USE OF BLUETOOTH IN AUTOMATION TECHNOLOGY

SATAKUNTA UNIVERSITY OF APPLIED SCIENCES
SCHOOL OF TECHNOLOGY PORI
BACHELOR'S DEGREE PROGRAMME IN MECHANICAL ENGINEERING
AUTOMATION ENGINEERING AND MAINTENANCE TECHNOLOGY
JULY 2006
MÄKELÄ MIKA

USE OF BLUETOOTH IN AUTOMATION TECHNOLOGY

Mäkelä, Mika
Satakunta University of Applied Sciences
School of technology Pori
Bachelor's Degree Programme in Mechanical Engineering
Field of specialisation: Automation Engineering and Maintenance Technology
July 2006
Commissioned by: Hanzehogeschool Groningen
Supervisor: Eisema, Wouter
Pages: 59

Keywords: wireless, research, application, future

ABSTRACT

In this thesis the main goal was to clearly describe Bluetooth technology's course of action and consider its utilization in Automation field. The research was commissioned by Hanzehogeschool Groningen.

Research was done by using information from internet pages and books from the library. The starting point of the thesis began witch basic knowledge of Bluetooth Technology. The basics were experienced very important and consequently they were produced faithfully. This thesis was made from Bluetooth version 1.2, because it supposedly was the most used version at this moment.

Bluetooth applications tried to come as clear and multi-faceted as possible. The making of this thesis was to consider both the benefits and the drawbacks of Bluetooth technology in different use-targets. All examples tried to represent as simply as possible, so that the idea of Bluetooth applications was understood clearly. In addition, a survey was provided in this thesis of the future applications and the latest version of Bluetooth.

It was mentioned that Bluetooth is an excellent aid for future automation applications. On the other hand, it was noticed, some use-targets, where Bluetooth technology has to develop more to be suited to these tasks.

BLUETOOTHIN KÄYTTÖ AUTOMAATIO TEKNIKASSA

Mäkelä, Mika
Satakunnan Ammattikorkeakoulu
Tekniikan Porin yksikkö
Konetekniikan insinöörin koulutusohjelma
Automaatio- ja kunnossapitotekniikan suuntautumisvaihtoehto
Heinäkuu 2006
Työn tilaaja: Hanzehogeschool Groningen
Ohjaaja: Eisema, Wouter
Sivumäärä: 59

Avain sanat: langaton, tutkimus, sovellus, tulevaisuus

TIIVISTELMÄ

Tämän opinnäytetyön päätavoite oli selvittää Bluetooth:in toiminta-tapa ja sen käyttömahdollisuuksia automaatiotekniikan-alalla. Tämän tutkimuksen tehtiin Hanzehogeschool Groningenin tilauksesta.

Tutkimus tehtiin käyttäen hyväksi internetistä löytyviä tietolähteitä sekä kirjastosta löytyviä alaan liittyviä teoksia. Tutkielman lähtökohtana pidettiin hyvää Bluetooth teknologian perusteiden tietämystä. Perusteet koettiin tärkeiksi ja ne esitettiin huolellisesti. Opinnäytetyö tehtiin Bluetooth:in versiosta 1.2, koska sen oletettiin olevan käytetyin versio tällä hetkellä.

Bluetooth sovellukset pyrittiin tuomaan esille mahdollisimman selkeästi ja monipuolisesti. Tutkielmaa tehdessä huomioitiin sekä Bluetooth tekniikan edut että haitat eri käyttö-kohteissa. Esimerkkitapaukset pyrittiin kuvaamaan mahdollisen yksinkertaisesti, jotta kuva Bluetooth:in käytöstä saatiin selkeäksi ja ymmärrettäväksi. Lisäksi opinnäytetyössä luotiin myös katsaus tulevaisuuden sovelluksiin sekä uusimpaan Bluetooth versioon.

Bluetooth:in todettiin olevan loistava apu tulevaisuuden automaatio-sovelluksille. Toisaalta huomattiin joitakin kohteita joissa Bluetooth teknologian tulee kehittyä paremmaksi sopiakseen käyttökohteeseen.

TABLE OF CONTENTS

LIST OF ABBREVATIONS

ACL	Asynchronous Connection Less
AM_ADDR	Active Member Address = MAC
ARQ	Automatic Repeat Request
AT	Attention Sequence Commands
BD_ADDR	Bluetooth Device Address
BER	Bit Error Rate
CAC	Channel access code
CRC	Cyclical Redundancy Checking
CVSD	Continuously Variable Slope Delta modulation
DAC	Device access code
DSSS	Direct Sequence Spread Spectrum
EDR	Enhanced Data Rate
FD/TDD	Frequency-hop time-division-duplex
FEC	Forward Error Rate
FHSS	Frequency Hopping Spread Spectrum
GAP	Generic Access Profile
GFSK	Gaussian Frequency Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HCI	Host Controller Interface
HEC	Header error control
IAC	Inquiry access code
IEEE	Institute of Electrical an Electronics Engineers
IF	Intermediate Frequency
ISM	Industrial-Scientific-Medical
LAN	Local Area Network
LC	Link Controller
LM	Link Manager
LMP	Link Manager Protocol
MAC	AM_ADDR

OBEX	Object exchange Protocol
PDU	Protocol Data Units
PLC	Programmable Logic Controller
PIN	Personal Identification Number
PPP	Point-to-Point Protocol
QoS	Quality of Service
RF	Radio Frequency
RSSI	Receiver Signal Strength Indicator
SAR	Segmentation and Reassembly
SDP	Service Discovery Protocol
SCO	Synchronous Connection Oriented
SIG	Bluetooth Special Interest Group
SPP	Serial Port Profile
TCS BIN	Telephony Control Protocol
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TDMS	Transition Minimized Differential Signalling
UWB	Ultra-wide-band
VLSI	Very large-scaled integration
WAP	Wireless Application Protocol
WPAN	Wireless Personal Area Network
XOR	Exclusive or

PREFACE

I have made this Bachelor's thesis in Hanzehogeschool Groningen. This thesis is made on research project, which intention was clear out Bluetooth technology's operation and its possibilities in Automation technology. I like to thank Hanzehogeschool Groningen for opportunity to make this thesis.

I would like to thank my thesis's supervisor Mr. Wouter Eisema for his help and guiding. And I also want to express my thanks to whole personnel of Hanzehogeschool Groningen who are been so helpful and comfortable towards me.

Special thanks to Turkka Ruohoneva. Without his computer making of this thesis would have been almost impossible. Thanks to Juuso Ala-Uotila for excellent real-time guidance. Thanks to Maija Malinen and my family for encourage me to do this project.

I also want to thank all people who made this final project possible. And in addition, thanks to people of Plutolaan Student house. We had great time together. And in general, thanks to all people in Groningen for being so liberal and open-minded that this is easy place to stay.

