Fu-Tien Hsiao

Youhui Zhao

Vedrana Andersen

Signal Processing in WLAN, Sensor Networks and RFID

Project supervisors:

John Aasted Sørensen

Jianjun Chen

ITU, Copenhagen, May 2005.

PREFACE

As we entered the 21st century, the use of wireless communication technologies is exploding rapidly, including cellular phones, satellite phones, wireless local area networks, personal digital assistants, radio frequency identification and sensor networks. IT University of Copenhagen is a university concerned with this new technology trend.

The project “Signal Processing in WLAN, Sensor Neworks and RFID”, given by Mobile Communications and Signal Processing group, provides the basic and straightforward principles of the architecture of WLAN (IEEE 802.11b), radio propagation (in an indoor environment), radio frequency identification, and packet capture programming implemented in C language, which is also the goal of this project report. Besides, we include four experiments to see if the relationship between access point and mobile station is identical to the principles we are talking about in the theoretical part.

We would like to thank our supervisors John Aasted Sørensen and Jianjun Chen for their valuable comments and suggestions.

TABLE OF CONTENTS

1 INTRODUCTION

This project report is a result of a 4 weeks project "Signal Processing in WLAN, Sensor Networks and RFID" carried out at ITU of Copenhagen in May 2005. The report is divided in two parts, theoretical and experimental. Theoretical part of the report follows to a great extend the structure of the lessons arranged in the first week of the project period. In the experimental part we describe the experiments we designed and carried out in the second and third week of the project period.

As in the lessons, in the theoretic part of the project report we touched upon three wireless environments: wireless LANs, sensor networks and RFID. The focus was put on wireless LAN, which is already in a widespread use, and is still rapidly gaining popularity, mostly due to installation simplicity and mobility it provides. Here we described types of networks, network services and management operations. One of the most commonly followed wireless LAN specifications is IEEE 802.11b, and that is also the one we are referring to most often.

Sensor networks share many similarities with wireless LAN, but there are also many differences between wires LAN and sensor networks, because of sensor networks' specific functions. Writing about sensor networks, we focused on design factors and challenges. We also included a short introduction to RFID, which is as well a wireless environment. RFID is interesting because it is an emerging technology, which will surly find its use. The theoretical part of our project report ends with a short explanation of radio propagation, which is used by all wireless devices. This part is serving as a basis for experiments we conducted.

The experimental part contains four experiments. The most evident experiment following from the radio propagation lessons was estimating distance–power gradient for the indoor environment, and our measurements were in accordance with the indoor propagation model. Our second experiment investigates a possibility of detecting people between an access point and a mobile station and, according to our results; it should be possible to do so. With the third experiment we were testing antennas omnidirectionality. We found out that antenna does not radiate uniformly in all directions, not even just in horizontal plane. The last experiment was our attempt to find a relation between room's size and received signal power. The results of this experiment didn't fully fulfil our expectations, probably because of many factors we could not control. All software used in the experiments can be found in appendices.

2 THEORETICAL BACKGROUND

2.1 WIRELESS LOCAL AREA NETWORKS

In this part of the project report, we refer mostly to [1]

2.1.1 What is wireless networking?

WLAN is an acronym for wireless local area network. One characteristic of local area network is that they use high-frequency radio waves rather than wires to communicate between nodes. The term wireless networking refers to technology that enables two or at more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs. This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity with business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment. [2]

2.1.2 802.11 nomenclature and design

IEEE 802.11 are specifications for wireless LAN technologies, focused on the two lowest layers of the networking protocol stack: data link layer and physical layer.

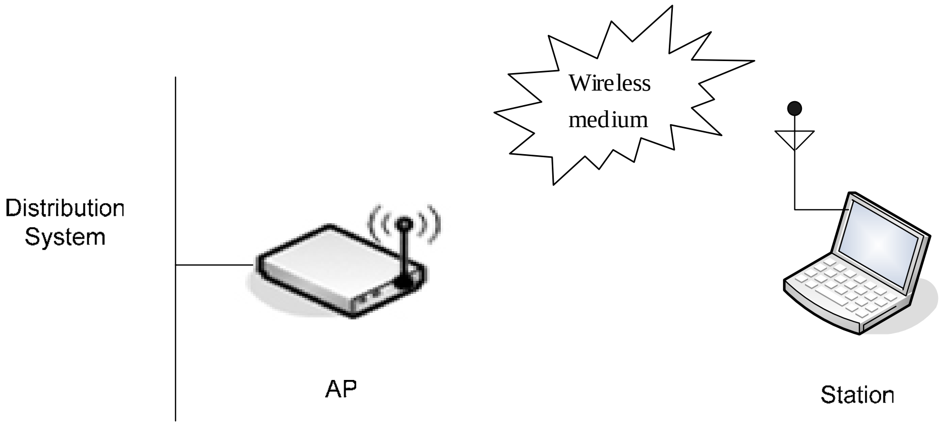

Figure 2.1 Components of 802.11 LAN

Figure 2.1 shows major physical components of 802.11 LAN, and those are:

- Distribution system – logical component used to forward frames to their destination, also called backbone network.
- Access Points – performs wireless-to-wired bridging and a number of other functions.
- Wireless Medium – used to move frames from one station to another,
- Stations – devices with network interface, typically laptops.

2.1.3 Types of networks

The basic building block of an 802.11 network is the basic service set (BBS), which is simply a group of stations that communicate with each other. Communications take place within a somewhat fuzzy area, called the basic service area, defined by the propagation characteristics of the wireless medium. BSSs come in the two flavors, shown on Figure 2.2.

1. Independent BSS (IBSS) – Stations communicate directly with each other.
2. Infrastructure BSS – Stations communicate relayed through an access point.

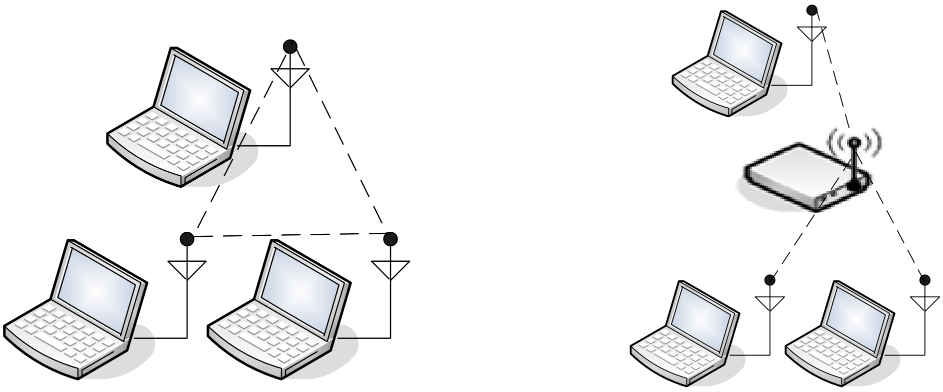

Figure 2.2 Independent BSS (left) and infrastructure BSS (right)

Extended Service Set (ESS) shown on Figure 2.3 provides network coverage to larger areas. It is created by linking more BBSs using backbone network.

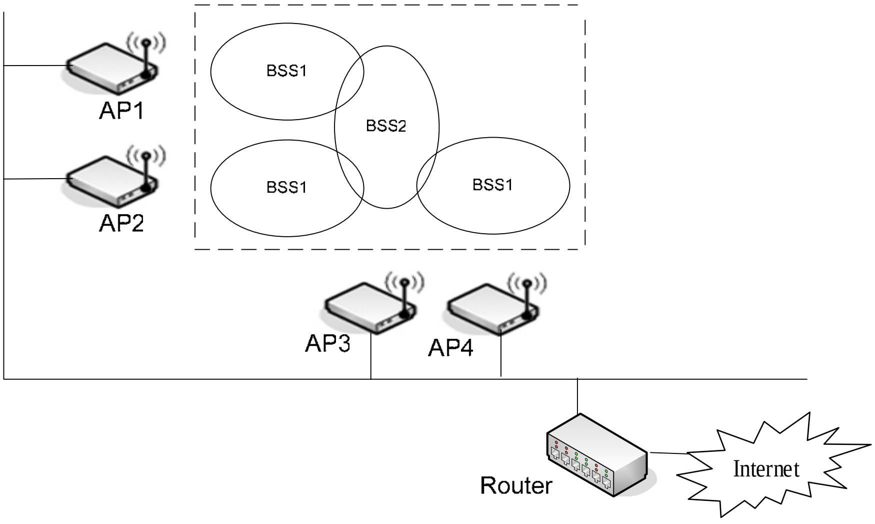

Figure 2.3 Extended service set

2.1.4 Network services

In order to define a network technology we need to define the services it offers, which allows equipment vendors to implement them. There are two forms of network services:

Distribution system services connect access points to the distribution system:

- Distribution – service used in frame delivery to determine destination address in infrastructure networks.
- Integration – frame delivery to an IEEE 802 LAN outside the wireless network.
- Association – used to establish the AP, which serves as the gateway to a particular mobile station.
- Reassociation – used to change the AP, which serves as the gateway to a particular mobile station.
- Disassociation – removes the wireless station from the network.

Station services are provided by both mobile stations and the wireless interface on access points:

- Authentication – establish identity prior to establishing association.
- Deauthentication – used to terminate authentication, and by extension, association.
- Privacy – provides protection against eavesdropping.
- MSDU delivery – delivers data to recipient.

2.1.5. Managements operations

Management architecture

The 802.11 management architecture is composed of three components: the MAC layer management entity (MLME), a physical-layer management entity (PLME), and a system management entity (SME). The relation ship is shown at Figure 2.4.

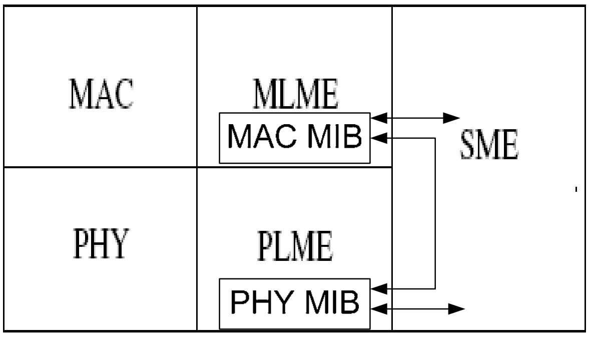

Figure 2.4 Management architecture

Scanning

If we are in the wireless world and we want to use a network the stations must identify a compatible network before joining it. The process of identifying existing networks in the area is called scanning.

Several parameters are used in the scanning procedure. The user may specify these parameters. Many implementations have default values for these parameters in the driver.

BSSType – scanning can specify whether to seek out independent ad hoc networks, infrastructure networks, or all networks.

BSSID – scan for a specific network to join (individual), or any network that is willing to allow it to join (broadcast).

SSID – assigns a string of bits to an extended service set (network name).

ScanType – active scanning uses the transmission of Probe Request while passive scanning saves battery power by listening for Beacon frames.

ChannelList – specifying a list of channels to try. With direct-sequence products, it is a list of channels. With frequency-hopping products, it is a hop pattern.

ProbeDelay – delay before probe a channel in active scanning begins, to ensure that an empty or lightly loaded channel does not completely block the scan.

MinChannelTime and MaxChannelTime-specified in time units (TUs), specify the minimum and maximum amount of time that the scan works with any particular channel.

Types of scanning

1. Passive Scanning (Figure 2.5) does not require transmitting. The MS uses a passive scan to find BSSs in its area; it hears Beacon frames from different APs, and then decides which AP matches parameters with BSS.

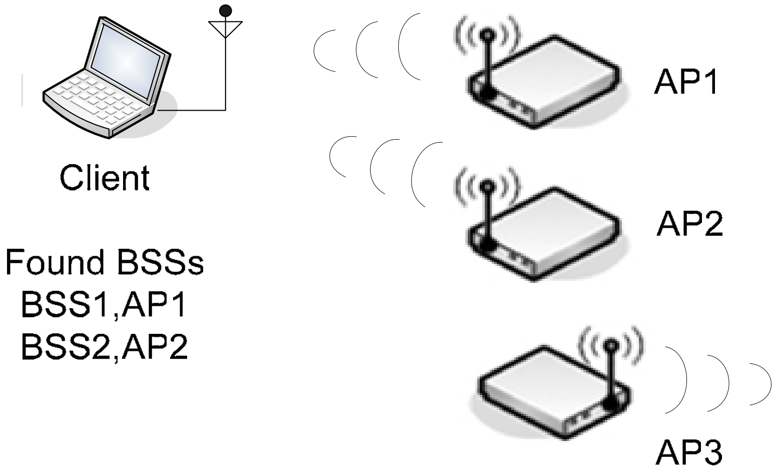

Figure 2.5 Passive scanning

2. Active Scanning (Figure 2.6) – station transmits a probe request to which APs response. The scanning station transmits the Probe Request after gaining access to the medium. APs respond with a Probe Request that reports their network's parameters.

