2002:125 CIV

LULEÅ UNIVERSITY OF TECHNOLOGY

MASTER'S THESIS

Positioning with Bluetooth, IrDA and RFID

JOSEF HALLBERG
MARCUS NILSSON

MASTER OF SCIENCE PROGRAMME

Department of Computer Science and Electrical Engineering
Division of Computer Engineering

2002:125 CIV • ISSN: 1402 - 1617 • ISRN: LTU - EX - - 02/125 - - SE

APPLE 1013

Positioning with Bluetooth, IrDA and RFID

Marcus Nilsson
Josef Hallberg

Luleå University of Technology
Department of Computer Science and
Electrical Engineering

Abstract

We are living in the information era, people are getting more mobile and the technology is constantly advancing. Technologies that were once static in location are now becoming mobile and constantly changing position. Information that never changed before must now be dynamic and change as the user is moving around. By providing a location to applications we cannot only change position related information, but also open doors to applications and functions that were not possible before.

The Alipes project was initiated at the Center for Distance-spanning Technology (CDT) in Luleå. The purpose of this project is to create an architecture for location aware applications. Several positioning systems are already supported, such as Global Positioning System (GPS), Mobile Positioning System (MPS), and WaveLAN. MPS is however not very accurate and GPS typically will not work indoors.WaveLAN has a good accuarcy and do work indoors, but is too power consuming. Thus, there is a need for a positioning system that is accurate, works indoors and has low powerconsumption.

This report focuses on three systems with low powerconsumption, capable of close range positioning indoors as well as outdoors. These systems are: IrDA, RFID and Bluetooth. As a result of an evaluation of the three systems, a Bluetooth positioning system was implemented and included into the Alipes platform.

PREFACE

This master thesis was performed at Luleå University of Technology, from September 2001 to January 2002. The thesis includes an overview of IrDA, RFID and Bluetooth as well as an evaluation of the three for positioning tasks. The thesis also describes the implementation of a Bluetooth positioning system into the Alipes platform.

The authors would like to thank: James Nord for solving our insolvable problems, Kåre Synnes for supervising our work, Sven Molin for letting the Ericsson Bluetooth starter kits be at our disposal and Per Lindgren for being our examiner. We would also like to thank all co-workers at “Programvaruteknik” (PVT)

TABLE OF CONTENTS

SECTION 1 INTRODUCTION 6

1.1 Structure of this report 6

1.2 The Alipes platform 6
1.2.1 Advantages of the Alipes Platform 6
1.2.2 The Alipes architecture 7
1.2.3 Applications on the Alipes Platform 9

1.3 Purpose and Goals 9

SECTION 2 TECHNOLOGY OVERVIEW 10

2.1 Introduction to IrDA 10
2.1.1 IrDA Protocols 10
2.1.2 IrDA Physical Layer 10
2.1.3 Ir Link Access Protocol (IrLAP) 13
2.1.4 Ir Link Management Protocol (IrLMP) 15
2.1.5 Security of IrDA 16

2.2 Introduction to RFID 16
2.2.1 How does RFID work? 16
2.2.2 Frequencies 19
2.2.3 Standards 21

2.3 Introduction to Bluetooth 21
2.3.1 Radio 22
2.3.2 Baseband 23
2.3.3 The Link Controller 25
2.3.4 The Link Manager 26
2.3.5 Logical Link Control and Adaptation Protocol 27
2.3.6 RFCOMM 28
2.3.7 The Service Discovery Protocol 28
2.3.8 Encryption and Security 29

SECTION 3 EVALUATION 32

3.1 Positioning task 32

3.2 Network 32

3.3 Exchange of position 32

3.4 Security 33

3.5 Physical aspects 33
3.5.1 Range 33
3.5.2 Power consumption 33
3.5.3 Angle 34
3.5.4 Accuracy 34

3.6 Automation 34

3.7 Reliability 35
3.7.1 Interference 35

3.7.2 Correction 35

3.8 Summary 35

3.9 Other possible technologies 36
3.9.1 Home RF 36

SECTION 4 IMPLEMENTATION OF BLUETOOTH 38

4.1 Environment 38

4.2 Design 38
4.2.1 Native 40
4.2.2 Java 40
4.2.3 Triangulation Algorithm 43

4.3 Testing 46
4.3.1 Reliability 46
4.3.2 Signal Strength 47
4.3.3 Field test 47

SECTION 5 CONCLUSION AND DISCUSSION 50

5.1 Further Work 50

REFERENCES 52

APPENDIX A. ABBREVIATIONS AND ACRONYMS 54

APPENDIX B. THE OPTIONAL IRDA PROTOCOLS 57

SECTION 1 INTRODUCTION

1.1 STRUCTURE OF THIS REPORT

The report is organized as follows:

- Section 1 – Introduction. A description of why this work was done and a description of the Alipes platform that this work was made for.
- Section 2 – Technology overview. A description of IrDA, RFID and Bluetooth, how they work and their characteristics
- Section 3 – Evaluation. We look into different aspects that are of importance for the positioning task. A comparison is made between IrDA, RFID and Bluetooth and the most suitable candidate is selected.
- Section 4 – Implementation of Bluetooth. A description of our implementation of Bluetooth on the Alipes platform.
- Section 5 – Conclusion and discussion. Conclusion and discussion of our work. Also a list of further work that could be done to enhance the performance and/or functionality.

1.2 THE ALIPES PLATFORM

Mobile applications are growing in number as more people starts to use mobile devices in their every day life. More people are also using services requiring some kind of wireless communication technology such as GSM, GPRS, UMTS, WaveLAN and Bluetooth. There are already many services available online for the mobile user but there is still a market for more services.

Providing a positioning system enables many new services to be implemented for the mobile user: Map retrieval, search for “close by” services such as restaurants and other facilities, what bus to take to get to a certain place, to name a few. This is what the Alipes project focuses on, to provide an efficient positioning platform for mobile devices.

There are many positioning systems but only a few attempts to bring these systems into one platform where they work seamlessly together. The Alipes project is one of those platforms, where several positioning systems work together and provide an architecture for location aware applications. There are several advantages to gain from bringing several positioning systems into one platform.

1.2.1 Advantages of the Alipes Platform

A few of the advantages of having a platform with several positioning sources are: Higher accuracy and use of other positioning sources not supported by the device itself.

1.2.1.1 Higher accuracy

By taking advantage of several positioning systems it is possible to give a more exact location by calculating the intersection of two positions given by different systems.

Calculating the intersection may be an all too processor intensive task for some mobile devices, in which case the position given with highest accuracy may be chosen.

1.2.1.2 Using device external positioning devices

By taking advantage of the ad hoc network functionality that some communication systems provide, a device can make indirect use of positioning systems not supported by the device itself.

Example: Device A is equipped with both GPS and Bluetooth. Device A is able to get a position using GPS. Another device, only equipped with Bluetooth may now get a position from device A by connecting via Bluetooth. Thus other devices may make indirect use of the GPS position given to device A.

1.2.2 The Alipes architecture

The architecture is devided into four sections: the Positioning Platform, the Privacy and Security handler, the Map Service and the service Infobase. Figure 1.1-1 shows the structure of the Alipes Platform, with the four sections. For detailed information about the Alipes Platform see "An Architecture for Location Aware Applications" by James Nord, Kåre Synnes, Peter Parnes at Department of Computer Science, Luleå University of Technology, Sweden.

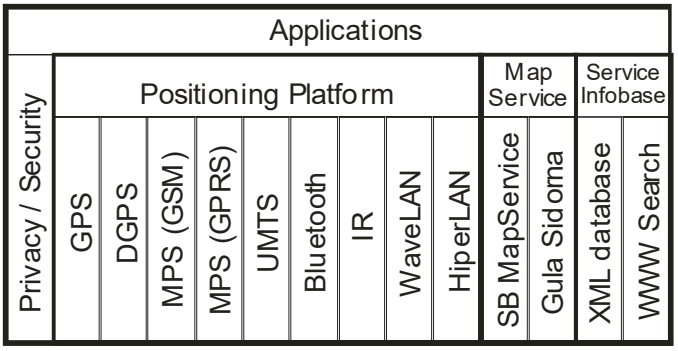

Figure 1.1-1: The Alipes Architecture

1.2.2.1 The positioning platform

The positioning platform is responsible for collecting the data from all the positioning modules and combining them into a single position with accuracy.

The platform can use both push and pull devices. Push devices send the position in constant intervals (example: GPS systems) while pull devices only send the position when requested to do so (example: MPS systems).

The results from the different positioning modules are translated into a

common format, the Generic Positioning Protocol (GPP) which is used by the platform.

1.2.2.2 Generic Positioning Protocol

Even though the different positioning systems have the same purpose, reporting a position, they are still different protocols that need a common interface in order to work together. This is the task of the Generic Positioning Protocol (GPP). There are a few required features of the GPP. These are:

1. Structured and hierarchical format, for simple parser implementation.
2. Humanly readable, to aid debugging.
3. A few simple message types:
    a. Capability request
    b. Capability reply
    c. Data request
    d. Data reply

In order to satisfy these features the protocol was implemented in XML.

1.2.2.3 Privacy and Security

Some security precautions are taken to avoid users feeling monitored or fear the information being used for unintended purposes. The user has the possibility to turn off the positioning. The user also has knowledge about how the position information is being used and/or a log of accesses to it.

The user owns his/her position and any external service has to request permission from the user's application in order to obtain the position. It is possible to query the platform for a position, but that will result in a request to the application. The application can accept, deny or ask the user to manually make the decision.

To avoid security breaches positioning sources are divided into two groups: trusted and non-trusted positioning sources. Trusted are those sources which the user can authenticate, such as a GPS module. Non trusted sources are other mobile devices within WaveLAN or Bluetooth range that have no method for authentication. In this case the positioning platform will prioritize trusted sources.

To keep false information at a minimum, no positioning information gained via peer to peer will be forwarded to other devices. Thus no Bluetooth or WaveLAN device will forward any position gained from another Bluetooth or WaveLAN device.

1.2.2.4 Map Service

The map service allows an application to retrieve maps for a certain position. The service is built on a scheme that will make the service generic and simple to change when it comes to the underlying map database and retrieval system. It can use several map databases such as

the Telia Yellow Pages (Gula Sidorna) in Sweden. The service will also return the most suitable map for the situation, based on the scale of the requested map.

1.2.2.5 Service Infobase

The service infobase provides methods for finding published services by searching a database or the internet for information that matches the criteria. An example of this could be a user searching for a restaurant in the immediate vicinity. The service can then search the database for restaurants and return the matches, and in some cases even further information such as a guide of how to get there or even a menu.

1.2.3 Applications on the Alipes Platform

The Alipes Platform provides a good base for applications in need of position information. Two examples of application using the Alipes Platform are FriendFinder and Geonotes.

FriendFinder is an application, based on simple map navigation, where the positions of registered friends are marked on the map.

GeoNotes is a system for virtual notes on a physical location, much like placing Post-It notes on the walls around you.

1.3 PURPOSE AND GOALS

The purpose of this work is to find the most suitable communication system to implement for short range positioning. There are a few requirements that the system should be able to fulfill. These requests are listed below, in order of importance.

1. It should be able to use the methods, provided by the Alipes platform, to position a mobile terminal.
2. It should be able to provide a connection (network) because it enhances the value of the position. With a network connection relevant information can be downloaded, such as maps.
3. It should be able to exchange positioning information between clients.

Based on these requirements the best suitable communication system should be implemented, tested and integrated into the Alipes Platform.

SECTION 2 TECHNOLOGY OVERVIEW

2.1 INTRODUCTION TO IRDA

IrDA (Infrared Data Association) is a communication system based on infrared light. It is commonly used in mobile devices for cheap point-to-point communication. Digital cameras, mobile phones and laptops are just a few examples of devices that often use IrDA for wireless communication.

2.1.1 IrDA Protocols

IrDA Protocols consist of a mandatory set of protocols and a set of optional protocols. Figure 2.1-1 shows how the IrDA protocol stack is layered. The most important protocols are of course the mandatory protocols: PHY (Physical Signaling Layer), irLAP (Link Access Protocol) and IrLMP (Link Management Protocol).

Among the optional protocols Tiny TP, IrTran-P, IrOBEX, IrLAN, IrCOMM and IrMC can be found. A brief description of these protocols can be found in Appendix B.

<table>
<tr><td>IrTran-P</td><td>IrOBEX</td><td>IrLAN</td><td>IrCOMM</td><td>IrMC</td></tr>
<tr><td>LM-IAS</td><td colspan="4">Tiny Transport Protocol – Tiny TP</td></tr>
<tr><td colspan="5">Ir Link Magement - MUX - IrLMP</td></tr>
<tr><td colspan="5">Ir Link Access Protocol - IrLAP</td></tr>
<tr><td colspan="2">Asynchronous Serial Ir
9600bps – 115.2kbps</td><td colspan="2">Synchronous Serial Ir
1.152 Mbps</td><td>Synchronous 4PPM
4Mbps</td></tr>
</table>

Figure 2.1-1: The IrDA Data Protocols

2.1.2 IrDA Physical Layer

The physical layer contains the actual Ir transducer module. The physical layer is responsible for transmitting and receiving Ir signals and also encode/decode these signals for the IrLAP layer.

