which may set the station in "power save" mode or "active" mode.

More Data Subfield – This field indicates that more frames are buffered to this station.

WEP Subfield – This bit is indicating that the frame body is encrypted according to the WEP algorithm.

Order Subfield – This bit that this frame is being sent using the Strictly-Ordered Service class. The Strictly-Ordered Service Class is defined for users that cannot accept change of the ordering between Unicast frames and Multicast frames.

Duration/ID Field

This field have two different meanings depending on the frame type:

- In Power-Save Poll messages this is the Station ID.
- In all other messages this is the duration value used for the NAV calculation.

Address Fields

The frame may contain up to four addresses depending on the ToDS and FromDS defined in the control field:

- **Address-1** is the recipient address. If ToDS is set it is the AP Address, if it's not set this is the end-station address.
- **Address-2** is the transmitter address. If FromDS is set this is the AP Address, if it is not set this is the station address.
- **Address-3** is in most cases the remaining, missing address. On a frame with FromDS set to 1 the Adress-3 is the original Source Address, if the FromDS is set, then Address-3 is the destination Address.
- **Address-4** is used in special cases where a Wireless Distribution System is used, and the frame is being transmitted from one Access Point to another. Both the ToDS and FromDS bits are set, so both the original Destination and the original Source Addresses are missing.

Sequence Control Field

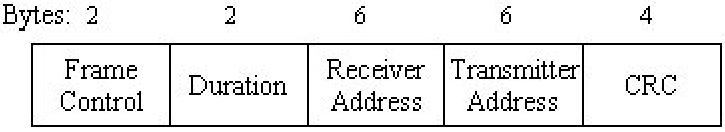
This field is used to represent the order of different fragments belonging to the same Frame and to recognize packet duplications. It contains the two subfields "Fragment Number" and "Sequence Number", which define the frame and the number of the fragment in the frame.

CRC Field

This field contains a 32-bit Cyclic Redundancy Check.

2.6.4 Most Common Frame Formats

RTS Frame Format

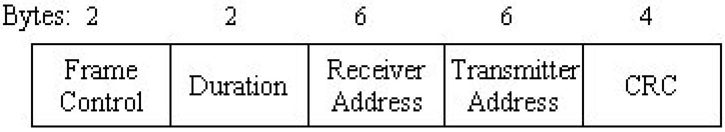


Bytes: 2	2	6	6	4
Frame Control	Duration	Receiver Address	Transmitter Address	CRC

Figure 12 RTS frame format

The receiver address (RA) in the frame represents the address of the station on the wireless network that is the intended immediate recipient of the next Data or Management frame. The transmitter address (TA) is the address of the station transmitting the RTS frame. The duration value is the time, in microseconds, required to transmit the next Data or Management frame plus one CTS frame, one ACK frame and three SIFS intervals.

CTS Frame Format

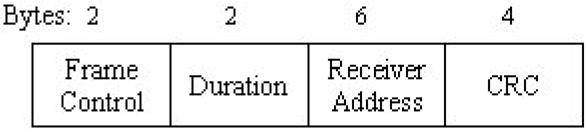


Bytes: 2	2	6	6	4
Frame Control	Duration	Receiver Address	Transmitter Address	CRC

Figure 13 CTS frame format

There is a relationship between certain fields in the CTS frame and the RTS frame, since the CTS is a response to the receipt of a RTS frame. The transmitter address (TA) from the RTS frame is copied to the receiver address (RA) field in the CTS frame, since this is the address it will respond to. The duration value it obtained from the duration field of the immediately previous RTS frame, minus the time, in microseconds, required transmitting the CTS frame and its SIFS interval.

ACK Frame Format



Bytes: 2	2	6	4
Frame Control	Duration	Receiver Address	CRC

Figure 14 ACK frame format

The receiver address (RA) field of the ACK frame is copied from the Adress-2 field of the immediately previous frame. If the More Fragment bit was set to 0 in the Frame Control field of the previous frame, the Duration value is set to 0, otherwise the Duration value is obtained from the duration field of the previous frame, minus the time, in microseconds, required to transmit the ACK frame and its SIFS interval.

2.6.5 Wireless LANs Operations

Two of the key operations in the wireless LANs are the method a station use to join an existing cell and how to support roaming in a WLAN.

Joining an existing cell
There are three periods of time when a station will need to access an existing basic service set (BSS). These are after power-up, after sleep mode, or when entering a BSS area. The station needs to get synchronisation information from the AP or from the other station when in Ad-hoc mode. The station can use two methods to get this information:

1. **Active Scanning** – With this method the station tries to locate an Access Point by transmitting probe request frames and wait for probe response packets from the AP.
2. **Passive Scanning** – With this method the station just waits for a Beacon frame from the AP. The Beacon frame contains synchronization information and provides the station with the synchronization information it needs.

The method the station chooses to use depends on the power consumption of the station and its performance.

Authentication and association process
After the station has located an Access Point, and decides to join its BSS, it must go through an authentication process. This is the interchange of information between the AP and the station, where each side proves the knowledge of a given password.

After the station is authenticated an association process starts. This is the exchange of information about the stations and BSS capabilities and makes the DSS to know about the current position to the station. A station cannot transmit or receive data frames before the association process is finished.

Roaming
Roaming is the process of moving from one cell (or BSS) to another without losing connection. The 802.11 standard does not define how roaming should be performed, but defines the basic methods for how to make it possible. These include active/passive scanning and the re-association process, where the station that is roaming from one AP to another becomes associated with the new one.

Keeping Synchronization
It is necessary having the stations synchronized in order to make the hopping synchronized, and because of other functions like power saving. On infrastructure BSS this is achieved by all the stations updating their clocks according to the AP’s clock. With the use of beacon frames (these frames contains the value of the Ap’s clock at the moment of transmission) the stations keeps synchronized.

2.7 Hiperlan 2 specification

Here we will try to give an introduction of HiperLAN/2 (High Performance Radio Local Area Network type 2). This is the next generation of WLAN technology. HiperLAN/2 is a standard being developed by the project BRAN (Broadband Radio Access Network) that is a part of ETSI (European Telecommunications Standards Institute), which can be, used worldwide.

The Hiperlan standards provide features and capabilities similar to those of the IEEE 802.11 wireless local area network standards, used in the U.S. and other adopting countries. HiperLAN/1 provides communications at up to 20 Mbps in the 5-GHz range of the radio frequency spectrum. HiperLan2 is, operating in the 5 GHz frequency spectrums, allowing data rates up to 54 Mbps. The Mobile Terminals (MT) communicates with the Access Points (AP) over an air interface as defined by the HiperLAN/2 standard. There is also an option with direct mode communication directly between two mobile stations.

A HiperLAN/2 network for business environment consists typically of a number of APs each of them covers a certain geographic area. Together they form a radio access network with full or partial coverage of an area of almost any size. The coverage areas may or may not overlap each other, thus simplifying roaming of terminals inside the radio access network. Each AP serves a number of mobile stations which have to a be associated to it. In the case where the quality of the radio link degrades to an unacceptable level, the terminal may move to another AP by performing handover.

The radio uses Orthogonal Frequency division Multiplex (OFDM), which is a radio technology ideal for broadband applications in a highly dispersive radio environments, where multiple reflections could cause delay spread and severe degradation of radio performance. OFDM is very efficient in time-dispersive environments, e.g. within offices, where the transmitted radio signals are reflected from many points, leading to different propagation times before they eventually reach the receiver. Above the physical layer, the Medium Access Control (MAC) protocol is all new which implements a form of dynamic time-division duplex to allow for most efficient utilization of radio resources. The MAC layer is developed and optimised for radio communication and realizes new features such as Quality of Service (QoS) for real time multimedia applications and very efficient power save control.

2.7.1 Architecture

HIPERLAN/2 radio access network can be used with a variety of core networks. This is possible due to a flexible architecture applied by all BRAN (Broadband Radio Access Networks) standards, which defines core network independent physical (PHY) layer and data link control (DLC) layers and set of core network specific convergence layers (CL) at the top of the DLC layer (see figure 15 below)

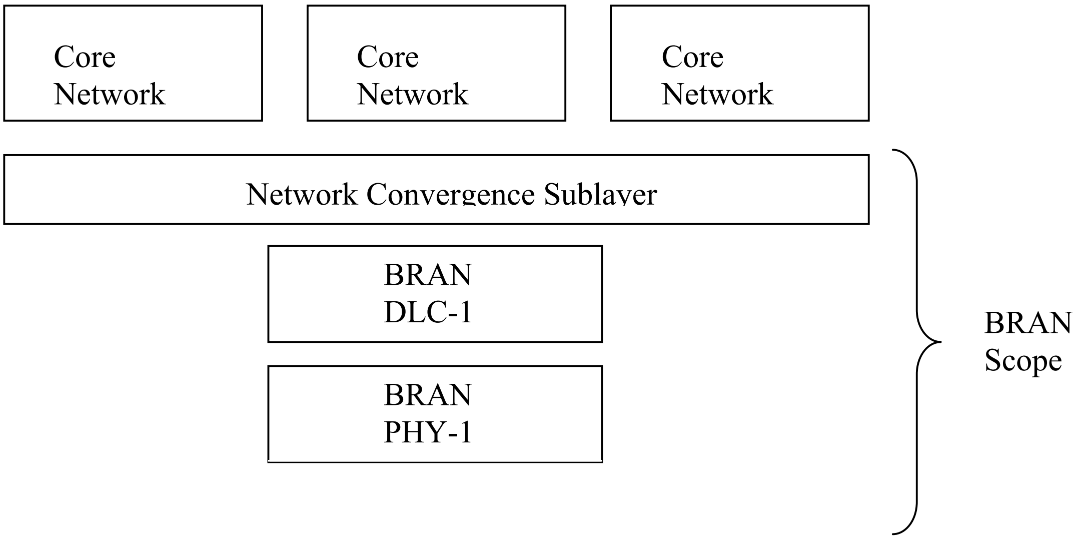


Figure 15 HiperLAN Architecture

The Physical Layer (PHY)
The PHY layer maps MAC PDUs to PHY PDUs and adds PHY signalling such as system parameters and headers intended for RF signal synchronization. The signal modulation is based on the Orthogonal Frequency Division Multiplexing (OFDM) with several sub-carrier modulation and forward error correction combinations that allow coping with various channel configurations.

The Data Link Control (DLC) layer
Two specifications address the basic part of the DLC layer. The first one includes the basic data transport functions consisting of Error Control protocol and Medium Access Control (MAC) protocol. The second specification defines the Radio Link Control (RLC) Sublayer that is used for exchanging data in the control plane between an access point and a mobile terminal. Furthermore, two specifications are developed for Home and Business profiles of the DLC. The air interface of HIPERLAN/2 is based on TDD and dynamic TDMA.

Convergence Layers (CL)
A CL has two main functions: Adapting service requests from higher layers to the services offered by the DLC and converting the higher layer packets with fixed or variable size into

fixed-size DLC Service Data Units that is used within the DLC. Convergence layers have been developed for Ethernet (IP based) applications, cell based core networks as ATM and for IEEE1394 protocols and applications. In addition, it is scheduled to define access interface(s) to the 3rd generation mobile in cooperation with the ETSI Project UMTS and 3GPP.

2.7.2 Features of HiperLAN/2

High-speed transmission
As mentioned earlier HiperLAN/2 has a very high transmission rate, which at the physical layer extends up to 54 Mbps and on layer 3 up to 25 Mbps. To achieve this OFDM is used to transmit the analogue signals.

Connection oriented
In A HiperLAN/2 network, data is transmitted on connection between the mobile station and the access point that have been established prior to the transmission using signalling functions of the HiperLAN/2 control plane. Connections are time-division-multiplexed over the air interface. There are two types of connections, point-to-point and point-to-multipoint. Point-to-point connections are bi-directional whereas point-to-multipoint are unidirectional in the direction towards the mobile terminal. In addition, there are also a dedicated broadcast channel through which traffic reaches all terminals from one AP.

QoS support
The connection-oriented nature of HiperLAN/2 makes it straightforward to implement support for QoS. Each connection can be assigned a specific QoS, for instance in terms of bandwidth, delay, jitter, bit error rate, etc. It is also possible to use a more simplistic approach, where each connection can be assigned a priority level relative to other connections.
This QoS support in combination with the high transmission rate facilitates the simultaneous transmission of many different types of data streams, e.g. video, and data.

Automatic frequency allocation
In a HiperLAN/2 network, there is no need for manual frequency planning as in cellular networks like GSM. The radio base stations, APs in HiperLAN/2, have a build-in support for automatically selecting an appropriate radio channel for transmission within each APs coverage area. An AP listens to neighbouring APs as well as to other radio sources in the environment, and selects an appropriate radio channel based on both what radio channels are already in use by other APs and to minimize interference with the environment.

Security support
The HiperLAN/2 network has support for both authentication and encryption. With authentication both the AP and the Mobile station (MT) can authenticate each other to ensure authorized access to the network (from the AP point of view) or to ensure access to a valid network operator (from MTs point of view). Authentication relies on the existence of a supporting function, such as a directory service, but which is outside the scope of HiperLAN/2.
The user traffic on established connections can be encrypted to protect against eavesdropping and a man-in-middle attacks.

The default encryption scheme is based on DES in output feedback mode with 56 bits key. Optionally, triple DES or no encryption can be selected. The Diffie-Hellmann key exchange procedure is used for the creation of the encryption key.

Mobility support
The MT will see that it transmits and receives data/to from the "nearest" AP, or more correctly speaking the MT uses the AP with the best radio signal as measured by the signal to noise ratio. Thus, as the user and the MT moves around, the MT may detect that there is an alternative AP with better radio transmission performance than the AP which the MT which is currently associated to. The MT will then order a hand over to this AP. All established connections will be moved to this new AP resulting in that the MT stays associated to the HiperLAN/2 network and can continue its communication. During handover, some packet loss may occur.
If an MT moves out of radio coverage for a certain time, the MT may loos its association to the HiperLAN/2 network resulting in the release of all connections.

Network & application independent
The HiperLAN2 protocol stack has a flexible architecture for easy adaptation and integration with a variety of fixed networks. A HiperLAN2 network can for instance be used as the "last hop" wireless segment of a switched Ethernet, but it may also be used in other configurations, e.g. as an access network to 3 rd generation cellular networks. All applications which today run over a fixed infrastructure can also run over a HiperLAN2 network.

Power save
In HiperLAN2, the mechanism to allow for an MT to save power is based on MT-initiated negotiation of sleep periods. The MT may at any time request the AP to enter a low power state (specific per MT), and requests for a specific sleep period. At the expiration of the negotiated sleep period, the MT searches for the presence of any wake up indication from the AP. In the absence of the wake up indication the MT reverts back to its low power state for the next sleep period, and so forth. An AP will defer any pending data to an MT until the corresponding sleep period expires. Different sleep periods are supported to allow for either short latency requirement or low power requirement.

2.8 802.11a

IEEE 802.11a is an extension of IEEE 802.11.
802.11a uses OFDM system. The radio frequency LAN system is initially aimed for the 5.15-5.25, 5.25-5,35 and 5.725-5.825 GHz unlicensed national information structure (U-NII) bands, as regulated in the United States by the Code of Federal Regulations, Title 47, section 15.407. The OFDM system provides a wireless LAN with data payload communication capabilities of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. The support of transmitting and receiving at data rates of 6, 12 and 24 Mbps is mandatory. The system uses 52 subcarriers that are modulated using binary or quadrature phase shift keying (BPSK/QPSK), 16-quadrature amplitude modulation (QAM), or 64-QAM. Forward error correction coding (convoluting coding) is used with a coding rate of ½, 2/3 or ¾.

In a multiple cell network topology, overlapping and/or adjacent cells using different channels can operate simultaneously.

Table 1 Maximum power levels for the United States

Frequency band (GHz)	Maximum output power with up to 6 dBi antenna gain (mW)
5.15 – 5.25	40 (2.5 mW/MHz)
5.25 – 5.35	200 (12.5 mW/MHz)
5.725 – 5.825	800 (50 mW/MHz)

2.8.1 802.11a VS HiperLAN 2

At the first glance at 802.11a and HiperLAN 2 both standards look quite the same, since they both work in the same 5 GHz band and are they are both capable of 54 Mbps data transfer rate.

The main difference between these two standards is that HiperLAN 2 has a strong security support which includes built-in support for encryption and authentication. For encryption HiperLAN 2 uses DES (Data Encryption standard), which an algorithm for data encryption based on a 64 bit secret key, or triple DES. The 802.11a uses 40 bit RC4 (which can be extended to 128 bit).

802.11a has a connection less medium access control while HiperLAN 2 is connection oriented.

QoS (Quality of Service) 802.11a uses Point Control Function that allows certain time slots being allocated for realtime-critical traffic. HiperLAN 2 uses RVSP (Resource Reservation Protocol), which is widely used in connection-oriented networks. This protocol makes it easy to make each connection to be assigned with a specific QoS (for instance in terms of bandwidth, delay and jitter etc).

The fixed network support for 802.11a is only Ethernet, while HiperLAN 2 supports Ethernet, IP, ATM, UMTS, FireWire and PPP.

802.11a has no Radio link quality control, while HiperLAN 2 has Link Adaption that makes it possible for a mobile station to listen on other AP’s and choose the one with best signal automatically.

802.11a is from IEEE standardisation organisation and HiperLAN 2 standard is made from the ETSI BRAN. In the 802.11a standard there is only specifications for US regarding frequency allocation and power output. This indicates that 802.11a is intended to be used in the US and HiperLAN 2 in Europe.

3 Factors affecting coverage within a room

The next step in our thesis was to find a model of coverage within a room. We knew that this part is one of the challenges in WLAN and very important in order to be able to plan the layout of WLANs. If you are to make a model of coverage, you must naturally know what affects the coverage. For that reason before we see on any mathematical models, the different factors affecting coverage will be described. Below at figure 16 displays an overview of what some of the most important factors affecting the coverage.

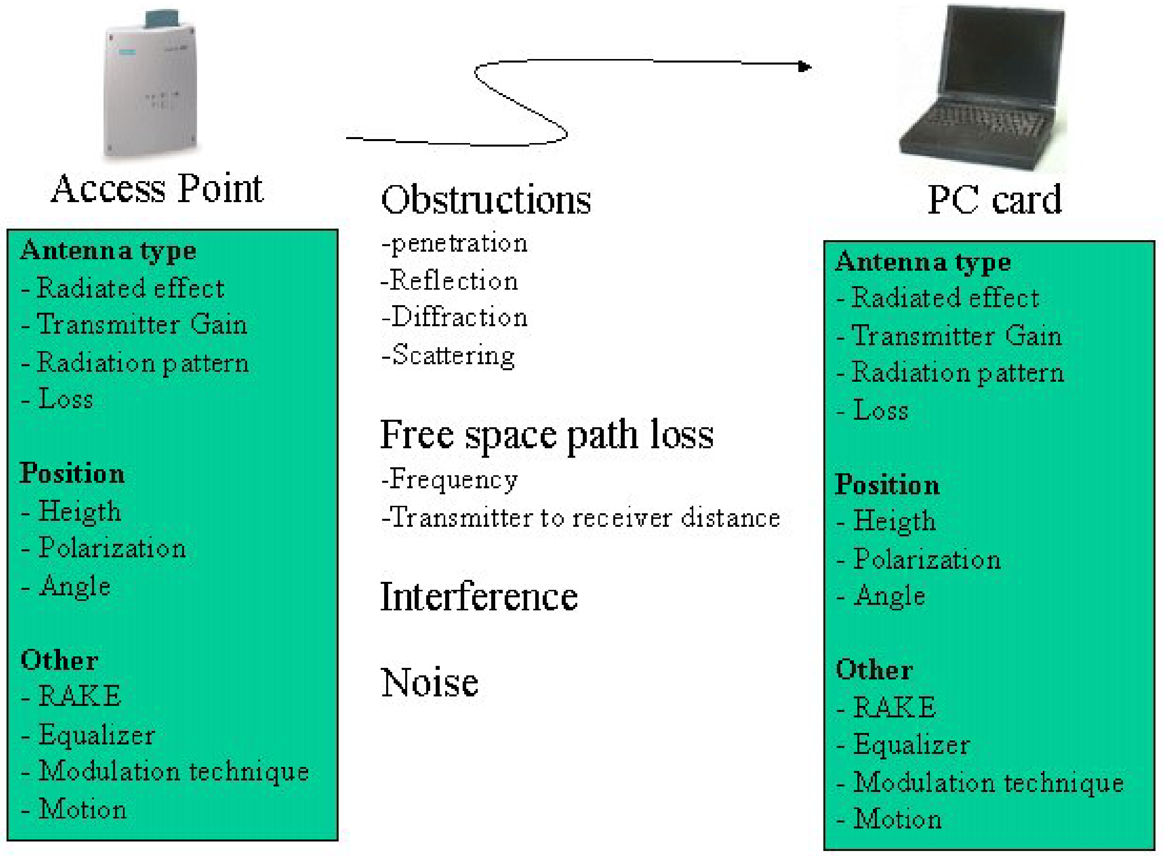


Figure 16 Factors affecting the coverage

3.1 Antennas

The spectrum used in WLAN is on 2,4 GHz band and in the 5 GHz band. The WLAN systems can be used indoor as well as outdoor. Outdoor WLAN can be used as a link between two points or point to multipoint. Many different types of antennas can be used in WLANS to tailor your output to the environment. To describe the antennas there are many different characterizations.