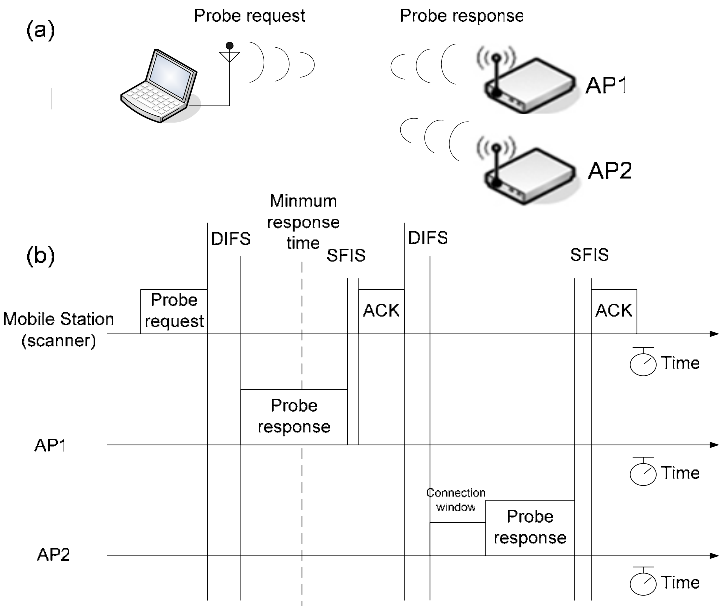

Figure 2.6 Active scanning

Scan Report

A scan report is generated at the conclusion of a scan. The report lists all the BSSs that the scan discovered and their parameters. The complete parameter list enables the scanning station to join any of the networks that is discovered. In addition to the BSSID, SSID; and BSSType, the parameters also include:

Beacon interval (integer) – Each BSS can transmit Beacon frames at its own specific interval, measured in TUs.

DTIM period (integer) – DTIM frames are used as part of the power-saving mechanism.

Timing parameters – Two fields assist in synchronizing the station's timer to the timer used by a BSS. The Timestamp field indicates the value of the timer received by the scanning station; the other field is an offset to enable a station to match timing information to join a particular BSS.

PHY parameters, CF parameters, and IBSS parameters – These three facets of the network have their own parameters sets.

BSSBasicRateSet – This is the list of data rates, which must be supported by any station wishing to join the network.

Joining

After compiling the scan results, a station can elect to join one of the BSSs. Joining is a precursor to association; it does not enable network access. Authentication and association are the preconditions.

Authentication

Authentication is implicitly provided by physical access; it's a one-way street. Stations wishing to join a network must authenticate it, but networks are under no obligation to authenticate themselves to their stations.

1. Open-system authentication is the only method required by 802.11. In this authentication, the AP accepts the MS at face value without verifying its identity. It consists of two frames, the first one exchanging MAC address used as station identifier of the sender; AP processes the authentication request and returns its response.
2. Shared-key authentication requires a shared key be distributed to stations before attempting authentication. This authentication consists of four frames while exchanging: the first frame identifies authentication algorithm and the sequence number; the second frame serves as a challenge; the third frame is the MS's response to the challenge; after receiving the third frame, the AP attempts to decrypt it and verify the WEP integrity check.

Preauthentication

Stations must authenticate with an access point before associating with it, but nothing in 802.11 requires that authentication takes place immediately before association. Stations can authenticate with several AP during the scanning process so that when association is required, the station is already authenticated. This is called preauthentication.

Association

Once authentication has completed, stations can associate with an AP to gain full access to the network. Association is a record keeping procedure that allows the distribution system to track the location of each MS, so frames destined for the MS can be forwarded to the correct AP The association procedure is shown at Figure 2.7.

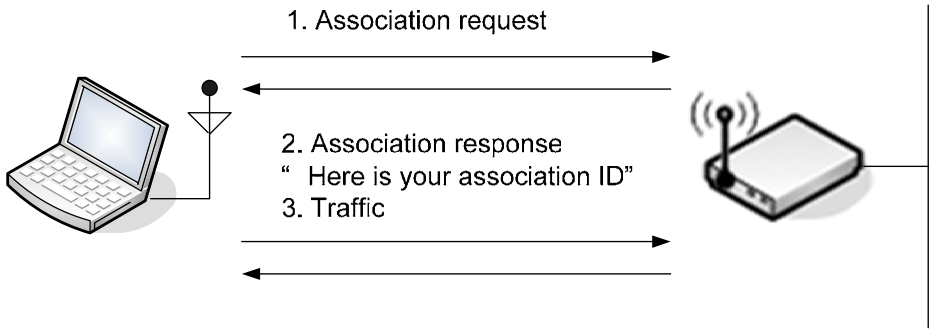

Figure 2.7 Association Procedure

2.2 SENSOR NETWORKS

Sensor networks are made of a large number of low-cost, low-power sensor nodes densely deployed in environment, wirelessly communicating with each other. The nodes can be sensing temperature, vibration, pressure, acceleration…There is a wide range of possible applications.

The sensor nodes are usually scattered in a sensor field as shown in Figure 2.8. Each of these scattered sensor node has the capabilities to collect data and route data back to the sink. Data are routed back to the sink by a multi-hop infrastructure less architecture through the sink. The sink may communicate with the task manager node via Internet or satellite. [3][4][5][6]

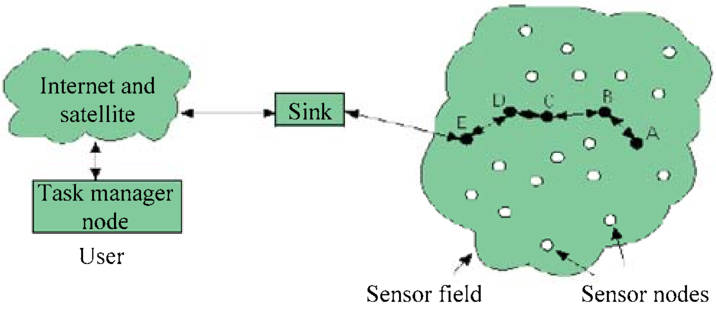

Figure 2.8 Sensor nodes scattered in a sensor field

2.2.1 Design factors

The design of the sensor network is influenced by many factors, including fault tolerance, scalability, production costs, operating environment, sensor network topology, hardware constraints, transmission media, and power consumption, these influencing factors can be used to compare different schemes.

<u>Fault Tolerance</u>

Sensor nodes may fail or be blocked due to lack of power, or have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network.

<u>Scalability</u>

Scalability is depended what is your requirement or what type of application of sensor network we need. Its can be few of nodes of sensor network or million, then they used higher density for sensor network. Density range can from few nodes to few hundred nodes in region. The diameter is less then 10m. Density can μ be calculated using formula $\mu(R) = (N \cdot \pi R^2)/A$

<u>Production Costs</u>

Since sensor networks consist of a large number of sensor nodes, we have to keep cost of each sensor very low, then we can control the overall cost of network.

<u>Hardware Constraints</u>

A sensor node is made up of four basic components:

1. Sensing unit-composes two subunits: sensors and analog-to-digital converters (ADCs)
2. A processing unit-associate with a small storage unit manages the procedures that carry out the tasks.

3. A transceiver unit-connects the nodes to the network
4. Power unit-supported by power scavenging units.

Sensor Network Topology

When we examine issues related to topology maintenance and change in three phases:

1. Pre-deployment and deployment phase,
2. Post-deployment phase,
3. Re-deployment of additional nodes phase.

Environment

Sensor nodes are densely deployed either very close or directly in side the phenomenon, they may be work in the interior of large machinery.

Transmission Media

Communication nodes are linked by a wireless medium, which can be formed radio, infrared, or optional media.

Power Consumption

The wireless sensor node can only de equipped with a limit power source (<0.5Ah, 1.2V). The main task of sensor node in a sensor field is to detect events, perform quick local data processing, and then transmit the data. Power Consumption can be dividing into three domains: sensing, communication, and the data processing.

2.2.2 Attributes of Sensor Networks

Sensors	Size: small (micro-electro mechanical system, MEMS), large (radars, satellites) Number : small ,large Type: passive (acoustic, seismic, video, IR, magnetic), active (radar, ladar) Composition or mix: homogenous (factory networks), heterogeneous (different types of sensors) Spatial coverage: dense, sparse Deployment : fixed and planned (factory network), ad hoc (air-dropped) Dynamics: stationary (seismic sensors), mobile (e.g. on robot vehicles)
Sensing entities of interest	Extent : distributed (environmental monitoring), localized (target tracking) Mobility : static, dynamic Nature : cooperative (e.g. traffic control), non-cooperative (military targets)
Operation environment	Benign (factory floor), adverse (battlefield)
Communication	Networking: wired, wireless; Bandwidth: high, low
Processing architecture	Centralized (all data sent to central site), distributed(located at sensor or other sites),hybrid
Energy availability	Constrained (e.g. in small sensors), unconstrained (e.g. in large sensors)

2.2.3 Protocol stack

The protocol stack used by the sink and sensor nodes shown in Figure 2.9. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes.

Protocol stack consists of the physical layer, data link layer, and network layer, transport layer, application layer, power management plane, mobility management, and the task management.

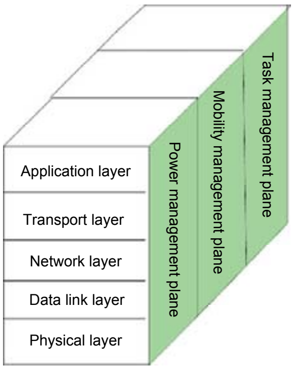

Figure 2.9 Protocol stack

All 802 networks have both a MAC and a Physical (PHY) component. The MAC is a set of rules to determine how to access the medium and send data, but the details of transmission and reception are left to the PHY.

2.2.4 New applications in sensor networks

Research on sensor networks was originally motivated by military applications. Example of military sensor networks range from large-scale acoustic surveillance systems for ocean surveillance to small networks of unattended ground sensors for ground target detection.

Infrastructure Security

Sensor networks can be used for infrastructure security and counterterrorism applications. Critical buildings and facilities such as power plants and communication centres have to be protected from potential. Networks of other sensors can be deployed around their facilities.

Environment and Habitat Monitoring Industrial Sensing

Environment and habitat monitoring is a natural candidate for applying sensor networks, since the variable to be monitored.

Industrial Sensing

Commercial industry has long been interested in sensing as a means of lowering cost and improving machine performance and maintainability. Spectral sensors are one of example of sensing in an industrial environment.

Traffic Control

Sensor networks have been used for vehicle traffic monitoring and control for quite a while. Most traffic intersections have either overhead or buried sensors to detect vehicles and control traffic lights. Furthermore, video cameras are frequently used to monitor road segments with heavy traffic, with the video sent to human operators at central locations.

2.3 RADIO FREQUENCY IDENTIFICTION

Radio frequency identification (RFID) technology provides a means of automatic identification. It is already widely used in animal tagging and electronic payment, such as Transport for London ‘Oyster Cards’. Many other potential applications such as improving supply chain efficiency and reducing crime are being investigated. This note provides an overview of the technology; its current and prospective uses, and outlines the factors limiting its uptake. It then discusses measures being taken to address growing concerns over privacy.

2.3.1 Background

RFID tagging is a form of Automatic Identification and data Capture (AIDC) technology where data stored on a tag is transferred via a radio frequency link. A RFID reader communicates with the tag to infer the identity of the object to which the tag is attached. The principle is similar to the more familiar bar code, where data are transferred optically. However, RFID has advantages over bar codes, such as the ability to store large amounts of data and to read many tags simultaneously.

An RFID system consists of three components: an antenna and transceiver (often combined into one reader) and a transponder (the tag).

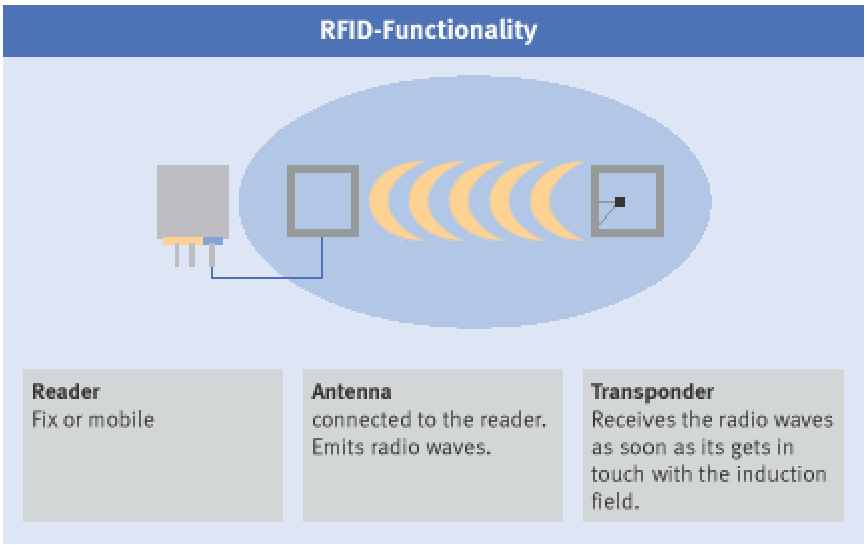

Figure 2.10 Components of RFID

The antenna uses radio frequency waves to transmit a signal that activates the transponder. When activated, the tag transmits data back to the antenna. The data is used to notify a programmable logic controller that an action should occur. The action could be as simple as raising an access gate or as complicated as interfacing with a database to carry out a monetary transaction. Low-frequency RFID systems (30 KHz to 500 KHz) have short transmission ranges (generally less than six feet). High-frequency RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer longer transmission ranges (more than 90 feet). In general, the higher the frequency, the more expensive the system. [7]

2.3.2 Properties of RFID systems

The properties of a given RFID system depend on several key parameters:

- The range of a RFID system depends on the frequency, power of the reader, and the material between the tag and the reader. The presence of metal and liquids reduces the range of the ultra high frequency RFID systems. The range can be up to a few meters for passive systems but in excess of 100 m for active systems due to the onboard battery that facilitates increased radio transmitter power.
- The tag size increases at lower frequencies (LF), since the tag incorporates the antenna, and larger antennae are needed to transmit lower frequencies. The chip can be as small as 1 mm2, but the antenna is much larger (of the order of centimeters). The antennae for LF tags are metal wire coils, but for higher frequencies they can be printed onto paper using conductive inks.
- As the frequency increases, the read rate, and thus the amount of data that can be transferred in a given time, increases. This is important when many tagged goods need to be read in a short time.
- The cost of tags tends to decrease as the frequency increases, although active tags cost much more than passive tags, irrespective of frequency. Also, the longer the range required and the more information stored, then the more costly the tag. [8]

2.3.3 Types of RFID systems

The first major category of choice is between active and passive transponders. Active contain a battery to provide their energy, while passive extract energy from the energising field of the reader. For passive transponders a second category of choice is in the type of protocol, being either a Reader-talks-first (RTF) or a Tag-talks-first (TTF) protocol. RTF protocols generate much higher levels of interference compared to TTF protocols meaning fewer readers can operate in close proximity. [9]

2.3.4 The benefits of RFID technology

The RFID system allows manufacturers, retailers, and suppliers to efficiently collect, manage, distribute, and store information on inventory, business processes, and security controls. RFID will allow: retailers to identify potential delays and shortages; grocery stores to eliminate or reduce item spoilage; toll systems to identify and collect auto tolls on roadways; suppliers to track shipments; and in the case of critical materials, RFID will allow receiving authorities to verify the security and authentication of shipped items. These uses are seen as only the beginning, and as RFID is deployed across different sectors and services, increasing efficiency and visibility, several other applications and benefits may arise. The technology itself offers several improvements over its predecessor technologies – the barcode and magnetic stripe cards. The central data feature of RFID technology is the Electronic Product Code (EPC), which is viewed by many in the industry as the nextgeneration barcode or Universal Product Code (UPC). This EPC code can carry more data, than the UPC code and can be reprogrammed with new information if necessary. Like the UPC, the EPC code consists of a series of numbers that identify the manufacturer and product type. The EPC code also includes an extra set of digits to identify unique items.

2.4 RADIO PROPAGATION

In this part of the project report, we refer mostly to [10]

2.4.1 Introduction of wireless propagation

Wireless communication basically divides into two sets: LOS path and multipath propagation. Here are the examples of multipath in different radio channels.

1. LOS (Line of Sight) path

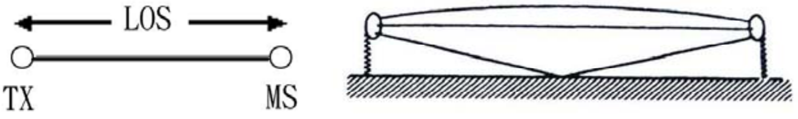

Figure 2.11 LOS path

Figure 2.11 represents a line of sight microwave radio link, as is widely used in nationwide networks for terrestrial communications.

2. Multipath propagation.

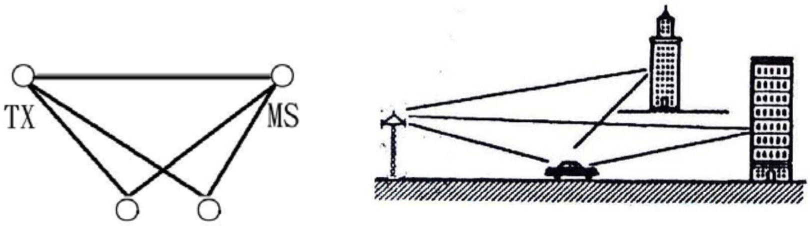

Figure 2.12 Multipath propagation

Figure 2.12 represents a mobile radio scenario where the received signal arrives by several paths bounced from large objects.

2.4.2 Wireless propagation in an indoor environment.

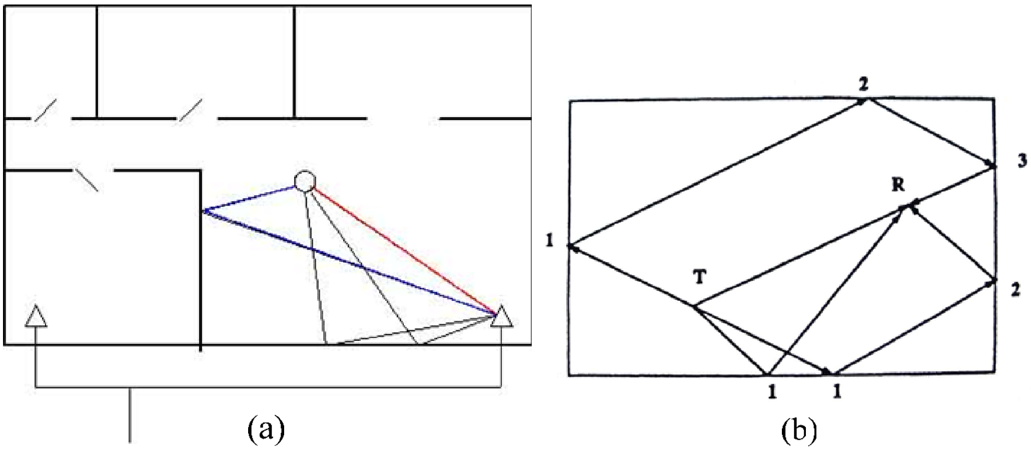

Figure 2.13 Indoor environment

Figure 2.13 (a) shows an indoor environment, red line represents LOS propagation, and blue line represents Mulitpath propagation. Figure 2.13 (b) shows reflections for ray tracing in a rectangular room, with examples of LOS and first-, second- and third-order reflected paths. After the reflection, there'll be some delay for propagation and some loosing of energy.

Typical values for WLAN and Antenna

The speed of radio wave is equal to the speed of light $c = 3\times10^{8} m/s$. In IEEE 802.11b, frequency is $F_0 = 2.4GHz$, wavelength $\lambda = c/f = 3\times10^{8}/2.4\times10^{9} = 12.5cm$, and $P_T \approx 100mW$. Hence, the size of antenna is around one half or one fourth of λ, 3 *cm* or 6*cm*.

Antenna is the link to the physical transmission shown at Figure 2.14.

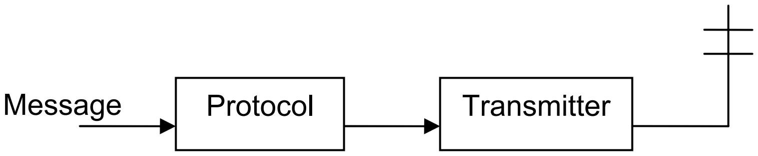

Figure 2.14 Antenna – link to the physical transmission

Constructive and Destructive Interference.

In Figure 2.15, we can find that wave A and B is constructive interference, wave A and C is destructive interference.

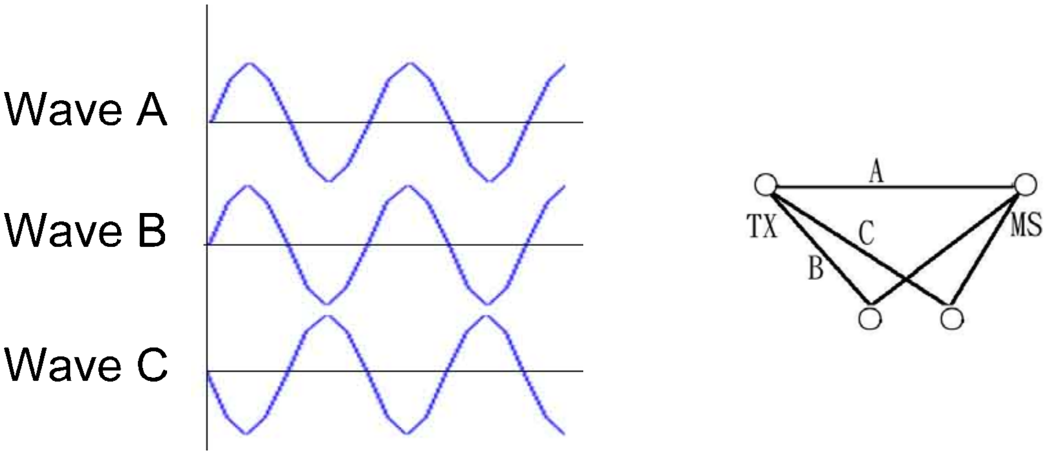

Figure 2.15 Constructive and destructive interference

Wave A is in LOS path, wave B is in multipath propagation and very similar to wave A. Wave C is in multipath propagation but half the wavelength delayed. Due to the constructive and destructive interference of multipath components received at the different locations, multipath propagation causes substantial variation in the amplitude of a received radio signals.

2.4.3 Narrowband signals in free space:

Free space provides the ideal environment for single-path communication. To analyze the multipath condition, we start with a simplified description of radio propagation in a single-path free space channel.

Relationship between received power and transmitted power

In free space, the relationship between transmitted power P_T and received power P_R is given by

$$P_R = G_T G_R \left[\frac{\lambda}{4\pi d} \right]^2 P_T \qquad \text{(a)}$$

where:

- G_T and G_R are the factors related to the direction of antenna, but we don't discuss further.
- d is the distance between transmitter and receiver
- λ is the wavelength of transmitter signal.

Received power at the distance of one meter

If we define P_0 as power received at the distance of one meter,

$$P_0 = G_T G_R \left[\frac{\lambda}{4\pi} \right]^2 P_T$$

and assume the components G_T, G_R, λ, P_T are constant, we can reduce the equation (a) into

$$P_R = \frac{P_0}{d^2} \qquad \text{(b)}$$

Hence, P_0 is a constant and P_R is directly proportional to $\frac{1}{d^2}$. For example, if the distance d changes into 3d, the received power P_R becomes $\frac{1}{9} P_R$.

Another representation of received power in dBm

We change the unit of received power into dBm so that we can find a linear relationship between $P_R dBm$ and $\log_{10} d$.

$$P_R dBm = 10\log_{10} \frac{P_r}{1 \cdot mW}$$

So we rewrite equation (b) into

$$10\log_{10} P_R = 10\log_{10} (\frac{P_0}{d^2}) = 10\log_{10} P_0 - 20\log_{10} d \qquad \text{(c)}$$

In this case, when there is a fixed AP and a moving MS, $10\log_{10} P_0$ is a constant and $20\log_{10} d$ is variable.

2.4.4 Multipath fading and narrowband signals

Except for the LOS path, all paths are going through at least one order of reflection, transmission or diffraction before arriving at the receiver. If the path has been reflected K_i times before arriving at the receiver, and at each reflection the reflection coefficient is a_{ij}, the overall reflection factor is

$$a_i = a_{i1}a_{i2}a_{i3}... = \prod_{j=1}^{Ki} aij$$

Therefore, the amplitudes of the signals received from paths other than the LOS path are subject to reflection and the distance-attenuation factor.

Figure below shows the received power in decibels versus distance, where the receiver is located at the center of a 50×50 m^2 room and the transmitter is along a line straight from 2 m to 20 m from the receiver.

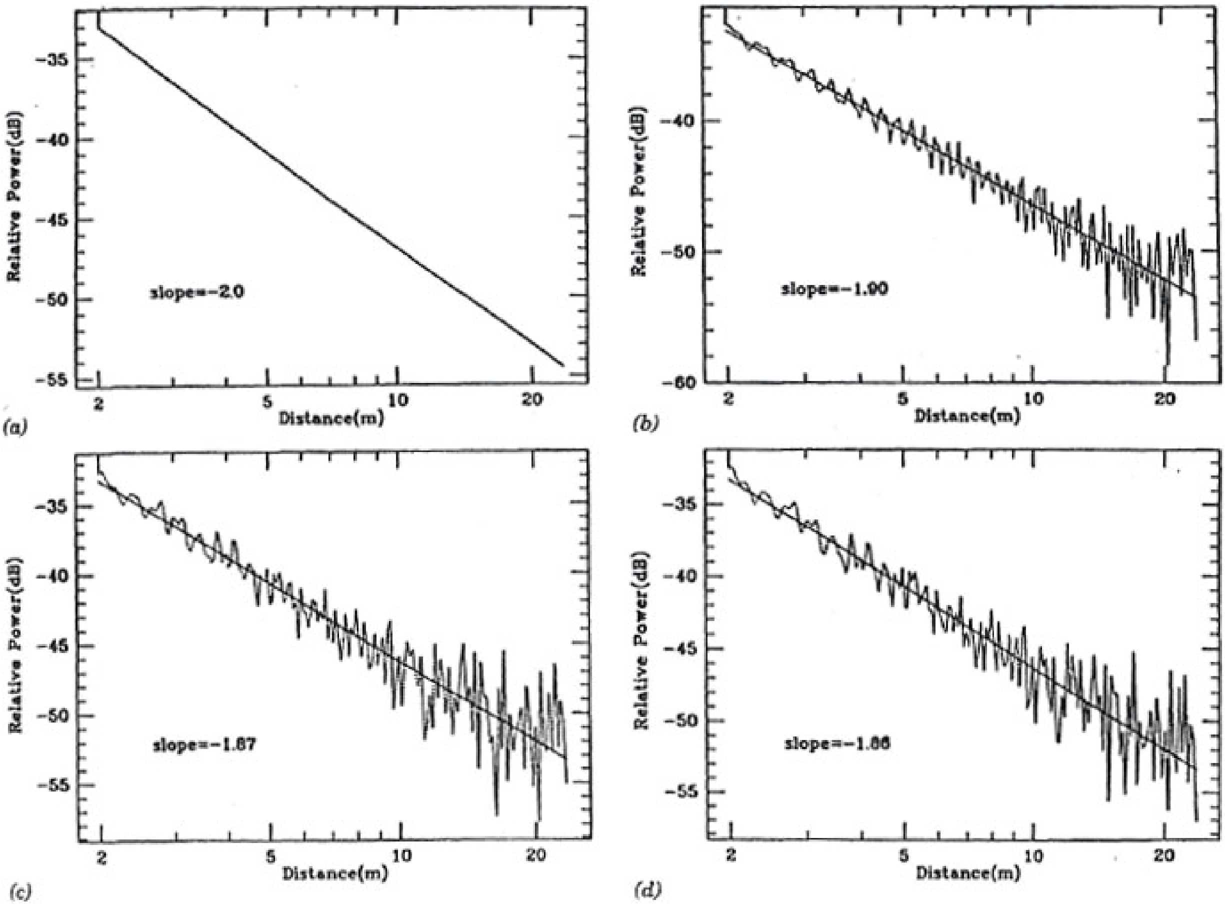

Figure 2.16 Received narrowband power obtained from two dimensional ray tracing in a room

Figure 2.16 (a) gives the results obtained from LOS path, and Figure 2.16 (b), (c), (d) include the first-, second-, and third-order reflections. Obviously, since α goes from 1.90 to 1.86, second- and third-order contribute very little to the received power. Therefore, the gradient (α is 1.90, 1.87, 1.86) remains very nearly the same as for free space (α is 2).