In figure 2.1-2 we can see an IR transducer module. This figure shows the electrical signal going from a serial bit stream in stage [1] to an optical signal in stage [3]. The electrical signals in stage [2] correspond to the optical signals at [3].

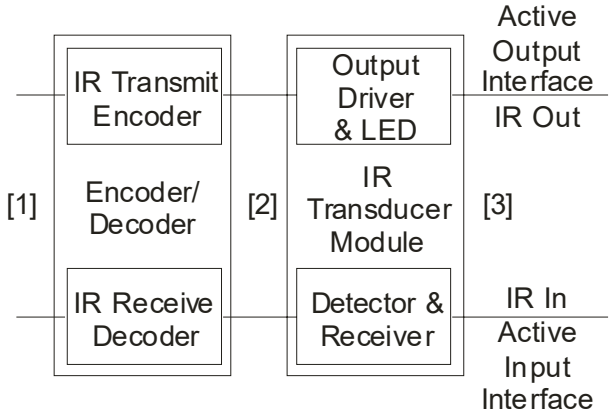

Figure 2.1-2: Ir Transducer Module

Though there are many aspects of the physical layer to learn, only a few of them are interesting for positioning. Such aspects are: physical aspects as acceptable range and angle, interference, capacity and formats.

2.1.2.1 Physical aspects of the IrDA Physical Layer

As Ir is light being transmitted there are several limitations in range and angle that other systems, like radio links, do not have. These limitations consist of limited range, line of sight and limited viewing angles.

Range of an IrDA device

The range is at least one meter and in some cases even up to two meters. There is also a low power version and the range for that is typically 20-30 cm depending. As of now the range is fairly short but ranges up to ten meters are under development, though this will still be limited to line of sight as well as limited transmitting and receiving angles.

Optical angle limitations of an IrDA device

The figure 2.1-4 shows how the optical signals are limited by angles in the transmitter and receiver. The transmitter has a typical limitation of 15° to 30° from the optical axis, also called half angle as shown in figure 2.1-3. The receiver is limited to 15° half angle or just above, which can be seen in figure 2.1-4.

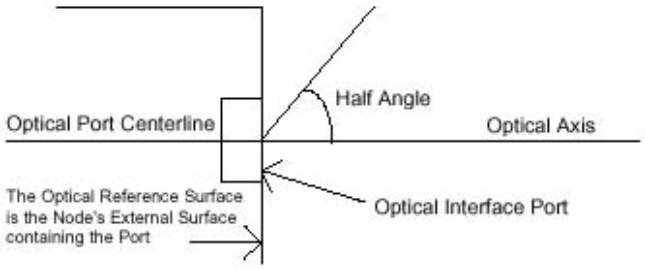

Figure 2.1-.3: Optical port geometry

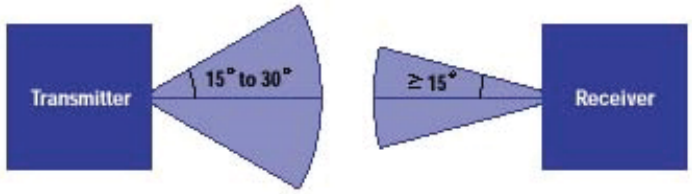

Figure 2.1-4: Optical angle limitations

Power consumption

IrDA has low power consumption and there are several procedures for saving power such as sniffing which will be described later. There is also a low power version with less range as mentioned earlier. This version consumes 10 times less power compared to the standard version.

2.1.2.2 The capacity and formats of the IrDA physical layer

The IrDA physical layer is split into three distinct data rate ranges: 2400bps to 115,200bps, 1.152 Mbps, and 4 Mbps. Initial protocol negotiations takes place at 9600 bps, making this data rate compulsory. All other rates are optional and can be added if a device requires a higher data rate.

Infrared receivers contain a long-pass filter to remove background daylight. This long-pass filter forces the use of encoding on the link to ensure that long strings of zeros or ones are not lost in transmission.

2400 bps to 115,200 bps link

For slower connections (2400 bps to 115,200 bps link) hardware cost can be kept to a minimum by implementing the protocol, packet framing and CRC calculation in software on the host processor. Asynchronous framing is used.

115,200 bps link and above

At speeds above 115,200 bps, packet framing, CRC generation and checking become a significant burden to the host processor. At 1.152 Mbps, these tasks are performed in hardware by a packet framer. Higher level protocols are less processor intensive than packet framing or CRC generation and are still implemented in software on the host processor. Synchronous framing is used.

4 Mbps (4 PPM) link

As in the 1.152 Mbps link, packet framing, CRC generation and checking are performed in hardware to relieve the burden on the host processor, while higher level protocols are implemented in software on the host processor. Pulse Position Modulation (PPM) framing is used.

The 4 Mbps link uses a new encoding scheme and a new, more robust packet structure. A phase-locked loop replaces edge detection as the means of recovering the sampling clock from the received signal.

2.1.2.3 Interference on the IrDA physical layer

Background light and electromagnetic fields are two factors that may interfere with the IrDA physical layer. There are basically four ambient interference conditions which the receiver is to handle correctly. The conditions are to be applied separately.

1. Electromagnetic field: 3 V/m maximum
2. Sunlight: 10 kilolux maximum at the optical port
3. Incandescent Lighting: 1000 lux maximum
4. Fluorescent Lighting: 1000 lux maximum

There is also the aspect of distance between transmitter and receiver which has been discussed earlier.

The interference can be seen with the Bit Error Ratio (BER), which is the number of errors divided by the total number of bits. The BER should be no greater than 10^{-8}.

2.1.3 Ir Link Access Protocol (IrLAP)

The purpose of the IrLAP layer is to establish connection between IrDA devices. In doing so the IrLAP layer must deal with discovering hidden nodes, address conflicts and handling requests and confirmations to upper layers. The IrLAP layer is located right on top of the physical layer and the framer in the protocol stack.

There are basically two states of the IrLAP: Primary (master) and Secondary (slave). The master is the one telling all connected devices which one is allowed to send at the moment. Only one device is allowed to send simultaneously. Thus the master play an important role in making sure this is obeyed by all secondary devices.

2.1.3.1 Discovering of other IrDA devices

There are three discovering services: request, indication and confirm. The "request" is used to find out what, if any, devices are within communication range and if they are available for connection. "Confirm" returns a list with all available devices. Finally, the "indication" is used to send information about the device that sends a request, to other devices.

2.1.3.2 Connection of IrDA devices

A device who wants to broadcast its desire to connect may do so by using a procedure called sniffing, which is a power conservative procedure. A device that wants to connect and approaches a network of Ir devices is called a hidden node. This device needs to listen and wait until spoken to, before it can connect to the network. This procedure is also a part of the sniffing procedure.

The basic procedure of the Sniffing device

1. A sniffing device wakes up and listens for a short period of time. If it hears traffic it goes back to sleep.
2. If it does not hear traffic it transmits an exchange identification (XID) response frame with a special value unique to the sniffing

procedure. This XID indicates that the device desires to be connected as a slave.

3. The device then waits a short period for a message directed to it. If such a message arrives the device can connect.
4. If no frames are sent to it, the Sniffing device goes to sleep (usually 2 – 3 seconds) and starts the procedure again. If it hears traffic not directed to it, it is assumed to be connection traffic and the device cannot connect.

Modes for connection

IrLAP is built around two modes of operation, corresponding to whether or not a connection exists. The two modes are: Normal Disconnect Mode (NDM) and Normal Response Mode (NRM).

NDM is also known as the contention state, and is the default state of disconnected devices. In order to connect from this state the device must first listen for a time greater than 500 milliseconds. If no traffic is detected during this time then the media is considered to be available for establishment of a connection.

NRM is the mode of operation for connected devices. Once both sides are talking using the best possible communication parameters (established during NDM), higher stack layers use normal command and response frames to exchange information.

2.1.3.3 Address conflicts

The address conflict services are used to resolve device address conflicts. If the discovery log contains entries for more than one device with the same device address, the address conflicts service may be invoked in order to cause the IrLAP layers of the conflicting devices to select new non-conflicting device addresses. The IrLAP addresses are 32-bit randomly selected addresses. On an address collision a new random address is selected.

2.1.3.4 IrLAP Services

Once the connection has been established, the IrLAP starts to work as a kind of message handling service for the upper layers. As help, the IrLAP have four generic types of service primitive:

1. Request: Passed from the Upper Layer to invoke a service.
2. Indication: Passed from IrLAP to the Upper Layer to indicate an event or notify the Upper Layer of an IrLAP initiated action.
3. Response: Passed from the Upper Layer to acknowledge some procedure invoked by an indication primitive.
4. Passed from IrLAP to the Upper Layer to convey the result of the previous service request.

In figure 2.1-5 is a graphical representation of how these primitives are related to each other.

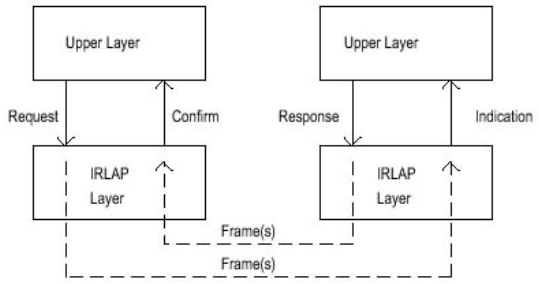

Figure 2.1-5: IrLAP Services

2.1.4 Ir Link Management Protocol (IrLMP)

The IrLMP protocol has many functions. Among these are multiplexing the link, accessing information about what services are present on another device and control of the link in general such as creating an ad hoc network functionality.

2.1.4.1 Link Management Multiplexer (LM-MUX)

The IrLMP multiplexer, LM-MUX, makes it possible for several clients to connect to the IrLAP connection thus relieving the client entity of the requirement of coordinating access to the single IrLAP connection. In order to do this, LM-MUX uses several of the IrLAP services such as discovery, link control and data transfer. When several clients are connected to the IrLAP protocol by using the LM-MUX, the LM-MUX is called being in Multiplexed Mode.

Some protocols and applications may require special control of a service access point in order to achieve a reduced, dependable latency and/or control the link turnaround through their use of the link. This special case is called Exclusive Mode.

2.1.4.2 Information Access Service (LM-IAS)

The IAS, or Information Access Service, acts as the “yellow pages” for a device. A full IAS implementation consists of client and server components. The client is the component that makes inquiries about services on the other device using the Information Access Protocol (IAP, used only within the IAS). The server is the component that knows how to respond to inquiries from an IAS client. The server uses an information base of objects supplied by the local services/applications.

The LM-IAS Information Base

The IAS Information Base is a collection of objects that describes the services available for incoming connections. It consists of a class name and one or more attributes. They are quite similar to entries in the yellow pages of a phone book. The class name is equivalent to the business name in the phone book; it is the official published name of the service or application. IAS clients will inquire about a service using this name. The attributes contain information which can be compared to the phone number, address or other characteristics of a business found in the yellow pages.

One important attribute is the Service Access Point Selector address

(LSAP-SEL address or service address), which is required in order to make a LMP connection to the service.

Getting information using the LM-IAS

There are a number of IAS operations defined in the IrLMP standard, but the most used and only required one is the one used to get values by providing class (GetValueByClass) from the IAS service. The procedure might be as follow:

IAS Query arguments:

- Class Name Length
- Class Name
- Attribute Name Length
- Attribute Name

Results:

- Return code:
  - 0: Success, results follow.
  - 1: No such class, no results follow.
  - 2: No such attribute, no results follow.

If the result code indicates success, the call returns the following information:

- List Length
- List of results
  - Object Identifier
  - Attribute value

2.1.5 Security of IrDA

IrDA contains no encryption or other means of security. Still, IrDA is considered secure because of the limited range and the fact that it requires line of sight. Someone wanting to eavesdrop on a communication needs to be in the direct vicinity of the communicating devices and on top of that stand within the angle limitations.

2.2 INTRODUCTION TO RFID

RFID is a technology that has a lot in common with the barcodes that we see everywhere in today's society. RFID is a work in progress to make a wireless identification system. This technology could replace barcodes in some areas but has also a much wider use.

2.2.1 How does RFID work?

RFID have three main parts. The transponder, also called an RF tag,

which contains the information in the system. The second part is the reader that gathers information from the transponder; this procedure can be seen in figure 2.2-1. A device to program the transponder is also required.