In Groningen 29 of June 2006

Mika Mäkelä

1 INTRODUCTION

It is said that History of Wireless Communications begins at 1896 when Guglielmo Marconi invented the wireless telegraph. In 1901, he sent telegraphic signal across the Atlantic Ocean from Cornwall to St. John's Newfouland. Distance of these places was 1800 miles. [3]

During the past two decades, technology and development of microelectronics and VLSI technology is going forward a lot. This development has driven the cost of many consumers down to an acceptable for average people. Nowadays, trend of different communication types leads to replacing the cables, providing mobility and freedom of movement for the users. Especially mobile phones are shown the way to these wireless communications. In today, the utilization of wireless techniques has spread its possibilities into different kind of application fields. One very interesting sphere of these is *mechanical engineering*. Usually many different wireless transmission methods were initially designed to office devices (printers, faxes, laptops, etc.) and mobile phones but also in the field of *Mechanical Engineering* were also interested for this trend. This wireless communication interested especially for their reliable, wireless, fast connection between two or several machines. They have requirements to reliable, fast and wireless connection between two machines. Bluetooth is one kind of solution to this problem.

Bluetooth is always-on, low cost, low power, radio frequency technology for short-range communications. Bluetooth can be used to replace the cables connecting portable/fixed electronic devices, build ad-hoc network or provide data/voice access points. Bluetooth was initially developed by Swedish mobile-phone maker Ericsson in 1994 as a way to let mobile-phone to make wireless connection with laptop computer. The name comes from 10^{th} century Viking king of Denmark, Harald Blåtand (Bluetooth). [24]

This thesis will focuses basics of Bluetooth technology version 1.2 and also present a couple of different automation application where Bluetooth can be used. Bluetooth technology has many applications which will be used in future.

Chapter 2 reviews the basics of Bluetooth technical solutions. It clears which Bluetooth solution consists of and what were the main goals of Bluetooth technology.

Chapter 3 describes in detail how Bluetooth specification works and what layers there are. The chapter includes accurate description of Bluetooth Radio Layer and Bluetooth Baseband.

Chapter 4 contains introduction of Bluetooth profiles. It is necessary for understanding the Bluetooth as a tool. This paragraph will give a good description what Bluetooth technology needs to work in different applications.

Chapter 5 go into security of Bluetooth in detail. It is very important to know how Bluetooth technology is secured and how it operates. Security is one of Bluetooth's trump cards among other wireless communication types.

Chapter 6 tell couple of typical automation applications of Bluetooth technology. With these examples, you will get better vision where Bluetooth can be used. The results of the experiment are then summarized in chapter 7.

2 BLUETOOTH TECHNICAN SOLUTIONS

The design of Bluetooth was started by setting up different goals, such than any other engineering project. Because Bluetooth was originally designed to mobile phones it seems clearly from the goals, like low cost and low power consumption. Looking at the next table gives a good view of Bluetooth Technical Solutions.

Technical Challenges	***Solutions***
Global operation	2.45GHz ISM band
Interference from other devices using ISM band and other Bluetooth devices	FHSS, Error correction coding
Low power consumption	Power control, Power-saving modes, Programmable packet length, Moderate date rate
Low cost	FHSS, TDMA, Low receiver sensitivity, Relaxed link bugdet, Low IF
Security	FHSS, Link layer security (Authentication and Encryption)
High error probability of wireless link	ARQ, FEC, CVSD (audio)
Voice/Data support	Circuit/Packet Switching

Table 2.10: Bluetooth Technical Solutions [1]

Because Bluetooth technology is designed to applications by different characters, the protocol stack has to be very flexible. However, main idea of creating protocol stacks has been to use as much already exist protocols. That make easier to connect already used applications to Bluetooth technology. It is also noteworthy thing that *data* and *voice* are separate already on low layers of stack. Figure 2.10 is typical Protocol Architecture of Bluetooth. Yellow colored squares are basic layers and red ones are profile- and protocol layers.

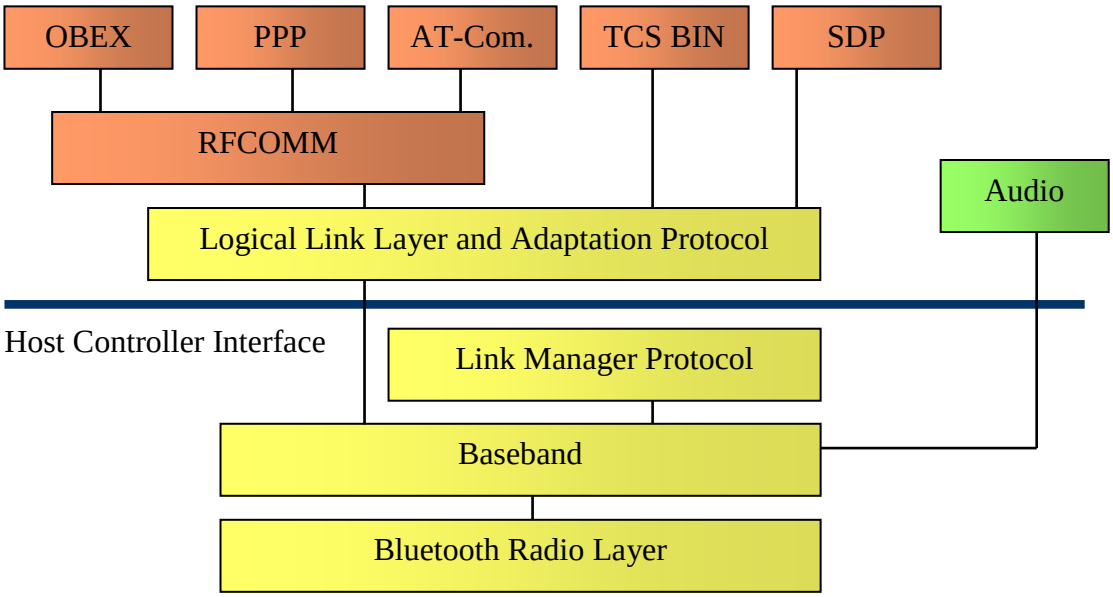

Figure 2.10: Bluetooth Specification Protocol Stack [2]

Documentation of Bluetooth can be splitted into two sections, the Bluetooth Specification and Bluetooth Profile.

- The *Specification* describes how the technology works (i.e. the Bluetooth protocol architecture),
- The *Profiles* describe how the technology is used (i.e. how different parts of the specification can be used to fulfil a desired function for a Bluetooth device) [2].

Above mentioned two sections are treated more better on the following two paragraphs.

3 BLUETOOTH SPECIFICATIONS

Unlike many other wireless standards, the *Bluetooth* wireless specification gives product developers both link layer and application layer definitions, which supports data and voice applications. First Bluetooth specification v1.0 was published in July 1999 and end of same year was published v1.0B. First qualified Bluetooth products based on v1.0B, but also this version has some problems. When v1.1 published in 2001, all former versions problems and contradictions were gathered and specification was also rewritten more clearly in some sections. At towards of year 2003, Bluetooth SIG developed v1.2. The 1.2 version provides backward-compatibility with the v1.1 specification and also includes new characteristic like address security, enhanced voice processing, faster connection setup, co-existence with 802.11 systems and improved quality services. Next will be handled Bluetooth version 1.2 specification more closer.