2.4.5 Indoor environment, modeling

Distance – power gradient α

We have discussed the relationship $P_R = \frac{P_0}{d^2}$ in the free space. Here we are going to discuss it in the indoor environment. The relationship for the indoor environment is

$$P_R = \frac{P_0}{d^\alpha}$$

The received power is proportional to the distance d between transmitter and receiver, raised to a certain exponent α, which is referred to as the distance-power gradient. When:

- $\alpha = 2$, the model is a free space. MB only receives the signal in LOS path.
- $\alpha < 2$, such as corridor in Figure 2.17(a), MB receives more signals, other than LOS path.
- $\alpha > 2$, there's no LOS in Figure 2.17(b). Transmitted wave goes through the metallic walls causing the attenuation.

Therefore, if α is bigger more power is lost.

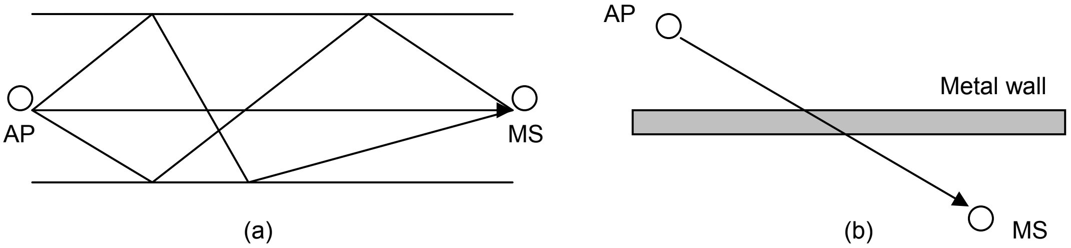

Figure 2.17 Corridor example and no LOS example

Measuring the distance-power gradient:
After normalizing, received power in *dBm* is plotted against distance on a logarithmic scale. The slope of the best-fit line through the measurements is taken as α*.* The relation is

$$10\log_{10} P_R = 10\log_{10} P_0 - \alpha \cdot 10\log_{10} d$$

where $10\log_{10} P_0$ is a constant and $\alpha \cdot 10\log_{10} d$ is a variable. We discuss this relationship in more detail next.

2.4.6 Linear regression

Figure 2.18 shows a set of wideband measurements of averaged received power taken in an indoor environment at distances from 1 to 20 m, together with the best-fit line through the measurements. But, how to plot the best-fit line? The technique to calculate the slope of the best-fit line is called linear regression.

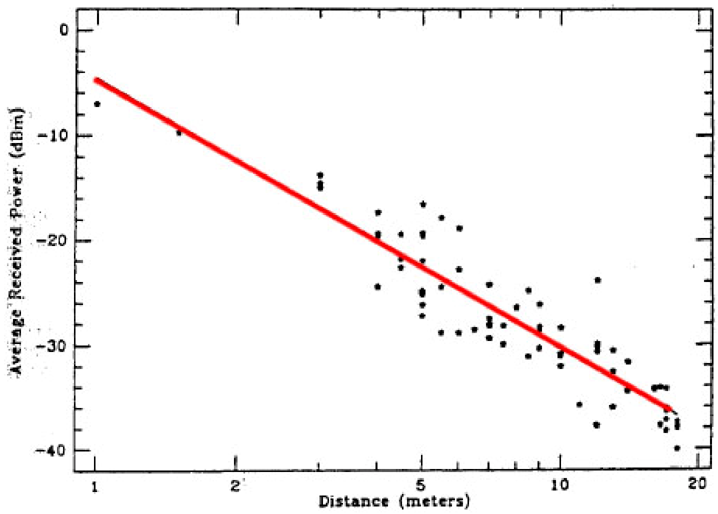

Figure 2.18 Measurements of received power

In the indoor model, the formula is $10\log_{10} P_R = 10\log_{10} P_0 - \alpha \cdot 10\log_{10} d$ where $10\log_{10} P_0$ is a constant and $\alpha \cdot 10\log_{10} d$ is a variable. Hence, we can rewrite it as $y = ax + b$ (α equals to -a). Through the measurements; we can get the datum of distance x and received power y. So, our goal is to find out a and b. Let's represent these in matrices:

$$y_i = ax_i + b$$

$$\Rightarrow \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} ax_1 + b \\ ax_2 + b \\ ax_3 + b \\ \vdots \\ ax_N + b \end{bmatrix} = \begin{bmatrix} x_1 & 1 \\ x_1 & 1 \\ x_1 & 1 \\ \vdots & \vdots \\ x_1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

$$\Rightarrow \quad Y = \qquad\qquad = XA$$

where Y is a given $N \times 1$ matrix, X is a given $N \times 2$ matrix, and A is a unknown 2×1 matrix ,

$A = \begin{bmatrix} a \\ b \end{bmatrix}$, and α equals to -*a*. How to solve A to get the gradient α ?

First we have to write *X* as a square matrix, and then multiplied by its inverse as below. By doing so, we get the gradient to plot the best-fit line through the measurements.

$$XA = Y$$

$$X^T XA = X^T Y$$

$$(X^T X)^{-1} X^T XA = (X^T X)^{-1} X^T Y$$

$$A = (X^T X)^{-1} X^T Y$$

2.5 WLAN PLANNING EXERCISE

The floor map of a building is given in Figure 2.19. One AP is already installed at the marked position in one room.

Walls ‘a’: Non-reflecting material.

Walls ‘k’, ‘c’ and ‘m’: All metal without holes. The attenuation of metal walls is 26dB per wall.

Walls ‘g’ and ‘h’: Concrete block walls. The attenuation of concrete walls is 13dB per wall.

All other walls are assumed not to interact with the electromagnetic waves.

We are asked to place additional AP’s in order to provide coverage of the whole building with as few AP’s as possible. The parameters are given as follows:

Transmit power of AP’s: $P_T = 15mW$

Carrier frequency $f = 2.4GHz$

The antennas are isotropic and have unit gains (i.e. $G_T = G_R = 1$)

The speed of light is $c = 3\times 10^8 m/s$

The received signal power should be at least -80dBm or higher at any location.

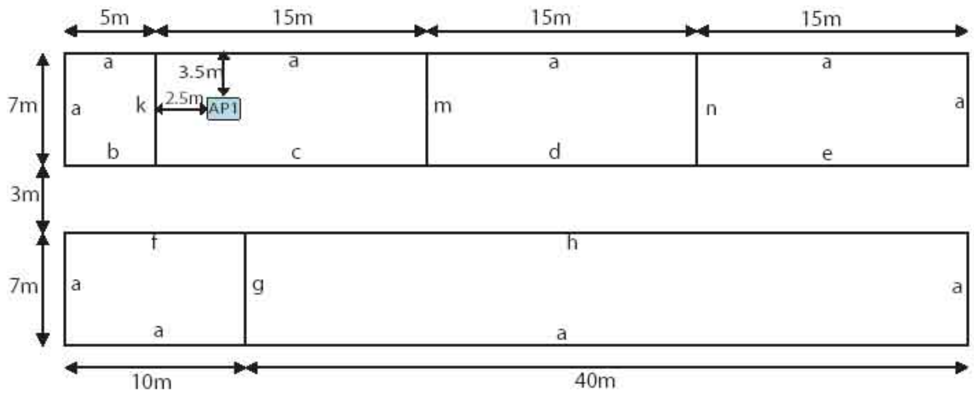

Figure 2.19 Floor map of a building

In addition to considering the attenuation of metal and concrete walls, due to walls ‘a’ are non-reflecting material, we can assume this floor as a free space model.

Matlab code

Here we write the Matlab program *Prdbm(wide, length, attenuation)* to calculate the power in dBm:

```
function Prdbm(wide, length, attenuation)
%% input
a= attenuation;  w= wide;  l= length;
distance=(w^2+l^2)^(0.5);                 %% the distance between MS and AP

Gt=1; Gr=1; Pt=15; f=2.4*10^9; c=3*10^8;  %% here are known variables

%% formula in free space model (alpha is 2)
WaveLength=c/f;
Po=Gt*Gr*(WaveLength/(4*pi*1))^2*Pt;   %% Po is Pr as d=1;
Prdbm=10*log10(Po/(distance)^2)-a      %% calculate Pr and subtract the attenuation
```

Because the received signal power should be at least –80dBm, after the calculation, the maximum distance is 387 m. It means that if all the walls don’t interact with the electromagnetic wave, any location in this floor can receive enough strength.

The strength from AP1

The signal strength form AP1 is shown on Figure 2.20.

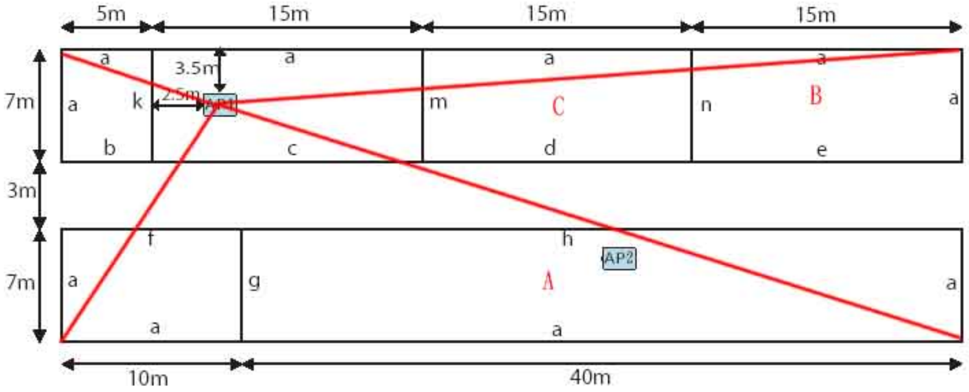

Figure 2.20 The strength from AP1

For up left corner: the signal only goes through the wall k (att=26dBm), Prdbm(3.5,7.5,26)=-73 dBm. Hence, for down left: -78 dBm; up right: -87 dBm; up down:-101 dBm. Because every room has different material walls, we have to consider the strength in the room A and B which couldn't get enough strength. As for room C: Prdbm(3.5,27.5,26)= -83, it also can't have enough strength

Therefore, we set another AP2 in room A to cover rooms A, B, and C.

The strength from AP2

The signal strength form AP2 is shown on Figure 2.21.

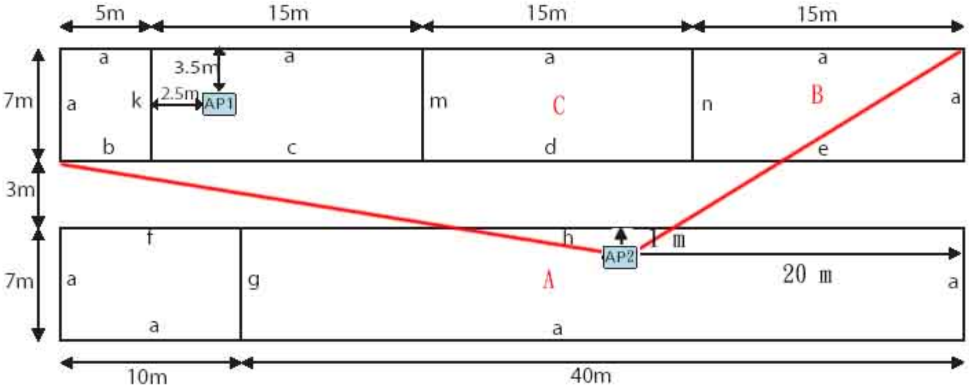

Figure 2.21 The strength from AP2

For room A: due to the maximum distance in free space is 385 m, any location in room A could get enough strength.

For room B and C: Because wall 'd', 'n' and 'e' don't interact with waves, it just goes through concrete wall 'h'.The weakest strength in room B and C is Prdbm(11,20,13)= -69, so it's alright.