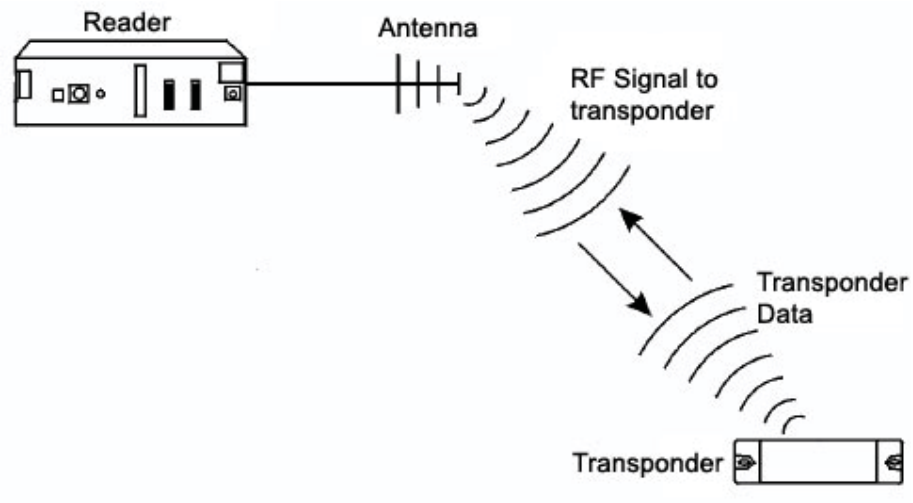

Figure 2.2-1: A reader sending a request and a transponder sending the data back

2.2.1.1 Transponder

A transponder responds by transmitting its data whenever it receives a predefined signal from the reader. Data within the transponder may provide identification for goods, animals, items in manufacture, a location or an individual. But the transponders are not limited to identification only and can also provide other data that is of interest for the specific situation.

A simple view of the design of a transponder can be seen in figure 2.2-2. As can be seen there is a part with digital circuitry where some logic is present. Simple transponders lack some of these logic parts while other, more complex transponders are capable of encryption of messages using a known encryption key. Thus there is a possibility of secure transmissions between RFID reader and transponder.

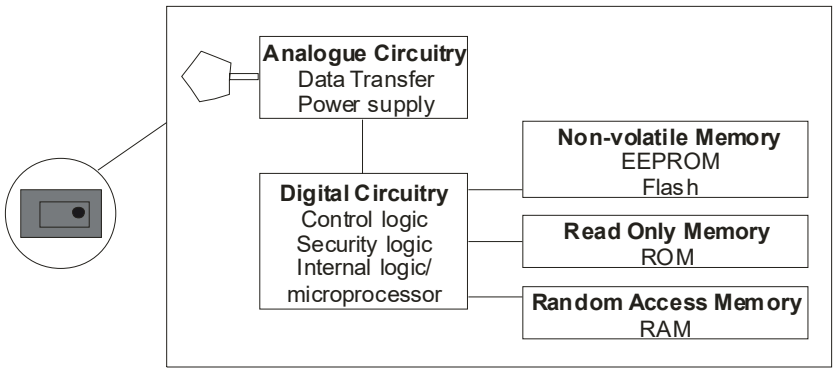

Figure 2.2-2: A simple view of the design of a transponder

How are these transponders powered?

There are two different ways to power the transponder. The passive

transponder does not have its own power source. It gets its power by deriving it from the field generated by the reader. Later it uses this power to transmit its data back to the reader. Because of this the passive transponder will have an infinite lifetime as long as the circuit is intact.

The other way is to simply put some kind of power source in the transponder. This is referred to as an active transponder. Because of the nature of the power source, these transponders will have a finite lifetime. But the power consumption is very low and life spans up to 10 years are possible.

The active transponders are capable of responding with greater power than the passive transponder and therefore have a greater range, higher data transmissions rates when used in higher frequency and better noise immunity than the passive transponder.

Data storage in transponder

Transponders can be of the type ROM, WROM or RAM or a combination of these. Which type depends on what the transponder will be used for. ROM versions are of course cheaper and can be smaller because they do not need a power source and the extra circuits for writing. Writing is much more energy demanding so the writeable transponders are always active transponders.

Physical form

Transponders can have almost any kind of shape, size and protective housing. Transponders that are designed for animal tracking can be small as a pencil led in diameter and ten millimeters in length. If your application needs to identify trees or wooden items the transponder can be shaped as a screw. They can also be as the heavy-duty 120 by 100 by 50 millimeters rectangular transponders used to track inter-modal containers.

2.2.1.2 RFID readers

The reader is the more complex part of the RFID system. The reader is responsible to activate the transponder by sending a predefined wave to it. When the transponder responds the reader should read the signal, decode and store the data so that it later can pass it to a computer or another device that can recognize the data and put it in a context. Of course these two parts can be in the same device so that the reader can work with the data directly. Different readers can vary quite a lot in complexity, depending on what kind of transponders it can read and what functions it performs on the read data. The reader can perform different functions like quite sophisticated signal conditioning, parity error checking and correction.

Multiple transponders in the interrogation zone

A problem that can occur in an area with many transponders is that two or more of them are in the same reader interrogation zone. They will then all transmit their data as a response to the reader's signal. One technique for the reader to organize the different tags in this scenario is referred to as "Hands Down Polling".

After the reader has received its data from the transponder it will perform some algorithm to decide if this is a repeated transmission and if that is the case it will instruct the transponder to cease transmitting. This communication between the transponder and reader is called “Command Response Protocol”.

An alternative approach that has more security but is slower than “Hands down pulling” is “Hands up pulling”. In this case the reader will look for transponders with specific identities and read them in turn. A variety of other techniques have been developed to improve the process of batch reading.

2.2.1.3 RFID transponder programmers

The transponders that have memory of type ROM are programmed in their constructions and are not programmable in a later state. The WROM or RAM versions are programmable and for this purpose you have a RFID transponder programmer. The RFID transponder programmer communicates with the transponder in similar ways as the reader. It will send commands that will tell the transponder to receive data, which is then gathered by the active transponder and stored in memory.

RFID Programming devices are generally made to handle only a single transponder, however development is now satisfying the need to selectively program a number of transponders that are present in the range of the programming device.

2.2.1.4 Range

The range of RFID systems vary depending on what they are designed for. Range differs between contact and up to 20m. The difference is caused by different power usage and used frequency. Longer range devices require more power and more complex circuits. The maximum allowed power for different frequencies vary from country to country and thus it may differ some.

The range from which the programmer can work is generally less than that of the reader. In some cases near contact is required.

2.2.2 Frequencies

There are no standard frequencies for RFID, but there are some different ranges that are more common. Regulations make these ranges differ in different countries.

2.2.2.1 13.56 MHz or <135 kHz

Today the vast majority of the transponders in the 13.56MHz and the range less than 135 kHz range are passive. The basic operation principle for these frequencies is energy and data transmission using inductive coupling. This is a technique that is also used in transformers. The antenna of the reader generates a magnetic field, which induces a voltage in the coil of the transponder and supplies the transponder with energy. Changing one parameter of the transmitting field results in data transmission from the reader to the transponder. The different parameters that can be changed are amplitude, frequency or phase.

By changing the load of the field the transponder can transmit data back to the reader. Changing the amplitude and/or the phase makes a change in the load.

Strength

The RF field at 13.56MHz is barely absorbed by water or human tissue, and can therefore work in an environment where humans and water block the way between the reader and transponder.

Inductive RFID systems are operated in near field. This makes it less sensitive to disturbing influences of adjacent systems or external noise.

Weaknesses

Shielding or reflection effects make the RF field at 13.56 MHz sensitive to metal parts in the operating zone. Because of the vector characteristics that the magnetic fields have, the orientation of the transponder will have an impact on the distance that is achievable. Using a more complex transmission antenna can solve this orientation-sensitivity. An example of this is to generate rotating fields.

2.2.2.2 400-1000 MHz UHF and 2450 MHz microwave

In the UHF and microwave frequency range the way of communication is through conventional electromagnetic wave propagation, seen in figure 2.2-3. When the transponders are passive this is also the source of energy.

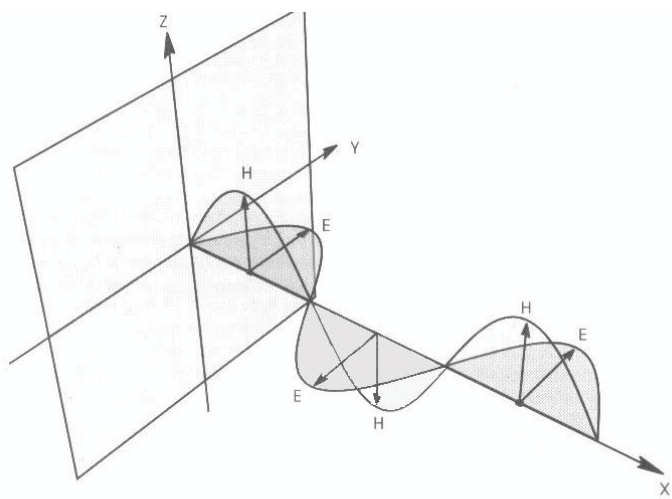

Figure 2.2-3: Electromagnetic wave propagation- the electric "E" component is at right angles to, but in phase with the magnetic (H) component.

The reader transmits an EM wave; witch propagates outwards with a spherical wave front. The transponders that are in this field will be immersed by this propagating wave and collect some of the energy as it passes.

Data is transmitted between the reader and the transponder in the same way as it is done in the lower frequencies.

The allowed power for these signals is regulated differently in different countries and as this is a parameter for the performance (range) of the RFID system, the achievable performance will differ for different countries.

Behavior

UHF signals are related to light and will behave in a similar way. They can be reflected by radio conductive reflective surfaces, they can be refracted as they pass across the barrier between dissimilar dielectric media or they can be diffracted around a sharp edge. This can be both an advantage and a disadvantage. For example a wave that is reflected can reach areas that would not be reachable in other cases. However a reflected wave can also cross itself and if the waves are not in phase it can nullify or dampen the signal. If the reflected and the original signal are in phase it will result in an amplification of the signal.

Strength

RFID systems in the UHF and microwave band can have greater range than the ones in lower frequencies. The amount electric noise from florescent light, motors etc is minimal when using the UHF band. At around 900 MHz there is very little electric noise.

The nature of UHF makes it possible to design a relatively small directional antenna. Equipped with this antenna a reader can be directed towards a group of specific transponders or one specific transponder. In this case the reader will be more immune against potential interference from other readers or transmitter sources.

Weaknesses

Electromagnetic energy that passes through anything besides vacuum will lose some of its energy as heat in the substance. The amount of energy that is absorbed is dependent on the characteristics of the material.

The orientation of the transponder's antenna with respect to the reader's antenna affects the possible range. If the antenna has linear polarization and the transponder's antenna is at a right angle with respect to the reader's antenna, the resulting signal will be null. To achieve the maximum range the antennas must be in the same orientation. With a non-linear polarization of the reader's antenna the transponder's orientation will not be important.

2.2.3 Standards

Many of the standards that have been developed for barcodes are also applicable for RFID. But today there are no standards designed for the communication between reader and transponder. In most cases this makes devices from different manufacturers incompatible with each other.

2.3 INTRODUCTION TO BLUETOOTH

Bluetooth is a low cost, low power, short range radio technology

originally developed as a cable replacement to connect devices such as mobile phones, headsets, PDA's and portable computers. By enabling a standard way for these accessories to communicate, Bluetooth has created the expression Personal Area Network (PAN). PAN is a close range network that connects your personal electronic equipment.

There are many protocols in the Bluetooth stack. Some or parts of them are required, while others are optional. The Bluetooth specifications are divided into two major parts. These parts do not need to be separate parts in the implementation. However it might be a smart decision to implement them separately because of the different requirements of the two parts.

One of the parts is the Bluetooth module, it contains the protocols that are responsible for finding and connecting to other devices. The second is the Bluetooth host, which is responsible for doing what the device was built to do. Some of the host implementation is part of the Bluetooth specification while some is product dependant.

The protocols that are of interest in our work are:

- The Bluetooth module
  - Radio
  - Baseband
  - The link Controller
  - The link manager
- The Bluetooth host
  - Logical link control and adaptation protocol
  - RFCOMM
  - The service discovery protocol

2.3.1 Radio

Bluetooth uses the unlicensed ISM band. The ISM band is available in countries all over the world but it does not have the same frequency range in all countries. In table 2.3-1 there is an overview of the ISM band in the world.

2.3.1.1 Frequency hopping

The ISM band is a rather crowded frequency band and therefore Bluetooth implements frequency hopping to avoid collision with radio waves from other sources. The ISM bandwidth is divided into 79 channels. Fewer channels are offered in some countries where the ISM band is smaller, which can be seen in table 2.3-1.

Geographic Area	ISM Band (GHz)	Available Channels
France	2.4465-2.4835	23
Rest of World	2.4000-2.4835	79

Table 2.3-1 table over the unlicensed ISM band in the world

The Bluetooth devices will jump between these channels 1600 times per second in a pseudo random order. This makes it unlikely that interference in one channel will disturb the communication between two devices for a longer period.

The pseudo random order of hopping for the devices in a piconet is derived from the master's clock and device address.

2.3.1.2 Power and range

The Bluetooth specification has 3 different power classes:

1. 100 mW
2. 2.5 mW
3. 1 mW

The range for power class 3 is typically up to 10m, for power class 2 it is typically up to 20m and in power class 1 the typical max range is 100 m.