3.1.1 Antenna characteristics

Isotropic Antenna
A hypothetical, lossless antenna that has a equal radiation intensity in all directions. Used as a 0 dB gain reference in directivity calculation (gain).

Antenna Gain
The antenna gain is a measure of the antenna directivity. It is defined as the ratio of the radiation intensity in a given direction to the intensity that would have been obtained if the power accepted by the antenna were radiated equally in all directions. Antenna gain is expressed in dBi (dB gain with respect to an isotropic source).

Radiation pattern
A graphical representation in either polar or rectangular coordinates of the spatial energy distribution of an antenna.

Side lobes
The side lobes are the radiation lobes in any direction other than the main lobe.

Omni directional antenna
Radiates and receives equally in all directions in azimuth. The following (figure 17) diagram shows the radiation pattern of an omnidirectional antenna with its side lobes in polar form. As showed at the figure below seen from the side.

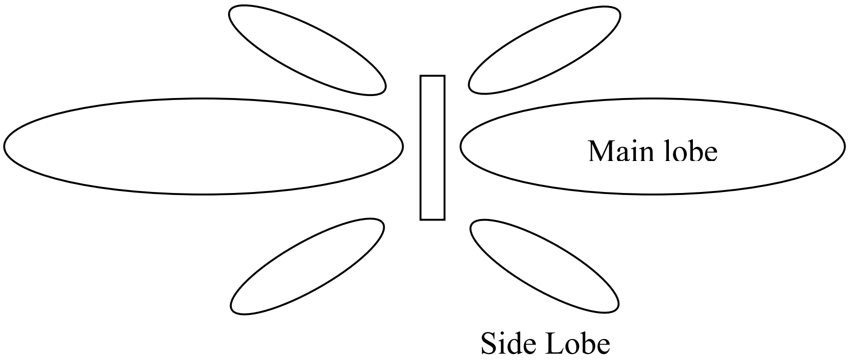


Figure 17 Omni directional antenna

Directional antenna

Radiates and receives most of the signal power in one direction. The following diagram (figure18) shows the radiation pattern of an antenna with its side lobes in polar form:

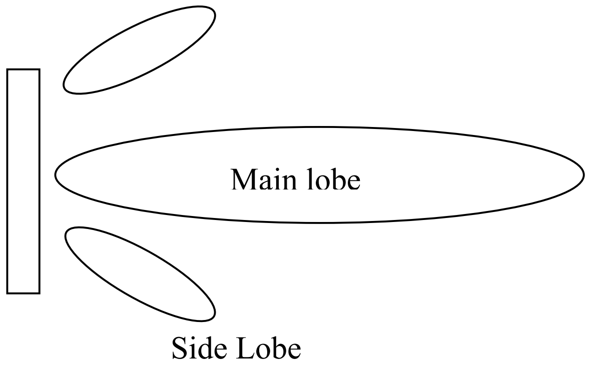


Figure 18 Directional antenna

Antenna beamwidth

The directiveness of a directional antenna is defined as the angle between two half-power (-3dB) points on either side of the main lobe of radiation.

3.1.2 Antenna types

Dipole antenna

A dipole antenna is a straight electrical conductor measuring 1/2 wavelength from end to end and connected at the centre to a radio frequency. This antenna, also called a *doublet*, is one of the simplest types of antennas, and constitutes the main RF radiating and receiving element in various sophisticated types of antennas. The dipole is inherently a balanced antenna, because it is bilaterally symmetrical. For best performance, a dipole antenna should be more than 1/2 wavelength above the ground, the surface of a body of water, or other horizontal, conducting medium such as sheet metal roofing. The element should also be at least several wavelengths away from electrically conducting obstructions such as supporting towers, utility wires, guy wires, and other antennas.

Coaxial antenna

A coaxial antenna is a variant of the dipole antenna, designed for use with an unbalanced feed line. One side of the antenna element consists of a hollow conducting tube through which a coaxial cable passes. The shield of the cable is connected to the end of the tube at the centre of the radiating element. The centre conductor of the cable is connected to the other half of the radiating element. The element can be oriented in any fashion, although it is usually vertical.

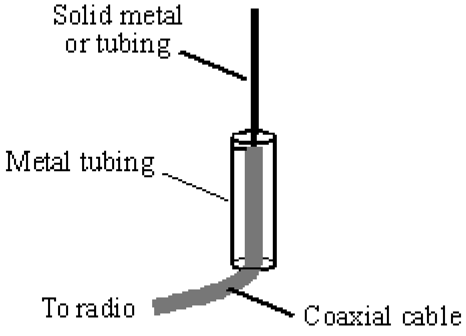


Figure 19 Coaxial antenna

Dish antenna
A dish antenna, also known simply as a *dish*, is common in microwave systems.
A dish antenna consists of an active, or driven, element and a passive parabolic or spherical reflector. The driven element can be a dipole antenna or a horn antenna. The reflector has a diameter of at least several wavelengths. As the wavelength increases (and the frequency decreases), the minimum required dish diameter becomes larger.
When the dipole or horn is properly positioned and aimed, incoming electromagnetic fields bounce off the reflector, and the energy converges on the driven element. If the horn or dipole is connected to a transmitter, the element emits electromagnetic waves that bounce off the reflector and propagate outward in a narrow beam.

3.2 Propagation in mobile radio systems

The radio channel is a limitation in performance of wireless radio systems. The path between the receiver and the transmitter may vary in many ways, with different obstructions. This makes it hard to predict the received signal or to analyse the radio channel. The modelling of a radio channel is typically done in a statistical fashion, based on measurements made specifically for an intended communication system or spectrum allocation. Most propagation systems are based on outdoor wireless systems and not concerned about indoor propagation. The field of indoor propagation is relatively new and the first research started in the early 1980s. The arrival of WLAN makes it even more necessary having indoor models to predict coverage. Under we will describe issues that are relevant when modelling propagation in indoor environments. Below you see a typical indoor propagation as a function of received power at a given distance between transmitter and receiver given in meters [1].

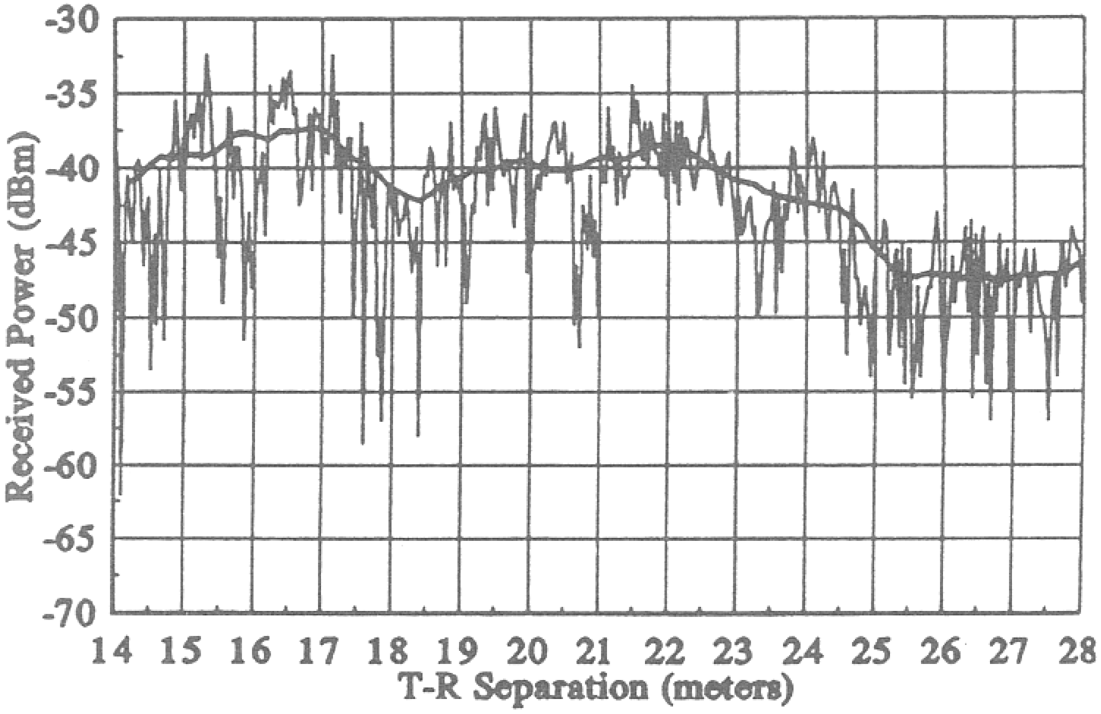


Figure 20 Received power at a given distance between transmitter and receiver

The figure illustrates that the average signal (the centre line) changes slowly with distance, but there is rapidly changes in the power when the receiver moves. The phenomena's behind the received power "behaviour" at the figure will thoroughly be described in the sections to come.

3.2.1 Free space propagation

It is called free space propagation when there is a line-of-sight path with no obstacles in the way between the transmitter and receiver. With free-space propagation the only loss is the decay of the signal as a function of the separation in meters between the transmitter and receiver. The decay of the signal is only affected by how the transmitter and receiver antennas are designed, how their radiation patterns are and so on. It is not affected by distortions in the propagation path.

3.2.2 Interference and noise

WLAN is sharing a common spectrum in the 2.400 - 2.4835 GHz band. Industry, Science and Medicine share the same band. This band is often just called ISM band. FCC regulations permit radiated power up to 1 watt in this band provided spread spectrum techniques are employed. Spread spectrum methods facilitate multiple users sharing the same spectrum in an unlicensed environment and offer interference rejection properties.

Interference

Radio frequency interference is one of the most important issues to be addressed in the design, operation and maintenance of wireless communication systems. Both intermodulation and intersymbol interference constitutes problems to account for in system planning.

Adjacent Interference
Adjacent interference results from signals that are adjacent in frequency to the desired signal. Adjacent channel interference results from imperfect receiver filters which allows nearby frequencies to leak into the pass band.

Co-channel Interference
Co-channel interference lies within the bandwidth of the victim receiver and arises principally from the transmitters using the same band.

Intermodulation distortion
Non-linear distortion in a system or transducer characterised by the appearance in the output of frequencies equal to the sums and differences of integral multiples of the two or more component frequencies present in the input waveform.

Intersymbol interference (ISI)
Intersymbol interference is caused by multipath in bandlimited (frequency selective) time dispersive channels distorts the transmitted signal, causing bit errors at the receiver.

Noise
The term noise refers to unwanted electrical signals that are always present in electrical systems. The presence of noise superimposed on a signal tends to obscure or mask the signal; it limits the receivers ability to make correct symbol decisions, and thereby limits the rate of information transmission. Noise arises from a variety of sources, both man-made and natural. Man-made noise includes such sources as spark plug ignition noise, switching transients, and other radiating electromagnetic signals. Natural noise includes electrical circuit and component noise, atmospheric disturbances, and galactic sources.

Thermal noise
Thermal noise is arising from the electrons in motion in all dissipative components – resistors, wires and so on. Because of crashes with atoms in the dissipative components, the electrons in motion will be depended on the temperature and produce a varying current. In addition we will get noise from active elements like for instance an amplifier. The more hot a source gets, the faster the electrons rotate and more noise is the result. The same electrons that are responsible for electrical conduction are also responsible for thermal noise.

Industry noise
The industry noise is mainly meant coming from machines of different kinds. i.e. electrical engines, high current lines, cars, aeroplanes etc. industry noise is often vertical polarized, that means that horizontal polarized antennas is less sensitive to this kind of noise than vertical polarized antennas.

Atmosphere noise
Atmospheric noise is coming from disturbance and “storms” in the ionosphere and the atmosphere, in thunderstorms especially that is the most common cause to the most noise.

Cosmic noise

Cosmic (or galactic) noise is in its characterization pretty much alike thermal noise. Cosmic noise lowers its intensity with increased frequency.

The figure 21 below illustrates what factors that will have an effect on the radio signal on its way from the sender to the receiver.

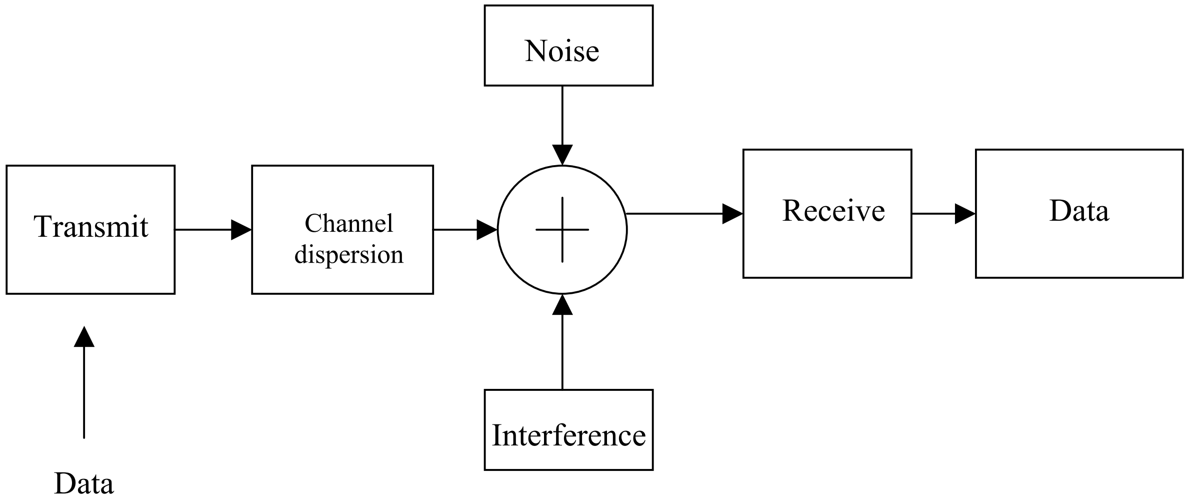


Figure 21 Factors that will have an effect on the radio signal

3.2.3 Interference from microwave ovens and Bluetooth

Microwave ovens
Microwave ovens work in the same frequency band as WLAN. Hence we will take a closer look at microwave ovens to find interfere with WLAN.

The heating source of residential microwave ovens is based on a single magnetron tube mostly positioned in an upper corner. Such oven as this produces an uneven heating effect, therefore, the usage of a rotating disk with rotated food on it are illuminated with a more even result. See figure 22 for the spectrum it occupies.

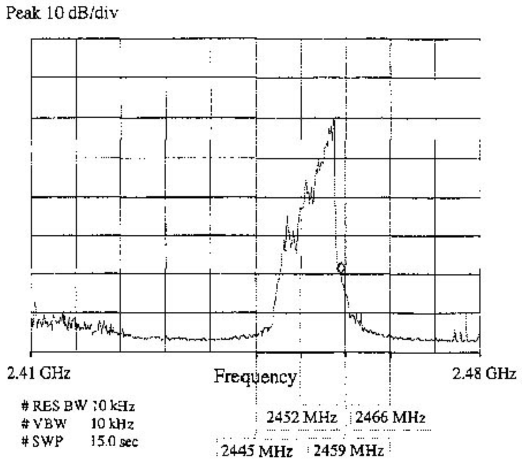


Figure 22 Max hold spectrum for residential microwave ovens

Microwave ovens, which are used for commercial applications, are based on two magnetron tubes, which are alternately active during one half of the mains power cycle of 20 msec. Commercial microwave ovens occupies a much wider spectrum than the residential ones see figure 23 and 24.

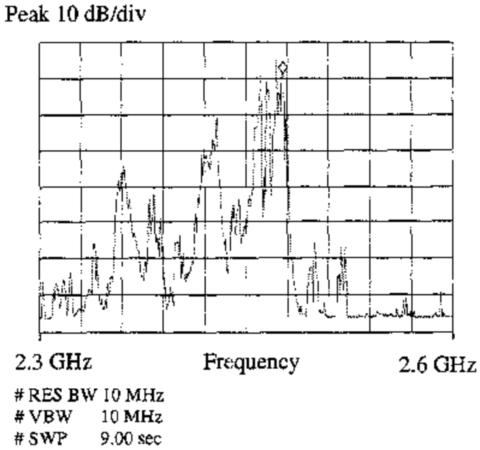


Figure 23 Max-hold spectrum for commercial microwave oven with rotating mirror plates.

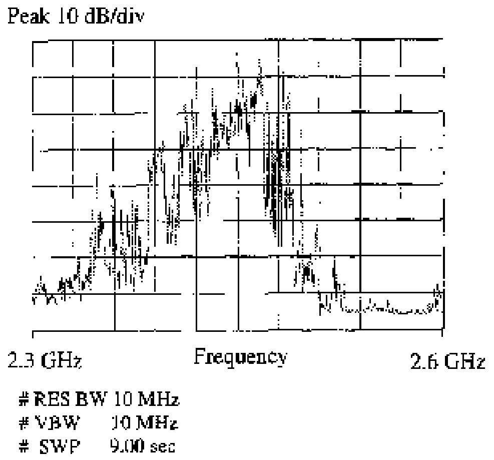


Figure 24 Max-hold spectrum for commercial microwave oven with reflector in bottom and ceiling

The noise that comes from the commercial ovens is a CW-like pulse. Pulse behaviour like this is also found in residential ovens, observed during the beginning and the end of the burst. The commercial ovens shows a random variation in frequency over tens of MHz.
CW interference affects DSSS systems differently than a FHSS system, since the receiver bandwidth for DSSS is much larger. With FHSS, the in band frequency range is much smaller, but the vulnerability to in band CW interference is much larger.
The higher sensitivity of FHSS to in-band CW interference shows that DSSS can persist interference better, before retransmission will occur. Residential ovens represent interference sources that occupy only a small part of the 2,4 GHz band, and are not active during most of the 20 msec power cycle. This allows DSSS to avoid usage of channels that do not fall inside the disturbed frequency zone around 2,45 GHz. At channels close to 2,45 GHz, the error recovery scheme takes advantage of the silent part of the 20 msec intervals. With FHSS, most hop channels are sufficiently separated from the disturbed zone. During the periods the disturbed hop channels must be used, the error recovery scheme also takes advantages of the silent part of the 20 msec intervals. [33], [38]

Bluetooth
Another technology that may interfere with WLAN is the Bluetooth technology.
Bluetooth (BT) provides interconnection of devices in the user's vicinity in a range of about 10 m, and it could become an official standard if adopted by IEEE 802.15, which seeks to develop a standard for personal area networks. The basic architectural unit in BT systems in the piconet composed of a master device and seven active slave devices at most, which are allowed to communicate with the master only. Since BT and 802.11 is working in the same 2,45 GHz band these two systems will interfere with each other.