3.1 Bluetooth Radio Layer

The lowest defined layer of the Bluetooth Specification is the Bluetooth Radio. The Radio layer defines the requirements for a Bluetooth transmitter operating in the 2,4 GHz the Industrial-Scientific-Medicinal (ISM) band (Figure 3.11). Bluetooth uses this frequency band because it’s an unlimited band and available in most countries. The use of this frequency band gives Bluetooth some benefits, like a small antenna is possible (λ= 12.3cm) and other hand use of higher frequency band may cause higher costs. [5]

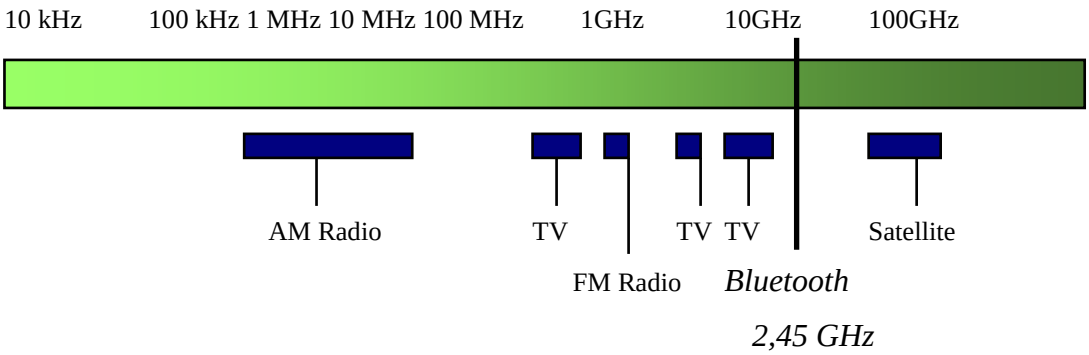

Figure 3.11 Situation of Bluetooth frequency band [6]

The ISM band is open to anyone and this fact causes some problems. The radio systems operating in this band must cope with several unpredictable sources of interference, such as baby monitors, garage door openers, cordless phones and microwave ovens (the strongest source of interference). The Bluetooth technology also has another problem: some countries use different frequency and bandwidth allocation. Table 3.1 shows this difficult situation in better detail. [2]

Area	Regulatory Range	RF Channels
U.S, most of Europe, and most other countries	2.4 to 2.4835 GHz	f = 2.402 + n MHz, n = 0,…,78
Japan	2.471 to 2.497 GHz	f = 2.473 + n MHz, n = 0,…,22
Spain	2.445 to 2.475 GHz	f = 2.449 + n MHz, n = 0,…,22
France	2.4465 to 2.4835 GHz	f = 2.454 + n MHz, n = 0,…,22

Table 3.11 International Bluetooth Frequency Allocations [5]

Nowadays this first version (same than in U.S.) is running. According to current version of Bluetooth specification, 79/23 hops system can not communicate each other and that causes big problems. One goal of the Bluetooth is to get a global standard and this is against it. However, all the time Bluetooth SIG has been actively lobbying those countries with different regulations. Spain, Japan and France are recently released the full ISM band. It is very likely to use the same band globally in the future. But still nowadays there are some different frequency versions. [2]

Frequency-hopping

Since, Bluetooth use same frequency than some other applications (like microwave oven), it has very big risk to interfere to them. This interference can be avoided using an adaptive scheme that finds an unused part of the spectrum, or it can be suppressed by means of spectrum spreading. For example in the US, radios operating in the 2.45 GHz ISM band are required to apply spectrum-spreading techniques if their transmitted power levels exceed 0 dBm. The Bluetooth SIG develop solution on this problem; Frequency-Hopping Spread Spectrum (FHSS). This kind of hopping is usual among low-power radios. So, Bluetooth radios use Frequency Hopping Spread Spectrum, since these technology better support low-cost, low-power radio implementations.

In this 2,4 GHz ISM band, the use of spread is mandatory. Although DSSS (Direct Sequence Spread Solutions) can achieve higher data rate (11Mb/s for IEEE 802.11b standard) this FHSS (Frequency-Hopping Spread Spectrum) has get advantage like low cost, low power and better security. FHSS can also handle near-far problem better than DSSS, because it can effectively block out of band signals. Considering the possible applications if Bluetooth, FHSS is better solution than DSSS. [1]

Frequency-hop systems divide the frequency band into wide frequency area. Thus influence of appear failures reduced on single, narrow frequency-band. This hopping sequence is calculated using the masters' Bluetooth Device Address. The Bluetooth channels use a frequency-hop time-division-duplex (TDD) scheme (Figure 3.1.2.) So, during a connection radio transmission hops from the one channel to another in a sporadically order. This same hopping sequence is shared by all of the devices on a single piconet. [7]

Maximum hop rate is 1600 hops per second and each channel is divided into 625 μs intervals (called slots). Each slot is used by a different hop frequency. One packet can be transmitted per interval/slot. The following slots are alternately used for transmitting and receiving. This communicate type is called Time Division Duplex (TDD). Next figure gives a better description from this. In the figure, k denotes the slot number and $f(k)$ is the physical channel selected during slot period k.

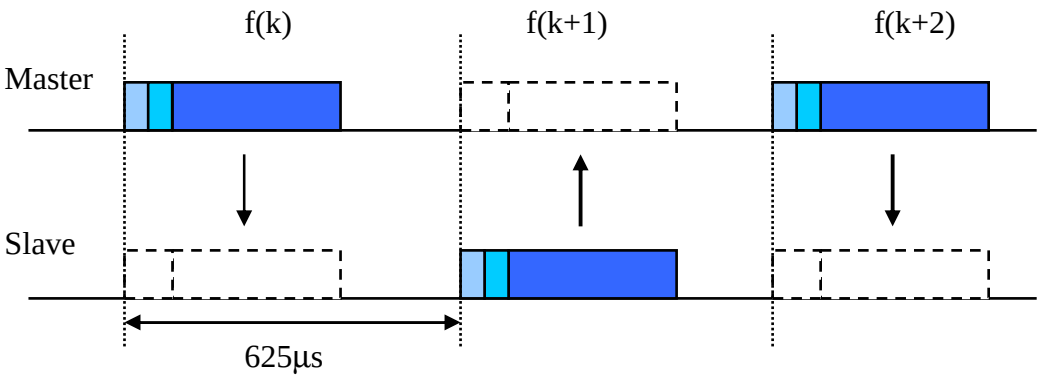

Figure 3.12: Frequency-Hop Time Division Duplex (TDD) [8]

Multislot packets

Transmission of a packet starts at the beginning of a slot. Packet lengths requiring 1, 3 or 5 (every other) slots are allowed. Because more than two devices can share one piconet at same time there have to be also other way. This other access technique is called Time Division Multiple Access (TDMA). TDMA is developed to multislot packets. That means the radio remains at the same at the same frequency until the entire packet has been sent. Following Figure 3.13 shows it. In the next slot after the multislot packet, the radio returns to the frequency required for its hopping sequence, so that during transmission. In this way two or four hop frequencies have been skipped.