2.3.2 Baseband

2.3.2.1 Slave/Master and networks

In Bluetooth one master and up to seven slaves form a simple Local Area Network called a piconet. All devices can be a Master or a slave depending on which device initiated the contact. The initiator becomes the Master, though this is not final; it can be changed afterwards. Some devices can be part of two piconets that then create something called a scatternet. Thus a scatternet is a connection between two or more piconets. A device that is part of more than one piconet can be master or slave in the different piconets independently with the exception that it can not take the role of master in both piconets as it will become one piconet.

Slaves are only allowed to send data to the master when they have been addressed by the master then the slave may only transmit to the master.

2.3.2.2 Physical Links

The radio link in a piconet is divided into time slots, where every other slot is for the Master and the other slots are for the slaves. In some circumstances a slave or master may transmit over 3 or 5 slots, however since these numbers are odd the next slot will be a master slot if a slave was sending and vice versa.

ACL

The ACL link exists as soon as a connection is established between two devices. It is used for sending data. If the slave cannot determine if it was addressed in the master to slave slot it is not allowed to send in the next slave to master slot.

SCO

A master can handle up to three SCO links. These links can be to the same slave or to different slaves. A SCO link is a symmetric link between the master and the slave, most often used when streaming audio. When a SCO link is present, some of the master's slots are dedicated to this link

and the same thing with some of the slaves' slots. The amount of slots does not need to be the same in both directions.

Even if a slave cannot determine if a package on the SCO link is addressed to the slave it is still allowed to send on the next slave to master SCO slot. Packages on a SCO link are never retransmitted.

2.3.2.3 Package structure

The structure of the different packages in Bluetooth is very similar. There are two major package groups. These are closely related to the two possible links between devices. There are also some special package types such as NULL, POLL, FHS and ID. It is only the ID package that does not look as figure 2.3-1. The ID package has only the access Code.

Access Code	Header	Payload

Figure 2.3-1: the structure of a Bluetooth package

Access code

The packages start with the access code; it has the information about where the packages belong. There are four distinct access codes:

- Channel Access Code (CAC) – The CAC is used by all members in a piconet and is derived from the master in that piconet.
- Device Access Code (DAC) – Is used when paging a special device and is therefore derived from that device.
- General Inquiry Access Code (GIAC) – When there is no knowledge of what devices exist in the near area GIAC is used to signal inquiring.
- Dedicated Inquiry Access Code (DIAC) – Has the same use as GIAC, however it is used when the user wants to limit the responding devices to a chosen group.

Header

The header contains an address of the slave in the piconet and a type tag to identify the packages type and slot length. It also contains acknowledgement of the package that was received by the sender and a CRC for the header.

Payload ACL

ACL packages are used to send data containing up to 2712 bits of data. The payload of the ACL package contains not only the data but also an extra header that tells the receiving side if the payload contains a L2CAP message or a LMP message and the length of the data. It also contains a flow flag for the L2CAP level. L2CAP messages can be spawned over more than one ACL package, while LMP messages only can take one ACL package. A CRC is also part of the payload.

Payload SCO

In SCO the payload has a fixed size of 30 bytes. The data in this payload is 10, 20 or 30 bytes depending on the package type which selects the Forward Error Correction (FEC) ratio to use (1/3, 2/3 or none).

Mixed Payload

One of the package types is a mix of both ACL and SCO. In this package the SCO is 10 bytes long and has no FEC protection. The data in the ACL part can be up to 72 bits long and is protected with a 2/3 FEC ratio.

NULL

In this Package the payload is empty. It is used to acknowledge a package that is received when no data is ready to be sent back. The receiver does not need to acknowledge this package.

POLL

Has the same structure as the NULL package but the receiver of this package must acknowledge it even if it has no data to send. It will not be part of the normal acknowledgement and therefore it will not interfere with the acknowledge flags of data packages that are sent.

FHS

The FHS payload contains all the information that is needed in order to synchronize clock and hopping sequence with the sending device.

2.3.3 The Link Controller

The link controller is responsible for the different states of the Bluetooth device.

2.3.3.1 Link Controller States

Standby

When a device is in standby mode it is inactive and no data is transmitted. The radio is turned off and thus it can not detect any communication.

Inquiry

In Inquiry mode the device tries to discover nearby devices.

Inquiry scan

A device in Inquiry scan mode is listening for devices that are inquiring so that it can respond and acknowledge its presence.

Page

A device that has been put in Page mode is trying to establish connection with a device by addressing it directly

Page scan

Page scan mode is where a device is listening for another device to address it. Some devices only enter page scan when they have been inquired.

Connection – Active

The connection is active.

Connection – Hold

A device in Hold mode is inactive in the piconet for a period of time. During this time it can use the radio link to find new devices and connect to them. It may also enter low power sleep mode. The device still holds its piconet address when in this mode. After the time period has elapsed it will synchronize with the master and be an active part of the piconet.

Connection – Sniff

In sniff mode the device is set to listen in periodic interval where the length of the pause and listen time is decided by the slave and master together.

Connection – Park

Park mode is where the device gives up its piconet address. The difference from the standby mode is that it will still try to be synchronized with the master in order to reconnect to a piconet faster. In Park mode the device can enter low power sleep mode, in which case it will only wake up for certain beacons to keep synchronization with the master. When awoken from sleep mode it will try to resynchronize with the Master.

2.3.3.2 Master/slave switch

In some circumstances the device that initiated the connection may not want to continue the master role, or a slave might want to take over the role as master. In order to solve this, the Bluetooth specification contains a method for a master and a slave to change roles. The master is always the one that initiates the change, but a slave can request a change from the master.

2.3.4 The Link Manager

The link manager is as the name suggests the part that establishes and manages the link. It puts the link in a different mode depending on what commands it receives from the user or the link manager on the other side of the link.

2.3.4.1 Link configuration

When connected to the link manager the master can configure the link by asking, or in some cases force the slave to change the link. The slave can also request a change in the link but the request must always be accepted by the master.

SCO

If the master wants to establish a SCO link it sends a request to the slave with the suggested parameters for the link. This request is either accepted or rejected by the slave.

If the slave wants to establish a connection it sends a request to the master. Since the master is the one who handles the piconet, the slave

does not know the best parameters for the SCO link. The master will therefore send a request back to the slave with the parameters it has chosen. This request is then accepted by the slave and the link is established.

There are three different package types that are available for SCO links. The differences between these packages are how resistant they are to high BER.

ACL

Bluetooth specifies three different sizes for packages on the ACL link. 1, 2 or 3 slots are available and the maximum size is decided by the master. A slave that receives an order about changing the maximum size of the package cannot reject it and must comply. As before a slave can request a change of the maximum size, but this request may be rejected by the master. The ACL links always start at a maximum of 1 slot.

On a noisy link the probability of bit error is high and longer packages should therefore be avoided.

There are also two different kinds of packages for protection against high BER. As in the SCO link, FEC is used, however in ACL only 2/3 and none is available.

Power control

To save energy the power of the signal to and from devices should be set to a minimum. The receiver can by measuring the strength of the received signal determine if the power is too high or too low. The link manager can then request the link manager on the other side to increase or decrease the power of the signal. If the signal is already at its maximum and an increase message is received the receiver responds with a maximum message. Equally if it is at a minimum and it gets a decrease message, in which case a minimum message will be issued. No acknowledge is required as the sender will see if the power is increased or decreased.

2.3.4.2 Supported features

Some of the features in the Bluetooth specification are optional. Because of this there is a need to find out what features the other side of the link supports. This can be done by the Link manager. There is also a way to find out the version of the link manager on the other side.

2.3.5 Logical Link Control and Adaptation Protocol

The Logical Link Control and Adaptation Protocol (L2CAP) is used to pass data and messages between the upper layer protocols and the lower layer protocols.

- It can multiplex between different upper layer protocols and thus make them share the lower layer link.

- It supports larger package size to ease the transferring of packages from upper layers, which are often bigger than the packages in the Bluetooth's baseband.

All applications must use L2CAP to communicate over Bluetooth, either directly or through some other protocol that uses L2CAP.

2.3.5.1 Channels

The L2CAP uses channel ID to distinguish between different connections. Some of these ID numbers are reserved for the more important upper layers such as RFCOMM and SDP.

2.3.6 RFCOMM

RFCOMM emulates the serial cable line settings and status of an RS-232 serial port. It is based on the GSM TS 07.10 standard, which is an asymmetric protocol used by GSM cellular phones to multiplex several streams of data onto a physical serial cable. RFCOMM is used by almost all applications that sends data over Bluetooth. This is because only a few protocols will communicate with the lower layers without going through RFCOMM.

RFCOMM uses the L2CAP protocol, so an L2CAP connection must have been established before an RFCOMM connection can be established.

2.3.6.1 Types of RFCOMM devices

RFCOMM has support for two different types of serial devices.

- Type 1 – Internal emulated serial port (or equivalent)
- Type 2 – Intermediate device with physical serial port.

2.3.6.2 Channels

RFCOMM uses channels to distinguish between different services from the upper layers. The Maximum amount of channels that can be assigned to services at one time is 30. The channel address is 5 bits, but value 0 and value 31 are reserved. RFCOMM must keep a record over which service is assigned to what channel at any given time to be able to send the data to the right application.

2.3.7 The Service Discovery Protocol

The Bluetooth specification is designed to be implemented on devices that are moving around a lot. That means it will have to discover new devices and new services while it is moving around. To handle this, the Bluetooth specification includes a protocol to discover what services exist on a connected device.

A device that is offering a service through SDP is a SDP server and a device that is looking for a service using SDP is a SDP client.

2.3.7.1 The SDP database

The SDP database is simply a set of records describing all the services that a Bluetooth device can offer to another Bluetooth device.

Service Attributes

Every service in the SDP database has a couple of attributes that are associated to it. Some of these are common for all services. Some of the

common attributes are: identity for the service, icon for the service in a user interface, name of the service and so on.

An attribute contains three parts. The first is the type of the data, second is the length of the data and finally in the attribute record comes the data.

2.3.7.2 Browsing

To make the process of finding the service you want easier, services are arranged in a hierarchy structure. Clients begin to examine the root of the hierarchical and follow the leaves until the desired service is reached. The service can also be addressed directly by searching for its Universally Unique Identifier (UUID).

It is up to the service provider to arrange the hierarchy and what services that will be possible to browse. An example of how a hierarchy tree may look like can be seen in figure 2.3-3.

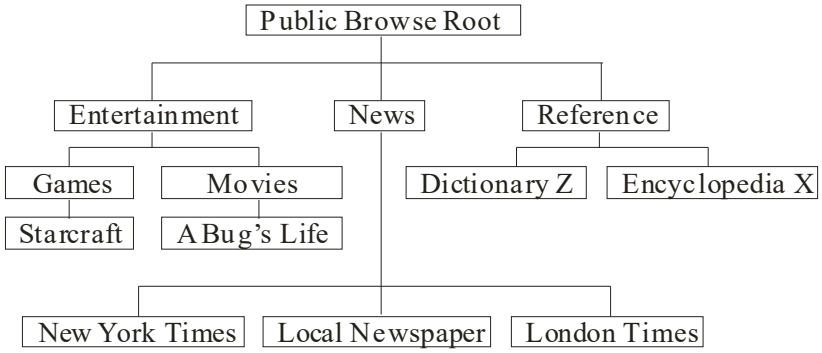

Figure 2.3-3: Example of hierarchy in a SDP server

2.3.7.3 Universally Unique Identifiers (UUIDS)

Every service has a unique identifier to separate it from other services. This identification is of the type Universally Unique Identifiers (UUID). The UUID is 128 bit long.

The standard profiles and services

The Bluetooth specification has many services that are already defined. The UUID for these services are most likely going to be used frequently and thus they have 16 bits and 32 bits alias to save bandwidth. The aliases can easily be transformed between each other and/or to the 128 bit UUID. When two different sizes of UUID's are going to be compared, the smaller one is transformed to the same size as the larger one.

New services

If a manufacturer has developed a new service that he wants to show in the SDP database he is allowed to assign his own UUID. The process of making an UUID is designed so that the UUID will be unique and not conflict with any other service. Because of this no organization is needed to handle new UUIDS.

2.3.8 Encryption and Security

Since the data in Bluetooth is carried by radio waves anyone with the

right equipment could get this data. The FHSS algorithm in Bluetooth is making this very difficult by hopping to a new pseudo random frequency 1600 times per second; however it can still be done. To authenticate devices and to secure the data over the link, Bluetooth has various kinds of security modes.

2.3.8.1 Keys and encryption

The base for the encryption in Bluetooth is a variant of the SAFER+ cipher. Cylink Corporation designed it as a candidate for the U.S. Advanced Encryption Standard (AES).

There are different kinds of keys defined in the Bluetooth specification. Some of them are created as they are being used while others can be the same the entire lifespan of the device.

Link Key

Link keys are used to authenticate Bluetooth devices but are also used to generate encryption keys. Link keys can be either semi-permanent or temporary.

Master Key

Master keys are used for point to multipoint communication and may replace the current link key for a time period.

Unit Key

The unit key is often ROM-based and is created during factory setup. It is unlikely that the unit key will change.

Combination Key

The combination key is a combination of the two communicating devices' unit keys. It is often used to replace the unit key.

Initialization Key

Initialization keys are used as link keys during a single session and are only used if no combination keys or unit keys have been exchanged.