We also consider the corridor, its weakest strength Prdbm(4,30,13)= -71.

Conclusion

So, AP1 and AP2 can give enough strength for MS in any location in this floor.

In this exercise, the distance attenuation is not the main factor but the material wall is. That's the reason why we have to consider the room with different material walls.

3 EXPERIMENTS

3.1 DESCRIPTION OF THE SOFTWARE FOR MEASURING RECEIVED SIGNAL POWER

In this part of the project report, we refer mostly to [11][12][13][14][15]

The starting point of all our experiments was measuring the received signal power. The transmitter was an access point (AP), and the receiver (mobile station, MS) was a laptop running on Linux and equipped with WLAN card.

By running a simple shell script we set the operating mode of WLAN driver and chose the working channel (using wireless extensions), and started a packed capture program in C.

Packet capture program extensively uses open source packet capture library, PCAP which makes it possible to get packets in their raw form directly from the device driver, in our case WLAN driver. This is illustrated on Figure 3.1 where both client and AP are laptops with WLAN card. Using PCAP we could actually capture all packets arriving to WLAN card, including beacons (in our experiments we used only beacons), and the packets reported were not translated - they included prism header, MAC header and payload.

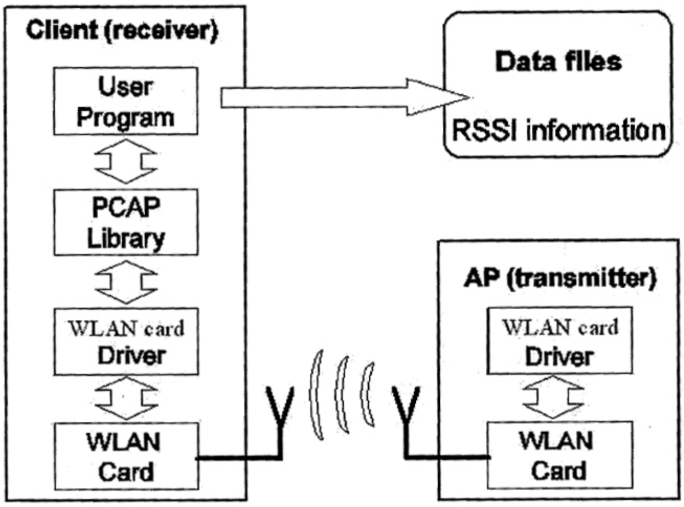

Figure 3.1 Software architecture of AP and client

Basic packet capture program (as it was provided by supervisors) consists of a main method and a callback function. In the main method the network device is opened, filtering is prepared, and a loop for capturing packets is started. This loop calls callback function, each time a packet is captured. In the callback function data from packets is collected and/or printed. The structure of the prism header was already defined as a type, to make it easy to locate data.

We modified this program so that it suits our needs. (See appendix A, page 34) We first set filtering in the main method, so that only packets from our AP are captured. To do that we located source MAC address in MAC header, rewrote the filter expression, compiled the filter, and applied it. We also located MAC time in prism header and modified the callback function so that it prints the received power and MAC time in two textual files. We introduced some variables to calculate average, minimal and maximal received signal power. Those values were printed on the screen for a better immediate control of our measurements.

The results from the textual files were analyzed and plotted using four Matlab programs – one for each experiment. (See appendix B, page 36)

3.2 ESTIMATING DISTANCE – POWER GRADIENT

3.2.1 Description of the experiment

Idea

The starting point of this set of experiments is the indoor propagation model, with the distance – power relation

$$P_r = \frac{P_0}{d^{\alpha}}$$

The distance – power relation, where P_r and P_0 are expressed in decibels relative to one milliwatt, is given by

$$P_r \text{dBm} = P_0 \text{dBm} - 10\alpha \log_{10} d$$

If we measure received power at different distances, and plot P_rdBm against $\log_{10}d$, we can estimate α (distance – power gradient) from the slope of the best-fit line through the measurements. The aim of this experiment was to estimate α for different indoor settings.

Realization

Measurements were carried out in three different settings:

1. "Open corridor" – in the half-open (west) corridor at the 3rd floor of ITU building, AP was fixed at one end of the corridor, and measurements were taken every 2m from the AP. (Figure 3.2)
2. "Closed corridor" – in the closed corridor (wing D) at the 3rd floor of ITU building, AP was fixed at one end of the corridor, and measurements were taken every 2m from the AP.
3. "Between floors" – in the half-open (west) corridor of ITU building, AP was fixed at one end of the corridor on the 2nd floor, and measurements were taken on the 3rd floor, with 2m distance between measurements. We measured the height of one floor, so we could calculated the distance from AP to MS.

We used Matlab to plot the data and to calculate α. For every distance we plotted all measured values of received power, and the average received power. Distance – power gradient α was calculated from all measured values by least squares fitting method. We also calculated correlation coefficient, which gives the overall quality of a least squares fitting. Perfect fit has a correlation coefficient of 1, while uncorrelated data results in a correlation coefficient of 0.

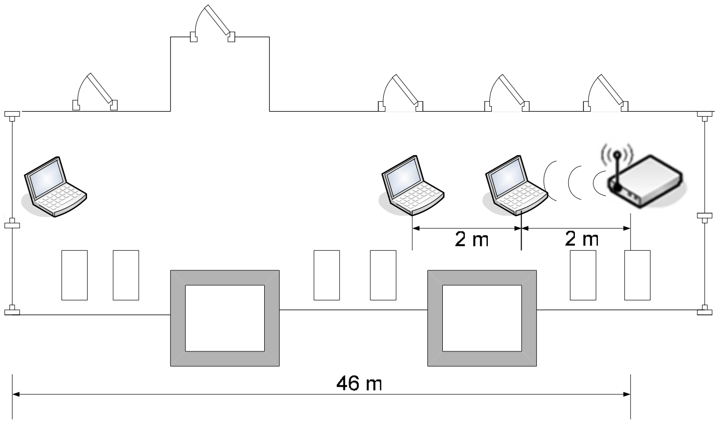

Figure 3.2 Estimating α in the open corridor

Expectations

We expected the distance – power gradient to be slightly less than 2 in the open corridor. In the closed corridor we expected to find a value smaller than in the open corridor. In between floors we expected to find α larger than in the open corridor, due to attenuation of the ceiling/floor.

3.2.2 Results

Measured received power values, estimations of distance – power gradient and correlation coefficients obtained for three different settings are shown in Figure 3.3, Figure 3.4 and Figure 3.5.

3.2.3 Conclusion

Received power values measured in the open corridor are not significantly different form those measured in the closed corridor. The estimated distance – power gradients are in both cases smaller than 2, and α value obtained from the closed corridor is smaller. All that is in accordance with the indoor propagation model and with our expectations.

Received power measured in between floors is significantly smaller due to attenuation of ceiling/floor, just as expected. In contrast to our expectations, α value obtained from those measurements is smaller than 2 and almost equal to open corridor setting. It could be concluded that the attenuation is constant, contributing only to P_0 value, and not contributing to α. However, we are not drawing any conclusions here (in light of our later experiment with antenna's omnidirectionality), because measurements were not made on the straight line from antenna: some of the measurements were actually made directly above antenna, and some were made 46m further down the corridor, almost in antennas horizontal plane.

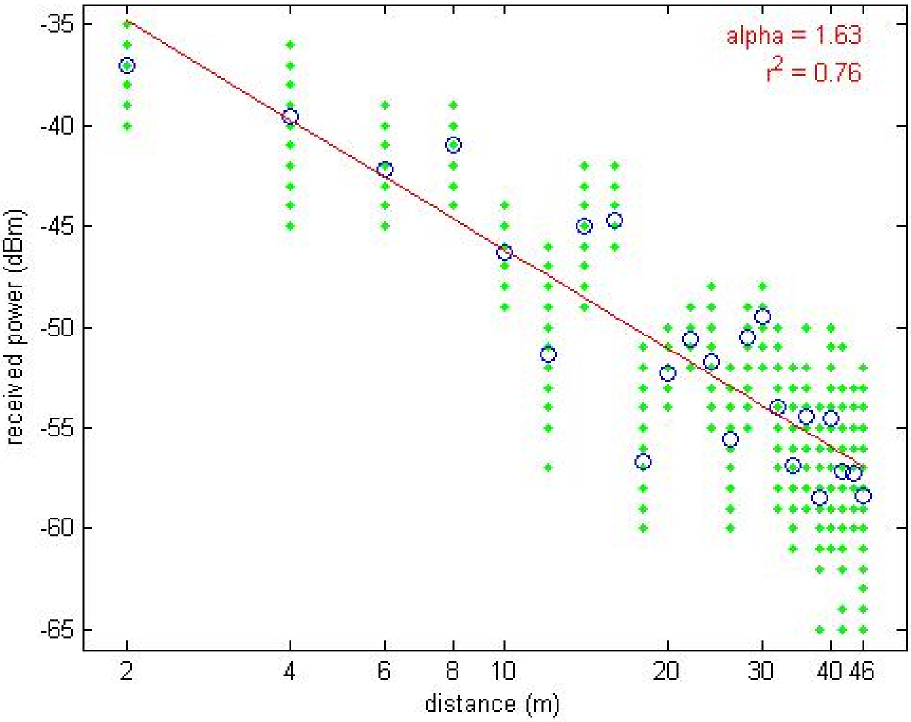

Figure 3.3 Open corridor, power – distance plot

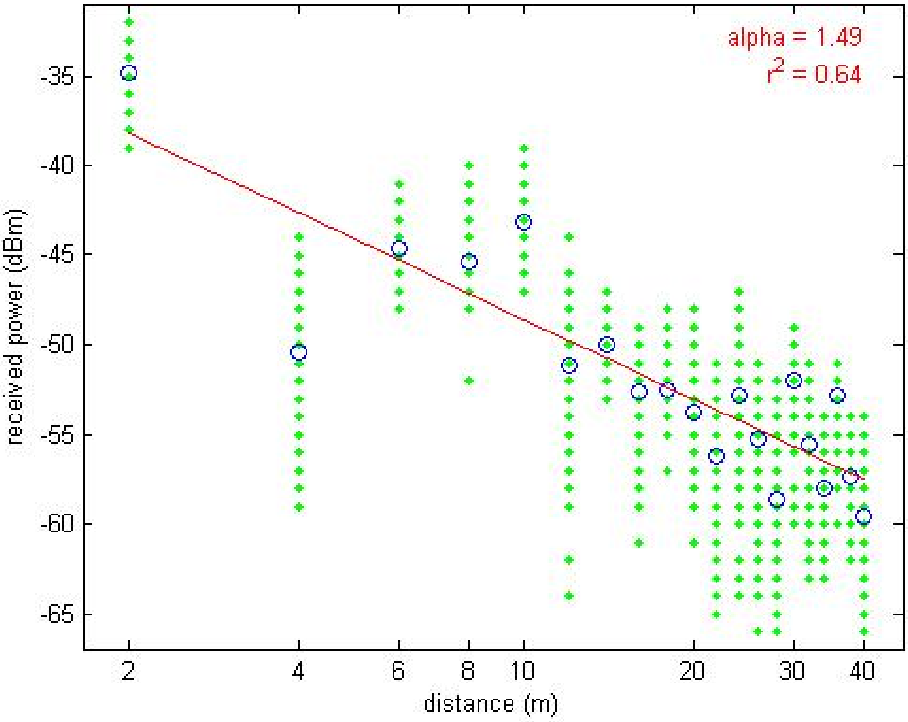

Figure 3.4 Closed corridor, power – distance plot

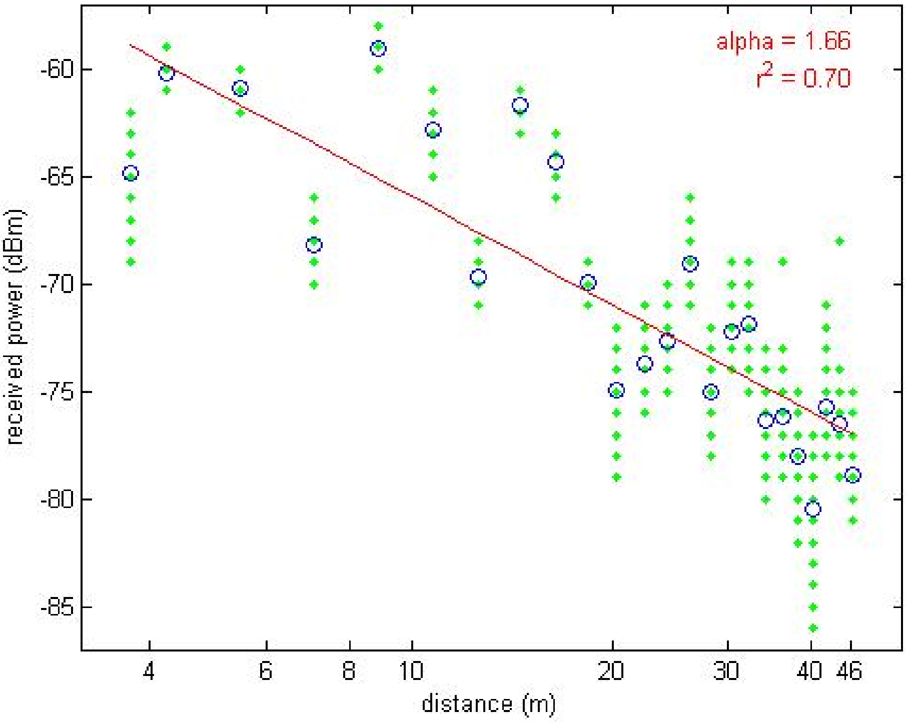

Figure 3.5 Between floors, power – distance plot

3.3 DETECTING PEOPLE BETWEEN ACCESS POINT AND MOBILE STATION

3.3.1 Description of the experiment

Idea and expectations

The aim of this experiment was to find out if we are able to detect people moving or standing in between AP and MS. We expected that the power received when there is a person standing on LOS between AP and MS would be smaller than the power received when there are no obstacles. We didn't know how strong that influence would be, so we wanted to investigate possibilities of detecting people between AP and MS.