Short BT facts
Bluetooth can provide a bit rate equal to 1 Mbps. A FHSS scheme is used at the physical level; each master chooses a different hopping sequence so that piconets can operate in the same area without interfering with each other. Hopping frequencies range over 79 frequency channels in the ISM band, each of the channels being 1 MHz wide. The nominal hop dwell time is equal to 625 μs. Sequences are created by generating several sub-sequences, each

composed of 32 hops at random over the first 64 MHz of the frequency spectrum; then the successive 32 MHz are skipped, and the next sub-sequence is randomly chosen among the following 64 MHz. The procedure is repeated until the hopping sequence is completed. A TDD technique is used to transmit and receive data in a piconet: each packet transmitted in a slot corresponds to the minimum dwell time; slots are centrally allocated by the master and alternately used for master and slave transmissions.

To calculate the degree of interference of these two systems is difficult, if not impossible because there will never be the same network topology of the two systems. There is common opinion that the systems will interfere with each other [36], [39], [40]. The interference will also be dependent of the distance to WLAN AP, PC cards and BT units.

3.3 Phenomena's during propagation

In an indoor environment there are naturally many obstructions that may be in the way of the electromagnetic waves path. These objects that may be all from walls, floor to furnishing is affecting the signal in different ways, and the most common materials are described generally below:

- Metal objects reflect radio signals. This means the signal won't pass through metal walls, in addition metal objects within a room reflect the signal and may cause multipath fading.
- Wood, glass, plastic and brick reflect part of the radio signals and let some pass through.
- Objects with high moisture content absorb most of the radio signal.

When the electromagnetic signal propagates through a room it's affected by many different phenomena's because of the different types of obstructions. The phenomena's that causes fading and loss to the signal must be taken into account when making a mathematical model of coverage in WLAN.

3.3.1 Reflection

Reflection occurs when a propagating electromagnetic wave impinges upon an object that has very large dimensions when compared to the wavelength of the propagating wave. Reflections occur from the surface of the earth, from walls and other objects as shown at figure 25.

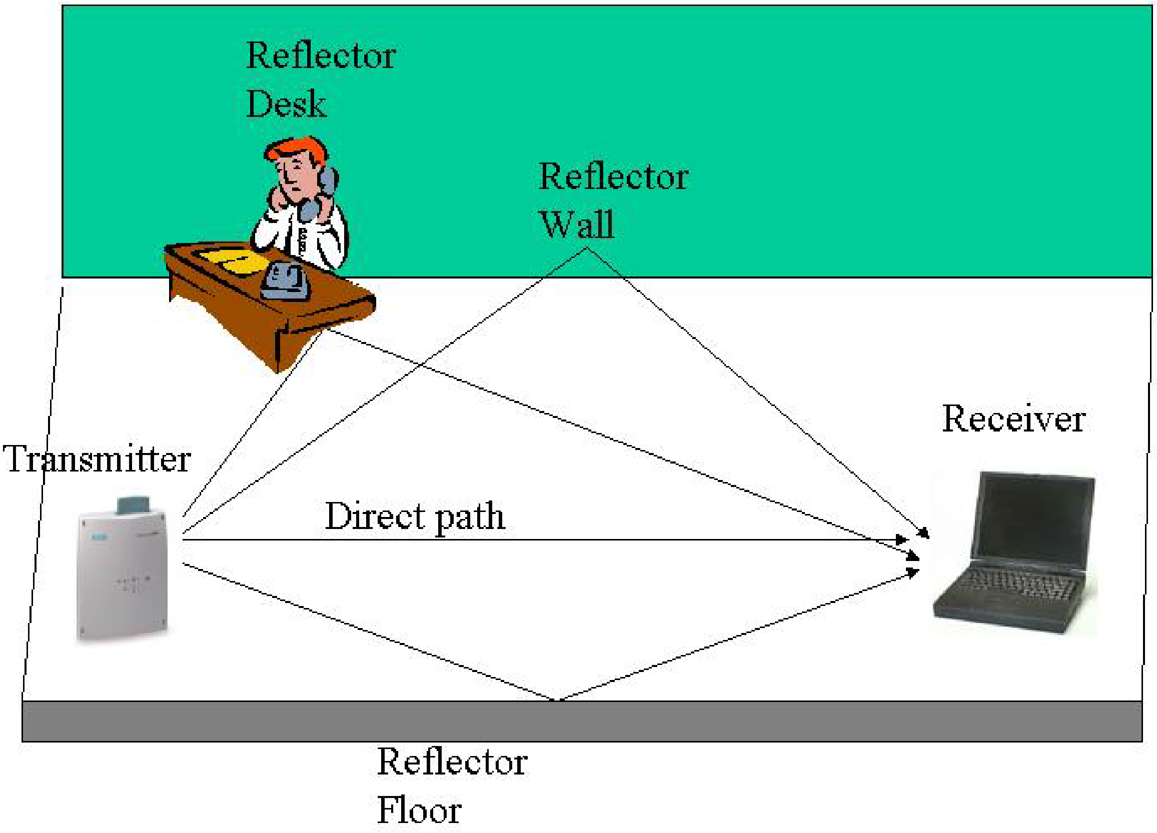


Figure 25 Reflection from different reflectors in a room

Multipath fading because of reflections
When an electromagnetic signal is transmitted trough the air it most likely will take many paths to the receiver because of reflections. Since the signal that is taking alternative paths will arrive slightly later then the direct signal, there will occur fading. This is because the reflected signals will have different amplitude than the direct signal when arriving at the receiver after some delay. All of these signals reaching the receiver result in a linear distorted version of the transmitted signal. The reflections make the channel impulse response of a wireless channel look like a series of pulses. Below at figure 26 we see a typical real measured indoor impulse response [32].

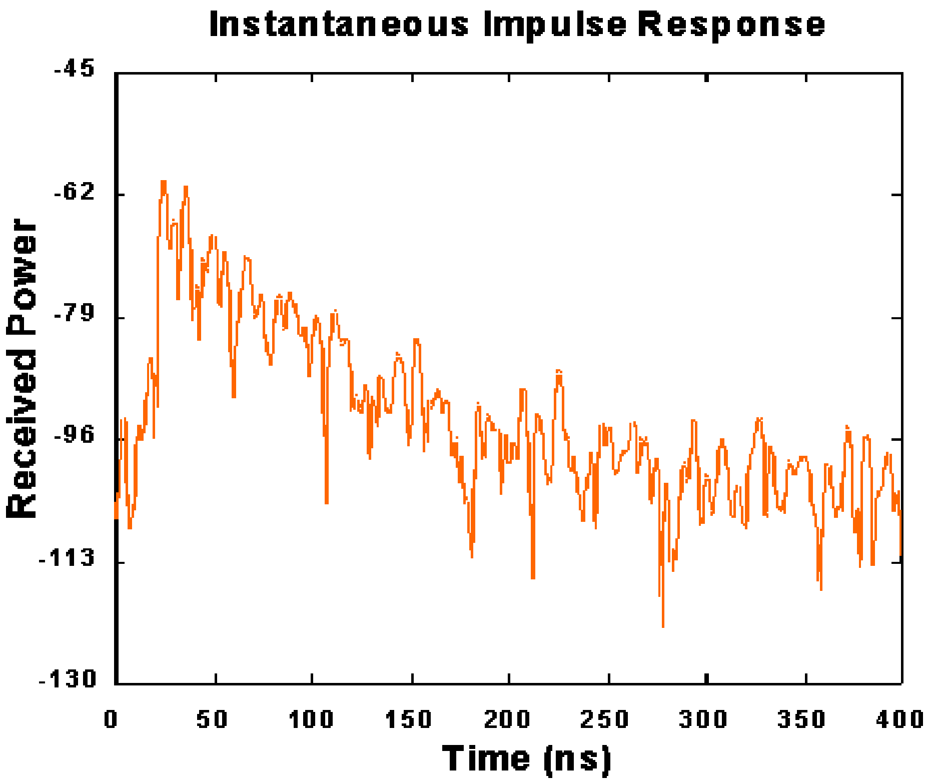


Figure 26 Instantaneous impulse response

From a real impulse response like above you may derive the pulses and the figure below shows an impulse response only showing the pulses from five different reflectors arriving some time after the direct the signal. There have been many measurements of delay spreads in different environments. Seidel and Rappaport reports delay spreads between 50 and 300 ns in pico-cellular channels. The length of the path and how much of the signal is absorbed when it reflects on a reflector affects the delay and amplitude.

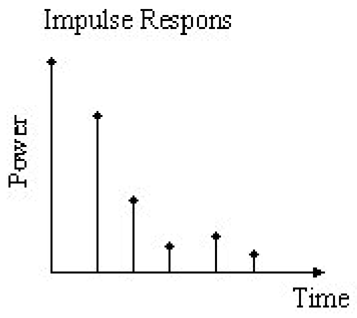


Figure 27 Impulse response for a multipath signal

Delay profile and some definitions
The delay profile is the expected power per unit of time received with a certain excess delay. It is obtained by averaging a large set of impulse responses(figure3.12).

The *Maximum delay time spread* is the total time interval during which reflections with significant energy arrive.
The *rms delay spread* is the standard deviation (root mean square) value of the delay of reflection, weighted proportional to the energy in the reflected waves.

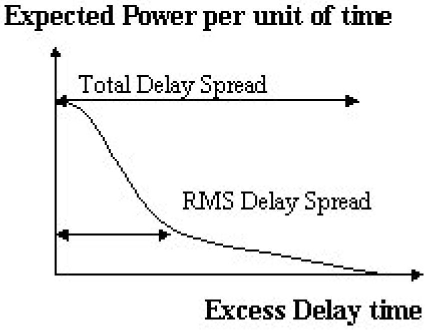


Figure 28 Delay profile

A typical indoor delay profile will have a more flat profile up to some point, and a tail of weaker reflections with larger delay. This is because early reflections will arrive with almost identical power.

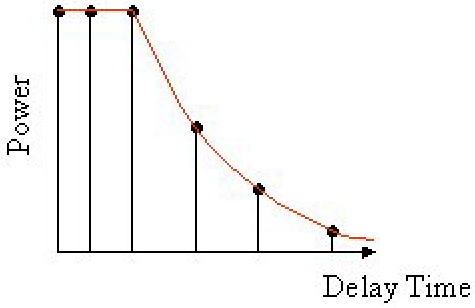


Figure 29 Typical indoor delay profile

Effects of different time delay spread
Multipath time delay spread causes intersymbol interference, which results in an irreducible BER floor for mobile systems. Based on results of simulations it is known that for all small delay spreads (relative to the symbol duration), flat fading are the dominant error mechanism. Flat fading is when the strength of the received signal changes with time due to fluctuations in the gain of the channel caused by multipath, but the spectrum of the transmission is preserved. Typical flat fading channels cause deep fades, and may require 20 or 30 dB more transmit power to achieve low bit error rates. For large delay spreads, timing error and ISI are the dominant error mechanisms.

Connection between RMS delays spread and Error Rate
The picture below is from a simulation that shows the connection between Symbol Error Rate and RMS path Delay spread [2]. The lowest curve is the one for CCK that is used in 802.11b for 5.5Mbps and 11Mbps transmissions.

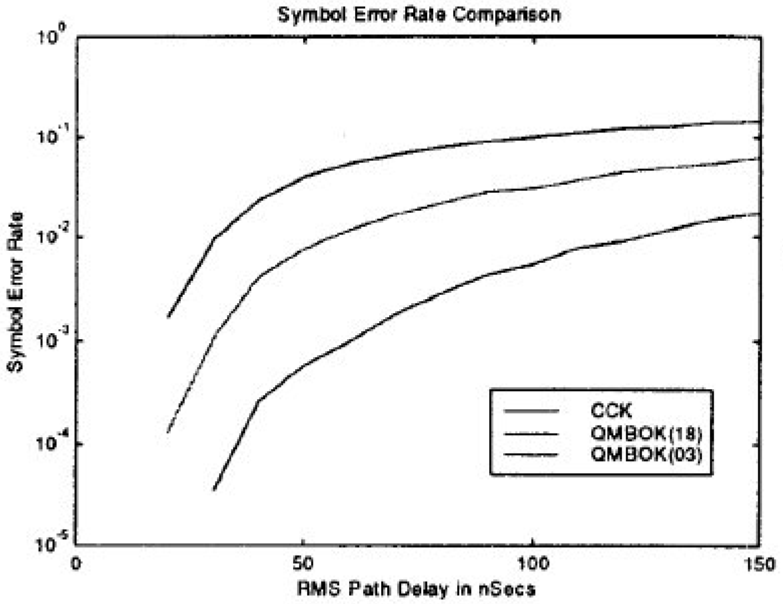


Figure 30 Symbol error rate comparison

Connection between transmitter to receiver distance and delay spread
The delay spread normally increases with the separation between the distance between transmitter and receiver antenna and how hostile the environment is. The figure 31 below shows measurements taken at Cory Hall at UC Berkeley [32].

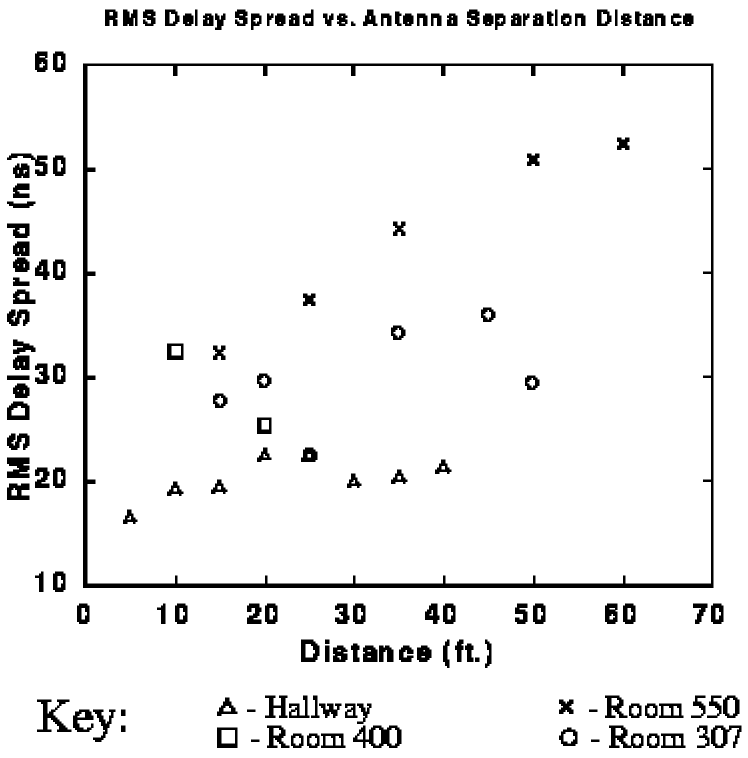


Figure 31 RMS delay spread vs. antenna separation distance

They found that Delay spread increased with the transmitter to receiver distance and the dimension of the room. But with small dimensions and the almost lack of obstacles the delay spread wouldn't increase with distance (like the hallway measurement).

Rake receiver and equalizer minimizes the ISI effect because of multipath fading
A RAKE receiver consists of a bank of correlators, each of which correlate to a particular multipath component of the desired signal. It combines the information obtained from several resolvable multipath components. The correlator's outputs may be weighted according to their relative strengths and summed to obtain the final estimate. A RAKE receiver can be used to improve performance where frequency-selective fading effects and multipath fading is occurring.

Equalization compensates for Intersymbol interference (ISI) created by multipath within time dispersive channels. If the modulation bandwidth exceeds the coherence bandwidth of the radio channel, ISI occurs and modulation pulses are spread in time. An equalizer within a receiver compensates for the average range of expected channel amplitude and delay characteristics. Equalizers must be adaptive since the channel is generally unknown and time varying.

3.3.2 Penetration

When a signal propagates through an indoor office environment it meets many obstacles and some of these it will penetrate. When penetrating a obstacle the signal will experience a loss depended of the thickness of the object and what material it is made of. The frequency of electromagnetic wave also decide how much of the signal that will come through the object. There exist a lot of measurements made of loss through different materials for WLAN. From Ericsson's "Wireless LAN User's Guide version 4.2" [3] we have table 2 that is representable of what loss to expect trough different types of materials.

Table 2 Penetration through different type of materials

Obstruction	Loss
Open space	0 dB
Window (non-metallic tint)	3 dB
Window (metallic tint)	5-8 dB
Light Wall (dry wall)	5-8 dB
Medium Wall (wood)	10 dB
Heavy Wall (solid core 6")	15-20 dB
Very Heavy Wall (solid core 12")	20-25 dB
Floor / Ceiling (solid core)	15-20 dB
Floor / Ceiling (heavy solid core)	20-25 dB

3.3.3 Diffraction

Diffraction occurs when the radio path between the transmitter and receiver is obstructed by a surface that has sharp irregularities (edges). The secondary waves resulting from the obstructing surface are present throughout the space and even behind the obstacle, giving rise to a bending of waves around the obstacle, even when a line-of-sight path does not exist between transmitter and receiver. At high frequencies, diffraction, like reflection, depends on the geometry of the object, as well as the amplitude, phase, and polarization of the incident wave at the point of diffraction.

Fresnel zones

Fresnel zones explain the concept of a diffraction loss as a function of the path difference around an object. Fresnel zones represents successive regions where secondary waves have path length from the transmitter to the receiver which are $n\lambda/2$ greater than the total path length of a line of sight path. Figure 32 shows Fresnel zones that are displayed as the concentric circles on the plane. The successive Fresnel zones have he effect of alternately providing constructive and destructive interference to the total received signal.
The radius of the n th Fresnel zone circle is defined by a approximate $r_{n:}$

$r_n = \sqrt{((n\lambda d_1 d_2)/(d_1+d_2))}$, *when* $d_{1,}\, d_2 >> r_n$

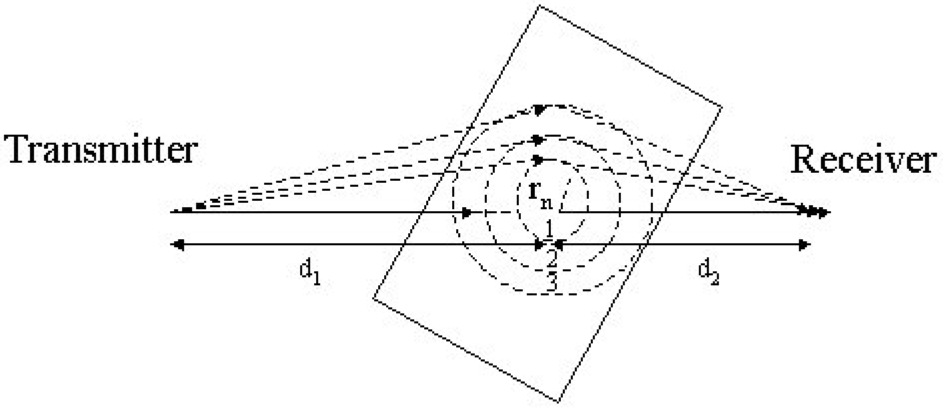


Figure 32 Concentric circles that define the boundaries of successive Fresnel zones

The excess total path length for a ray passing through a circle is nλ/2 where n is the circle number (integer). Figure 33 below shows when a obstacle blocks the path, then a series of ellipsoids can be constructed between a transmitter and a receiver by joining all the points for which the excess path delay is an integer multiple of half wavelengths. The ellipsoids represent the Fresnel zones.