Encryption key

Encryption keys are derived from the current link key, though it may be shortened due to national security export restrictions in some countries.

2.3.8.2 Security modes

There are three modes of security in Bluetooth, though a device does not need to have any security support.

- Security Mode 1 is none secure – Devices will not initiate any security procedure.
- Security Mode 2 gives Service Level-enforced security – The channel or service using an L2CAP connection decides if the link should be secure or not.
- Security Mode 3 is Link Level-enforced security – A device in

security mode 3 will initiate security procedures while the link managers are connecting.

2.3.8.3 Authentication

Authentication is used when two devices want to be sure that they share a common secret key. This secret key can be a fixed key that was created during manufacturing or a key derived from a PIN that the user has typed into one or both devices.

When two devices are authenticated the used key for that link may be saved until next time a connection is established. The link will then be secured almost immediately without the user(s) involvement.

2.3.8.4 IEE 802.15 – Wireless Personal Area Networks

The IEE 802.15 standard is derived from the Bluetooth standard and is focused on the so called Wireless Personal Area Networks (WPAN). It is not a product itself but rather a development of a standard, used in Bluetooth.

This is a standard that will most likely result in products which are very suitable for positioning systems, and thus worth keeping an eye on. However, at the current date the product in this category carrying most interest is Bluetooth.

SECTION 3 EVALUATION

We have looked at three different short range communication systems. Our purpose for this has been to select the most suitable system to use in a positioning task. In this section we will discuss advantages and disadvantages of each system in relevant areas.

3.1 POSITIONING TASK

The most important aspect is of course the possibility to position a mobile device. It is requested that it is able to use the methods provided by the Alipes platform for positioning. The position is to be presented in the GPP standard which means it would have to handle the four basic message types discussed in section 1.2.2.2.

All three of the technologies are able to store a position and communicate this position with bypassing devices that incorporate the same technology. This position can then be used to access further services within the Alipes Platform.

3.2 NETWORK

A network opens up for many further services such as map retrieval and other information about the area. Therefore it is important that the technology can provide a network access as well as a position. Bluetooth and IrDA are both designed for networks. Bluetooth delivers a maximum speed of 1Mbps while IrDA delivers a maximum speed of 4Mbps. RFID on the other hand is not able to provide anything besides the data stored in the RF tag.

3.3 EXCHANGE OF POSITION

Section 1.2.1.2 mentions using positioning sources not supported by the device itself. In order to do this the devices must be able to share positioning information between each other.

The RFID reader devices have no way of communicating between each other using the RFID communication system. There is also another aspect to RF tags that should be taken into consideration. This is that RF tags are manually programmed and can not change the positioning information without reprogramming, unless their identification number along with the position is stored in a location server and changed there. However, RFID have no means of providing a network connection so the lookup would have to go through some other communication system.

Bluetooth and IrDA are both able to share the position information with other devices. They can create networks with bypassing devices where they take a role of either master or slave. The roles of master and slave are dynamic in both Bluetooth and IrDA, though some IrDA devices may never be able to take the role of master because of its simplicity. Through the created networks they can easily share the position information they have.

3.4 SECURITY

The need for security is most apparent when some type of network connection is established. Thus there is no real need for advanced security in this kind of positioning task when it comes to RFID, although some RFID transponders are capable of encrypting messages. In the Bluetooth and IrDA case however, it is more important.

IrDA rely on the short range and limited angle for security. New devices must be approved by the device having the role of master in the network in order to connect. The only way to eavesdrop on a communication session is to be in the immediate vicinity, within angle and with line of sight.

Bluetooth has many security features. Both authentication and encryption of the link is incorporated. In section 2.3.8 there is a description of the Bluetooth security. It is easier to eavesdrop on Bluetooth than on IrDA since it has longer range, no limited angles and no requirement in line of sight.

3.5 PHYSICAL ASPECTS

There are a number of things to take into consideration when it comes to wireless communication. Such aspects can be range, angle and power consumption. However, for a positioning task it is also interesting to know what level of accuracy that is to expect from the device.

As seen in the description of the technologies each system has different range depending of various factors such as power and frequency use. For mobile devices it is important to conserve power and thus there needs to be a balance between range and power consumption.

3.5.1 Range

IrDA has a range of typically 1m, though there is a low power version that has a range of 20-30cm (section 2.1.2.1). Which range to pick depends on how much power that it is allowed to consume.

Bluetooth has a typical range from 10m to 100m depending on the power class of the device (section 2.3.1.2). At current date class 3, with a typical 10m radius is most common in mobile devices.

RFID vary quite a lot in range because of the non existing standard. Devices are created with the maximum range that the application requires. Range differs from contact up to 20m (section 2.2.1.4).

3.5.2 Power consumption

The positioning system is meant for mobile devices with limited power supply. Thus it is important to have communication systems that conserve power. All three systems are designed to consume very little power and are all suitable for mobile devices.

For devices with really low battery capacity there is a low power version of IrDA, then with a typical max range of 30cm. This low power version consumes about 1/10 of the power compared to the standard version

with a typical range of 1m (section 2.1.2.1). IrDA also have different modes where it conserves power when it is not used.

The RFID transponders can be both unpowered and powered. The unpowered transponders have shorter range than the powered ones and it requires more power in the reader (the mobile device). The variation in range causes similar variation in power consumption. The power consumption of RFID is further described in section 2.2.1.

Bluetooth is like IrDA designed with different modes that conserve power depending on how it is used. It also has the possibility to negotiate power consumption with another device to reach the lowest possible power consumption with remaining connection. The power consumption of Bluetooth is further described in section 2.3.1.2 and section 2.3.4.1.

3.5.3 Angle

Radio devices such as RFID and Bluetooth are not dependent on certain angles or line of sight. For IrDA the case is different. Section 2.1.2.1 describes the optical angle limitation for the IrDA. IrDA also requires line of sight.

3.5.4 Accuracy

Accuracy in these systems depends much on the maximum range of the systems. The longer the range the higher the error it can be. This is based on the assumption that only one position is read. However, there are methods of improving the accuracy. Bluetooth for example has point to multi point and may be able to read several positioning sources at once. From the information collected it can calculate a more accurate position. The optional power consumption function discussed in section 2.3.4.1 may also be used to calculate the distance to the positioning source. Combining these two techniques would give a more accurate position than each of them separately.

It would be possible to do similar calculations with RFID as with Bluetooth, although there is no signal strength to be read in RFID which would give a worst-case scenario of maximum range.

With IrDA it would be possible to make some accuracy improvement if the servers were to scan an area and, with knowledge of the physical limitations such as angle and range limitations, calculate a position. However, this would require many calculations on the server side which is not acceptable if a mobile device were to run a server. Any heavy calculations should, if possible, be run on the client to avoid having processor demanding server software.

3.6 AUTOMATION

The user would not want to obtain the position manually, thus it needs to be an automatic process. For this automatic device discovery and automatic service discovery helps.

All three systems have automatic device discovery which would find any new device within range and in the IrDA case, within angle (section

2.1.3.1, 2.2.1.2 and 2.3.3.1). Only IrDA and Bluetooth have automatic service discovery (section 2.1.4.2 and 2.3.7). The automatic service discovery checks if the positioning service is present in the discovered device. If there is no such service there is no need to ask for the position.

3.7 RELIABILITY

For both networking and position acquiring it is important that the link is reliable. Packet loss and bit errors have to be handled.

3.7.1 Interference

As described in section 2.1.2.3 there are several sources of interference that can affect IrDA. Light can be affected by other light sources and electromagnetic fields.

Bluetooth works in the ISM band which is a very crowded frequency band. Bluetooth have techniques to avoid interference by hopping in frequency (section 2.3.1.1).

RFID is also designed to work in the ISM band. There is no standard so systems designed to work in not so crowded frequency bands exist.

3.7.2 Correction

IrDA has CRC in order to discover errors in the received packets. It will request resending of lost packets and corrupted packets.

RFID can have CRC in order to discover errors in received data. RFID is not package based, thus lost packages do not exist, only corrupted data. It will request data again if corrupted or no data is received.

Bluetooth has both CRC, to check for errors, and FEC in order to restore corrupted data. The choice of protection is made depending on what link quality is used. Further description of error detection and correction in Bluetooth can be found in section 2.3.2.3 and 2.3.4.1.

3.8 SUMMARY

	IrDA	**RFID**	**Bluetooth**
Positioning task	Yes	Yes	Yes
Network	4 Mbps	N/A	1 Mbps
Exchange of position	Yes, limited	No	Yes
Security	Good	Good	Very Good
Range	Typically 1m	0 – 20m	100m/20m/10m
Power consumption	Low	Low	Low
Angle dependency	Yes, Line of sight	No	No
Accuracy	Range	Range/ (Triangulation)	Range/ (Triangulation)
Automatization	Yes	Some	Yes
Reliability	Very Good	Good	Very Good

Table 3.8-1: Summary of evaluation

Based on the requirements given in section 1.3 and some other important issues seen in this section, we summarize our conclusion for the theoretical part of this project.

All three systems, IrDA, RFID and Bluetooth are able to use the methods provided by the Alipes platform to position a mobile device.

RFID does not provide a network connection which was requested and thus it is not the technology we are looking for.

Even if IrDA is capable of exchanging positioning information between devices, its limits in range, angle and line of sight makes it less suitable for our purpose.

Bluetooth fulfills the three first requirements and is generally better in most areas. IrDA does have higher speed than Bluetooth but IrDA need line of sight which makes the system less user-friendly in a real scenario when a user wants a position. Thus Bluetooth wins in the end.

There are qualities of both RFID and IrDA that makes them interesting. RFID for example is cheap, especially the transponder that will contain the position. And compared to IrDA it has the advantage in the positioning since it is radio based and thus able to communicate in all directions. Since network is of importance, IrDA seems to be the better choice between the two.

Our conclusion is that Bluetooth is the best suitable short range communication system for the positioning task.

3.9 OTHER POSSIBLE TECHNOLOGIES

So far we have looked at three technologies for short range communication but there are more communication technologies that have some interesting aspects. One of these is Home RF.

3.9.1 Home RF

Home RF (Radio Frequency) is a radio based communication technology that shares many properties with both WaveLAN and Bluetooth. It works in the 2.4 GHz band and like Bluetooth it uses frequency hopping to avoid interference. Home RF surpasses Bluetooth in both range (50 meters) and speed (10 Mbps).

Home RF uses similar encryption as Bluetooth and along with frequency hopping it can be considered relatively secure. Like Bluetooth it has very low power consumption and therefore it is suitable for mobile devices. Automatic device discovery is also provided with Home RF, something that helps in a positioning task.

Is Home RF a technology suitable for positioning tasks? Yes, Home RF could be used in positioning tasks but it does not provide ad hoc connectivity like Bluetooth and thus only the control point can share a position. One of the requests for this work was that clients would be able to exchange positioning information with other clients, which is not possible with Home RF.

Home RF is not widely spread and is most suitable for cable replacement

in homes and home appliance such as wireless phones, wireless headphones, computers and so on. Home RF does not distinguish itself in any way compared to other radio based systems, such as Bluetooth, WaveLAN and RFID. Thus Home RF is not likely to be used for positioning.

SECTION 4 IMPLEMENTATION OF BLUETOOTH

This section describes our implementation of a Bluetooth based positioning system to work with the Alipes platform as a pull device.

4.1 ENVIRONMENT

The Alipes platform is developed in Java and therefore we chose to do as much as possible in Java. By this we gained easier integration with Alipes and also portable code to other OS's and platforms. However, since no public implementation of Bluetooth exists in Java at current date, we developed a library in C++ that the Java part could call through the java native interface. This library is a link between the Java side and the Bluetooth stack developed by Ericsson.

The hardware we used was two Bluetooth starter kits from Ericsson, connected to the computers through a serial cable. We also had two Bluetooth pc-cards and a Bluetooth USB device from 3Com, two Ipaqs from Compaq with Bluetooth that we used for testing.

4.2 DESIGN

The goal with our design was to make it flexible, meaning it would be easy to port the code to another operating system. To accomplish this we implemented the separate protocols (HCI, SDP, RFCOMM and L2CAP) in separate classes. We also implemented the different SDP data element types in separate classes to make porting easier.

In order to make further extensions of our positioning application easier, we made an extensive implementation of the Bluetooth interface in Java. Thus, the so called Native code in C++ covers many of the commands featured in the Bluetooth stack by Ericsson.