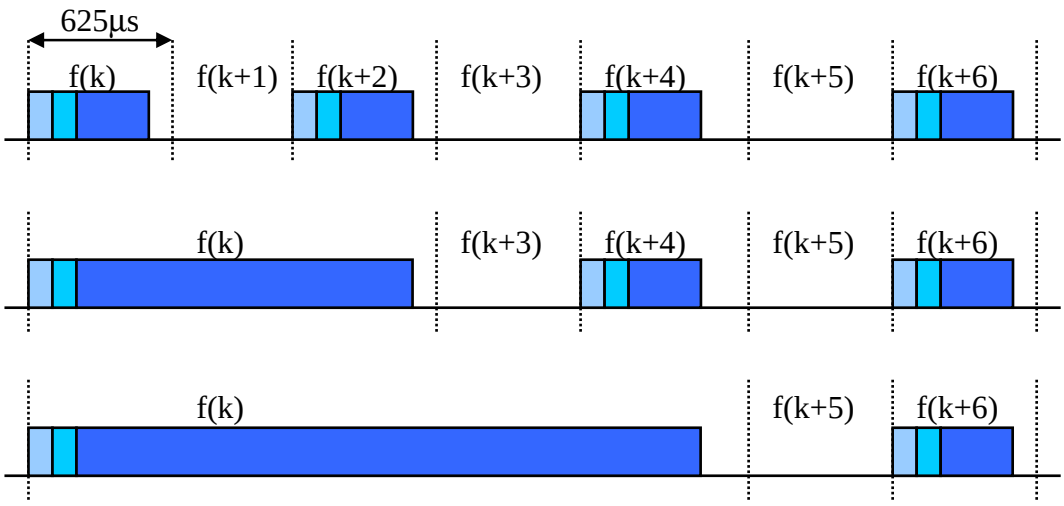

Figure 3.13: Example of Multipslot Packets [8]

The frequency-hop sequence is determined by the master in a piconet and it's a function of master's Bluetooth address. Every piconet has a unique set of master parameters which create a unique channel. Because there are many different piconets in the same area, every piconet should have different master who order the hop sequence.

This kind of frequency-hopping creates opportunities for low-cost, narrowband transceivers with maximum immunity to interference. But sometimes, interference disturbs a hop channel, causing faulty reception. When this happens, Bluetooth has error-correction schemes to restore these bit errors. This Error Correction will treat in paragraph 3.2.4. [7]

3.1.1 Transmitter characteristics

Bluetooth radio module uses Gaussian Frequency Shift Keying (GFSK) as its modulation method. In GFSK a binary zero is represented by a negative frequency deviation and a binary one by a negative frequency deviation. Bluetooth is set to 0.5 and the nominal modulation index is 0.3. [1]

With this GFSK modulation, a symbol rate of 1 Mbit/s can be achieved. In these countries (U.S and most of European countries), where the open band is 80 MHz or wider, 79 hop carries have been defined. But in countries (Japan, France, and Spain) where the band is narrower than above, only 23 hop carriers have been defined. However, on average the frequency-hop sequence visits each slot with equal probability. Following figure shows that curve. [7]

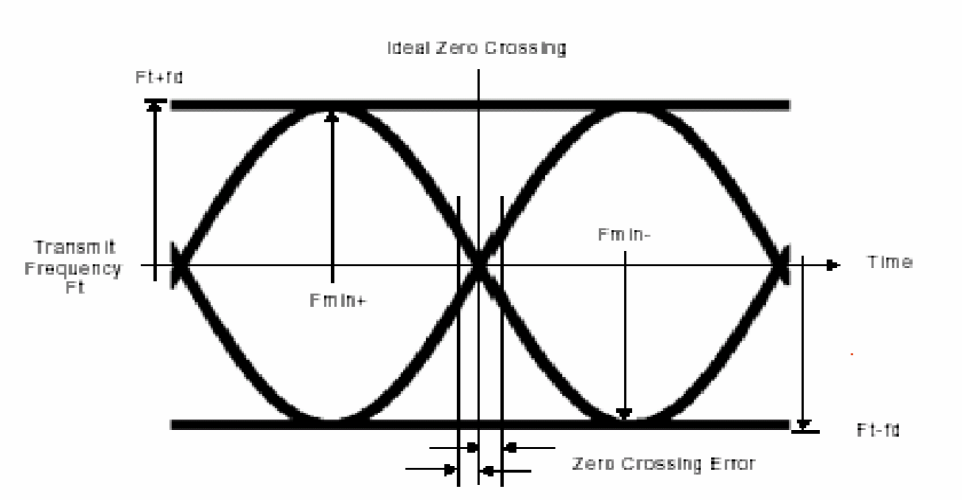

Figure 3.14: Gaussian Frequency Shift Keying [3]

Because Bluetooth was originally designed to mobile phones its power consumption is low. That shows also in Bluetooth radio layer. That is based on a nominal antenna power of 0dBm which consumes only little. [2]

There are three different power classes how Bluetooth devices are classified. These classes are produced in next table:

Power Class	Max Output Power [dBm]	Max range [m]
Class 1	20	~ 100
Class 2	4	~ 10
Class 3	0	~ 10

Table 3.12 Power Classes and Range [2]

The Bluetooth maximum operating range depends on the environment. For instance, if the space where Bluetooth is used is open, then unit may have larger operation range than place where some obstacles are.

Bluetooth's radio transmitter that is classified to class 1 has to have power control because it is mandatory on this class. This power control can rule consumption of power. That saves much of power, because you do not have to use full power if you do not need it, for instance short range contacting. This efficient using of power is

very critical for many portable devices. Power control can also minimize the interference to other devices.

3.1.2 Receiver Characteristics

One of main goals of Bluetooth was to be reliable. This reliability will achieve when bit error rate is low. So, it is defined as the input power level for which a raw bit error rate (BER) is better than 0.1 %. According to this rate, Bluetooth device's mandatory actual sensitive level has to be -70 dBm or better. Bluetooth's sensitivity is higher than many mobile phones. Thanks to developing of Bluetooth technology most of current Bluetooth devices have their actual sensitivity level better than the mandatory level.

Another goal of Bluetooth was to get low power consumption. Also in receiver this matter is consider. That is called Receiver Signal Strength Indicator (RSSI). RSSI is an optional feature, but most of vendors selected to implement it, because this will help reduce the power consumption.