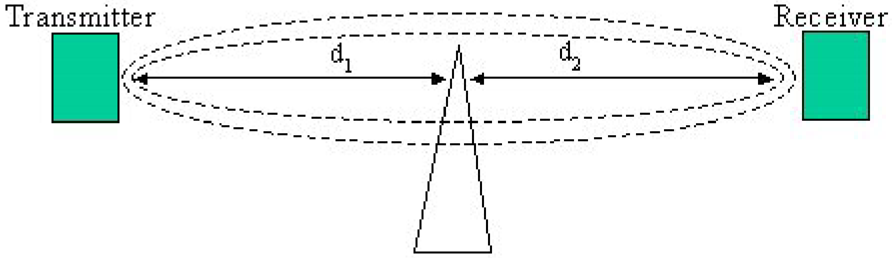


Figure 33 Fresnel zones displayed as ellipsoids

In mobile systems diffraction loss occurs from the blockage of secondary waves such that only a portion of the signal is diffracted around an obstacle. A rule of thumb used for line-of-sight microwave links is that as long as 55 % of the first Fresnel zone is kept clear, then further Fresnel zone clearance doesn't significantly alter the diffraction loss.

Knife-edge diffraction models

Generally it is impossible to make very precise estimates of the diffraction losses, and the prediction is a process of theoretical approximations modified by necessary empirical corrections. When we see on the loss of a single knife-edge we get a good overview of the significance of diffraction loss. To estimate diffraction loss we a use diffraction parameter expressed mathematically:

$v=h\sqrt{((2(d_1+d_2))/(\lambda d_1d_2))}$

Where the parameters are illustrated in figure 34 below.

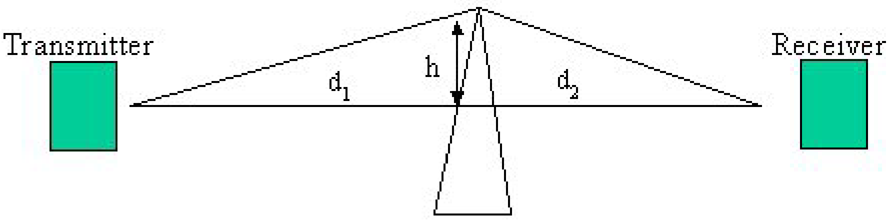


Figure 34 Knife-edge diffraction

A graphical representation of gain as a function of diffraction parameter is given in figure 35 [1].

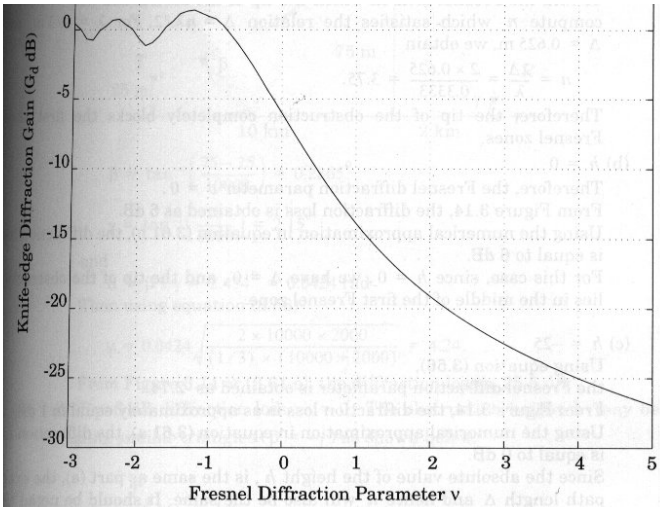


Figure 35 Fresnel diffraction parameter

There have also been made many models to estimate the diffraction loss for multiple obstructions, but we will not go further on this.

3.3.4 Scattering

Scattering occurs when the medium through which the wave travels consists of objects with dimensions that are small compared to the wavelength, and where the number of obstacles per unit volume is large. Scattered waves are produced by rough surfaces, small objects, or by other irregularities in the channel. In practice, foliage, street signs, and lampposts induce scattering in a mobile communications system.

3.3.5 Additional effects

Wave guiding

Wave guiding can be viewed as a particular propagation phenomena happening in corridors or tunnels. The power loss in such environment is most cases less than in free space. You may say there is a wave guiding gain. Power loss decreases with increasing frequency, which is proven for frequencies up to 17GHz simulations and measurements.

Movement

Extensive measurements carried out at the School of Electrical Engineering in Belgrade have shown that a portable terminal slowly moving through an indoor environment experiences Ricean or Rayleigh fading depending on whether LOS conditions exist or not. In the former case, Ricean K factor takes values in the range 2 to 10dB [42].

4 Model of coverage within a room for WLAN

Models prediction coverage for an AP is important in order to:

- Plan the cells placement so that the cells, having the same frequency area, aren't interfering with each other and cause errors.
- See how large areas you can cover with one AP.

The indoor propagation models are different from traditional propagation models in two aspects:

- The distances that are covered are much smaller.
- Variability of the environment is much greater for smaller separations between transmitter and receiver.

The prediction models are either theoretical or empirical. Almost all empirical models are based on the same general model (4.9).

4.1.1 Thresholds for having a connection

In our assignment we were only thinking of the coverage within one cell. When having this in mind we must define what are the thresholds for when a connection no longer exist. For WLAN there are two measures that are mentioned in the 802.11 and 802.11b specifications.

1. The FER (Frame Error Rate) shall be maximum $8*10^{-2}$, which also may be given in BER (Bit Error Rate), PER (Packet Error Rate) or SER (Symbol Error Rate).
2. The received signal strength at the antenna connector shall be at least –76dBm for 802.11b CCK modulation and –80dBm for 802.11 QPSK modulation.

4.2 Consideration of how to find a proper model

Our challenge was to find a suitable model for coverage of WLAN within a room. We started with a model from ETSI TR-101-112 ch. B.1.8 as a basis. This is a path loss model for indoor office test environment for the UMTS technology. We didn't know if this model would be useable for modelling coverage in WLAN. We intended to validate our base model basically on measured values and expected values (that we could derive from specifications of our equipment). The background of the model would have to be investigated before we could consider the indications given by our measured and expected values. Consequently we first have considered our base model validity on information we have found available.

4.3 Indoor office path loss model

Indoor office path loss model was the model that we had as a basis in order to find a model of coverage in WLAN. It is a model of indoor office path loss meant for UMTS. The model is taken from ETSI TR-101-112 ch. B.1.8, which is a specification of selecting procedures for the choice of radio transmission technologies of the UMTS.

Model description
The personal antenna height of 1.5 m was used in developing the propagation model for all test environments.

The indoor office path loss is based on the COST 231 [5] model that is defined as follows:

$$L = L_{FS} + L_c + \sum k_{wi} L_{wi} + n^{((n+2)/(n+1) - b)} * L_f \tag{4.1}$$

Where
L_{FS} = free space between transmitter and receiver
L_c = constant loss
k_{wi} = number of penetrated walls of type i
n = number of penetrated floors
L_{wi} = loss of wall type i
L_f = loss between adjacent floors
b = empirical parameters
NOTE 1: L_c normally is set to 37 dB.
NOTE 2: n = 4 is an average for indoor office environment. For capacity calculations in moderately pessimistic environments, the model can be modified to n = 3.

Table 3 Weighted average for loss categories

Loss category	**Description**	**Factor (dB)**
L_f	Typical floor structures (i.e. offices) - Hollow pot tiles - Reinforced concrete - Thickness typ. < 30 cm	18.3
L_{w1}	Light internal walls - Plasterboard - Walls with large numbers of holes (e.g. windows)	3.4
L_{w2}	Internal walls - Concrete, brick - Minimum number of holes	6.9

Under the simplifying assumptions of the office environment the indoor path loss model has the following form:

$$PL(R) = 37 + 30\mathit{Log}(R) + 18.3\, n^{((n+2) / (n+1) - 0.46)} \text{ dB} \tag{4.2}$$

Where:
R is the transmitter-receiver separation given in meters.
n is the number of floors in the path.

Since we are only considering the coverage within a room, the parts of the model that is concerning penetration through walls are removed. This leads to this model:

$$PL(R) = 37 + 30Log\,(R)\ dB \tag{4.3}$$

Background of the model
The path loss model is based on the COST 231 model, which made it natural to explore the "COST 231 Final report" from the Commission of the European Communities.

The COST 213 model is an empirical indoor model. It is a multi-wall model and gives the path loss as the free space loss added with losses introduced by the walls and floor penetrated by the direct path between the transmitter and receiver. It has been observed that the total floor loss is a non-linear function of the number of penetrated floors. The constant loss is a term, which results when wall losses are determined from measurements results, by using multiple linear regressions. Normally it is close to zero.

Hence the only loss in this model concerning us, were the free space path loss. We started exploring for other models of free space path loss, to possible find how the parameters in this model had been calculated.

4.4 Friis free space propagation model

For propagation distances *d* much larger than the antenna size, the far field of the generated electromagnetic wave dominates all other components. In free space, the energy radiated by an omni-directional antenna is spread over the surface of a sphere (figure 4.1). The surface area of a sphere of radius *d* is $(4\pi)^2d^2$.

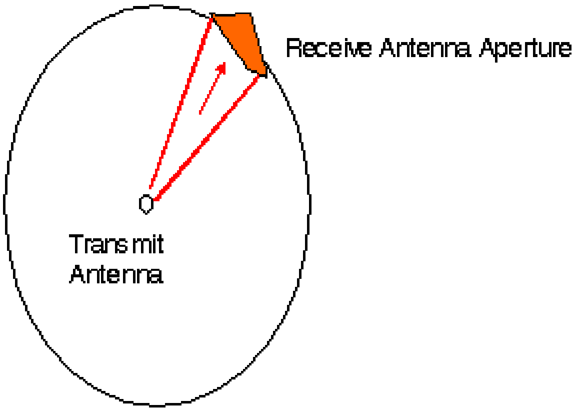


Figure 36 Received Antenna Aperture

Friis free space model of path loss calculates the received signal power at the receiver antenna with a known distance *d* to the transmitter antenna:

$$P_r(d)= P_tG_tG_r\lambda^2 / (4\pi)^2d^2L \tag{4.4}$$

$P_r(d)$ – is the received power
P_t – is the transmitted power
G_t – is the transmitter antenna gain
G_r – is the receiver antenna gain
λ – is the wavelength in meters
d – is the separation in meters between the receiver and transmitter antenna
L – is system loss not related to propagation

The path loss represents signal attenuation as a positive quantity measured in dB. It is defined as the difference in dB between the effective transmitter power and the received power.
The path loss for the model when antenna gains are included:

$$PL\ (dB) = 10 \log (P_t/P_r) = -\ 10 \log ((G_t G_r \lambda^2) / ((4\pi)^2 d^2))) \tag{4.5}$$

The path loss for the model with antennas that are assumed to have unity gain:

$$PL\ (dB) = 10 \log (P_t/P_r) = -\ 10 \log ((\lambda^2) / ((4\pi)^2 d^2))) \tag{4.6}$$

When the received effect at a distance (reference distance d_0) is known, the equation below can be used to find the received effect at a distance further away:

$$P_r(d)=P_r(d_0) + 20 \log(d_0/d) \tag{4.7}$$

This equation is easily transformed to path loss:

$$PL\ (d) = PL(d_0) + 20 \log (d/d_0) \tag{4.8}$$

Relationship to the indoor office path loss model (4.2)
Now we see there is an apparent relationship between the two models. They both operate with a reference point and have a logarithmic path loss from this reference point:

$PL\ (d) = PL(d_0) + 20 \log (d/d_0) \rightarrow PL(R) = 37 + 30 Log\ (R)$

According to the free space model the frequency (wavelength) of the signal affects the path loss. There is a difference in the spectrum allocations for UMTS and WLAN. In Europe and Asia UMTS allocates the bands 1920-1980 MHz for uplink and 2110-2170 MHz for downlink. The bandwidth for WLAN is from 2,400 to 2,483 GHZ.

To illustrate the magnitude of the difference in path loss due to frequency difference, we selected some frequency values for the two technologies. For UMTS we selected 2,0 GHz, while for WLAN we used 2,4 GHz and assumed no antenna gains and distance 1 meter (the reference point for the indoor office path loss model) using (4.6):

UMTS: $PL\ (dB)) = -\ 10 \log ((0,15)^2) / ((4\pi)^2 d^2))) = 38,46\ dB$

WLAN: $PL\ (dB)) = -\ 10 \log ((0,125)^2) / ((4\pi)^2 d^2))) = 40\ dB$

The approximate difference due to frequency is 1,5 dB. Additional antenna gain must be subtracted from the path loss, which possibly is the explanation for the reference value 37 dB at 1 meter for the indoor office path loss model.

The path loss from the reference point is:

Free space path loss model: *20 log (R),* where R is distance in meters if the d_0 is 1 meter

Indoor office path loss model: *30 log (R),* where R is distance in meters

The loss for the indoor office path loss model increases with a higher rate than the free space path model. To find the explanation behind the different rates of loss between the two models; more models would have to be explored.

4.5 Log-distance path loss model

Both theoretical and measurement-based propagation models indicate that average received signal power decreases logarithmically with distance. Indoor path loss has been shown by many researchers to obey the distance power law in equation:

$$PL\ (d) = PL\ (d_0) + 10n\ \log(d/d_0) + X_\sigma \tag{4.9}$$

n - path loss exponent
$PL(d_o)$ - the path loss at a close reference distance
X_σ - standard deviation

n is a path loss exponent value that depends on the type of environment. Table 4 below shows typical values for n [9]. X_σ is a normal random variable in dB having a standard deviation of σ dB. The reference path loss is calculated using the free space path loss model (4.4) or field measurements. The reference distance should always be in the far field of the antenna so that near-field effects can’t alter the reference path loss.

Table 4 Path loss exponents

Environment	Path loss exponent, n
In-building/factory with LOS condition	1.6 to 2
Indoor open plan, obstructed sight	2 to 4
Indoor, one to three floor separation, obstructed within residential building	4 to 6

The figure 37 shows the path loss curves for different path loss exponents (n).

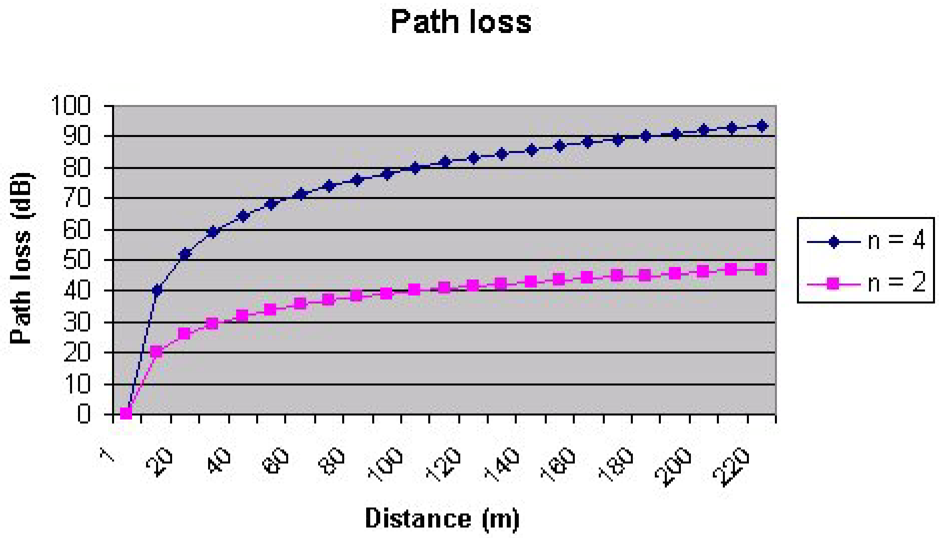


Figure 37 Path loss for different path loss exponents

This is a practical path loss estimation technique, which has the advantage of implicitly taking into account all the propagation factors.

Relationship to the indoor office path loss model
The indoor office model is apparently based on this general model. The path loss reference is 37 dB and the path loss exponent is 3.

However the indoor office path loss model isn't valid at other frequencies or environments than it is derived from. The path loss exponent they have chosen is probably an average value they preferred for some reason. Thus a proper model of coverage for our WLAN can only be established by making new measurements and calculations for the its transmission frequency and environment.

4.6 Model of coverage for WLAN

We chose the Log-distance path loss model as the base model. Since it is adjustable to different environments, when varying the path loss exponent. First we explored only the path loss aspect, not considering deviation:

$$PL\ (dB) = PL\ (d_0) + 10n \log(d/d_0) \qquad (4.10)$$

The information available to the user (who is setting up the WLAN) is varying. Different methods creating the model can be used, based on what the user find suitable:

1. Base it on theory and select path loss exponent from table
2. Base it on the specifications of the equipment
3. Base it on measurements

The first model is a completely theoretical model, which is possible to adjust. The second model is derived from the specifications of the equipment. The third model is derived from the measurements. With our measurements we obtain different path loss exponents for the different environments.

4.6.1 Model of coverage based on theory

The reference point at 1 meter is calculated with Friis free space path loss model (4.4):

$PL(1) = 10 \log ((G_t G_r \lambda^2) / ((4\pi)^2 d^2))) = 10 \log ((0{,}125)^2) / ((4\pi)^2 d^2))) = 40\ dB - G_t - G_r$

Having the reference path loss, the total path loss depending on the distance between the transmitter and receiver using equation 4.10 is:

$$PL(R) = 40 + (10 * n \log (R)\ ) - G_r - G_t \qquad (4.11)$$

Where R is number of meters, G_r is receiver antenna gain and G_t is transmitter antenna gain. The path loss exponent (n) can approximately be selected from table 4.

Having the total loss, the radiated effect from the transmitter can be used to calculate the received signal strength in dBm:

$$P_r(R) = P_t - (40 + 10 * n \log (R) - G_r - G_t) \qquad (4.12)$$

P_t is radiated effect from transmitter in dBm.

Using our equipment and the Master of Science laboratory room as an example
Radiated power P_t = 18 dBm, from specification of AP.
The receiver (laptop) can be placed at very diverse places in laboratory room, and some different path loss exponents depending on the placement were selected from table 4:

n = 1,8 , assuming a line of sight placement in the room.
n = 3 , assuming a average no line of sight placement in the room.
n = 4 , assuming a pessimistic no line of sight placement in the room.

Since we don’t know the gains, we assumed unity gain. Figure 38 displays the received signal strength with the different path loss exponents.