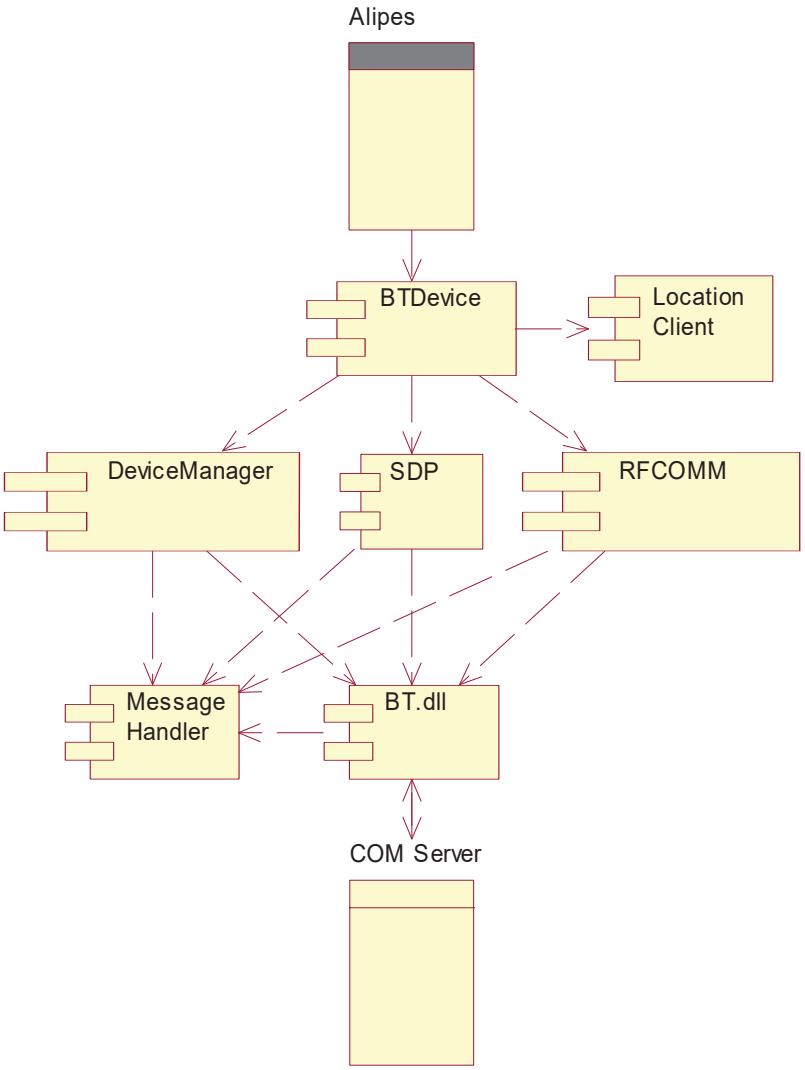

Figure 4.2-1: Component view of the Alipes platform device design

Our Bluetooth implementation for positioning is made to be run by the Alipes platform device, as can be seen in Figure 4.2-1. If a connected device does not have a positioning server the program will consult the Location Client with the unique identification number of the connected device as argument.

The DeviceManager handles the lower level protocols such as the hardware controller interface. SDP is the Service Discovery Protocol and it handles service searches and adding of services. RFCOMM is the serial port emulation protocol. These three parts are coordinated by BTDevice.

When DeviceManager, SDP or RFCOMM execute a command that utilizes a function in the native code (BT.dll) and a reply is expected, it will put itself on hold and start to wait for the message to be received in the Message Handler. Once the expected message is received in the

Message Handler it will wake up whoever is waiting for that particular message.

The native side is included in the component view, in form of the BT.dll component. This component handles all communication with the stack (the COM Server).

4.2.1 Native

The stack we call upon is a Component Object Model (COM) which is a binary standard that defines how objects are created and destroyed and, most importantly, how they interact with each other.

We call the defined functions in the COM from our native code and receive messages from the COM. These messages are dealt with, either by confirming the message directly, or by sending the message to our Java code.

4.2.2 Java

In the Java part of our implementation there are two distinctive parts: The Alipes platform device and the Server. Both of these parts use the Bluetooth interface which we implemented.

4.2.2.1 Bluetooth interface

The Bluetooth interface is written in a general way which would make our implementation suitable for other Bluetooth applications as well. Most of the standard functions are implemented, such as starting, connecting, adding services and attributes, searching for services and attributes and of course closing of protocols.

4.2.2.2 The Alipes platform device

The Alipes platform device makes use of the implemented Bluetooth interface in order to complete the positioning task. The complete task to retrieve a position is described in figure 4.2-2 as a flow diagram.

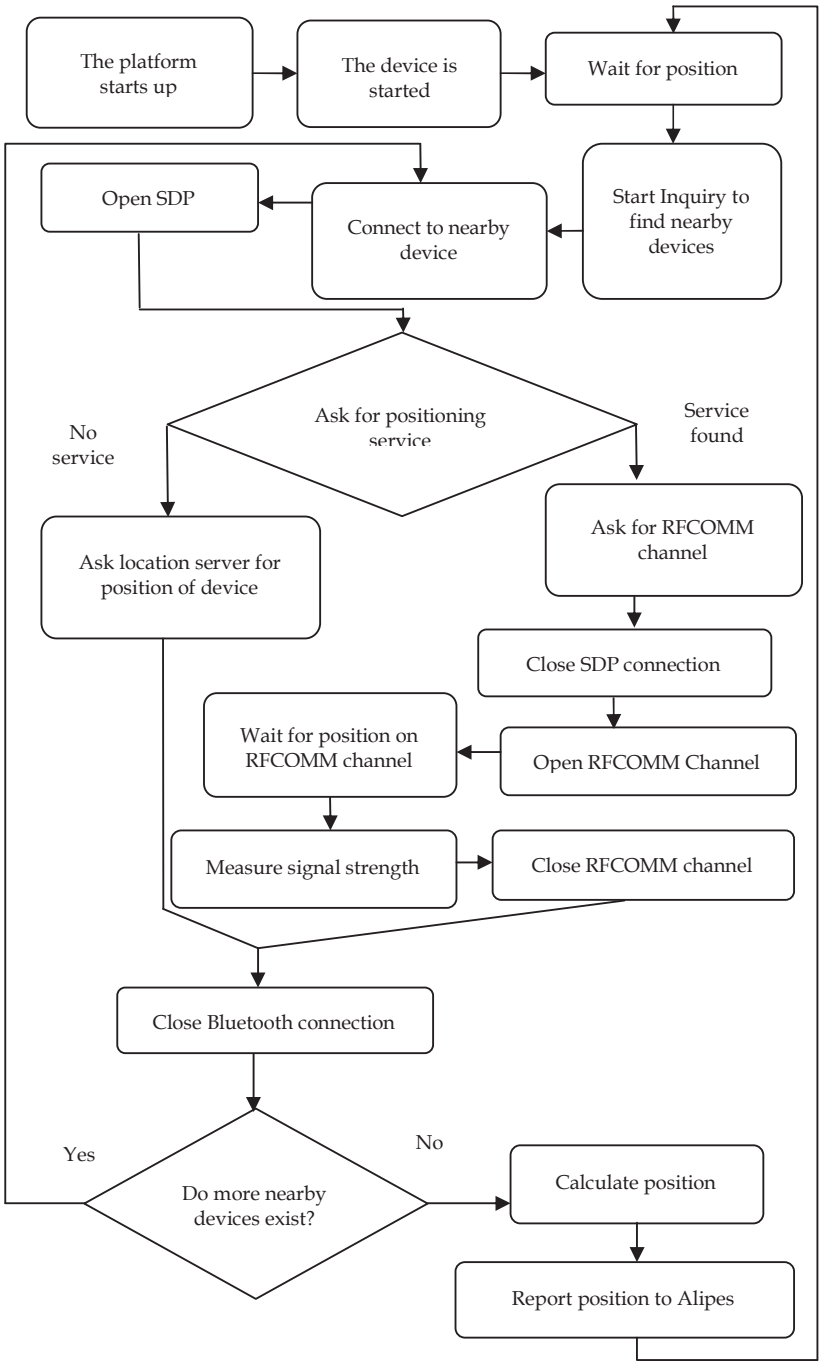

Figure 4.2-2: Flow diagram showing the position retrieving task on the client side.

4.2.2.3 Server implementation

Like the Alipes platform device the server makes use of the implemented Bluetooth interface. The procedure of the server is described in figure 4.2-3 as a flow diagram.

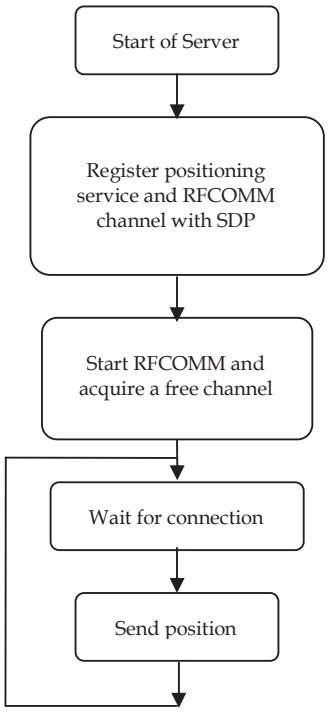

Figure 4.2-3: Flow diagram showing the process of the server.

The component view of the server is very similar to the one of the Alipes platform device. However, as can be seen in figure 4.2-4, the BTServer is the main application. At current date the Alipes platform is not made to run a server. When we made the ServerThread component we constructed it with the intention of sometime include it into the Alipes platform. The final specification for servers in the Alipes platform will determine how much change that will have to be done to our server in order to include it.

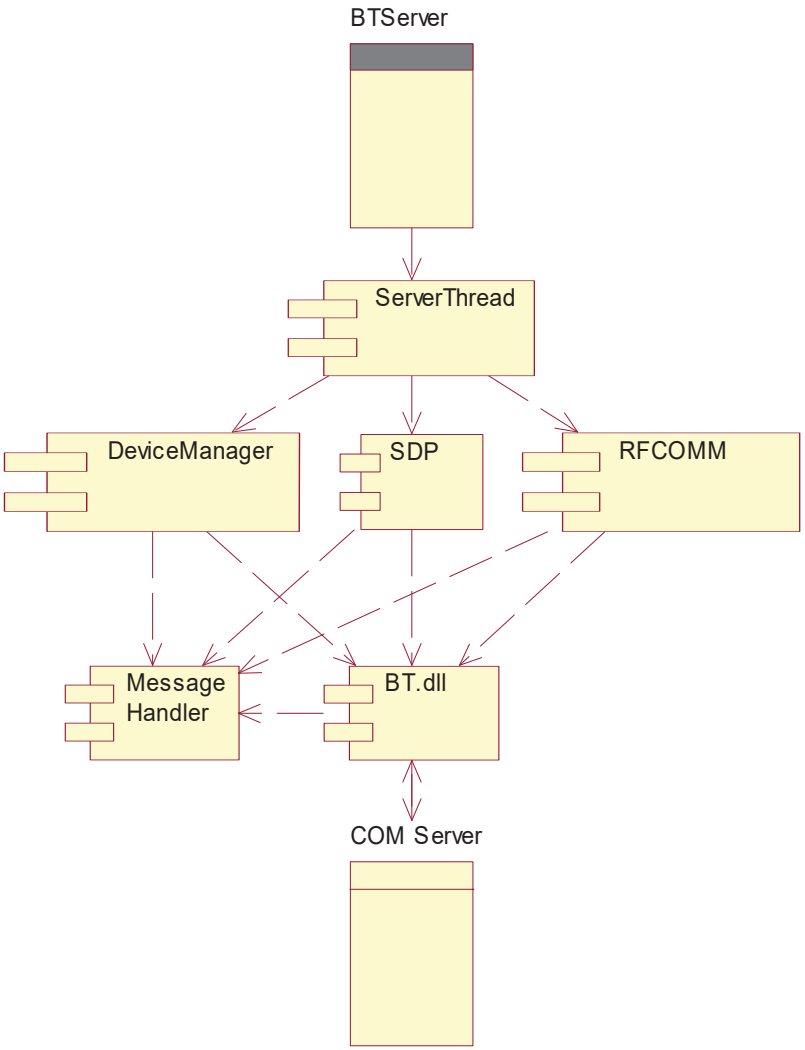

Figure 4.2-4: Component view of the server design

4.2.3 Triangulation Algorithm

To begin we determine the signal strength of the sending device. With this information we can theoretically determine the distance to the positioning source. If only one position source exist this is the only information we can get and our position is defined to be inside a circle around the positioning source with the radius equal to the calculated distance.

The distance from the sending source can be calculated by

$$P(d) = P(d_0) - 10 * n * \log(\frac{d}{d_0}) \quad \text{(Function 1)}$$

where P(d) is the signal strength at distance d, d_0 is a reference distance. $P(d_0)$ is then the signal strength at distance d_0. The variable n is

empirically decided and describes how the signal strength decreases with the distance.

After some modification, you can rewrite function 1, with the reference distance d_0 set to 1 m, to get the distance as a function of the signal strength.

$$d = 10^{\left(\frac{P_0 - P(d)}{10*n}\right)} \qquad \text{(Function 2)}$$

where P_0 is the signal strength at 1 m.

4.2.3.1 More than one position source

If we have more than one source for a position we will get one circle, as described earlier, for every position source as in figure 4.2-5.