Second benefit of RSSI is adjustment. RSSI compares the received signal power to upper and lower thresholds to see if it is within the "golden receive power range" and notifies the transmitter via Link Manager Protocol (LMP). LMP creates the control message, which it's sent to the opposite device in the packet format. The power amplifier gain on the transmitting side is modified depending on the control message. RSSI isn't very useful only for power control, but it's useful also for connection stability and synchronization. RSSI finds out if the receive power is in the desired range, so-called Golden Received Power Range. [9]

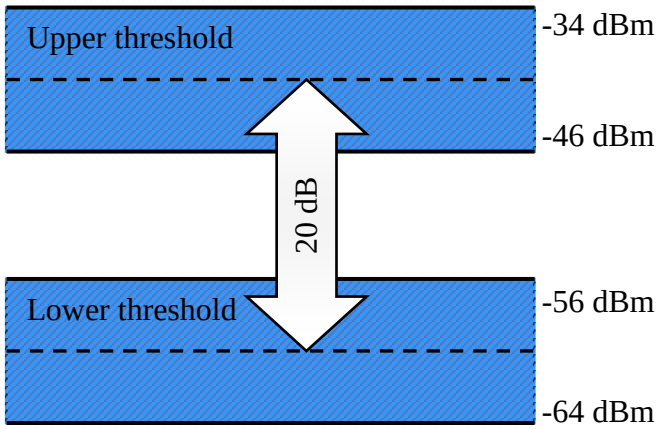

Figure 3.15: Golden Received Power Range [9]

Design of RF has very important role in current Bluetooth single chip implementation, because the cost of RF chip is the major part of most Bluetooth solutions at the moment. In future, it is expected that the cost of RF chips are also going cheaper.

3.2 Baseband of Bluetooth

Baseband of Bluetooth enables physical contact between Bluetooth Radio Frequency and Bluetooth device. Baseband layer uses inquiry and paging methods to synchronize hopping frequency and clock between different Bluetooth devices. Baseband will also define different link types. There are two kinds of types; Synchronous Connection Oriented (SCO) and Asynchronous Connection Less (ACL). It can also define what packet type are used there.

3.2.1 Networking

Bluetooth uses two kind of connection types, point-to-point and point-to-multipoint technologies. Couple of Bluetooth devices can share same channel in same piconet. Devices are connected to net using Ad-Hoc-technology. In that case, every single

device is free to enjoy and leave in piconet. First unit in piconet is master, and one master can have up to 7 active slaves. Then same master can have 256 parked slaves at same time. These master and slaves are physically identical units. The master decides the channel (hopping sequence) that is used. Every contact in piconet transfers via master, but slaves can have connection to other piconet. Although master dominate its piconet it is also possible that master and one of its slaves can change roles in some cases. This is very useful if the master wants to join to other piconet or make a new one. Only one unit can only be a master of one piconet, but it can also be a slave in other piconet at same time. Thus, one unit can be the member of two piconets. Figure 3.21 shows that. When many piconets are together, it is called a scatternet.

The benefits of the piconet or scatternet scheme are that it can contact many devices together in same physical area. This makes also use of the bandwidth more efficiently. In one scatternet can be up to 10 piconets at same with minimal risk to impact on each other.

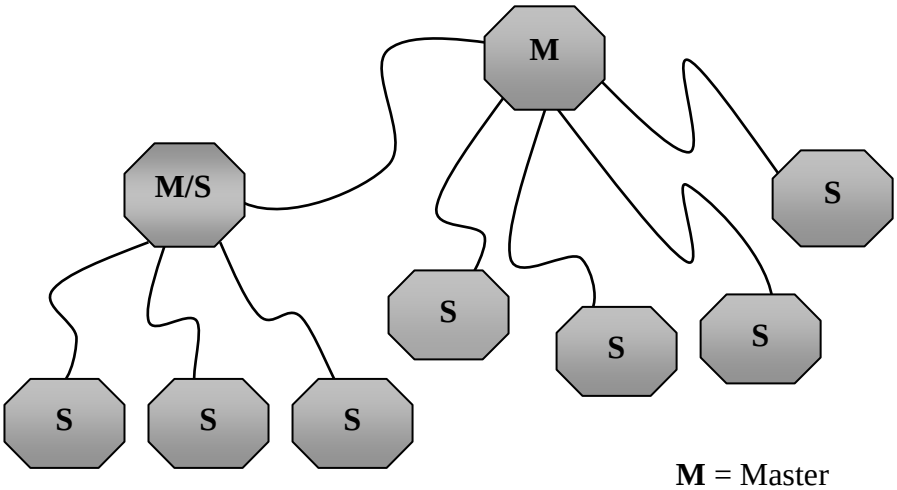

Figure 3.21: Master/Slave Relationships [5]

The piconets that join to scatternet will separate each other by its frequency and sequence-hopping. In addition piconets have not been synchronized to each other. The main idea of this topology is that every piconet will get own 1 MHz hopping-channel. If this will occur then the biggest possible data transmission capacity is available for every piconets.

Occasionally, some impacts can occur when piconets chose same sequence at same time. Benefit of Bluetooth system is that systems penetration capacity decreases very slowly because one piconet can have only one connection at same time. That means only one piconets traffic will disturb, not whole scatternet.

Every Bluetooth unit has a unique 48-bit Bluetooth device Address. So that device will be known in piconet, it has also 3-bit Active Member Address (AM_ADDR) given by master. Only devices which are on active mode can have this address. [1] + [10]

3.2.2 Physical Links

In Baseband two types of links can be established between master and slave:

- Synchronous Connection Oriented (SCO): This is synchronous point-to-point connection between master and a single slave. SCO makes a fixed bandwidth which is suitable for instance voice transfer. The master maintains the SCO link by using reserved slots of regular intervals. Simultaneous master can support up the tree SCO and slave can support to 2 SCO links. Both the master and slave can initiate a SCO link. The maximum data rate of SCO link is 64Kb/s and these packets are never retransmitted.
- Asynchronous Connection-Less (ACL): ACL is a point-to-multipoint link between master and the all slaves in the Piconet. The master can exchange packets with any slaves in these slots which are not reserved for SCO links. To exchange packets ACL link uses per-slot basis. The master can also change packets with slave who has already SCO link, but master can exist only one ACL link at a time (Figure 3.22). Differently than SCO packets, most ACL packets retransmission is applied. [5]

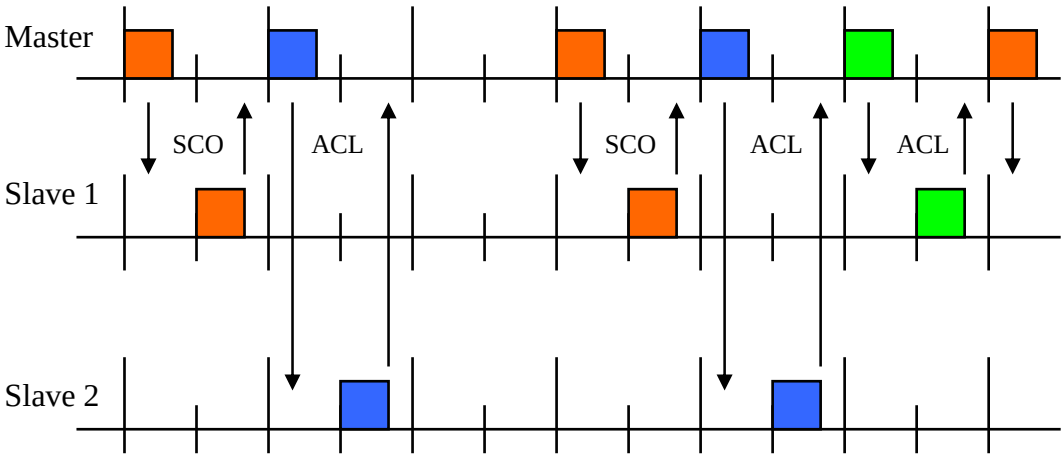

Figure 3.22: SCO and ACL links in same piconet [7]