LOS placement of the receiver:

$Pr(R) = P_t - (40 + 10 * n \log (R) - G_r - G_t) = 18\ dBm - (40 + 1{,}8 * 10 \log (R))\ dBm$

Average NLOS placement of the receiver:

$Pr(R) = P_t - (40 + 10 * n \log (R) - G_r - G_t) = 18\ dBm - (40 + 1{,}8 * 10 \log (R))\ dBm$

Pessimistic NLOS placement of the receiver:

$\mathrm{Pr(R)} = \mathrm{P_t} - (40 + 10 * \mathrm{n} \log (\mathrm{R}) - \mathrm{G_r} - \mathrm{G_t}) = 18\ \mathrm{dBm} - (40 + 4{,}0 * 10 \log (\mathrm{R}))\ \mathrm{dBm}$

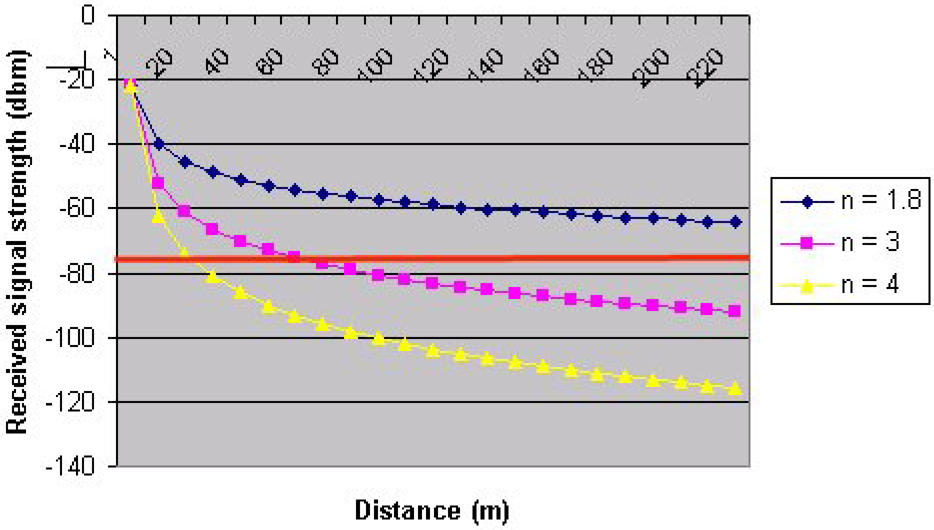


Figure 38 Received signal strength for different path loss exponents

Later this example was compared to the models based on measurements in the Master of Science lab in figure 50, seeing how close we came to the "real" model adjusted by our measurements.

4.6.2 Model of coverage based on specification of the equipment

We had the following equipment to our disposal:

- I-GATE 11M I/LAN Access Point shown at figure 39.

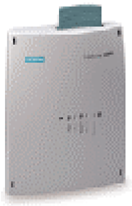


Figure 39 Access point

- 2 I-GATE 11M PC Cards shown at figure 40, which we installed in our laptops

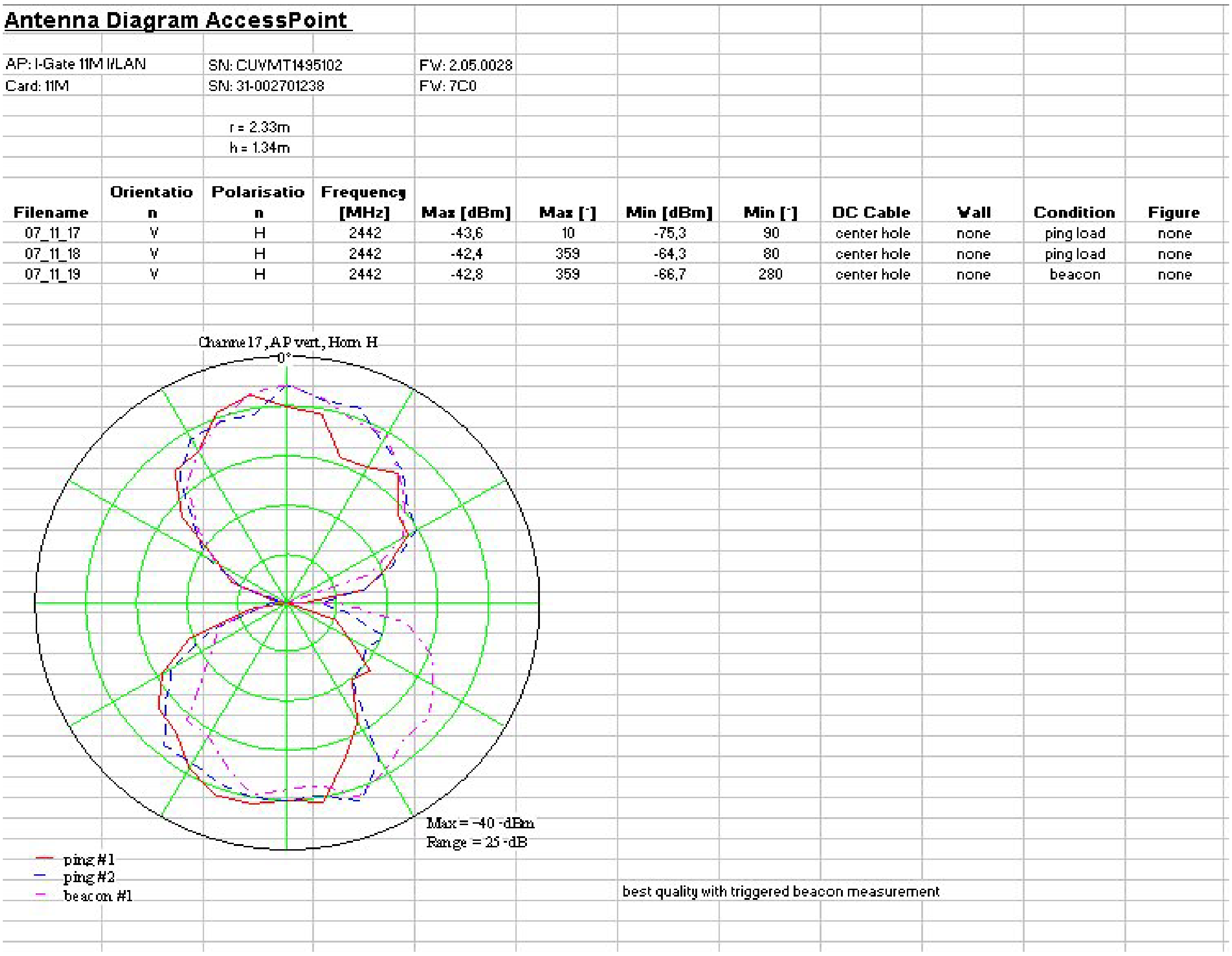
Figure 40 PC card

- 2 laptops, Dell Latitude CPi D266XT (figure 41) and Dell Inspirion 3800

Figure 41 Dell Latitude CPi D266XT

There were little specifications [appendix A] following the equipment. We sent requests to Siemens for antenna specifications and after a while, we received radiation diagrams for their AP (figure 42) and PC card [appendix B].

Sensible specifications
Transmission power: 63mW or +18dBm
Range: 60 meters
Bit error rate: 1 * 10^{-5}



Antenna Diagram AccessPoint

AP: I-Gate 11M WLAN	SN: CUVMT1495102	FW: 2.05.0028
Card: 11M	SN: 31-002701238	FW: 7C0

r = 2.33m
h = 1.34m

Filename	Orientation	Polarisation	Frequency [MHz]	Max [dBm]	Max [°]	Min [dBm]	Min [°]	DC Cable	Wall	Condition	Figure
07_11_17	V	H	2442	-43,6	10	-75,3	90	center hole	none	ping load	none
07_11_18	V	H	2442	-42,4	359	-64,3	80	center hole	none	ping load	none
07_11_19	V	H	2442	-42,8	359	-66,7	280	center hole	none	beacon	none

best quality with triggered beacon measurement

Figure 42 Radiation diagram for the AP when AP vertical and receiver horizontal

In the specifications (802.11b) it is given that the receiver shall at least tolerate signal strength of –76 dBm. Thus we have assumed that this is the signal strength at 60 meters that is the APs specified range.

According to the radiation diagram –42,4 dBm signal strength is received from the AP at a distance of 2,33 meters, which was measured in a laboratory room [appendix B].

Then the received signal strength at 2,33 meters could be used as a reference value:

$$P_r(2{,}33) = -42{,}2 \text{ dBm}$$

The advantage of using measured reference point is that the antenna gains are implicit in the measurement. Without measured reference point, Friis free space model must be used. Assuming no antenna gains (no gains given in the specification), this received signal strength is calculated using 4.4:

$$P_r\,(1) = P_r(R) = P_t - 10 \log ((G_tG_r\,\lambda^2) / ((4\pi)^2 d^2))))$$
$$=18 - (10 \log ((0{,}125)^2) / ((4\pi)^2 * 1^2))) = -22 \text{ dBm}$$

The range is specified by Siemens to be 60 meters. With a determined range the path loss exponent for the two models described above can be found using 4.8:

P(60) = $PL\ (d_0) + 10n\ log(d/d_0)$ = -42,4 - 10n log(60/2,33) = -76 dBm -> n = 2,38

P(60) = $PL\ (d_0) + 10n\ log(d/d_0)$ = (18 – 40) dB – 10n log (60) = -76 dBm -> n=3,03

Having the path loss exponents, two different models can be made out from their reference point. Having a measured reference point at 2,33 meters, this model is calculated.

$$P_r(R) = -42{,}4 + 23{,}8\ log(R/2{,}33)\ dBm \quad (4.13)$$

We refer to 4.13 as the measured model.

Having a calculated reference point at 1 meter, this model is calculated:

$$P_r(R) = -22 - (40 + 30{,}3\ log\ (R))\ dBm \quad (4.14)$$

We refer to 4.14 as the calculated model.

The calculated received signal strength for the two models are displayed at figure 43.

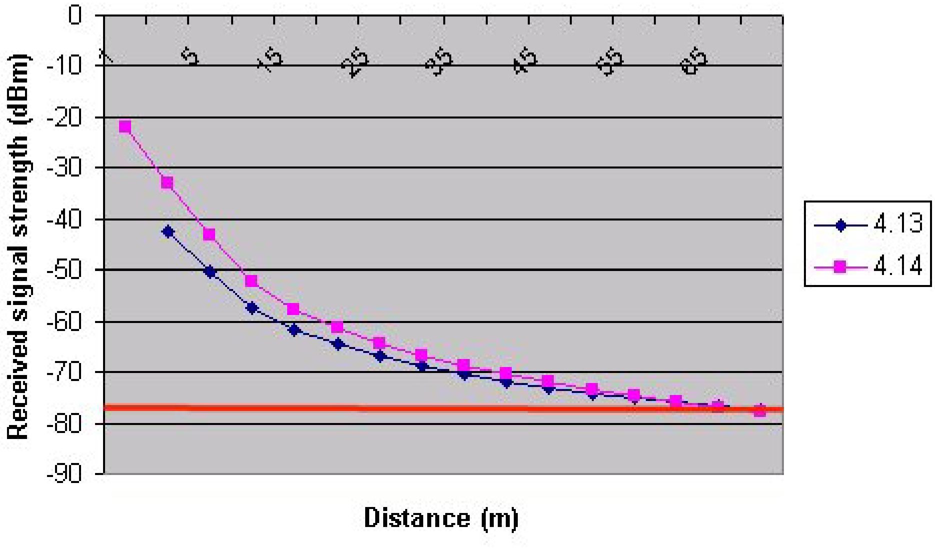


Figure 43 Calculated received signal strength for model 4.13 and 4.14

Making a model based on the specifications given from the supplier we can't know what kind of accuracy to expect. The range given by the supplier of our equipment was a static value. It seems like they have calculated it with the Log-distance path loss model (4.9) assuming the path loss exponent is 3. This was exactly the path loss exponent we found in our model (4.14) having a range at 60 meters. Also this was also the path loss exponent for the indoor office path loss model (4.2).

4.6.3 Selecting the path loss exponent for the model

With the model based on theory a path loss exponent has to be selected for your model. Table 4 can be used as a guide, but the values given are inaccurate. Thus we searched the literature for more precise values, unfortunately without result. The path loss exponent in free space has the value 2. We suggested a thought, that with free space path loss exponent as base, it’s possible to increase or decrease this value depending on factors. Then a table of different factors quantity of increase or decrease could be made. Hopefully this would result in a more accurate path loss exponent selection, but still keeping the model simple. To perform adjustments we suggest factors like:

- **Room dimensions (height, length, width of the room)**
  The path loss exponent generally increases with room dimensions (larger RMS delay spread). Hallways can give you wave guiding effects and result in very low path loss exponents.

- **Walls**
  Walls made of different materials like wood, concrete etc. have different absorbation/reflection characteristics.

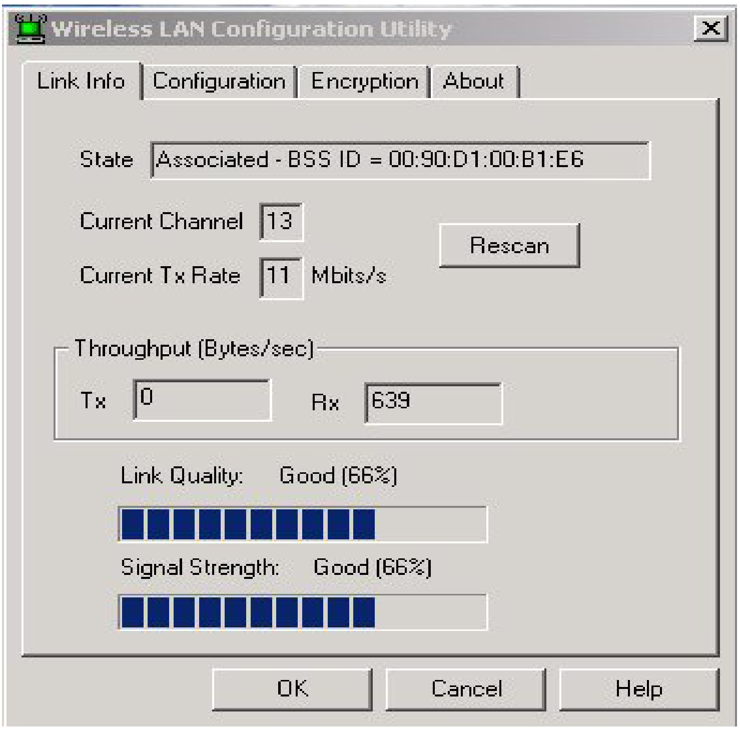
- **Objects**
  Objects in the line of sight path between transmitter receiver causing different phenomena’s; could be both loss and gain.

4.7 Model of coverage based on measurements

The discussed models above aren’t accurate adjusted to any specific environment. To make a more accurate model, adjustments based on measurements for each environment must be done.

4.7.1 Performing the measurements

To perform our measurements we had laptops with the application "Wireless LAN Configuration utility, PRISM 802.11 Wireless version 0.92” shown at figure 44.



State: Associated - BSS ID = 00:90:D1:00:B1:E6

Current Channel: 13

Current Tx Rate: 11 Mbits/s

Throughput (Bytes/sec)

Tx: 0

Rx: 639

Link Quality: Good (66%)

Signal Strength: Good (66%)

Figure 44 Wireless LAN configuration utility application

This application made measurement in percentage of “signal Strength” and “link quality”. The mathematical models that have been presented operate only with values in dBm. We had to figure out if it was possible to convert percentage measurements to dBm values.

We sent questions to Siemens who is selling the equipment, Intersil who is manufacturing the I-gate WLAN PC-cards and Neesus who are developing the application that is displaying the measurements, to see if they could help us:

From Neesus Datacom Inc we got this answer:

"The link quality and signal strength bars in the config utility are intended to provide not a quantitative measure but a qualitative measure. The values are derived from information reported by the MAC and are normalized to fit on the config bars."

Siemens gave us this answer:

"The % values are only indicated to roughly estimate the quality of the radio-link or to optimize the positioning of the stations.
The relation % vs dBm is not exactly defined because it depends on the Used PC Card, the PC driver version and the firmware version."

Although the received signal strength values couldn’t be seen directly as a dBm value, we performed some measurements in different environments. This was done to find out if there is a connection between our measurements and the models.

4.7.2 Measurements considerations

All of our measurements have been performed with the setup shown at figure 45 called setup1.

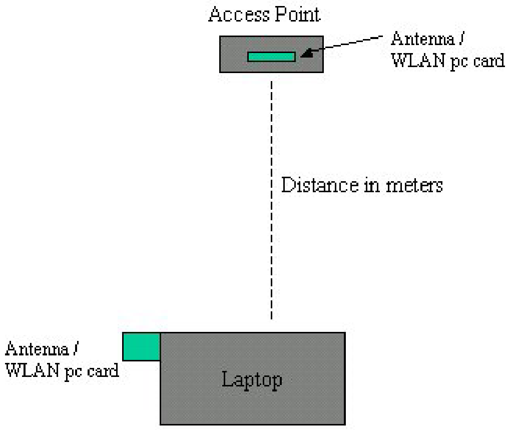


Figure 45 Setup 1 with 0° angle between AP and laptop (seen from above)

The AP was arranged at a height of 2 meters and the laptop at a desk at 0,72 meters height. We performed measurements in:

- Gymnasium
- Electro lab North-west
- Parking lot
- Master of Science lab

Measurements variations

Since the measurements varied greatly at the same point, we operated with mean values. Minimum measured signal strength was 26 % and no values where reported below this value without a failed connection. The lowest link quality measured was 6% (when signal strength was 26%). We also noticed that for higher values of the signal strength the link value in percentage is better than the signal strength in percentage. When the signal strength falls below 40-60 % then the link quality is lower.

4.7.3 Making a model

We observed that the curves of received signal strength seemed to be logarithmic like the other models we have described. The figure 46 below shows the measured signals contra a logarithmic curve.

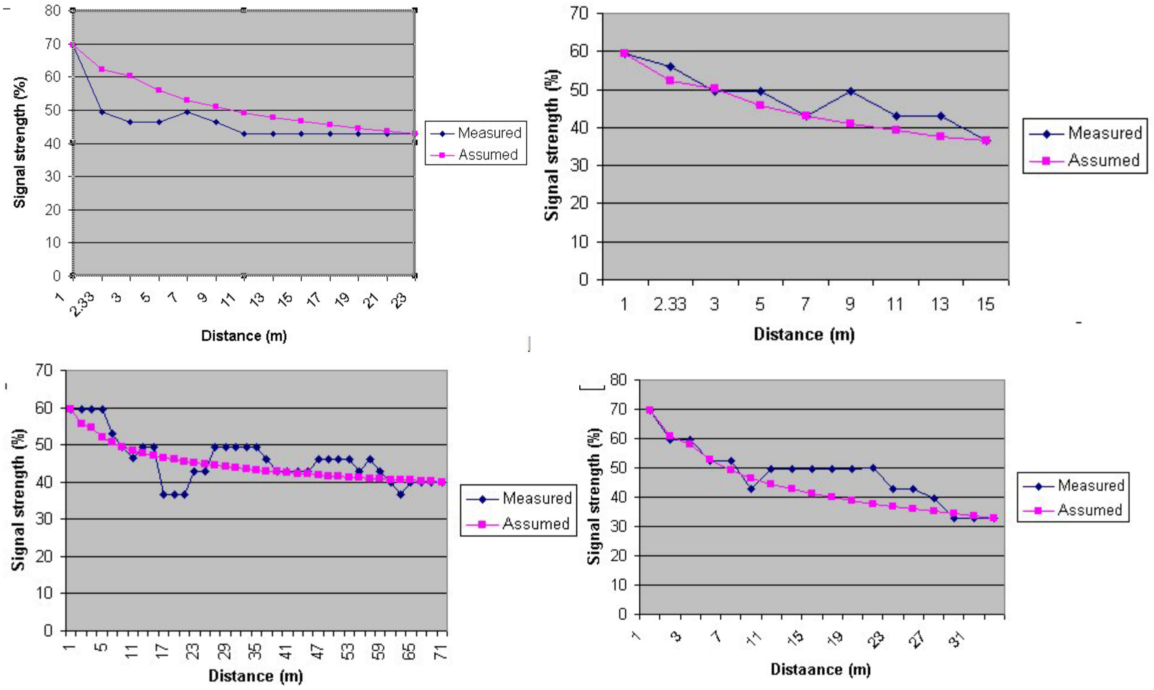


Figure 46 Measured signals versus logarithmic curve

In all of our environment measurements [appendix c] we ran out of space before connection failed. We don't know how the signal strength in % is scaled in the application. However one thing is for certain it isn't percentage of the original signal strength radiated from the transmitter. As a result we decided to use a logarithmic equation to assume when connection is lost (same as equation 4.10 only measuring in %), we refer to this as the percentage model:

$$P(R)= Pr(d_0) -10\ n\ (\log r/d_0)\ \% \qquad (4.15)$$

To find the path loss exponent for our new percentage model, we used the received signal strength at 1 meter as the reference point measurement *Pr(d_0)*. The outer point measurement (P(R)) as the signal strength received at a known distance (R). Having the path loss exponent we can find the range of our equipment in the environment we have measured (since we know connection is lost at signal strengths below 26 %).