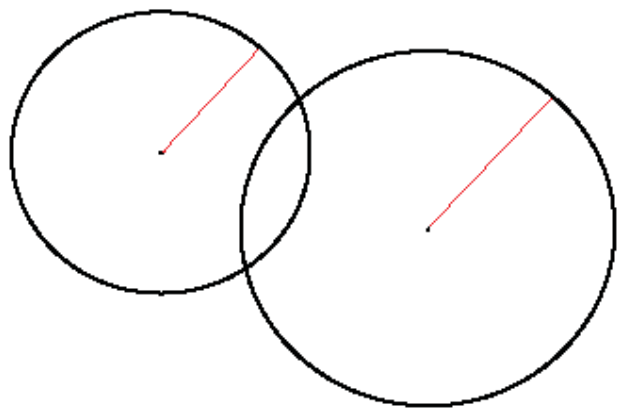

Figure 4.2-5: Two sources of position where the position of the receiving unit is somewhere where these circles intersect..

These circles can be combined to calculate a more accurate position. If we say that all the distances belongs to the set D. Every pair of distances (d_i,d_j), where both d_i and d_j belong to D, are analyzed to find the two intersections (marked in figure 4.2-6) between the two circles.

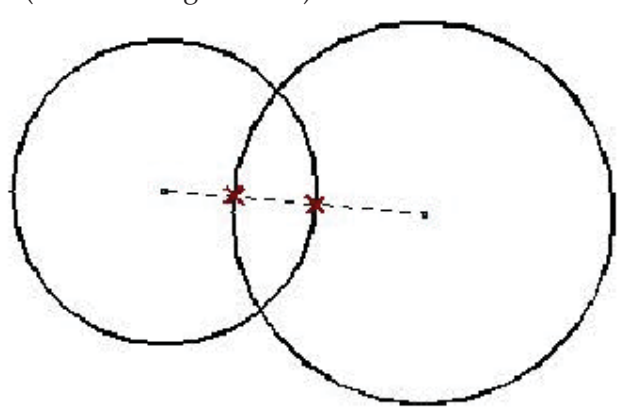

Figure 4.2-6: The intersection points between two circles

If we have two circles that do not intersect, the intersections are made between the circles and a line between the two origins, see figure 4.2-7.

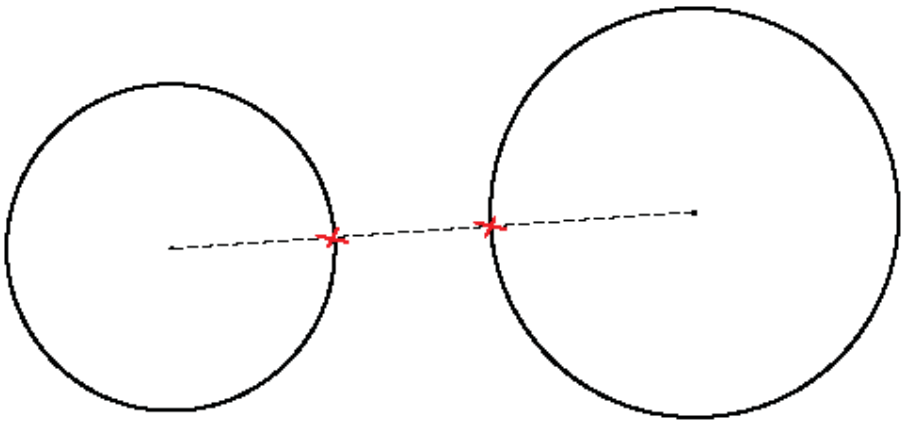

Figure 4.2-7: Two circles that do not intersect

When every pair of distances has been analyzed, we calculate the final position by taking the mean value of all intersection points as in figure 4.2-8.

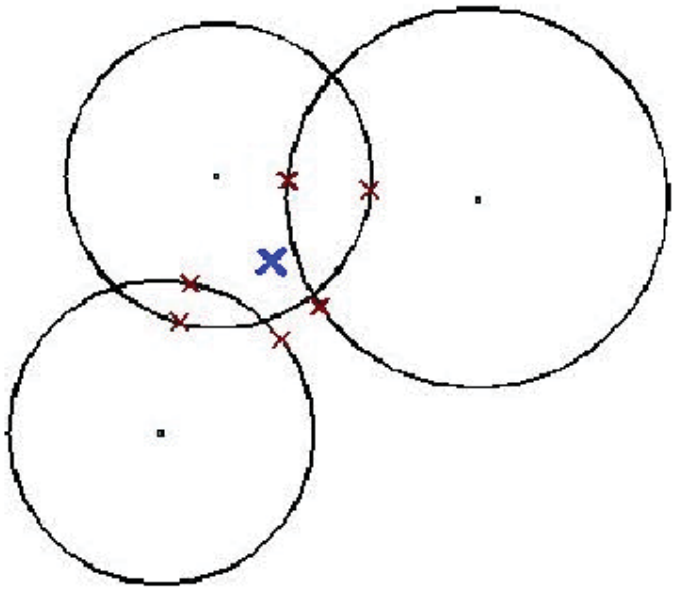

Figure 4.2-8: The mean value of all intersection points are calculated and estimated as the real position marked in the picture with the big blue cross.

To calculate the intersection points of two circles, P3 and P4 in figure 4.2-9, we start by obtaining the angles v1 and v2.

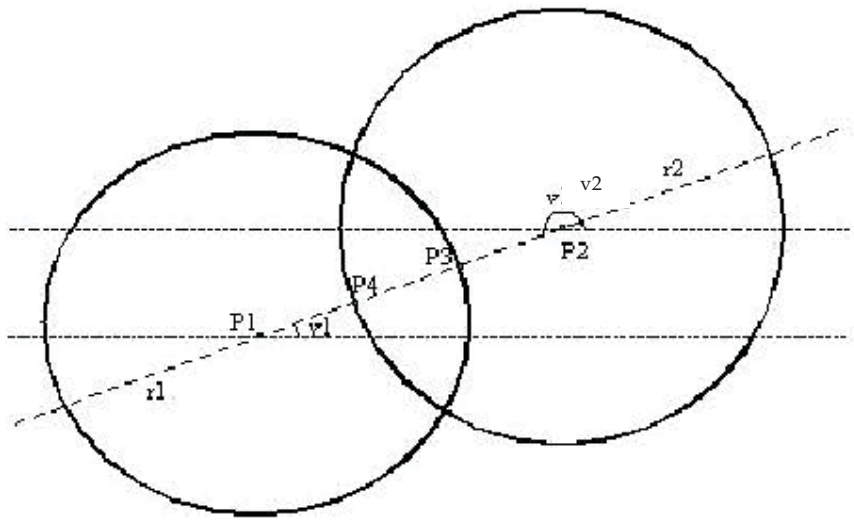

Figure 4.2-9: The intersection points and the angles of interest for calculation

These angles are obtained by

$$v_1 = \tan^{-1}\left(\frac{y_2 - y_1}{x_2 - x_1}\right) \text{ and } v_2 = v_1 + \pi$$

where (x_1, y_1) are the coordinates in the position P1 and (x_2, y_2) are the coordinates in the position P2.

P3 = (x_3, y_3) is then calculated by using the trigonometric functions:

$$x_3 = x_1 + \cos(v_1) * r_1 \text{ and } y_3 = y_1 + \sin(v_1) * r_1$$

P4 = (x_4, y_4) is then calculated in the same way:

$$x_4 = x_2 + \cos(v_2) * r_2 \text{ and } y_4 = y_2 + \sin(v_2) * r_2$$

where r1 and r2 are the radius for the circles.

4.3 TESTING

After and also during the implementation we tested our design and the implemented code. There were 4 different things that we wanted to test: reliability, the signal strengths relation to the distance, performance and also how things would work under more realistic circumstances.

4.3.1 Reliability

To test the reliability of our applications, we started both the server and the client and made them run nonstop for a long period. While they where running we monitored the progress to see that nothing unaccepted happened.

After running for several hours the server was still running without a flaw, however the client had crashed. When checking the log we found that there was something wrong with the timeout when connected to a device. We tested two versions of the client in order to fix the problem. One version with the built in timeout and one with both the built in time

out and the timeout functions included with the stack. With the built in timeouts the program would freeze completely and with the added timeout functions the program would go on but never manage to open another connection since a connection was still waiting for a response or timeout. Our conclusion is that it is an error in the Ericsson Bluetooth stack , which is beyond our control.

4.3.2 Signal Strength

To give as accurate position as possible, the relation of the signal strength and the distance must be tested. The algorithm we discussed in 4.2.3 had a variable that was not defined and the value of this variable was to be determined by tests.

When testing the signal strength in relation to distance it proved to be less reliable than we expected. Our tests showed no relation between low received signal strength and long distance and vice versa. Therefore we decided not to use the received signal strength in our positioning calculations as was proposed in 3.5.4.

4.3.3 Field test

The field test was made to test the setup in a more realistic environment. We set up five devices excluding the client device in a corridor. One of the devices (device B in figure 4.3-1) was running our server software which means it could provide its own position. The other devices (device A, C, D and E in figure 4.3-1) were not running any position server software but had their addresses associated to their position in the location-server database.

Signal strength to determine distance was not used in this test since earlier tests had shown it to be an unreliable source. Thus, the distance was hard-coded to 10 meters.

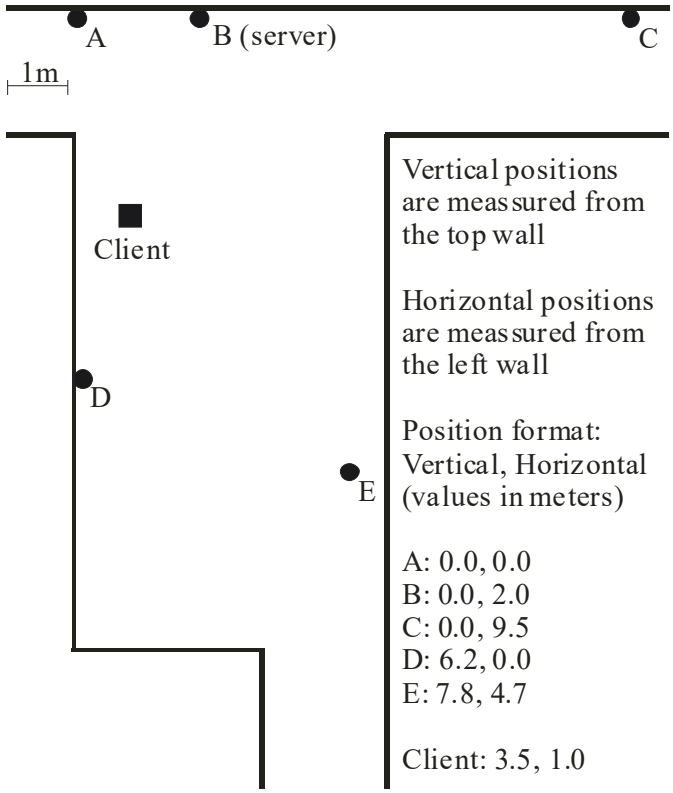

Figure 4.3-1: The field-test setup

The test was performed by letting the client search for a position in its surrounding. For every connection made the time was recorded. The resulting position of the triangulation and the total time for the search was reported in the end. A few of our test-runs can be seen in table 4.3-1.

4.3.3.1 Results from test-run

Test-run nr	1	2	3	4	5
Connect time for A (ms)	1092	2263	431	2875	1712
Connect time for B (ms)	2744	3767	2594	5147	2133
Connect time for C (ms)	5137	5158			2504
Connect time for D (ms)	4386	2063	901	2373	5147
Connect time for E (ms)	5168	2894	1933	2384	4326
Total test-run time (ms)	23764	21391	11156	18076	21140
Reported position	2.07, 0.67	3,50, 1.67	3.50, 1.65	4.67, 1.57	1.95, 4.05

Table 4.3-1: Results from test-runs

Table 4.3-1 shows five of our results that we feel are representative for the field test as the other tests are similar to one of these five. The shaded areas are detected devices where no connection could be made. The blank areas are devices that could not be detected at all.

Range

As seen in figure 4.3-1, device C is approximately 10 meter from the

client. The Bluetooth devices used in this test are of power-class 3 which have a typical max range of 10 meters. Our test confirms this as we can see that device C have very few successful connections and are not even found in some cases.

Our hard-coded value for the distance (10 meters) was therefore a good choice.

Accuracy

In section 3.5.4 we stated that the accuracy is the range of the device or a calculated value. The maximum range have been proved to be approximately 10 meters in normal environments and our tests gives us an accuracy that is better than 10 meters. Assuming the position source has a correct position the accuracy of position over Bluetooth can be said to be 10 meters. Triangulation will in most cases give a better result than 10 meters. We can see this in our tests if the reported position in table 4.3-1 is compared to the real position of 3.5, 1.0. Even though all our tests give us a better result than 10 meters the theoretical worst case is still 10 meters.

Performance

The total connection time consists of two parts: one that is proportional to the number of discovered devices and another that is not. Most of the time is spent waiting for the connections to be established and since this is a linear procedure it will increase the total time with the number of devices as seen in table 4.3-1. If the different connections could be made simultaneously it would mean a great increase in performance.

The performance of the part that does not depend on the number of devices detected might be possible to improve by optimization. This performance increase is very small compared to the performance increase of connecting to several devices simultaneously.