We decided to plot the measured received power against MAC time, to get a more realistic picture then if assuming equal time intervals between packets.

Realization

We put the AP and MS on 2m distance and measured received power in 3 situations:

1. "No obstacles" – all packets were received without any obstacles on LOS.
2. "Crossing LOS" – 3 persons were repeatedly crossing LOS, while the measurements were taken.
3. "Standing on LOS" – 3 persons were standing on LOS while the measurements were taken.

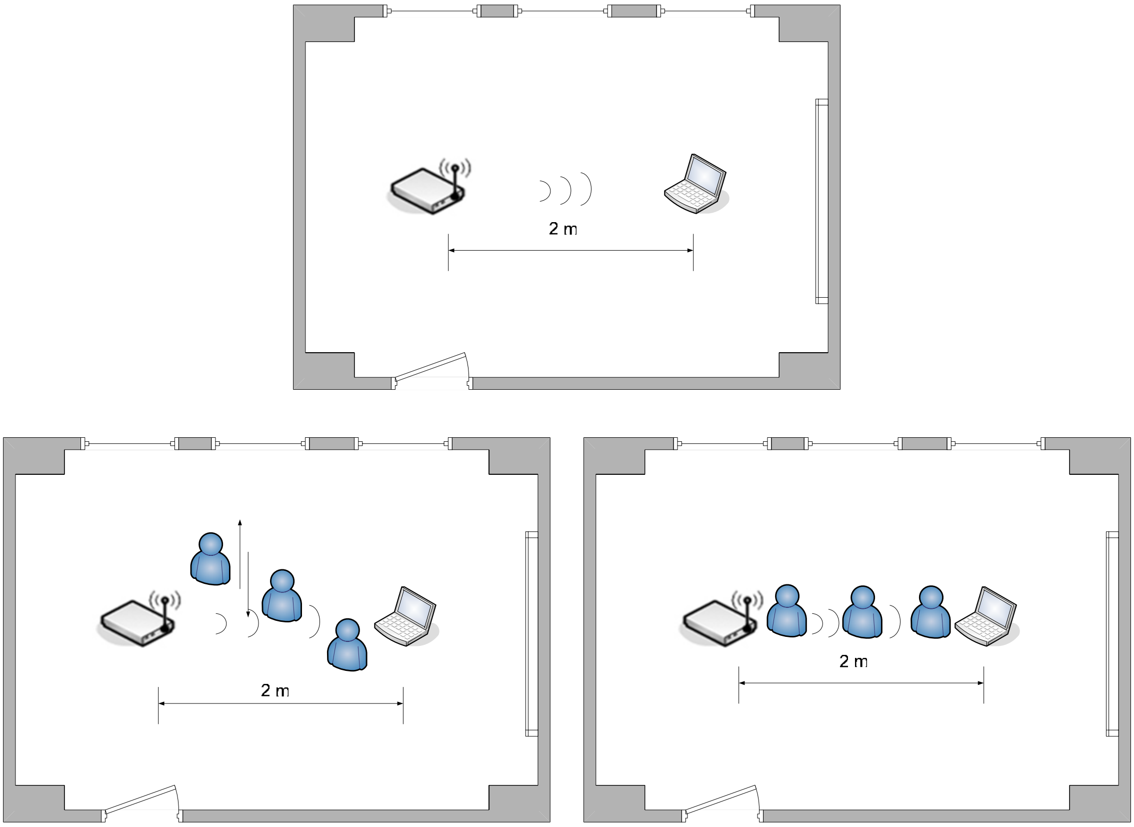

Figure 3.6 Detecting people, up: no obstacles, down left: crossing LOS, down right: standing on LOS

We did the experiment with 3 persons, because we wanted to be sure to detect obstacles on our plots. We repeated the experiment a few times, to be able to see a pattern.

3.3.2 Results

The results of our experiment are shown on Figure 3.7 where the blue line represents situation with no obstacles, the green line represents crossing LOS situation, and the red line represents standing on LOS situation. The average received power, range of measured values, and minimal and maximal measured value for each situation are shown in Table 3.1.

The results of a repeated experiment are shown in Figure 3.8 and Table 3.2.

Table 3.1 Detecting people, attempt 1

	Average received power (dBm)	Range of received powers (dBm)	Minimal received power (dBm)	Maximal received power (dBm)
No obstacles	-31.5	7	-35	-28
Crossing LOS	-36.8	19	-48	-29
Standing on LOS	-42.8	8	-47	-39

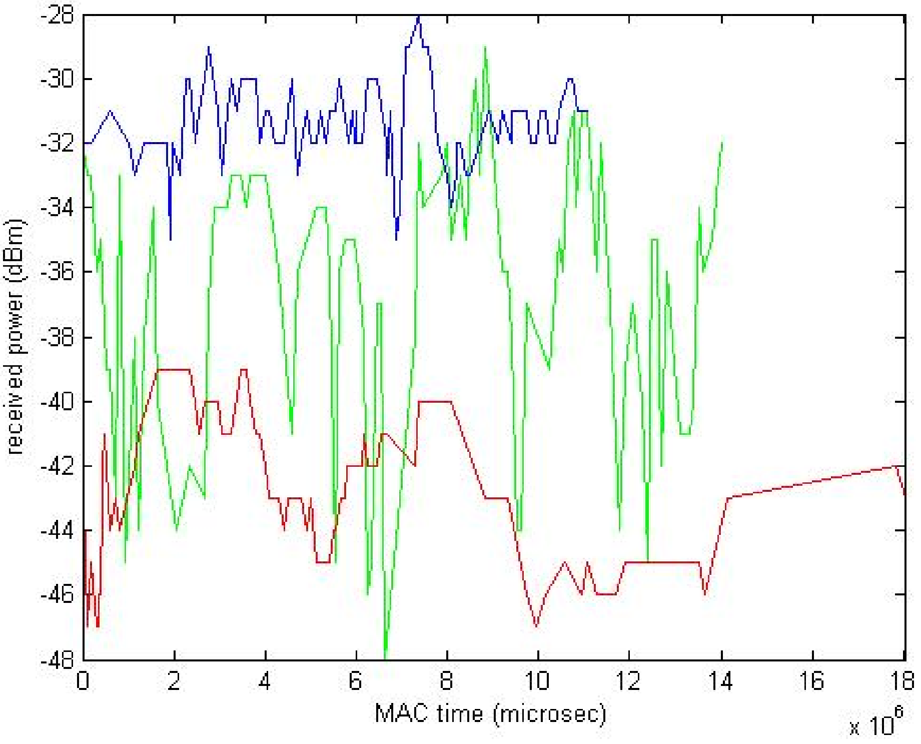

Figure 3.7 Detecting people - attempt 1

Table 3.2 Detecting people, attempt 2

	Average received power (dBm)	Range of received powers (dBm)	Minimal received power (dBm)	Maximal received power (dBm)
No obstacles	-34.4	6	-36	-30
Crossing LOS	-36.6	21	-50	-29
Standing on LOS	-48.2	9	-53	-44

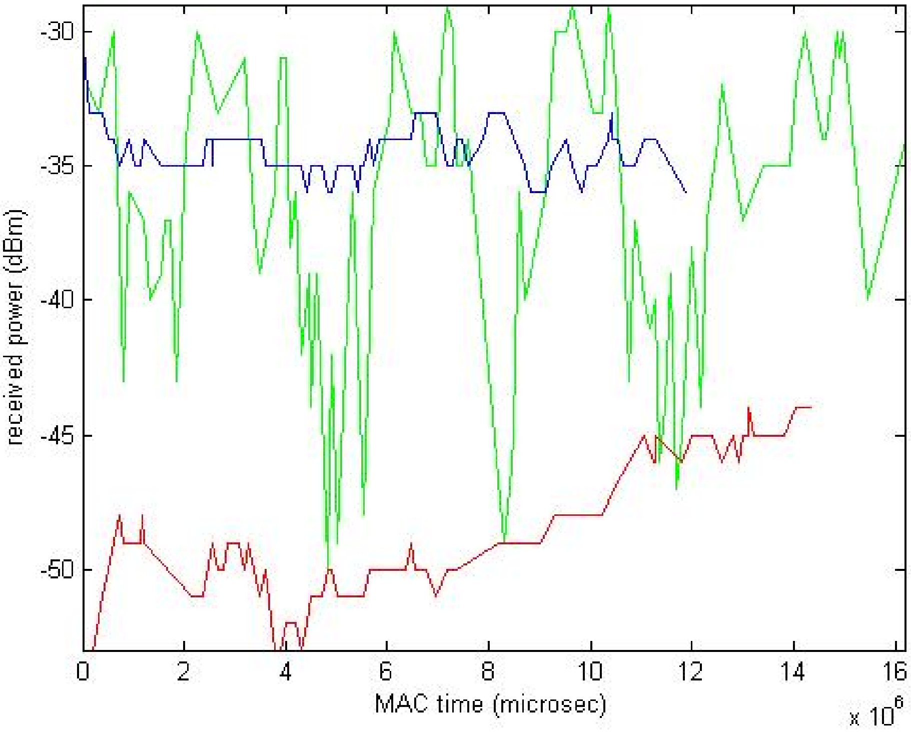

Figure 3.8 Detecting people - attempt 2

3.3.3 Conclusion

From the results of our experiment we can conclude that 3 persons crossing or standing on LOS decrease the signal strength for approximately 10dBm, which is more than the normal fluctuation of signal strength. Indeed, even the worst measurement without any obstacles was always better then the best measurement with 3 persons standing on LOS. Therefore it is not difficult to detect 3 persons standing on LOS. The received power measured when people were crossing LOS is, as expected, oscillating greatly and taking the values of both the situation without obstacles and the situation where people were standing on LOS.

Looking at the plots, we noticed that the time needed to receive 100 packets is shortest in the situation where there were no obstacles on LOS. The only packets exchanged between our AP and MS were beacons, and we can assume that beacons are transmitted with more-or-less constant frequency. Therefore we concluded that some packets were lost when there were people between AP and MS compared to no obstacles situation.

The logical continuation of this experiment would be to try to detect one person moving or standing between AP and MS.

3.4 TESTING ANTENNAS OMNIDIRECTIONALITY

3.4.1 Description of the experiment

The aim of this experiment was to test if the antenna of our AP is omnidirectional. Omnidirectional antenna radiates uniformly in all directions, or at least in the horizontal plane. We chose to put the AP and MS at the fixed positions and to rotate the antenna, measuring the signal strength for the different angles.

The antenna of our AP looks like a rod that is normally pointing upwards, but it could also be tilted. So it was possible to do two sets of measures (Figure 3.9):

1. Testing antenna's omnidirectionality in the horizontal plane. The antenna of AP was pointing upwards, the AP was rotated in the horizontal plane and the received signal power was measured at the fixed distance. We didn't expect great variations of signal strength. We did expect some slight variations and we believed that those variations would be symmetrical. We decided to test the whole circle so that we could notice the symmetry. AP was rotated for 15 degrees between measurements. The distance was first 1m, and we repeated the experiment at 2m distance. We expected to find great similarity between those two sets of measures.
2. Testing antenna's omnidirectionality in the plane containing antenna's rod. We made a series of measurements where the tip of the antenna was first pointing to MS, and then we gradually tipped it upwards, and finally tipped it down again so that it points away from the MS. The distance was 1m, and the antenna was tilted for 15 degrees between measurements. We expected that received power would be greatest when the antenna is pointing upwards, and that the power will be minimal when antenna is pointing to or away from MS.

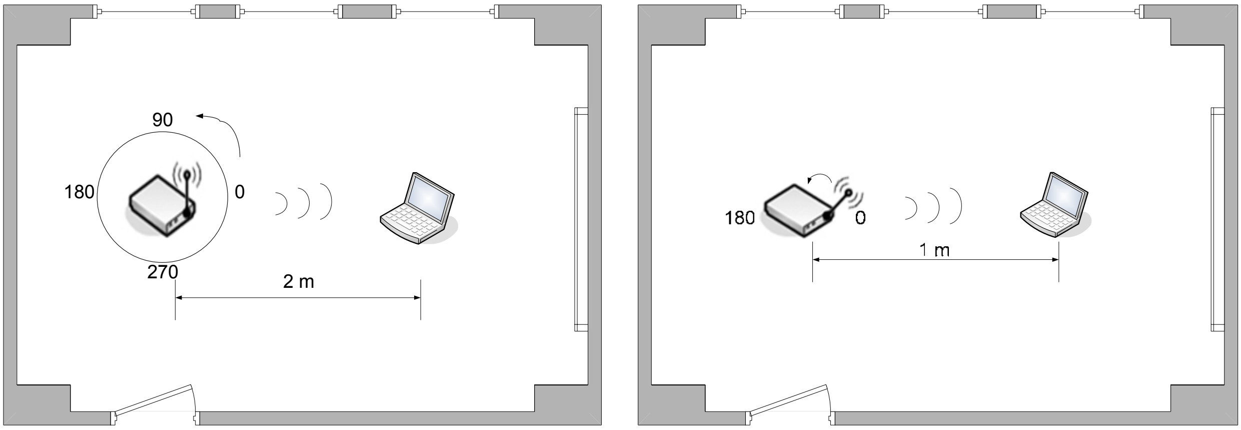

Figure 3.9 Testing antennas omnidirectionality

3.4.2 Results

Results of the first part of the experiment, testing antenna's omnidirectionality in the horizontal plane, are shown in Figure 3.10 and Figure 3.11. The line is drawn through the average received power for a given angle. Results of testing antennas omnidirectionality in the plane that contains antenna's rod are shown in the Figure 3.12. The angle in this plot is the angle between antenna's rod and the line connecting AP and MS.