Connecting percentage model to calculated model

To find approximately the received signal strength in dBm we had to try to connect the models. The only way we found to connect the percentage to Friis model to calculate dBm, was to observe when the connection failed. The connection failed in our percentage measurement when it fell below 26 %. We had –76 dBm at lowest acceptable value from 802.11b specification as the threshold value for received signal strength. We also had to take a measurement at the same height in the gymnasium at one-meter distance. This gave us a reference point connection.

1meter:	69,5 %	->	-22dBm
Connection lost at R distance:	26 %	->	-76dBm

Thus we can use the range and reference points calculated to convert the percentage model to the calculated model with its dBm values.

Converting percentage to dB
With these assumptions the models are connected in respect to dB verses percentage. When you have the received signal strength in percentage you can find the received signal strength in dBm. Since both scales logarithmic and have the same curve, a converting factor can be made.

Converting factor x = (76 dBm - 22 dBm)/ (69,5 % - 26 %) = 1,24

If measured 10 % signal strength loss between two points, the use of the converting factor will give us the amount of dBm loss:
1,24 dBm *10 = 12,4 dBm loss

On the background of the factor above we get the following table:

Table 5 Percent to dBm conversion table

%	dBm
100	15,8
90	3,4
80	-9
70	-21,4
69,5	-22,02
60	-33,8
50	-46,2
40	-58,6
30	-71
26	-75,96
20	-83,4
10	-95,8
0	-108,2

From this table we can create this graph (figure 47), which illustrates what approximately dB values to expect when measuring in percent:

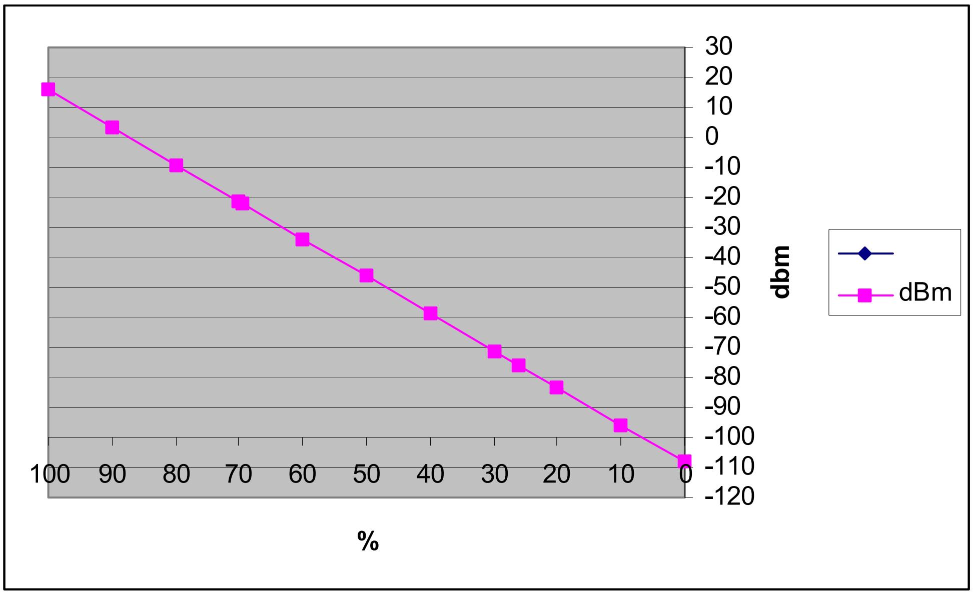


Figure 47 Graph showing percent to dBm conversion

Measurements distance

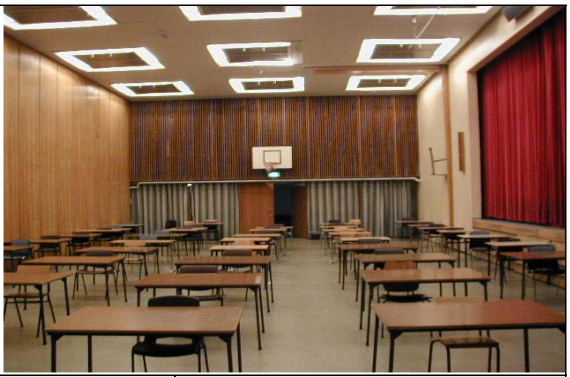
Since all our measurements were based on "ground distance" the real distance through air was larger especially in the start of our measurements, due to the height difference between AP and laptop at approximately 1,30 meters. Making the real distance x = $\sqrt{}(1,3^2+R^2)$. This must be taken into account at small distances. Though the difference will not be noticeable at larger distances (example only 8,4 cm difference at 10 meters).

4.7.4 Model of coverage in gymnasium

Table 6 Room descriptions gymnasium

<table>
<tr><td colspan="2"><b>Dimensions</b>
Length = 23
Height = 6
Width = 10

<b>Walls</b>
Walls of wood and concrete. A few windows.

<b>Objects</b>
Desks (Not obstructing the line of sight)</td><td></td></tr>
<tr><th>Reference point P(d₀), d₀=1</th><th>Distance to outer point</th><th>Outer point</th></tr>
<tr><td><i>P(1) = 69,5 %</i></td><td>R = 23 meters</td><td>P(23) = 43 %</td></tr>
</table>

Calculating the path loss exponent for the percentage model (4.15):

$P(R)= Pr(d_0) – 10\ n\ (\log r/d_0) \text{ -> } 43 = 69,5 – n \log (23/1) \quad \text{->} \qquad n=1,946$

Calculating the range:

$69,5 - 19,46\ \log (R) = 26\ \%$ -> $R=10^{2,21}=171,93\ meter$

Inserting path loss exponent in our percentage model:

$$P(R)= 69,5 - 19,46 \log (R)\ \% \tag{4.16}$$

Having the calculated range we can find the path loss exponent for the calculated model (4.14):

$P(171,93)= -22 - 10n \log (171,93) = -76\ dBm$ -> $n=2,42$

Inserting the path loss exponent for Friis model:

$$P(R)= -22 + 24,2 \log (R))\ dBm \tag{4.17}$$

4.7.5 Model of coverage in Electro lab north-west

Table 7 Room descriptions Electro lab north-west

<table>
<tr><td colspan="2"><b>Dimensions</b>
Length = 33 meter
Høyde = 2,5 – 3,0 meter
Bredde = 5 meter

<b>Walls</b>
Heavy walls and windows.

<b>Objects</b>
Desks, computers and pillars,…</td><td> </td></tr>
<tr><td><b>Reference point P(d₀), d₀=1</b></td><td><b>Distance to outer point</b></td><td><b>Outer point</b></td></tr>
<tr><td><i>P(1) = 69,5 %</i></td><td>R = 33 meters</td><td>P(33) = 33 %</td></tr>
</table>

Calculating the path loss exponent for the percentage model (4.15):

$P(R)= Pr(d_0) - 10\ n\ (\log r/d_0)$ -> $43 = 33= 69,5 - n \log (33/1)$ -> $n=2,404$

Calculating the range:

$69,5 - 24,04 \log (R) = 26\ \%$ -> $R=10^{1,81}=64,48\ meter$

Inserting path loss exponent in our percentage model:

$$P(R)= 69,5 - 24,04 \log(R)\ \% \tag{4.18}$$

Having the calculated range we can find the path loss exponent for the calculated model (4.14):

$P(64,48)= -22 - 10n \log (64,48) = -76\ dBm$ -> $n=2,98$

Inserting the path loss exponent for Calculated model:

$$P(R)= -22 - 29,8 \log (R))\ dBm \qquad (4.19)$$

4.7.6 Model of coverage at parking lot

Table 8 Environment description parking lot

<table>
<tr><td colspan="2">Dimensions
Length = 71 meter

<b>Walls</b>
None

<b>Objects</b>
None</td><td> </td></tr>
<tr><th>Reference point P(d₀), d₀=1</th><th>Distance to outer point</th><th>Outer point</th></tr>
<tr><td><i>P(1) = 69,5 %</i></td><td>R = 71 meters</td><td>P(71) = 40 %</td></tr>
</table>

Calculating the path loss exponent for the percentage model (4.15):

$P(R)= Pr(d_0) – 10\ n\ (\log r/d_0) -> 40 = 69,5 – 10\ n \log (71/1)$ -> $n=1,738$

Calculating the range:

$69,5 – 17,38 \log (R) = 26\ \%$ -> $R=10^{2,50}=318\ meter$

Inserting path loss exponent in our percentage model:

$$P(R)= 69,5 – 17,38 \log(R)\ \% \qquad (4.20)$$

Having the calculated range we can find the path loss exponent for the calculated model (4.14):

$P(318)= -22 - 10n \log (318) = -76\ dBm$ -> $n=2,15$

Inserting the path loss exponent for calculated model:

$$P(R)= -22 - 21{,}5 \log (R)) \text{ dBm} \qquad (4.21)$$

4.7.7 Model of coverage in Master of Science lab with LOS

Table 9 Room descriptions Master of Science lab

<table>
<tr><td colspan="2"><b>Dimensions</b>
Length = 15 meter
Width = 8 meter
Height = 3 meter

<b>Walls</b>
Heavy wall, Light wall, windows

<b>Objects</b>
Desks, moveable closets, small light walls.</td><td> </td></tr>
<tr><td><b>Reference point P(d₀), d₀=1</b></td><td><b>Distance to outer point</b></td><td><b>Outer point</b></td></tr>
<tr><td><i>P(1) = 69,5 %</i></td><td>R = 15 meters</td><td>P(15) = 53 %</td></tr>
</table>

Calculating the path loss exponent for the percentage model (4.15):

$P(R)= Pr(d_0) – 10\, n\, (\log r/d_0)$ -> $53 = 69{,}5 – 10\, n \log (15/1)$ -> $n=11{,}76$

Calculating the range:

$69{,}5 – 11{,}76\ \log (R) = 26\ \%$ -> $R=10^{3,70} =5000$ *meter*

Inserting path loss exponent in our percentage model:

$$P(R)= 69{,}5 – 11{,}76 \log(R)\ \% \qquad (4.22)$$

Having the calculated range we can find the path loss exponent for the calculated model (4.14):

$P(5000)= -22 - 10n \log (5000) = -76$ *dBm* -> $n=1{,}46$

Inserting the path loss exponent for calculated model:

$$P(R)= -22 - 14{,}6 \log (R)) \text{ dBm} \qquad (4.23)$$

4.7.8 Model of coverage in Master of Science lab with NLOS

In this measurement we placed the laptop at a realistic place in the lab. These placements there were varying line of sight to the AP, mostly no line of sight.

Calculating the path loss exponent for the percentage model (4.15):

$P(R)= Pr(d_0) – 10\ n\ (\log r/d_0)$ -> $36,5 = 69,5 – 10\ n \log (15/1)$ -> $n=2,81$

Calculating the range:

$69,5 – 28,1 \log (R) = 26\ \%$ -> $R=10^{1,55}=35,32$ *meter*

Inserting path loss exponent in our percentage model:

$$P(R)= 69,5 – 28,1 \log(R)\ \% \qquad (4.24)$$

Having the calculated range we can find the path loss exponent for the calculated model (4.14):

$P(35,32)= -22 - 10n \log (35,32) = -76$ *dBm* -> $n=3,49$

Inserting the path loss exponent for calculated model:

$$P(R)= -22 – 34,9 \log (R))\ dBm \qquad (4.25)$$

4.7.9 Comparing environments

The calculated model for each environment is displayed at figure 48. From this figure you can approximately find the received signal strength in percentage for the different environments at a given distance between AP and the laptop. The red line at 26 percentages illustrates when connection is assumed to be lost.

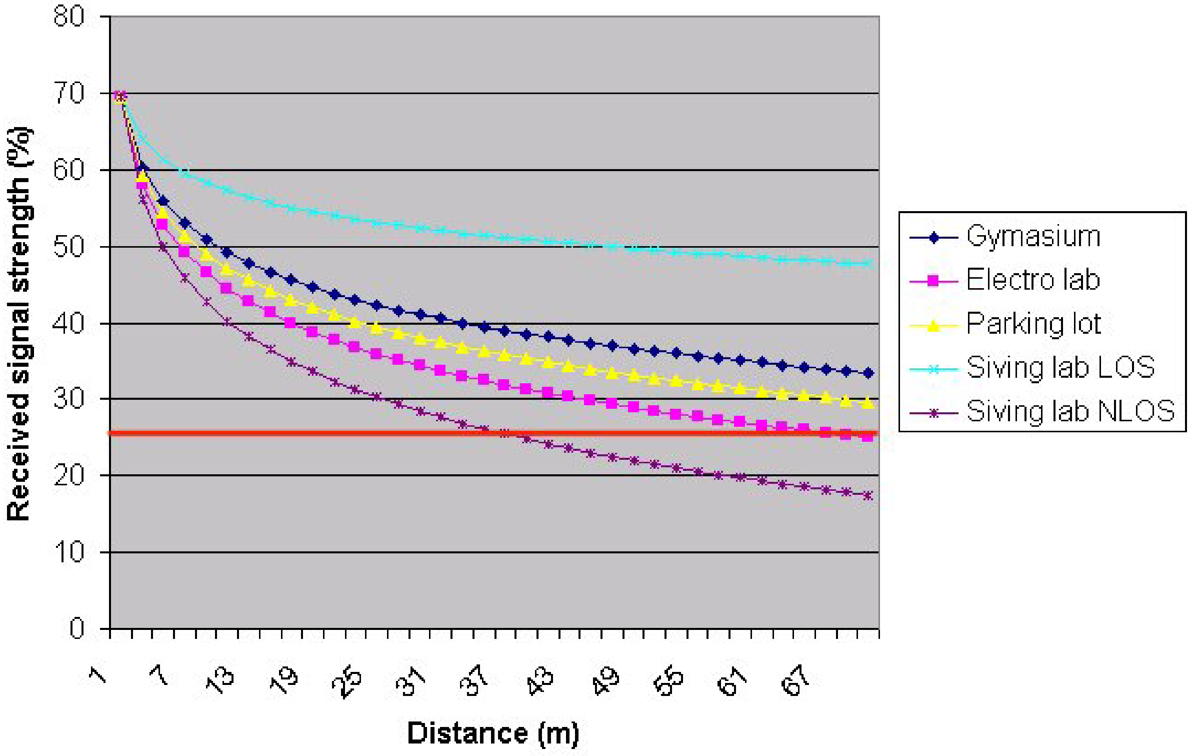


Figure 48 Comparing environments with the percentage model

The calculated model for each environment is displayed at figure 49. From this figure you can approximately find the received signal strength in dBm for the different environments at a given distance between AP and the laptop. The red line at –76 dBm illustrates when connection is assumed to be lost.

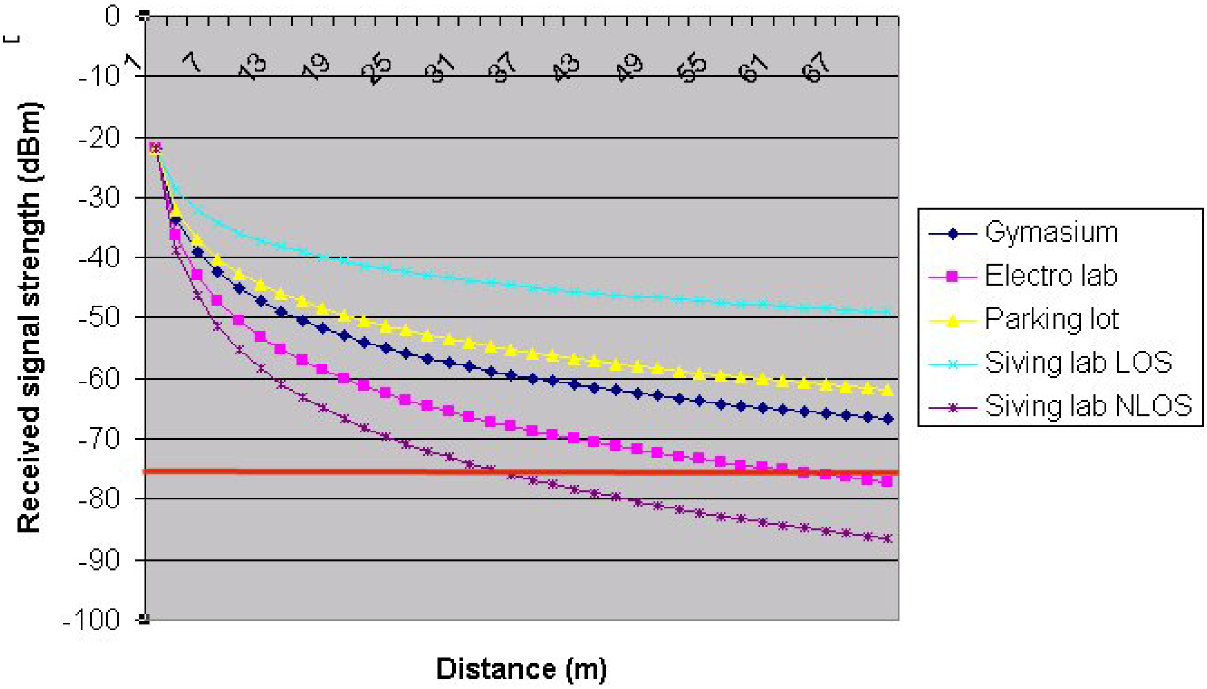


Figure 49 Comparing different environments with the calculated model

Figure 50 shows the example in section 4.5.1, where we are selecting the path loss exponent from table 4.2. We observe that our calculated model, which is adjusted due to our measurements, is in the middle of the pessimistic choice of NLOS path loss exponent and the average. The path loss exponent we selected for LOS is little too high according to our calculated model.

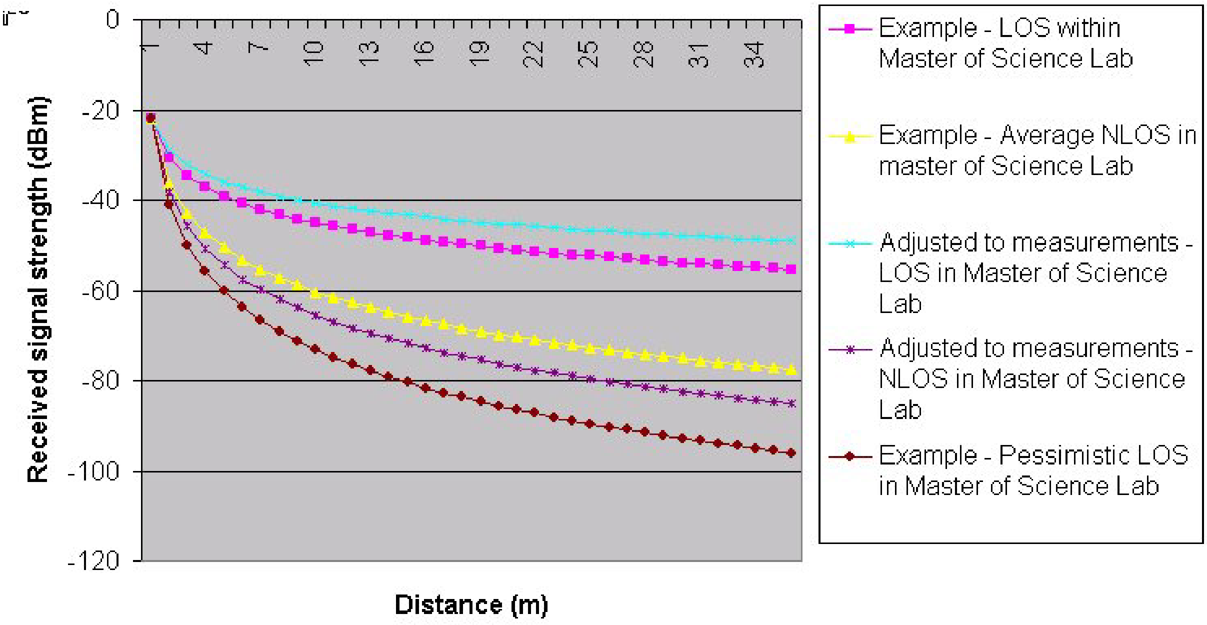


Figure 50 Comparing example to our adjusted calculated model

4.7.10 Other measurements of interest

In addition we could derive some indications from our measurements

- Effect of varying angle between AP and laptop.
- How big is the signal strength variation at a point with the respect to distance between receiver and transmitter or different environments.