Miscellaneous observations

The resulting positions in table 4.3-1 always end up in the middle of the retrieved positions. This is because of the triangulation. When there are positioning sources surrounding the client the position is more likely to be better than if only one randomly chosen position source were to be used.

This test has also shown that Bluetooth is not perfect when trying to connect. Despite several tests we could never connect to all devices during the same test-run. Device C (figure 4.3-1) is far away from the Client and located behind a corner. The signal strength between the client and Device C is therefore very weak, and as radio waves are sensitive to even the slightest change in the environment the signal strength will sometimes fall under the minimum.

SECTION 5 CONCLUSION AND DISCUSSION

Many different aspects should be taken into account when choosing a communication system for a positioning application. Are we only interested in the position or should the technology be able to work in other ways too? What is the accuracy of the technology and how reliable is it?

In this report we have discussed the best solution considering a few starting points. These starting points are its possibility to be integrated in the Alipes platform, its ability to provide a network connection and its ability to share a position with other devices. As a consequence of these starting points Bluetooth was the technology of choice. If we would have been more interested in price and accuracy instead of network and sharing of position, RFID would be a better alternative.

The test of our implementation showed that Bluetooth can function very well as a position transmitter and/or receiver. The tests also showed that Bluetooth is not very fast but fast enough to meet most position requirements that the Alipes platform have today.

Bluetooth is a rather inexpensive and small size solution and will therefore probably be integrated in a range of different devices. This puts Bluetooth in a very interesting position in the Alipes project. As more Bluetooth devices are used in the daily life, we will have more possible position sources. Bluetooth has the ability to share its position. A device could therefore in theory receive a position from a trusted device 100 meters away or more. The position would of-course be forwarded several times in this scenario and therefore be very inaccurate. With the use of our location server, even the devices that do not use Alipes can be used as position sources.

Alipes is designed to be a generic platform for applications using positioning. It should be able to adapt to different scenarios and situations. RFID would be interesting to implement as a next step because of its low price and therefore the possibility to have a lot of tags spread out to increase accuracy.

5.1 FURTHER WORK

One of the positive sides of Bluetooth is its ability to create small networks with nearby Bluetooth devices. The master device is able to communicate with several slave devices simultaneously. This fact can be used to speed up the connection process by connecting to all discovered devices simultaneously.

The “Bluetooth starter kit” from Ericsson used in this project does not support more then one Bluetooth connection at the same time. Our code is prepared for simultaneous connecting but is at time of writing not using this feature. By introducing a “thread pool” to the Alipes platform device we are able to run each connection as a separate thread. Once we have access to hardware with the newer Bluetooth standard we will be able to implement the simultaneous connecting feature, without much

extra work.

Multicasting is also something that could be implemented. The multicasting would work by letting a server send a position over a channel that is connected to a group of devices. If several devices were to connect to the server at the same time they would all be able to receive the position when it is being sent. This would not give any improvement in speed if only one device is connected and the gain if several devices were connected is very small.

A more interesting improvement would be to let the device maintain connection to the server as long as it is able to. If a device wants to check for a position over and over it would be spared the effort of reconnecting to the known server. This would most likely save both time and power for the device. This however does not only come with advantages but also flaws. There is a limit of seven connections that a server may uphold and if devices were to stay connected it would run out of free connections. This would both hinder new devices from getting a position but it would also hinder the server from doing anything else that is using the Bluetooth too.

A few restrictions could be added in order to limit the downsides of letting devices stay connected to a server. One of these restrictions could be to limit the number of connections allowed for the positioning service. The Server would then use “first in, first out” (FIFO) to supply connections to new devices that wishes to connect.

The Java APIs for Bluetooth is about to be released. Changing our implementation to use these APIs instead of the COM and the native interface should not be too much work. However, at current date only the Java API documentation have been released. Our hope is that with the Java APIs it will be even easier to port our code to different Bluetooth hardware.

REFERENCES

- Alipes

  [1] James Nord, Kåre Synnes, Peter Parnes at Department of Computer Science, Luleå University of Technology, Sweden "An Architecture for Location Aware Applications" June 01, 2001

  [2] Kåre Synnes, James Nord, Peter Parnes at Centre for Distance-spanning Technology and Christian Lundberg at Department of Environmental Planning and Design "Seamless Positioning of Mobile Devices in the Alipes Architecture" 2001

- IrDA

  [3] IrDA, "Serial Infrared Physical Layer Specification" v 1.3, October 15, 1998

  [4] IrDA, "Serial Infrared Link Access Protocol (IrLAP)" v 1.1, June 16, 1996

  [5] IrDA, "Link Management Protocol" v 1.1, January 23, 1996

  [6] Patrick J. Megowan, David W. Suvak, Charles D. Knutson at Extended Systems. "IrDA Infrared Communication: An Overview"

  [7] Stuart Williams at HP Laboratories "IrDA: Past, Present and Future" February 2000

  [8] Ian Miller, Martin Beale, Bryan J. Donoghue, Kirk W. Lindstrom, Stuart Willams at Hewlett-Packard "The IrDA Standards for High-Speed Infrared Communications" February 1996

- RFID

  [9] AIM inc. "Radio Frequency Identification – RFID. A Basic primer" v 1.11, September 28, 1999

  [10] Paul Chartier, Prof/Dr Anthony Furness "A Study of Data Carrier Issues for the Next Generation of Integrated AIDC Technology" 1998

  [11] AIM inc. "Radio Frequency Identification – RFID. A Glossary" v 1.2, August 23, 2001

  [12] AIM inc. "Draft Paper on the Characteristics of RFID-Systems" v 1.0, July 2000

  [13] RF-ID.com http://www.rf-id.com/rfidtech.htm

- Bluetooth

  [14] Jennifer Bray and Charles F Sturman "Bluetooth: Connect Without Cables" 2001, Prentice-Hall. ISBN 0-13-089840-6

  [15] AU Systems "Bluetooth Whitepaper", v 1.1, January 2000

  [16] Amre El-Hoiydi "Interference between Bluetooth Networks – Upper Bound on the Packet Error Rate" IEEE Communication letters, Vol. 5, No. 6, June, 2001

  [17] Xircom "Bluetooth: Technical Background" 2000

[18] Jaap Haartsen, Mahmoud Naghshineh, Jon Inouye, Olaf J. Joerssen, Warren Allen "Bluetooth: Vision, Goals, and Architecture" Mobile Computing and Communications Review, Volume 1, Number 2

[19] Jaap C. Haartsen, Sven Mattisson "Bluetooth – A New Low-Power Radio Interface providing Short-Range Connectivity" IEEE Proceedings of the IEEE, Vol. 88, No. 10, October 2000

[20] Christian Scheingenschlögl, Anton Heigl "Development of a Service Discovery Architecture for the Bluetooth Radio System"

[21] Jaap C. Haartsen, Ericsson Radio Systems B.V. "The Blueooth Radio Systems" IEEE Personal Communication, February 2000

[22] Bluetooth "Specification of the Bluetooth system: Wireless connection made easy – Core" v 1.1, February 22, 2001

[23] Bluetooth "Specification of the Bluetooth system: Wireless connection made easy – Profiles" v 1.1, February 22, 2001

[24] Bluetooth http://www.bluetooth.com

- Other Technologies

[25] HomeRF, "Wireless Networking Choices for the Broadband Internet Home" 2001 (www.homerf.org)

[26] HomeRF, http://www.homerf.org, September, 2001

[27] IEE 802.15 Working Group for WPANs http://grouper.ieee.org/groups/802/15/, September, 2001

- Evaluation

[28] Dave Suvak at Extended Systems, Inc."IrDA and Bluetooth: A Complementary Comparison" 2000

APPENDIX A. ABBREVIATIONS AND ACRONYMS

ACL	-	Asynchronous Connection-Less
AES	-	Advanced Encryption Standard
API	-	Application Program Interface
ASIC	-	Application Specific Integrated Circuits
BER	-	Bit Error Ratio
BlueTooth	-	Short distance wireless cable replacement technology
CAC	-	Channel Access Code
CRC	-	Cyclic Redundancy Check
DAC	-	Device Access Code
DGPS	-	Differential Global Positioning System
DIAC	-	Dedicated Inquiry Access Code
EEPROM	-	Electrically Erasable Programmable Read-Only Memory
EM	-	Electro Magnetic
FEC	-	Forward Error Correction
FHS	-	Frequency Hop Synchronization
FHSS	-	Frequency Hop Spread Spectrum
FIFO	-	First In First Out
GIAC	-	General Inquiry Access Code
GPP	-	Generic Positioning Protocol
GPRS	-	General Packet Radio Service
GPS	-	Global Positioning System
GSM	-	Global System for Mobile Communications
Gula Sidorna	-	Yellow pages
HCI	-	Host Controller Interface
HiperLAN	-	A technology for wireless networks
Home RF	-	A radio based network solution target for regular homes
IAP	-	Information Access Protocol
IAS	-	Information Access Service
IEEE 802.15	-	A future standard for Wireless Personal Area Network
IrCOMM	-	Infrared Communications Protocol
IrDA	-	Infrared Data Association

IrDA Lite	-	Minimal IrDA Protocol Implementation
IrLAN	-	Infrared Local Area Network
IrLAP	-	Infrared Link Access Protocol
IrLMP	-	Infrared Link Management Protocol
IrMC	-	Infrared Mobile Communications
IrOBEX	-	Infrared Object Exchange Protocol
IrTran-P	-	Infrared Transfer Picture
ISM	-	Industrial, Scientific and Medical
kbps	-	Kilobits per second
L2CAP	-	Logical link control and adaptation protocol
LM-IAS	-	Link Management Information Access Service
LM-MUX	-	Link Management Multiplexer
LMP	-	Link Management Protocol
LSAP-SEL	-	Link Service Access Point Selector
Mbps	-	Megabits per second
MHz	-	Megahertz
MPS	-	Mobile Positioning System
NDM	-	Normal Disconnect Mode
NRM	-	Normal Response Mode
PAN	-	Personal Area Network
PDA	-	Personal Digital Assistant
PHY	-	Physical Signaling Layer
Piconet	-	Network of Bluetooth devices. One master with one up to seven slaves.
PPM	-	Pulse Position Modulation
RAM	-	Random Access Memory
RF	-	Radio Frequency
RFCOMM	-	Radio Frequency Communications Protocol
RFID	-	Radio Frequency Identification
ROM	-	Read Only Memory
SAR	-	Segmentation And Reassembly
SB	-	"Sammhällsbyggnads teknik" – A department at Luleå University of Technology
Scatternet	-	Network of piconets.
SCO	-	Synchronous Connection Oriented
SDP	-	Service Discovery Protocol

SDU	-	Service Data Unit
Tiny TP, TTP	-	Infrared Tiny Transport Protocol
UHF	-	Ultra High Frequency
UMTS	-	Universal Mobile Telecommunications System
UUID	-	Universally Unique Identifier
WaveLAN	-	Wave based Local Area Network
WPAN	-	Wireless Personal Area Network
WROM	-	Write once Read Only Memory
XID	-	Exchange Identification
XML	-	Extended Markup Languag

APPENDIX B. THE OPTIONAL IRDA PROTOCOLS

There are several protocols above the Link Management Protocol. Some of these are more important than others. The most important of these optional protocols is the Tiny TP, which is used in most communication.

To help communication to the outside there are also other protocols like IrCOMM that provides serial and parallel port emulation, IrLAN that provides wireless access to local area networks and IrOBEX that provides an object exchange service similar to HTTP.

Some mobile devices need a specification on how to communicate with each other. Digital Image capture devices/cameras and mobile telephony and communication devices are such examples. For these there are separate protocols: IrTran-P for image exchange and IrMC for information exchange in telephony and communication devices.

Smaller mobile devices with limited bandwidth and capacity may need a specialized set of IrDA instructions. For this there is a protocol called IrDA Lite. It provides methods of reducing the size of IrDA code while maintaining compatibility with full implementations.

Tiny TP (TTP)

Tiny TP has two functions:

- Flow control on a per-LMP-connection (per channel) basis.
- Segmentation and reassembly (SAR).

Flow control

Per-channel flow control is currently the most important use of TTP. The IrLAP protocol does offer flow control but in the case of multiplexing, another flow control is needed in order to make it work efficiently. The flow control in TTP is a credit based scheme and it works as follows:

- At connection, some credit is extended by each side. One credit corresponds with permission to send one LMP packet. If one side sends a credit, it must be able to accept a maximum sized packet. The number of credits one side can send depends entirely on how much buffer space that is available.
- Sending data causes credit to be used up (one unit of credit per packet sent).
- Periodically, the receiver issues more credit.
- If a sender has no credit, no data movement can occur, except a credit-only packet, which can always be sent; it is not a subject to flow control.

Although this description talks about the sender and receiver as if those roles were fixed, it is common for both sides of a LMP connection to send and receive.

Segmentation and Reassembly

Some devices with low capacity might not be able to accept full size packages. To solve this problem there is function called "segmentation and reassembly" (SAR) that chops large data packages into pieces, sends the pieces and then puts the data back together on the other side. The entire piece of data being chopped up and reconstituted is called an SDU, or Service Data Unit. The maximum SDU size is negotiated when the TTP/LMP connection is first made.