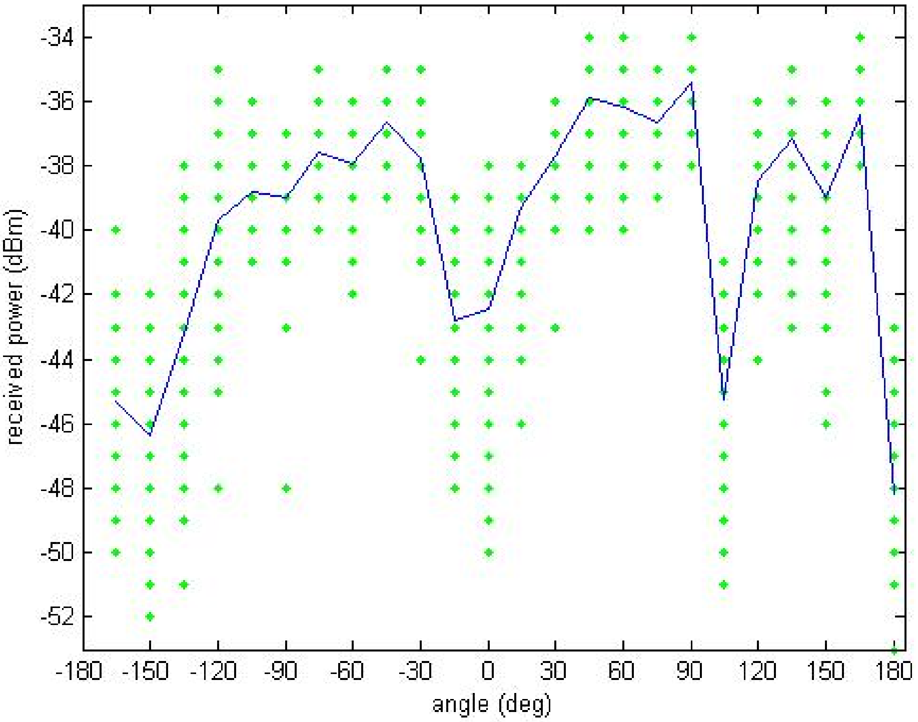

Figure 3.10 Testing omnidirectionality in horizontal plane, distance 1m

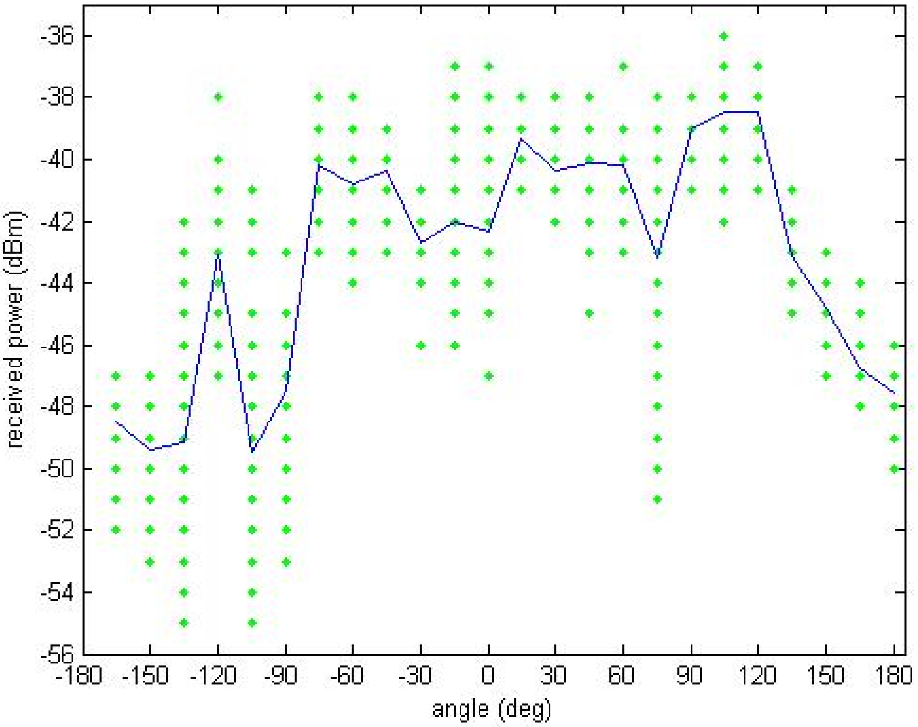

Figure 3.11 Testing omnidirectionality in horizontal plane, distance 2m

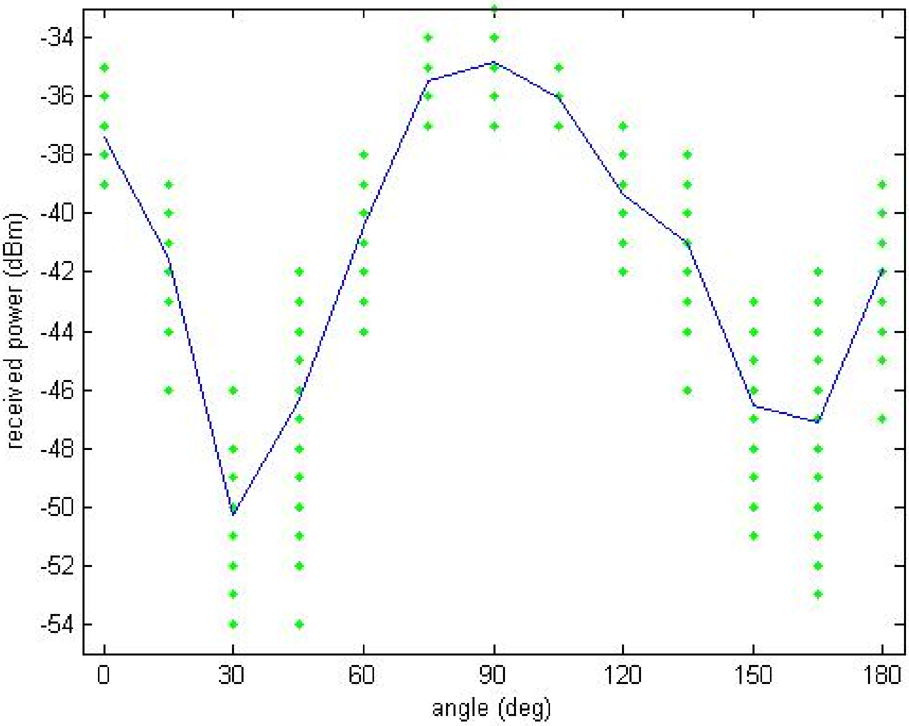

Figure 3.12 Testing omnidirectionality in the plane containing the antenna

3.4.3 Conclusion

The variations of received power measured in antenna's horizontal plane were greater then we expected (greater than 10dBm). There are traces of symmetry in the measurements, and traces of similarity between measurements at 1m and 2m, but those are not as evident as we expected. Still, we can conclude that the antenna of our AP is not omnidirectional in the horizontal plane.

As expected, the variations in the received power were greater when we were tilting the antenna. In this case the plot is also nicely symmetrical. As expected, the power received was maximal when the antenna was pointing upwards, but, contrary to our expectations, the minimal power was measured for the angle of 30 degrees, and not when the antenna is pointing to or away from the MS. Still, we can conclude that tilting the antenna greatly influences the reception of the signal.

3.5 FINDING RELATION BETWEEN ROOM SIZE AND RECEIVED SIGNAL POWER

3.5.1 Description of the experiment

Idea and expectations

With this experiment we tried to detect the multipath component of received power. The idea was to try to keep the LOS component fixed, by keeping AP and MS in the same relative position, and to make multipath components as different as possible. We expected multipath components to be greater in small rooms, because AP–wall–MS distance is smaller. Therefore we expected to measure greater received power in smaller rooms.

Realization

We measured the power received at 2m distance from AP. Measurements were carried out in the rooms of different sizes at ITU: toilet, kitchen, classroom 3A18, classroom 2A12, study room and the hall. In each room we placed the AP and MS at the room's center. We measured the area of each room, but we disregarded the height. Plotting received power against the area of the room was unpractical, so we plotted the received power values against the room's diagonal on the logarithmic scale and by doing so we keep the same dimension as in the experiment of estimation alpha.

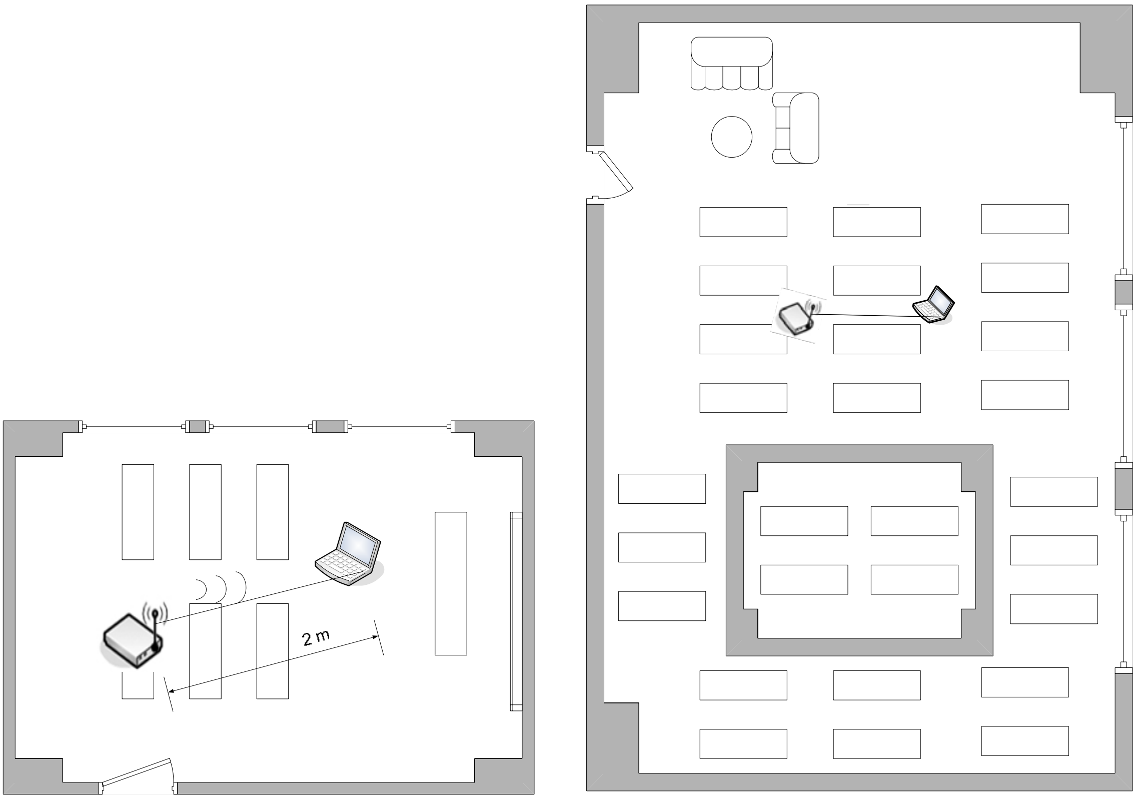

Figure 3.13 Measuring received signal power in the classroom and in the study room

3.5.2 Results

The measured values are shown in Figure 3.14.