3.2.3 Packets

There is couple of different packet types defined for baseband layer of Bluetooth system. Four packets are defined for both SCO and ACL links, these are ID, NULL, POLL, FHS (and DM1). These are control packets which are used for synchronization, polling and other channel control functions. Illustrative table is finding from APPENDIX 1. [2]

Each packets uses similar packet format. It consists of 3 entities; the access code (68/72 bits), the header (54 bits) and the payload (0-2745 bits). This packet format is illustrated in Figure 3.23.

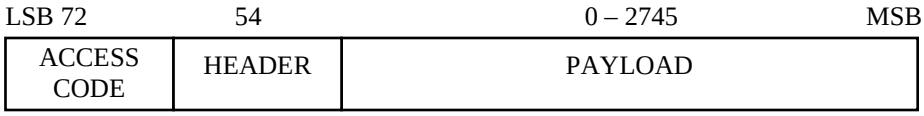

Figure 3.23: Bluetooth packet format in one slot [2]

Access Code

Each packet has 72-bits access code which is same for all packets in one piconet. Access codes are used for synchronization, identification and compensation of offset. There are tree types of access codes:

- Channel access code (CAC): To identify a piconet
- Device access code (DAC): To paging and subsequent responses
- Inquiry access code (IAC): To inquiry of purposes

The access code consists of a 4 bit preamble, a 64 bit synchronization word and possibly a 4-bit trailer (Figure 3.24). The preamble and trailer are used for DC (Direct Conversion) compensation. Sync Word is used to determine the timing. The access code is very robust and has well resistant to interference. [2]

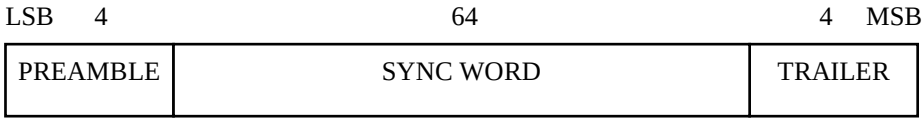

Figure 3.24: Bluetooth Access Code [10]

Packet Header

The Packet Header consists of six fields (Figure 3.25). The header starts with 3 bits Member Address (M_ADDR or MAC). With member address unit will know in a piconet. The 4-bit Type code specifies which packet type is used. These Flow, ARQN and SEQN bits are used to provide different data of packet. The last one is 8-bit Header error control (HEC). It is used protect the packet header. The header is protected by 1/3 rate Forward Error Rate (FEC) code because header includes very important information and is susceptible errors. Because of this 18 bit the header requires 54 bits on the packet [5]

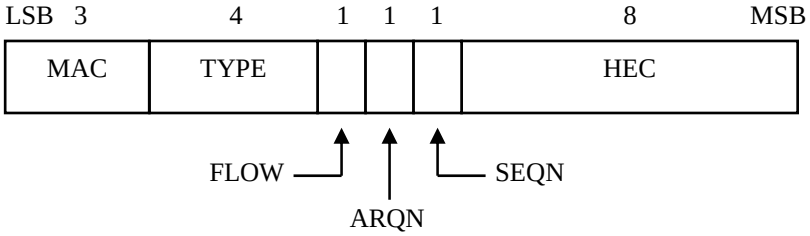

Figure 3.25: Bluetooth Header Code/Format [10]

Packet Payload

The Packet Payload can be different sizes, it depends the type of packet. For example, single-slot packet is smaller than multi-slot packet. The packet payload can

include either voice field, data field or both. The payload format consists of three fields:

- Payload Header: 8-bit header to single-slot packets and 16-bit header multi-slot packets.
- Payload Body: This contains user information.
- CRC: a 16-bit CRC code which is used on all data payloads.

The Payload Header consists of three fields:

- L_CH: used to identify logical channels
- Flow: Used to control flow at the L2CAP level.
- Length: Includes the size of payload, excluding header and CRC. In single-slot packets it is 5-bit and multi-slot packets it can be 8-bits.

3.2.4 Error Correction

There are three kinds of error correction schemes used in Baseband level:

- 1/3 rate Forward Error Correction (FEC)
- 2/3 rate FEC
- Automatic Repeat Request (ARQ)

The 1/3 rate FEC is used on the 18-bit packet header and also for the voice field in HV1 packet. The scheme sends three copies of each bit and it is usually used in links with very high probability of error. The 2/3 rate FEC is used in all DM packets and in data field DV-, FHS- and HV2 packets. The encoder is a form of Hamming code with parameters (15, 10). This scheme is suitable for medium rate data transmission.
The ARQ is unnumbered Bluetooth scheme and it is called fast ARQ scheme. This means that whenever the slave received the packet from master successfully, it announces it to master by send one bit reply to the master. After that when master get reply it will sent next packet. If there occur some failure (or a timeout occurs) master will send a new packet to slave. After that, master moves to next packet. Figure 1 illustrates this technology. This fast ARQ scheme helps to minimize the overhead of transmission. [1]

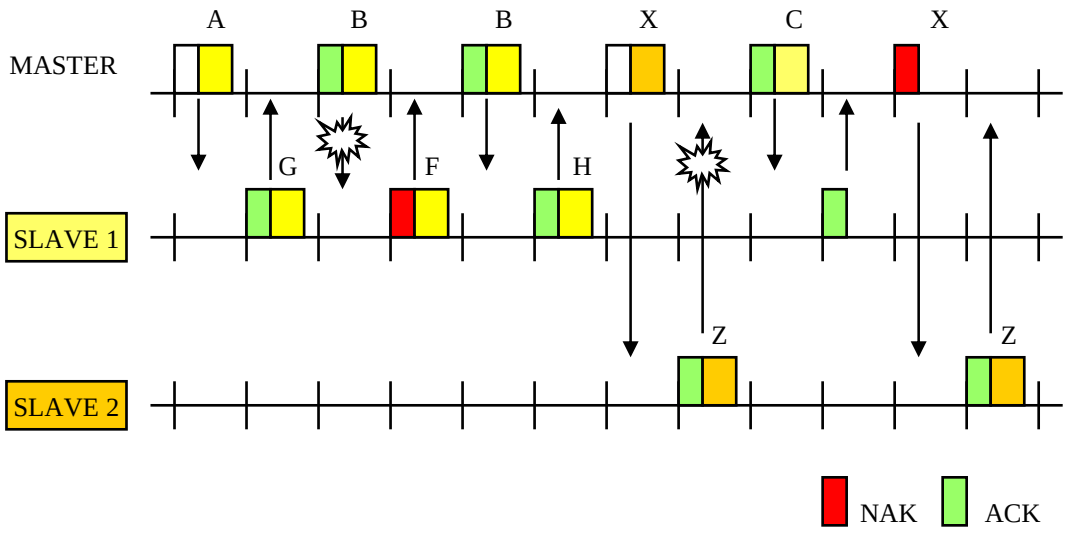

Figure 3.26: An Example of Retransmission Operation [1]

In additional to these three error correction schemes there is also two correction measures stated above;

- 8-bit Header Error Correction (HEC), which is used in header.
- 16-bit CRC, which is used to protect data payload.