Varying angle

We decided to take some measurements with different types of setup for our tests in order to varying angles between transmitter and receiver antennas. When varying the angles we get an idea of how the radiation pattern (figure 42) from the antennas affect the signal strength measured at the receiver. According to the radiation diagrams of the AP, the AP is sending out little power to the sides. In their measurements it's only –75,3 dBm when there is a 90° angle between the AP and the receiver at a distance of 2,33 meters versus –42,4 dBm when it's 0° angle between the transmitter and receiver. –75,3 dBm is a low value and approximately the threshold for minimum received signal. Figure 51 displays setup 2 with 90° angle between AP and laptop.

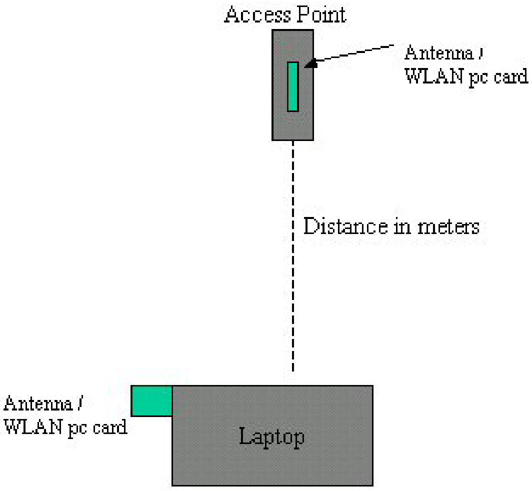


Figure 51 Setup 2 with 90° angle between AP and laptop (seen from above)

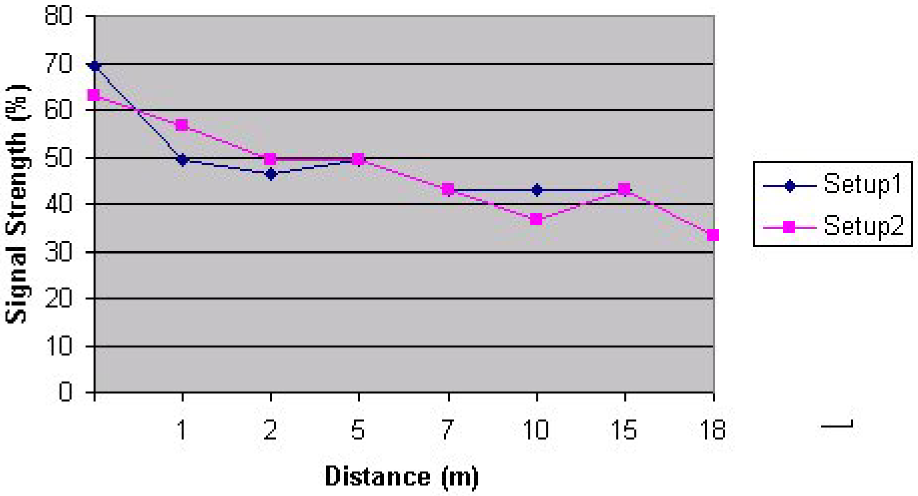


Figure 52 Difference between 90° angle and 0° in gymnasium

Setup 1 - 0° angle between AP and laptop
Setup 2 - 90° angle between AP and laptop

From measurements in gymnasium shown at figure 52, the average signal strength is approximate the same for setup 1 and setup 2. According to the signal radiation pattern the received signal strength from AP at an angle of 90° should have been considerably smaller than we have measured. The only explanation for this must be reflections from walls, ceiling, floor and the objects in the room.

To get something near free space measurements we took some measurements at the parking lot at HiA when there were no cars present. The only reflection would be ground reflection from the asphalt.

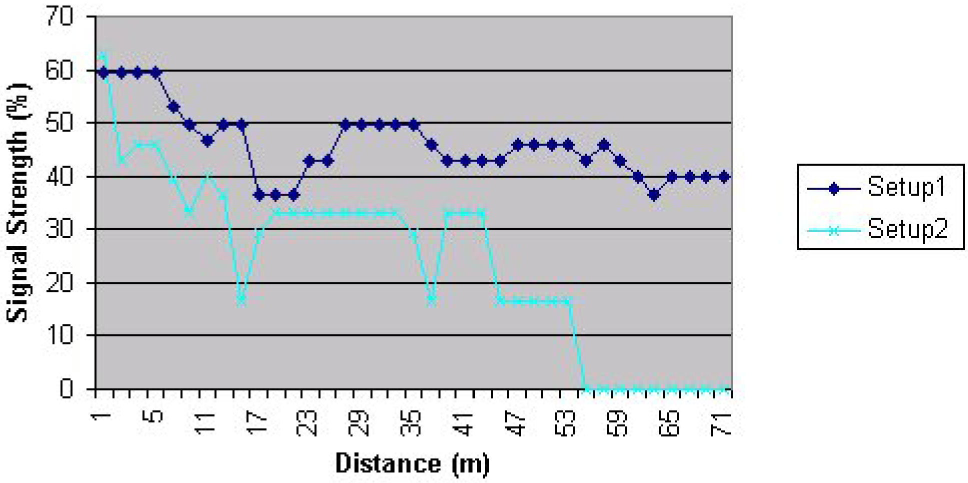


Figure 53 Difference between 90° angle and 0° at the parking lot

Setup 1 - 0° angle between AP and laptop

Setup 2 - 90˚ angle between AP and laptop

With this measurement the received signal strength, having a 90˚ angle between the AP and the receiver, received signal is much smaller. Exactly what we had expected for this measurement, since there is no walls the signal can be reflected from.

Variation in signal strength

The received signal strength at a point always fluctuates with time. This has to be taken into account when making a model. Like in model 4.9 there has to be assumed a standard deviation. The signal strength is varying approximately plus or minus 7 percentage at 30 meters distance at this measurement. This deviation has to be taken into account in your model. For the model in the Electro lab north-west we assume a standard deviation on 7 percentage or approximately 9 dB. See figure 54.

P(R)= 69,5 – 24,04log(R) % , plus or minus 7 %

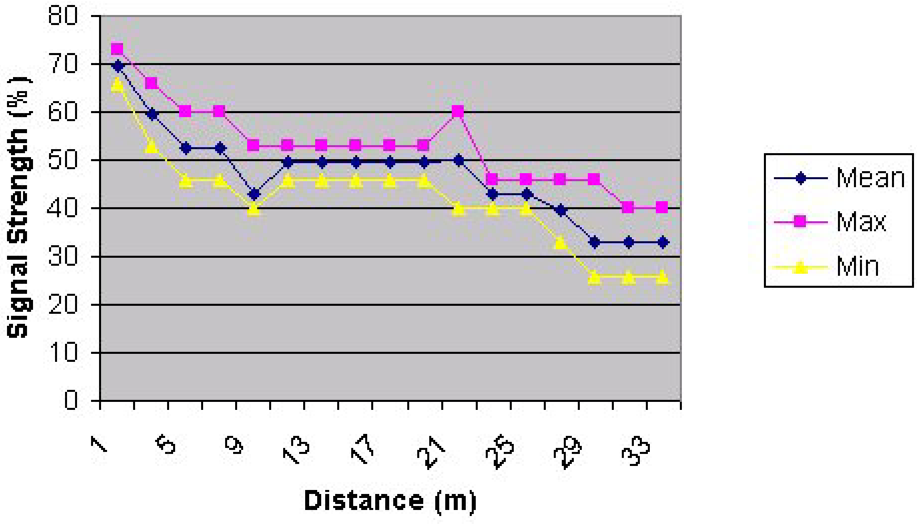


Figure 54 Measurements of variation from Electro lab North-west

4.8 Theoretical models

There are many different theoretical models where Ray-tracing and Finite-Difference Time-Domain models are most popular. These are described briefly below:

4.8.1 Ray-Tracing Models

The ray-tracing model calculates all possible signal paths from the transmitter to the receiver. In basic ray-tracing models, the prediction is based on the calculations of free-space transmissions and reflections from the walls. More complex ray-tracing algorithms include the mechanism of diffraction, diffuse wall scattering and transmission through various materials. In the end, the signal level at any specific location is obtained as a sum of the components of all paths between the transmitter and the receiver. The implementation of these models requires extensive computational resources. Computational time depends exponentially on the details included in the layout of the area. Therefore, the computational time of a small area with plenty of details can be greater than that of a big area that is relatively poor in details.

4.8.2 Finite-Difference Time-Domain (FDTD) Models

Radio propagation characteristics can be derived solving directly Maxwell's equations of electromagnetic wave propagation. The FDTD method is probably the most popular method for a numerical solution of Maxwell's equations. In this method, Maxwell's equations are approximated by a set of finite-difference equations. Similarly to the ray-tracing model, the FDTD models are very computationally demanding. The computational time depends proportionally on the size of the area to be analysed, but not significantly on the details involved. However, the number of nodes of the grid is exponentially related to the size of the area and the frequency of operation. The accuracy of the FDTD model is comparable to that of the ray-tracing models. The prediction is as accurate as the area layout database.

4.8.3 ETF-Artificial Neural Network (ANN) Model

The main problem presented by empirical models is their unsatisfactory accuracy. On the other hand, the theoretical models lack computational efficiency. A compromise can be made by the artificial neural network model. This model is based on multilayer perceptron feedforward neural networks. The implementation of an ANN model requires a database of the floor plan in which all particular locations are classified into several environmental categories, for example, wall, corridor, classroom, window, etc.

4.8.4 Channel model for indoor wireless communication

This is an example of a theoretical ray-tracing model. There are many channels models available for indoor environments. Most indoor environments have movements and objects that are added, removed or moved to other places. So it is almost impossible to know of all the reflectors, their position and absorption effect all the time. Thus indoor channel models are emulating the average behaviour of an environment. The average will naturally be very different for different types of indoor environments, like an indoor office with many small reflectors contra a hall with few reflectors.

There exist a lot of channel models in the literature, but the channel model with multipath fading that is recommended in the 802.11 WLAN standard is an exponential channel model. It is a bit pessimistic, but a reasonable representation of many real world indoor environments.

Some definitions:

The path delay profile for the model has the form:
$P[\tau] = (1/\tau_d) \exp(-\tau/\tau d)$

Where the τd parameter completely characterizes the path delay profile.
$\tau d = \tau\mu = \tau\sigma$

$\tau\mu$ Mean excess delay, the average delay of all the paths

$\tau\sigma$ RMS (root mean square) delay spread, is a measure of how spread the delays are about mean.

τm Maximum excess delay, is the last path delay with “any” noticeable amplitude (typically 20 dB below the peak amplitude).

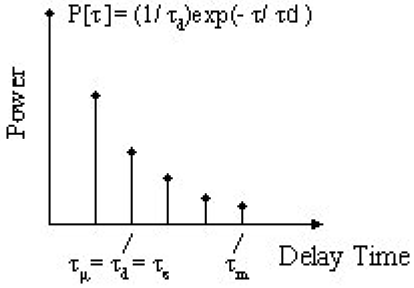
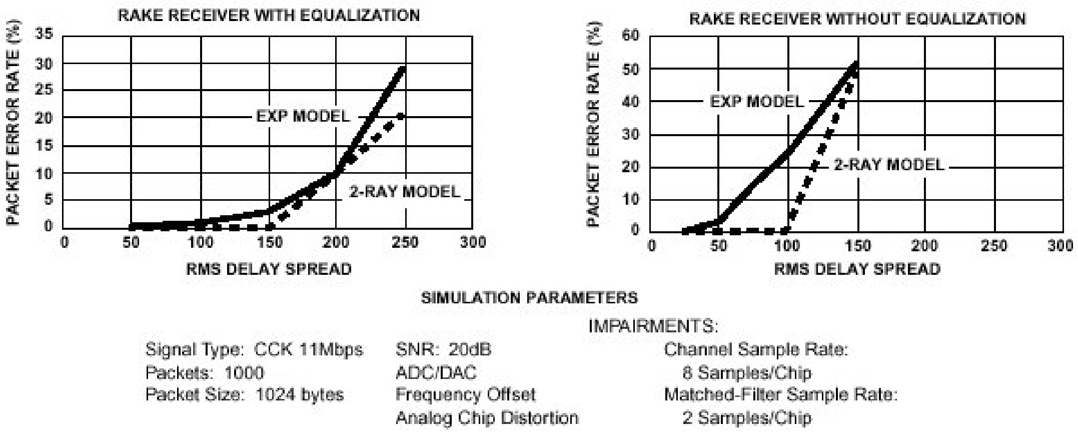


Figure 55 Path delay profile for an exponential channel model

$\tau m = (A * \tau d) / (10 * \log_{10}(e)$

A is the smallest “noticeable” amplitude relative to the line of sight signals amplitude (typical 20 dB).

Another way to find the coverage of a WLAN is to see how the range is limited by the FER. FER is mostly depended of the delay spread due to reflections (multipath fading). The FER threshold that can be accepted in 802.11b is $8*10^{-2}$, i.e. a higher error rate causes the connection to be lost. Figure 56 below is taken from “Multipath Measurements in Wireless LANs” by Intersil [4] and displays a simulation of the packet error rate PER as a function of RMS delay spread when using the exponential model. The left plot shows the performance with a RAKE receiver with equalization and the right plot shows the performance with RAKE receiver only. The intact line is showing the exponential model while the stippled line is for another model (a 2-ray model that are more inaccurate).



SIMULATION PARAMETERS

IMPAIRMENTS:

Signal Type: CCK 11Mbps	SNR: 20dB	Channel Sample Rate: 8 Samples/Chip
Packets: 1000	ADC/DAC	
Packet Size: 1024 bytes	Frequency Offset	Matched-Filter Sample Rate: 2 Samples/Chip
	Analog Chip Distortion	

Figure 56 PER as a function of RMS delay spread

5 Site survey for HiA's 3rd floor, old building in Grimstad

Inside a building there are several things to keep in mind when it comes to designing a wireless network. There are big variations in signal strength, concerning signal strength between floors, walls and there are random signal variations when people are moving around. Since the wireless link has a limited capacity (only 11 Mbps), it would be useful if the cells were as small as possible. This is because you may want to have as few people on each wireless link as possible to obtain a better bandwidth for each user. There should also be a possibility to use load balancing, so bandwidth given by two or three AP's that is covering the same area can be efficiently shared.

Site selection for Access points
When positioning Access Points, take into account the following:

Height – The AP should be put at least 1,5 meters above the floor, the AP should be put on a place clear of any high office partitions or tall pieces of furniture in the coverage area.

Central Location – The AP should be located in the intended coverage area. Good positions are:

- In the centre of a room
- In the centre of a corridor
- At the intersection of two corridors

Minimal Path Loss
Path loss is determined mainly by several factors:
- Distance between sites. Path loss is lower and system performance better when distances are short.
- Clearance. Path loss is minimized when there exits a clear line of sight.

Roaming
When any area in the building is within reception range of more than one Access Point, the cells coverage is overlapping. Each wireless station automatically establishes the best possible connection with one of the Access Points. Overlapping coverage areas are an important attribute of the wireless LAN setup, because this enables seamless roaming between overlapping cells. Roaming allows mobile users with portable stations to move freely between overlapping cells, constantly maintaining their network connection.

Load Balancing (Load sharing)
Congested areas with many users and heavy traffic load per unit may require a multi cell structure. In a multicell structure, several co-located APs "illuminate" the same area creating a common coverage area, which increases aggregate throughput. Stations inside the common coverage area automatically associate with the AP that is less loaded and provides the best signal quality. The stations are equally divided between the APs in order to equally share the load between all APs. This is an option on a few WLAN products; among them is Ericsson with their BreezeNET PRO.11 series.

5.1 Channel use

In the WLAN DSSS system there is only space for 3 AP's to cover the same area, as explained in chapter 2.6.2 under Direct-sequence spread spectrum. Placing more than one AP in the same building, you have to consider where you can place the others AP's in the same building. This is because you don't interfere with other AP's. If you are planning to have more than 3 AP's, you have to consider channel reuse and distance between AP's to avoid interference. The placement of the AP's that is shown in figure 57 is not wise if the wall doesn't absorb or reflect all the radiation from the devices. The result would be that they interfere with each other if they were set on the same channel. So keep in mind that walls absorbs/reflects only a limited (dependent on the type of wall) amount of the radiation from an AP.

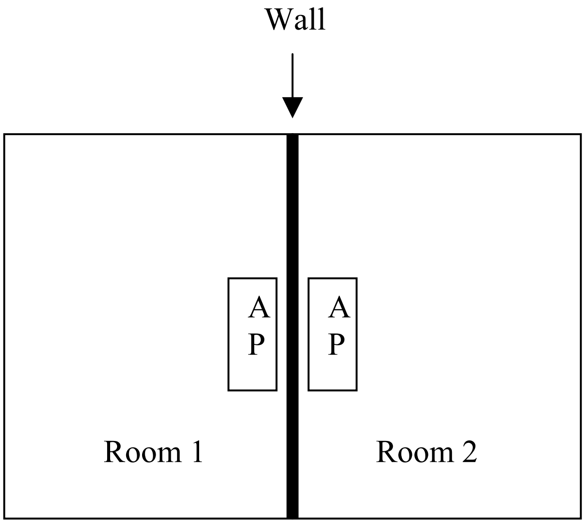


Figure 57 Interference from two AP's trough a wall

5.2 Coverage

We considered the placements of AP's in the northwest wing and Master of Science lab of HiA 3rd floor old building in Grimstad. We have found that the placement shown figure 58, gives the best coverage and throughput. The placements of the 3 AP's in the lab northwest must all use different channels. Then we must reuse one channel to cover the Master of Science lab.

We chose to reuse the channel used on AP 4 on AP 1, because they have a sufficient distance between them. To reuse a channel from AP 2 or 3 on AP 1 will result in interference, because the radiation will still be strong enough to interfere. The reuse of the AP's channels like as shown with AP 1 and AP4, will not interfere with each other, as long as AP 1 and AP 4 has a sufficient distance between them. There are also walls the signal must pass trough making the signal strength sufficiently weak and the interference will be negligible.