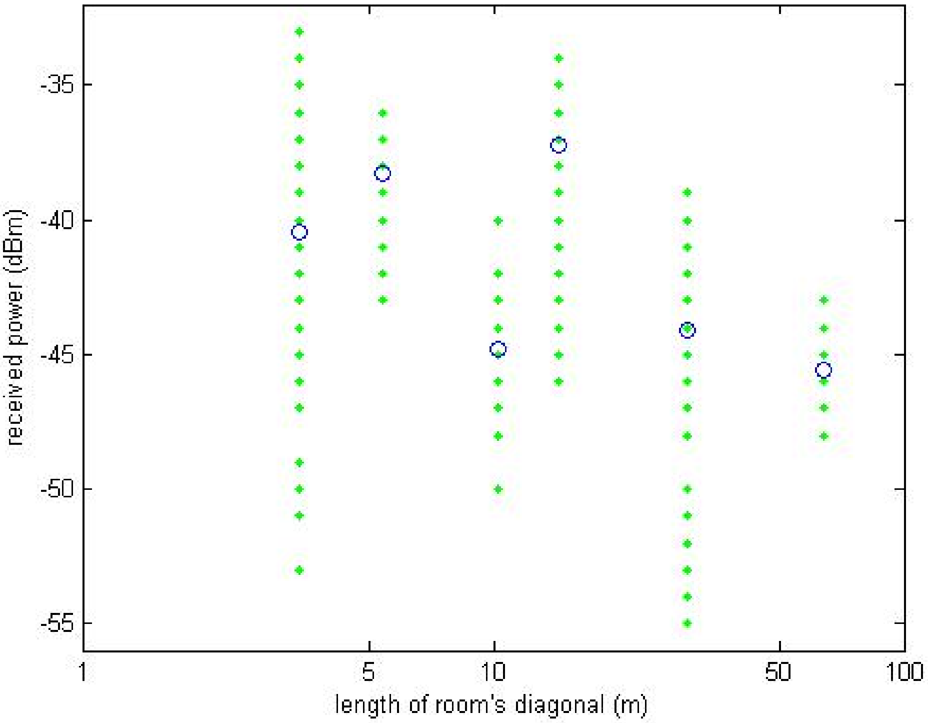

Figure 3.14 Relation between room's size and received power

3.5.3 Conclusion

The received power measured in the biggest room was smallest and the plot shows some characteristics of regression, but the relation between room size and received power is not as clear as we expected. We assume that the measured received power was influenced by many factors, which we could not control, for example: wall and floor material, position and the size of the windows, furniture in the room or shape of the room.

To improve this experiment, one should take the measurements in similar rooms that are differing only in size.

4 CONCLUSION

This project report is written as a closure of the “Signal Processing in WLAN, Sensor Networks and RFID” project. Both the project and the report consist of a theoretical and a practical part.

The theoretical part of the project helped us understand the flexibility and diversity of wireless LAN. Access points are by far the primary components in wireless LAN infrastructures. The 802.11 standard defines an access point as a communication hub for users of a wireless device to connect to a wired distribution system, such as an Ethernet network.

Considering sensor networks, we focused on design factors and attributes sensor networks,

Radio frequency identification (RFID) provides a means of automatic identification. It is interesting because it is a new technology.

To accomplish and fully understand the experimental part of the project we really needed to study the course material. Modifying packet capture program required some basic knowledge of C programming language and understanding the syntax of PCAP library which we didn’t posses in advance, so we learned a lot there. Retrieving and analyzing the data from the prism header and MAC header was a great practical example of how protocol stack actually works, wrapping payload by adding more and more headers for each layer.

To plan our experiment we needed to understand the principles of radio propagation. We designed a few simple experiments, so that our expectations were rather obvious. It was a pleasure to see our expectations being mostly fulfilled – the world is really behaving as we imagined it will be!

When processing the results of our experiments we were able to use and improve our Matlab programming skills.

All in all we feel that this project has given us a good basic understanding of wireless networking especially wireless LAN and by carrying out the experiments, we learned to understand principles of indoor radio propagation.

APPENDICES

A. Software for measuring received signal power

```
/**************running example*************************
Here is the command to compile this program:
[root@localhost]# gcc -o test test.c /usr/local/lib/libpcap.a */

#include <stdio.h>
#include <pcap.h>
#define _BSD_SOURCE 1
#define SIGNAL_LEVEL_TO_DBM(s)  (s-100)

int counter = 0;
int total_dbm = 0;
int min_dbm = 100;
int max_dbm = -200;
FILE* power_file; /* For saving signal power */
FILE* time_file; /* For saving MAC time */

typedef struct p80211item
{
   unsigned long   did;
   unsigned short  status;
   unsigned short  len;
   unsigned long   data;
} p80211item_t;

typedef struct prism_header
{
   unsigned long   msgcode;
   unsigned long   msglen;
   unsigned char   devname[16];
   p80211item_t    hosttime;
   p80211item_t    mactime;
   p80211item_t    channel;
   p80211item_t    rssi;
   p80211item_t    sq;
   p80211item_t    signal;
   p80211item_t    noise;
   p80211item_t    rate;
   p80211item_t    istx;
   p80211item_t    frmlen;
} prism_header_t;

pcap_t *descr; /* Session handler */

void callback_ReceivePacket (u_char *args, const struct pcap_pkthdr *header,
          const u_char *packet)
{
   prism_header_t* pPrismHeader = (prism_header_t*)packet;
   char dbm =  SIGNAL_LEVEL_TO_DBM(pPrismHeader->signal.data);
   long time = pPrismHeader->mactime.data;

   /* Collecting and saving data */
   counter++;
   total_dbm = total_dbm + dbm;
   if (dbm<min_dbm) min_dbm = dbm;
   if (dbm>max_dbm) max_dbm = dbm;

   printf("signal strength: %d\n", dbm);
   printf("counter: %d\n", counter);
   printf("\n");
   fprintf(power_file, "%d ", dbm);
   fprintf(time_file, "%d ", time);

   return;
}

int main(int argc, char** argv)
{
   int average;
   int ret = 0;

   bpf_u_int32 mask; /* Net mask */
   bpf_u_int32 net; /* IP */
   char errbuf[PCAP_ERRBUF_SIZE]; /* Error string */
   struct bpf_program fp; /* Compiled filter expression */
   char filter_app[] = "ether[154]==0x00 && ether[155]==0xa0 && "
           "ether[156]==0xc5  && ether[157]==0x9b && ether[158]==0x90 "
           "&& ether[159]==0x99"; /* Filter expression - source MAC address */
   //char filter_app[] = "\0";

   power_file = fopen("power.txt", "w");
   time_file = fopen("time.txt","w");

   /* Opening the network device for packet capture */
   descr = pcap_open_live("wlan0", BUFSIZ, 1, 0, errbuf);
   if (descr == NULL){
           printf("pcap_open_live(): %s\n", errbuf);
           exit(1);
   }

   /* Obtaining net mask and IP*/
   pcap_lookupnet("wlan0",&net,&mask,errbuf);

   /* Compiling filter expression into filter program */
   if (pcap_compile(descr, &fp, filter_app, 0, net) == -1){
           printf("pcap_compile: filter syntax error\n");
           exit(1);
   }

   /* Applying the filter */
   if (pcap_setfilter(descr, &fp) == -1){
           printf("pcap_setfilter failed\n");
           exit(1);
   }

   printf("Initialization is fine, start sniffing wlan0 now..\n");

   /* Capturing 100 packets, calling callback routine for each packet */
   ret = pcap_loop(descr, 100 , callback_ReceivePacket, NULL);

   /* Calculating and printing control values */
   average = total_dbm/counter;
   printf("Number of received packets: %d\n", counter);
   printf("Average signal power: %d\n", average);
   printf("Minimal received signal power: %d\n", min_dbm);
   printf("Maximal received signal power: %d\n", max_dbm);
   printf("\npcap_loop stopped, the return value is % d\n", ret);

   pcap_close(descr);
   fclose(power_file);
   fclose(time_file);
   return(0);
}
```

B. Matlab programs for analyzing and plotting the results

Plotting received power against distance on logarithmic scale

```
function PowerDistancePlot(n,f)

s=0;
if (nargin == 1)
    f=0;
    s=2;
end

% input
d=[];
dbm=[];
averagedbm=[];
da=[];

for k=s:2:n
    fileName = sprintf('power%03d.txt',k);
    tempdbm = load(fileName);
    d = [d, k*ones(1, length(tempdbm))];
    dbm = [dbm, tempdbm];
    averagedbm = [averagedbm, mean(tempdbm)];
    da = [da,k];
end

% corection of distance if in between floors
d=(d.^2 + (f*3.75)^2).^0.5;
da=(da.^2 + (f*3.75)^2).^0.5;

% plotting input data
d=log10(d);
da=log10(da);
plot(d,dbm,'.g');
hold on;
plot(da,averagedbm,'ob');

% calculating distance-power gradient
x=[d(:), ones(length(d),1)];
y=dbm';
a=x\y;
alpha=-a(1)/10;

% plotting the line
y=x*a;
plot(d,y,'r');

% calculating correlation coefficient
x2=[dbm(:), ones(length(dbm),1)];
y2=d';
a2=x2\y2;
r2=a(1)*a2(1);

% labels, text
xlabel('log10 of distance (m)');
ylabel('received power (dBm)');
tb = sprintf('alpha = %4.2f\nr^2 = %4.2f',alpha,r2);
text(max([d]),max([dbm,y']),tb,...
    'VerticalAlignment','top','HorizontalAlignment','right','color','r');
hold off;
```

Plotting received power against MAC time

```
function PowerTimePlot

% input
t0=load('time0.txt');
dbm0=load('power0.txt');
t1=load('time1.txt');
dbm1=load('power1.txt');
t2=load('time2.txt');
dbm2=load('power2.txt');

% calculating relative time
t0=t0-t0(1)*ones(1,length(t0));
t1=t1-t1(1)*ones(1,length(t1));
t2=t2-t2(1)*ones(1,length(t2));

% plotting
plot(t1,dbm1,'g',t0,dbm0,'b',t2,dbm2,'r');
xlabel('MAC time (microsec)');
ylabel('received power (dBm)');
axis([0, max([t0,t1,t2]), min([dbm0, dbm1, dbm2]), max([dbm0, dbm1,
dbm2])])

% analyzing data
average0=mean(dbm0)
range0=range(dbm0)
minmax0=[min(dbm0),max(dbm0)]
average1=mean(dbm1)
range1=range(dbm1)
minmax1=[min(dbm1),max(dbm1)]
average2=mean(dbm2)
range2=range(dbm2)
```

Plotting received power against angle

```
function PowerAnglePlot(n,f)

if (nargin == 1)
    f=0;
end

% input
ang=[];
dbm=[];
averagedbm=[];
anga=[];

for k=0:15:n
    fileName = sprintf('power%03d.txt',k);
    tempdbm = load(fileName);
    ang = [ang, k*ones(1, length(tempdbm))];
    dbm = [dbm, tempdbm];
    averagedbm = [averagedbm, mean(tempdbm)];
    anga = [anga,k];
end
```

```
% shifting angles so that center of symmetry is 0 deg
if (f==1)
    ang=ang-135;
    anga=anga-135;
    ang=[ang(2201:2400)-360, ang(1:2200)];
    dbm=[dbm(2201:2400),dbm(1:2200)];
    anga=[anga(23:24)-360,anga(1:22)];
    averagedbm=[averagedbm(23:24),averagedbm(1:22)];
end

% plotting
plot(ang,dbm,'.g');
hold on;
plot(anga,averagedbm,'-b');
xlabel('angle (deg)');
ylabel('received power (dBm)');
hold off;

average = mean(dbm)
rangedbm = range(dbm)
```

Plotting received power against room’s diagonal on logarithmic scale

```
function PowerSizePlot

l=[8.85, 4.45, 2.7, 61.0, 26.6, 11.75];
w=[5.25, 3.0, 2.0, 18.75, 13.1, 8.4];
diag=(l.^2+w.^2).^0.5

d=[];
dbm=[];
averagedbm=[];
da=[];

% input
for k=1:length(diag)
    fileName = sprintf('power%02d.txt',k);
    tempdbm = load(fileName);
    d = [d, diag(k)*ones(1, length(tempdbm))];
    dbm = [dbm, tempdbm];
    averagedbm = [averagedbm, mean(tempdbm)];
    da = [da,diag(k)];
end

% plotting input data
d=log10(d);
da=log10(da);
plot(d,dbm,'.g');
hold on;
plot(da, averagedbm,'ob');
xlabel('log10 of diagonal(m)');
ylabel('received power(dBm)');
```

BIBLIOGRAPHY

[1] Matthew S. Gast, ”802.11 Wireless Networks,” O'Reilly & Associates INC, pp 7-197, 2002.

[2] “What is wireless network?” http://www.winncom.com/html/wireless.shtml#1

[3] Ed Callaway Paul Gorday, Lance Hester, Jose A. Guiterrez Marco Naeve, Bob Heile, and Venkat Bahl, “Home Networking with IEEE 802.15.4,” IEEE Communications Magazine, pp. 70-77, August 2002.

[4] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Network,” IEEE Communications Magazine, pp. 102-114, August 2002.

[5] Deborah Estrin, David Culler, Kris Pister, and Gaurav Sukhatme, “Connecting the Physical World with Pervasive Networks,” PERVASIVE Computing, pp. 59-69, January-March 2002.

[6] Chee-Yee Chong and Srikanta P. Kumar, ”Sensor Networks: Evolution, Opportunities, and Challenges,” Proceedings of the IEEE, VOL.91, NO. 8, pp. 1247-1256, August 2003.

[7] “RFID Background,” http://www.seeburger.info/com/

[8] “Properties of RFID systems,” http://www.liberty-human-rights.org.uk/privacy/rfid-parli-briefing.pdf

[9] “Types of RFID systems,” http://rapidttp.com/transponder/

[10] Kaveh Pahlavan,”Wireless Information Network,” Wiley-Interscience, pp. 37-82, 1995.

[11] John Aasted Sørensen and Jianjun Chen, “Program outline,” Mobile Communications and Signal Processing group, May 2005.

[12] Andrew S. Tanenbaum, “Computer Networks,” Prentice Hall-International Editions, pp. 1996

[13] Tim Carstens, “Programming with PCAP,” http://www.tcpdump.org/pcap.htm.

[14] “PCAP,” http://www.tcpdump.org/pcap3_man.html

[15] “Packet Capture with LIBPACP and other Low Level Network Tricks”, http://www.cet.nau.edu/~mc8/Socket/Tutorials/section1.html