It is also possible that more than one error correction scheme is used and it makes Bluetooth more robust against errors.

3.2.5 Channel Control

In piconet operation is two kinds of controller states. These major states are:

- *Standby*, this is the default state. In this a low-power state only the native clock is running.
- *Connection*, this is a state when device is connected to a piconet as master or a slave and it can exchange packet using the channel access code and the master Bluetooth clock. [2]

In addition, there are seven interim substates (Figure 3.27). These states are used to add new slaves or establish a new piconet. These substates are followed:

- Page: Used to master to activate and connect to a slave.
- Page scan: Device is listening for a page with its own DAC.
- Inquiry: Device uses it to identify other devices within range.
- Inquiry scan: Device is listening for an inquiry.
- Master response: A device acting as a master receives a page from a slave.
- Slave response: A device acting as a slave responds a page from a master.
- Inquiry response: A device that has issued an inquiry receives as inquiry response.

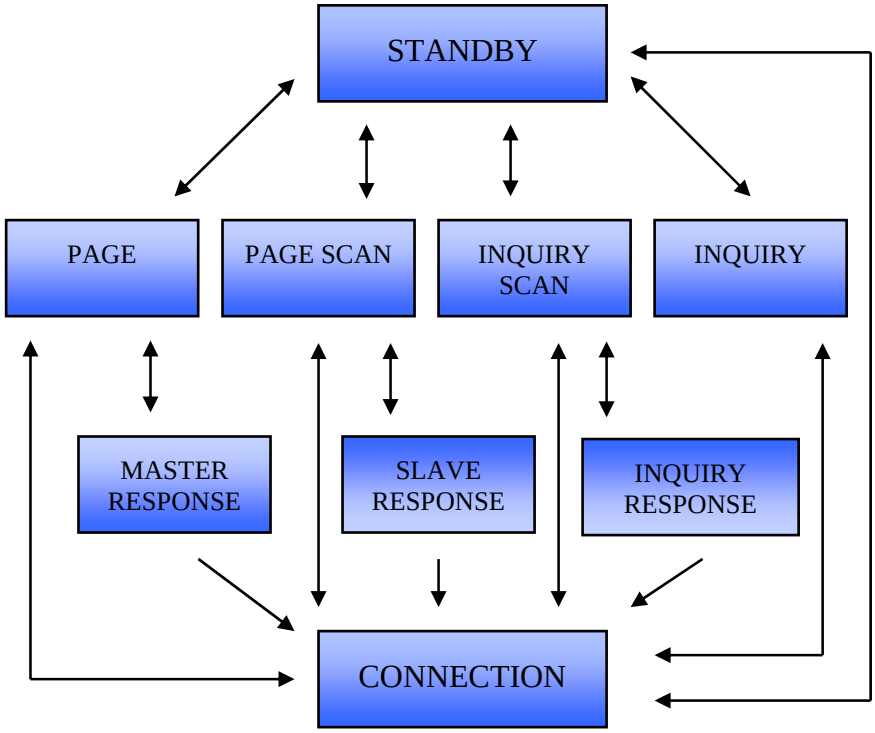

Figure 3.27: Bluetooth State Transition Diagram [5]

Bluetooth units default state is Standby. In Standby state, unit is in low-power mode. Only what it will do is scan for paging or inquiring messages for it. In Standby mode unit is under 1% of its duty cycle. To found a new connection the master has to know the Bluetooth Device Address of the slave, and correspondingly the slave need to know the timing of the master.

The first step of establishing a new connection is that unit (master) enters the inquiry state to see if there are other Bluetooth devices nearby. Another unit has to be in the inquiry scan state to receive its inquiry message. After receive slave will respond to the master with information of its Bluetooth device address. Next a master unit enters page state. The master will use slave's Bluetooth Device Address to form a paging message. The master send the paging message to slave unit which is in page scan state ready receive it and return a response. At lastly the master unit will sent a FHS packet to help the slave to synchronize the master clock. After that the connection between the master and the slave is established. [1]

The Bluetooth device in the connection state can be four different modes. These modes are: (Active mode, Hold mode, Sniff mode and Park mode.)

- Active Mode: In the active mode, the Bluetooth unit actively participates in the piconet. Active slaves listens in the master-to-slave slots for packets which are addressed to it. If there are no addressed packets, it may sleep until the next new master transmission. Sometimes the master transmits to the slave to maintain synchronization.
- Sniff Mode: In the sniff mode, the slave listens only specified slots for its messages, not every receive slot. Like this the slave can operate in reduced-power status the most of time. The sniff mode has highest duty cycle among three power saving modes.
- Hold Mode: In the hold mode, the slave wills reduce-power to sleep for present of period. After that period it restarts data transfers instantly. This period is negotiated between the master and the slave. Only an internal timer is running on this mode. Benefit of this is that, if slave unit have less power it can also demand to be put into hold mode.
- Park Mode: In the park mode, the unit has a low-power consumption and very little activity. The slave gives up its active-member-address and gets a new 8-bit parked-mode-address by master. The slave-unit is still synchronized to the piconet but does not participate in the traffic. With use of park mode, the piconet may have more than seven slaves. [5]

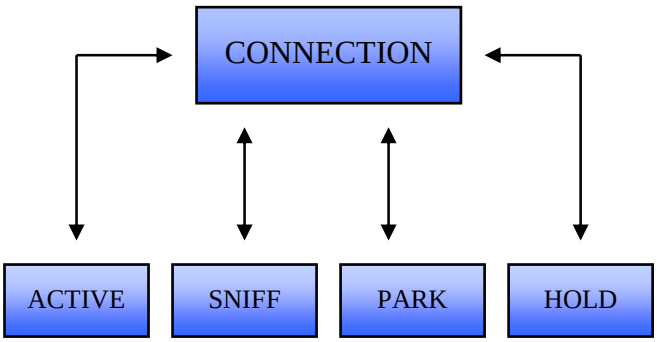

Figure 3.28: Connection modules [5]

By switching between active and park mode one piconet can have up to 256 members. And one unit can participate multiple piconets by putting itself into park mode in some piconets. By this way Bluetooth devices can build very big scatternets.

3.3 Link Manager Protocol (LMP) and Host Controller Interface (HCI)

The Bluetooth system is managed by Link Manager (LM) and it uses a Link Manager Protocol (LMP) to communicating with other LM's (other Bluetooth devices). The LMP handles for instance negotiates authentication parameters and the authentication procedure. In addition it carries out link setup, link configuration and power control etc.