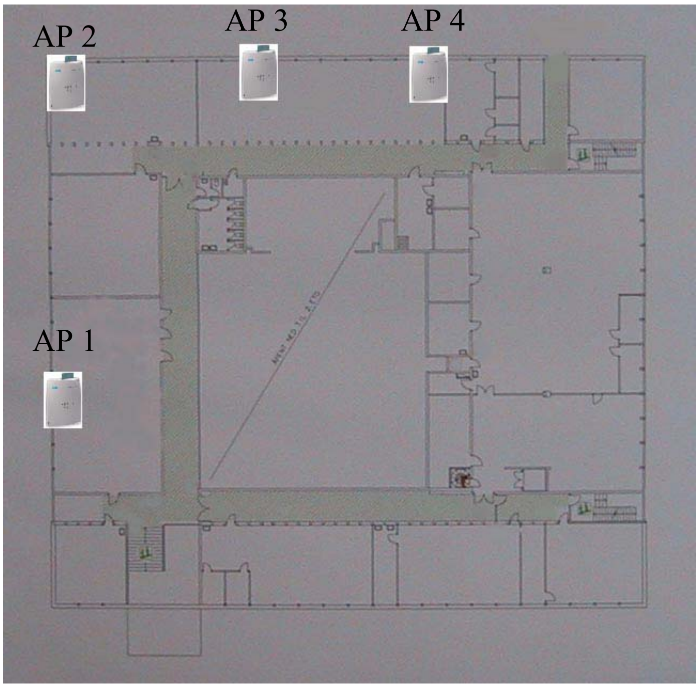


Figure 58 Showing the AP's placements in HiA 3rd floor old building in Grimstad

We could now show a practical use of our base model (4.10), which we had chosen for predicting the WLAN coverage.

$$PL\ (dB) = PL\ (d_0) + 10n\ \log(d/d_0)$$

Table 10 shows us the path loss we found in chapter four in our model, which was adjusted to the different environments. Since there are three different rooms/environments between the AP's you have to use an own model for each room. You can't just add the models we have found for each room with the distance that is passed the distance parameter. You have to calculate in the first room until you hit the first wall. Then you have to use this as the reference point for the next environment and its model. This gives you a higher reference point value, and you now have to divide the total distance to next target with the reference point distance. Hopefully this example will explain this further; from chapter four we have:

Table 10 Path loss exponents for HiA

Environment	Path loss exponent, n
Gymnasium	2,42
Electro lab north-west	2,98
Parking lot	2,15
Master of science lab with LOS	3,49
Master of science lab with NLOS	1,46

The distance between AP 1 and 4 is approx 35 meters and the signal propagates through three rooms:

1. Electro lab north-west n = 2,98, Distance = 5 meter
2. The hallway/top of the gymnasium - we had to select a, value n = 2, Distance = 15 meter.
3. Siving lab with LOS n = 1,46, Distance = 15 meter

Received signal at the end of first environment electro lab north-west:

1. P(5) = -22 – 29,8 log(5) = -42,8 dBm.

Received signal at the end of second environment hallway/top of the gymnasium:

2. P(20) = - 42,8 – 20 log(20/5) = -54,8 dBm

Received signal at the end of third environment Siving lab with LOS:

3. P(35) = -54,8 –14,8 log (35/20) = -58,4 dBm

In addition there are 3 concrete walls to pass, so we will add another factor taken from table 2 in chapter 2.4.2 penetration. From this table we get these values; Heavy Wall (solid core 6”): 15-20 dB attenuation. With 3 walls like this we are looking at a reduction of the radiation power with at least 35 dB.

P(35) = -54,8 –35 = -89,8 dBm

This shows us that the received radiation from AP 4 to AP 1 is sufficient low. If there were a free path between these two AP’s the received radiated power would be –58,4 dBm at best. But since its not a free path between AP 1 and 4 so we can safely assume that they will not interfere with each other because of the attenuation of the walls between them.

If we use the model between AP 1 and AP 3. We can check if it would be possible to reuse channels between these two. Between these two AP’s there is approximately 20 meters. The signal propagates through two rooms:

1. Electro lab north-west – n = 2,98 , Distance = 5 meter
2. Siving lab with LOS n = 1,46, Distance = 15 meter

Received signal at the end of first environment electro lab north-west:

1. P(5) = -22 – 29,8log(5) = -42,8 dBm.

Received signal at the end of second environment Siving lab with LOS:

2. P(20) = -42,8 –14,8 log (20/5) = -51,70 dBm

It is one light wall to pass and a heavy wall. These to walls will give approximately 5 + 15 dB attenuation.

P(35) = -51,7 –5-15 = -71,7dBm

This shows us that the received radiation from AP 3 to AP 1 probably isn't low enough, and they will interfere with each a since it is over the threshold for received signal strength at –76 dBm. To be on the safe side we have chosen to reuse the channels only on AP 4 on AP 1.

We have not performed any measurements of two AP's interfere with each other, using the same channel at different distances, in order o see when they start to decrease their ability to handle traffic.

5.3 Throughput

The four AP's that we have suggested the placements of is based on the use of Siemens I-Gate 11M I/LAN equipment. They don't support load sharing or variable radiated power adjustment. The total amount of wireless bandwidth available will be 44 Mbps. This might be enough for say 50 people, if users are spread evenly on all available AP's. The total amount of bandwidth to each user will be acceptable. If it should be additional AP's in this area there must be possible to adjust the power output on the AP's. This will make it possible to make even smaller cells, and the AP's will be able to stand closer to each other without interfering, and it would also be able to keep AP's radiation to only inside a room. It is also important to be able to adjust the power on the PC card as well, so they as well don't interfere with other units. Load sharing is also a possible way to increase bandwidth to users, because all users probably wont use full bandwidth all the time. Heavy working AP's could redirect users to other available AP's within the coverage area with lower traffic load. If there is plans to implement Bluetooth equipment, it will probably interfere with the WLAN environment and bandwidth will probably decrease. The extent of interference will be dependent of the distance to the WLAN and Bluetooth equipment.

6 Discussion

6.1 The model and the affecting factors

When taking this assignment we thought that it would be relatively easy to prove/find a model that could predict coverage for WLAN within a room. We had been given the "Propagation Model from ETSI TR-101-112 appendix B.1.8 "(see chapter 3.5.2), to base our model on and equipment to make measurements to see the validity of the model. We experienced relatively quickly that the modelling of coverage indoor was exceptionally complex and not at all an easy task. There exist a muddle of mathematical equations and models in order to describe different phenomena's affecting the electromagnetic waves propagation. In addition you must know all about the surrounding environment and the antennas that are used if you want to make a perfect model, which is obviously almost impossible. Predicting coverage in WLAN is complex, since it is affected by numerous of factors. The more you know about the path and its obstructions, the receiver and the transmitter antenna, the more accurate and complex you can make the model.

All the measurements we have taken, shows graphs that has a rapid fall in the beginning and a less fall at the end. Because of this we assume that we were dealing with logarithmic measurements. With this we could make assumptions to convert our percentage model to the log-distance path loss model

6.1.1 The path loss exponent

The models we have used, which could be adjusted to the different environments, are not at all complex. They're only varying the path loss exponent. The path loss exponent can be seen upon as a sum of all the different phenomena's affecting the propagating signal in an indoor environment. Instead of making the model more complex, we made proposal for a table of factors affecting the path loss exponent and their quantity of decrease or increase to the free space path loss exponent.

6.1.2 General about accuracy in mathematical models of coverage

All the mathematical calculations are in dB values. This is a logarithmic scale due to the significant span of received signal strength. If an AP sends out 63 mW the laptop can accept values below $1*10^{-7}$ mW and still have a connection. This illustrates the significant span of signal strength values that is to be measured and what grade of accuracy that is possible to achieve.

Factors that could affect the accuracy of our measurements

- Angle between transmitter and receiver wasn't exactly the same for each measurement.
- Desks we placed our laptops and AP on, had iron support/legs beneath.
- We were two students performing the measurements and probably making some interference.
- The distance between AP and receiver were approximately measured (give or take a few centimetres).

In addition we didn't know the gain from the receiver and transmitter antennas for our equipment, which add some dB uncertainty.

6.1.3 Lack of specification from supplier

The supplier who is providing the WLAN has a responsibility to the buyer, giving correct and sufficient specification of their equipment. What information that is sufficient is another question. The private user who is happy for an AP covering one or two rooms at home, will probably not need much more specification than output power and approximately range. However there are advanced users who demand several AP's, for better bandwidth and there is a great need for network planning.

6.2 The site survey

6.2.1 Coverage

We used our base model (4.10) to predict the coverage at HiA. Different placements had to be considered. The models we had made for each environment was only useable within the same room.

Since there was many different environments between the AP's you had to use an independent model for each environment, but you can't just add the models we have found for each room with the distance that is passed as the distance parameter. You have to calculate in the first room until you hit the first wall. Then you have to use this as the reference point for the next environment and its model. This gives you a higher reference point value, and you now have to divide the total distance to next target with the reference point distance.

The connection between the percentage models and the calculated models is based on many assumptions. This adds a lot of uncertainty to our calculated models measuring dBm, and the path loss exponent we found for environments. The connection had to be done to be able to create a model that calculates values in dB.

6.3 Future improvements

Measurement equipment
A proper analyzer that could measure signals at 2,4 GHz frequency could measure the received signal strength directly in dBm. With such equipment we could have made our measurements and models more accurate. A proper analyzer could also be used to find the signal impulse response. This could be used to predict the FER.

Finding the path loss exponent for the model
Making a table like we suggested for the path loss exponent would require a lot of measurements to be performed with required accurate equipment.

Finding attenuation through walls

Table 2 in this report regards attenuation through different types of walls. We don't know the correctness since we don't know how the company Ericsson measured it. If Ericsson has measured with the FHSS system or generally modulated radio waves. It would be more correct to make these measurements with a DSSS system and measure on HiA's building walls. Then the assumptions regarding coverage at HiA would be more correct. We would have measured this by ourselves but our AP had a breakdown.

AP-to-AP interference

Interference with AP's on the same channel should be investigated. Because that is a factor on range between to AP's on the same channel. It is important to know how close the AP's can be without any degradation of performance

7 Conclusion

7.1 The model and the affecting factors

The model we have found appropriate, and gives a good prediction in accordance to measurements we have taken, is the log-distance path loss model. We can't guarantee the correctness in our models since its based on assumptions.

The model is simple and gives approximate values. If you have selected the right path loss exponent, it in most cases would be sufficient accurate to plan a WLAN. Different path loss exponents have to be chosen for each environment. In all the tables we have found of path loss exponents there exists none exact values.

7.1.1 Selecting the path loss exponent

The idea of making a table of factors to increase the accuracy of the selected path loss exponent we think could help many to more precisely planning their WLAN. This still keeps the model simple but at the same time more precise.

7.1.2 Lack of specification from supplier

Predicting the coverage for a WLAN without having the sufficient specifications forces the prediction to be based on assumptions, like in our case. We didn't get any specifications about the antenna, except the two pages specification [appendix A] mentioning only a range (that's static) and transmitted output power from the AP.

7.2 The site survey

7.2.1 Coverage

We planned the WLAN layout at HiA and demonstrated the use of our model. With this model we could predict the received signal strength at a given point and which AP's that could interfere with each other. This was an easy way to predict the coverage at all given places in these environments. We can't guarantee the correctness of layout due to all the assumptions we had to make.

8 References

[1] Theodore S. Rappaport
Wireless Communications Principles & Practice, ISBN 0-13-375536-3, 1996

[2] Karen Halford, Steve Halford, Mark Webster and Carl Andren
Complementary code keying for RAKE-based indoor wireless communication, IEEE 1999

[3] Ericsson Radio Systems AB,
Wireless LAN User's Guide version 4.2, 1999

[4] Karen Halford and Mark Webster
Multipath Measurements in Wireless LANs, Intersil
http://www.intersil.com/data/AN/AN9/AN9895/AN9895.pdf

[5] Commission of the European Communities
COST 231 Final report, Digital mobile radio towards future generations systems

[6] Anand R. Prasad, Neeli R. Prasad, Ad Kamerman, Henri Moelard and Albert Eikelenboom
Indoor Wireless LAN's Deployment, Lucent Technologies, The Netherlands, 2000

[7] Bernard Sklar
Digital communications – Fundamentals and applications, Prentice Hall 1988

[8] Breezecom
IEEE 802.11 Technical Tutorial
http://www.breezecom.com/Materials/PDFFiles/802.11Tut.pdf

[9] EURESCOM
Project P816-PF, Implementation frameworks for integrated wireless-optical access networks, February 2000

[10] Gilbert Held
Data over wireless networks – Bluetooth, WAP & Wireless LANs, ISBN 0-07-212621-3, 2001

[11] Harri Holma and Antti Toskala
WCDMA for UMTS, ISBN 0-471-72051-8, June 2000

[14] Ericsson
Ericsson Press Releases, Ericsson demonstrates HiperLAN2 prototypes
http://www.ericsson.com/press/20001211-0067.html

[15] *Martin Johnsson*
HiperLAN/2 – The Broadband RadioTransmission Technology Operating in the 5 GHz Frequency Band, HiperLAN/2 Global Forum, 1999.Version 1.0
http://www.hiperlan2.com

[16] http://www.whatis.com

[17] TR 101 031 V2.2.1 (1999-01)
Broadband Radio Access Networks (BRAN); HIgh PErformance Radio Local Area Network (HIPERLAN) Type 2; Requirements and architectures for wireless broadband access
http://www.etsi.org/

[18] TR 101 031 V1.1.1 (1997-07)
Radio Equipment and Systems (RES);
HIgh PErformance Radio Local Area Networks (HIPERLAN); Requirements and architectures for Wireless ATM Access and Interconnection
http://www.etsi.org/bran/

[19] TR 101 054 V1.1.1 (1997-06)
Security Algorithms Group of Experts (SAGE);
Rules for the management of the
HIPERLAN Standard Encryption Algorithm (HSEA)
http://www.etsi.org/bran/

[20] ETSI TR 101 683 V1.1.1 (2000-02)
Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview
http://www.etsi.org/bran/

[21] ETSI TS 101 761-1 V1.2.1 (2000-11)
Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) Layer; Part 1: Basic Data Transport Functions
http://www.etsi.org/bran/

[22] Charles E. Perkins, Sun microsystems
Suns Microsystems IEEE communications Magazine, May 1997

[23] Charles E. Perkins
Mobile IP Design Principles and Practises, Addison-Wesley wireless communication series, 2nd printing, ISBN 0-201-63469, 4January 1998.

[24] Bar-David, R. Krishnamoorty,
Barker Code Position Modulation for High Rate Communication in the ISM Bands, IEEE 1996

[25] Vectors Technology brief
Dell – 802.11 wireless security in business networks, February 2001.
http://www.dell.com/us/en/gen/topics/vectors_2001-wireless_Security.htm

[26] Eirik Rossen, digitoday/data
Trådløse lokalnett er grunnleggende usikre, 6.2.2001
http://digitoday.no/digi98.nsf/pub/dd20010206092310_ero_35234607

[27] ISAAC
Internet Security, Applications, Authentication and Cryptography
Security of the WEP algorithm
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[28] Old Colorado City Communications and the National science foundation wireless field tests
UCLA Critique of 802.11 Wireless
The Current Assessment of Public Nomadic Wireless Computing As of May 10, 2000
http://wireless.oldcolo.com/biology/Progress2001/UCLASummary.htm

[29] Institute of Electrical and Electronics Engineers, Inc.
ISO/IEC 8802-11, ANSI /IEEE std 802.11, ISBN 0-7381-1658-0, First edition 1999-08-20

[30] Institute of Electrical and Electronics Engineers, Inc.
IEEE std 802.11a-1999, 30. December 1999, ISBN 0-7381-1809-5

[31|] Institute of Electrical and Electronics Engineers, Inc.
IEEE std 802.11b-1999, 20. January 2000, ISBN 0-7381-1811-7

[32] John Davis, II
Indoor Propagation at 2.4 GHz, 1997
http://wireless.per.nl/multimed/cdrom97/2_4ghz.htm

[33] Intersil Corporation
Effects of Microwave Interference On IEEE 802.11WLAN Reliability, Submission to IEEE P802.11Wireless LANs, May 1998
http://www.wlana.com/learn/microreliab.pdf

[34] Wlana
Introduction to wireless LANs
http://www.wlana.com/learn/intro.pdf

[36] Jim Zyren, Intersil Corporation
Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment, June 8, 1999.
http://www.wlana.com/learn/reliabwlan.pdf

[37] Wlana
Wireless LAN Security White Paper
http://www.wlana.com/learn/security.htm

[38] Ad Kamerman, Nedim Erkocevic,
Microwave oven interference on wireless LANs operating in the 2,4 GHz ISM band, IEEE 1997

[39] Carla F. Chiasserini, Ramesh R. Rao,
Performance of IEEE 802.11 WLANs in a Bluetooth environment,

IEEE 2000.

[40] Matthew B. Shoemake, Ph.D., Texas Instruments
Wi-Fi (IEEE 802.11b) and Bluetooth Coexistence Issues and Solutions for the 2.4 GHz ISM Band
http://www.alltalking.com/Change/pdf/coexistence.pdf

[41] Kazuhiro Takaya, Yuji Maeda and Nobuo Kuwabara, NTT multimedia Networks Laboratories
Interference Characteristics between 2.4 GHz-band Middle-speed Wireless LANs using Direct Sequence and Frequency Hopping

[42] Aleksandar Neskovic, Natascha Neskovic and George Paunovic, University of Belgrade
Modern approaches in modeling of mobile radio systems propagation environment, Third quarter 2000

9 Abbreviations and acronyms

ACK	acknowledgement
AP	access point
ATM	asynchronous transfer mode
BER	bit error rate
BPSK	binary phase shift keying
BRAN	broadband radio access network
BSS	basic service net
BT	bluetooth
CCITT	international telegraph and telephone consultative committee (now ITU-T)
CCK	complimentary code keying
CL	convergence layer
CRC	cyclic redundancy check
CSMA	carrier sense multiple access
CSMA/CA	CSMA with collission avoidance
CSMA/CD	CSMA with collission detect
CTS	clear to send
CW	continues wave
DBPSK	differential binary phase-shift keying
DES	data encryption standard
DIFS	distributed inter frame space
DIFS	distributed IFS
DLC	data link control
DQPSK	differential quadrature phase-shift keying
DS	direct sequence
DS	distribution system
DSSS	direct sequence spread spectrum
EIFS	extended IFS
ESS	extended service set
ETSI	european telecommunication standards institute
FA	foreign agent
FCC	code of federal regulations
FER	frame error rate
FH	frequency hopping
FHSS	frequency hopping spread spectrum
FireWire	IEEE 1394 standard
FSK	frequency-shift keying
GFSK	gaussian frequency-shift keying
GSM	global system for mobile communications
HA	home agent
HEC	header error check
HiA	høgskolen i agder
HiperLAN	high performance radio local area network
ICMP	Internet control message protocol
IEEE	Institute of electrical and electronical engineers
IFS	inter frame space
IP	internet protocol
IR	infrared
ISI	intersymbol interference

ISM	industrial, scientific and medical
ISAAC	internet security applications and cryptography
IV	initialiazation vector
LAN	local area network
LOS	line of sight
MAC	media access control
MT	mobile terminal
NAV	network allocation vector
NLOS	no line of sight
NRZ	non-return to zero
OFDM	orthogonal frequency dividsion multiplexing
OSI	open system interconnection
PC	personal computer
PDA	personal digital assistant
PER	packet error rate
PHY	physical (layer)
PIFS	point coordination IFS
PPP	point to point protocol
PRN	pseudo-random number
PRNG	pseudo-random number generator
QoS	quality of service
QPSK	quadrature phase-shift keying
RA	receiver address
RMS	root mean square
RTS	request to send
RVSP	resource reservation protocol
SER	symbol error rate
SFD	start frame delimiter
SIFS	short interframe space
SSID	service set identifier
STA	station
SYNC	synchronization
TA	transmitter address
TCP	transmission control protocol
UDP	user datagram protocol
UMTS	universal mobile telephony system
US	united states
VPN	virtual privat network
WEP	wired equivalent privacy
WLAN	Wireless local area network

10 Appendix

[A] Siemens
Technical data I-GATE 11M I/LAN Accesspoint

[B] Siemens
Diagrams

[C] Measurements taken from different locations