To get its work done, LM uses the services of Link Controller (LC). LMP messages are used to make connections, net control and carry out safety features. LMP essentially consists of a number of Protocol Data Units (PDU). These PDUs are sent from one unit to another. Messages are always sent as single slot packets with 1-byte payload header. [2] + [5]

The LMP offers Host Controller Interface (HCI) to upper layers. The HCI provides a command interface to the baseband controller and link manager, and access to hardware status and control registers. The HCI exist 3 sections;

- The Host
- Transport Layer
- Host Controller

Every one of these sections has a different role to play in the HCI system. More information about LMP and HCI can be found on Bluetooth SIG's WebPages**.**

3.4. Logical Link Control and Adaptation Protocol (L2CAP)

Logical Link Control and Adaptation Protocol (L2CAP) is the protocol which most applications would interact unless a host controller is used. It makes possible to connection-oriented and connectionless data services of upper layers, so that different applications can use that protocol what they want, like RFCOMM, TCP/IP or SDP. [9]

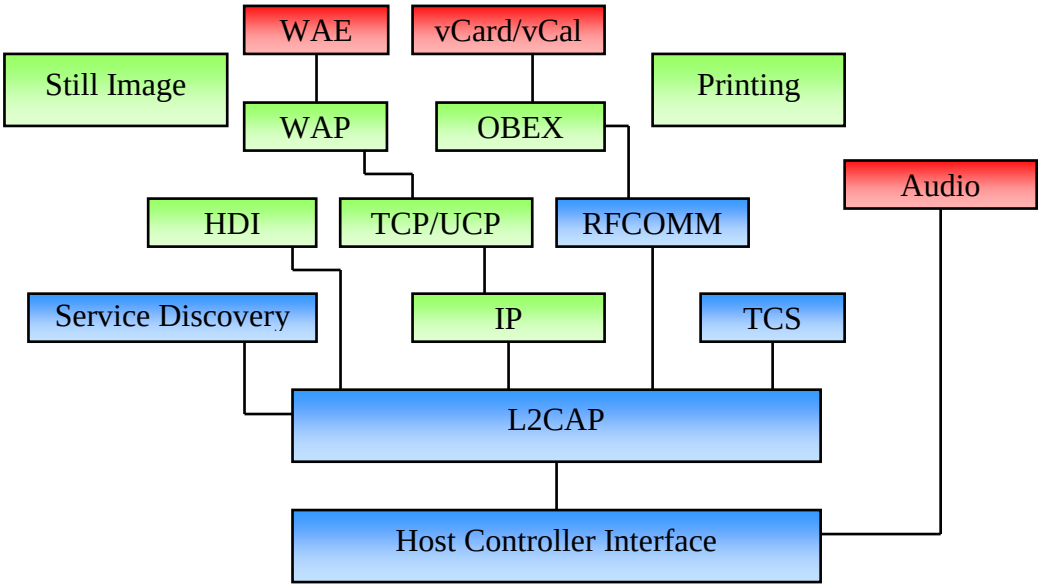

Figure 3.41: Protocol Layers [9]

Main duties of the L2CAP are:

- *Multiplexing*: The L2CAP must support protocol multiplexing, because the Baseband can not do it. The L2CAP must be able to distinguish between upper layer protocols like SDP an RFCOMM.
- *Segmentation and Reassembly (SAR)*: Because L2CAP itself accept packets sized up to 64kB, but the Baseband packets can accept a payload of at most 2745 bits, it have to segmented packets into multiple smaller Baseband packets.
- *Quality of Service (QoS)*: The L2CAP connection establishment process allows the exchange of information regarding the quality of QoS expected between two Bluetooth units. L2CAP checks it the link is capable of providing and provides it if possible.
- *Group's abstraction*: In Baseband protocol devices synchronize hopping together using the same clock (master's clock). In L2CAP group abstraction permit implementations to efficiently map protocol groups on to piconet. Without this group abstraction, higher level protocols would need to be exposed to the Baseband Protocol and Link Manager functionality in order to manage groups efficiently. [2]

3.5 Upper Layers

In Bluetooth protocol architecture is couple of layers upside of L2CAP. Here are the general of them:

- *RFCOMM*

  RFCOMM is the cable replacement protocol which is based the ETSI standard TS 07.10. RFCOMM enables the replacement of serial port cables with the minimum of modulation of existing devices. It is used to provide emulations of RS232 serial ports over the L2CAP protocol. It makes possible up to 60 contemporary connections between two Bluetooth devices. [2]

- *Service Discovery Protocol (SDP)*

  The Service Discovery Protocol (SDP) is a simple protocol with minimal requirements on the underlying transport. It enables the devices to find which services are available in proximity and characteristics of the services. [2] + [5]

- *Point to Point Protocol (PPP)*

  The PPP is an Internet standard protocol for transporting IP datagram's over a point-to-point link.

- *TCP/UDP/IP*

  These are the foundation protocols of the TCP/IP protocol suite.

- *Object exchange protocol (OBEX)*

  This is a session-level protocol developed by the Infrared Data Association for the exchange of objects.

- *WAE/WAP*

  Bluetooth incorporates the wireless application environment and the wireless applications protocol into its architecture.

- *Telephony Control Protocol (TCS BIN)*

  This is a bit-oriented protocol which is meant to transmitting of speech and data calls between Bluetooth devices.

- *Attention Sequence Commands (AT)*

  Is a protocol for to help modem contacts.

4 BLUETOOTH PROFILES

One of Bluetooth's main aims was that different Bluetooth-units from different vendors be able to communicate each other seamlessly. Because Bluetooth technology is suitable for many different devices, so it is not possible that every unit can communicate in the same way. The Bluetooth SIG took this into consideration when they were designing Bluetooth communications. For this reason devices are divided in groups (profiles), which each support some certain features. With these profiles Bluetooth connection can be used in different applications regardless of devices. [11]

There are 26 Profiles and 3 protocols described in version 1.2 specification. Each profile is designed for a specific task. Four profiles are foundation profiles, providing the building blocks upon which other profiles are constructed. Then the rest ones are usage profiles. These usage profiles defined the ways how Bluetooth technology can be used. [3]

The Bluetooth profiles also provide the foundation for future user models and profiles. A one profile can be described as a vertical clice through the protocol stack, without one slice stack is handicapped. It means that each profile is important to form working connection between Bluetooth devices. For instance, if you need to use Fax profile on your application, so you have to also use Serial Port profile and General Access Profile. This procedure is used to decrease to the risk of interoperability between different manufacturer's products, because now they can easily check how they have to build their own Bluetooth unit/connection. [3]

Bluetooth profiles, protocols and these dependences for each other are illustrated on Figure 1. The profiles are produced one on top of the other. The profile witch is above other profile is dependence all these profiles which are under it. After figure there is short description for each protocol and profile.
[2] + [3]

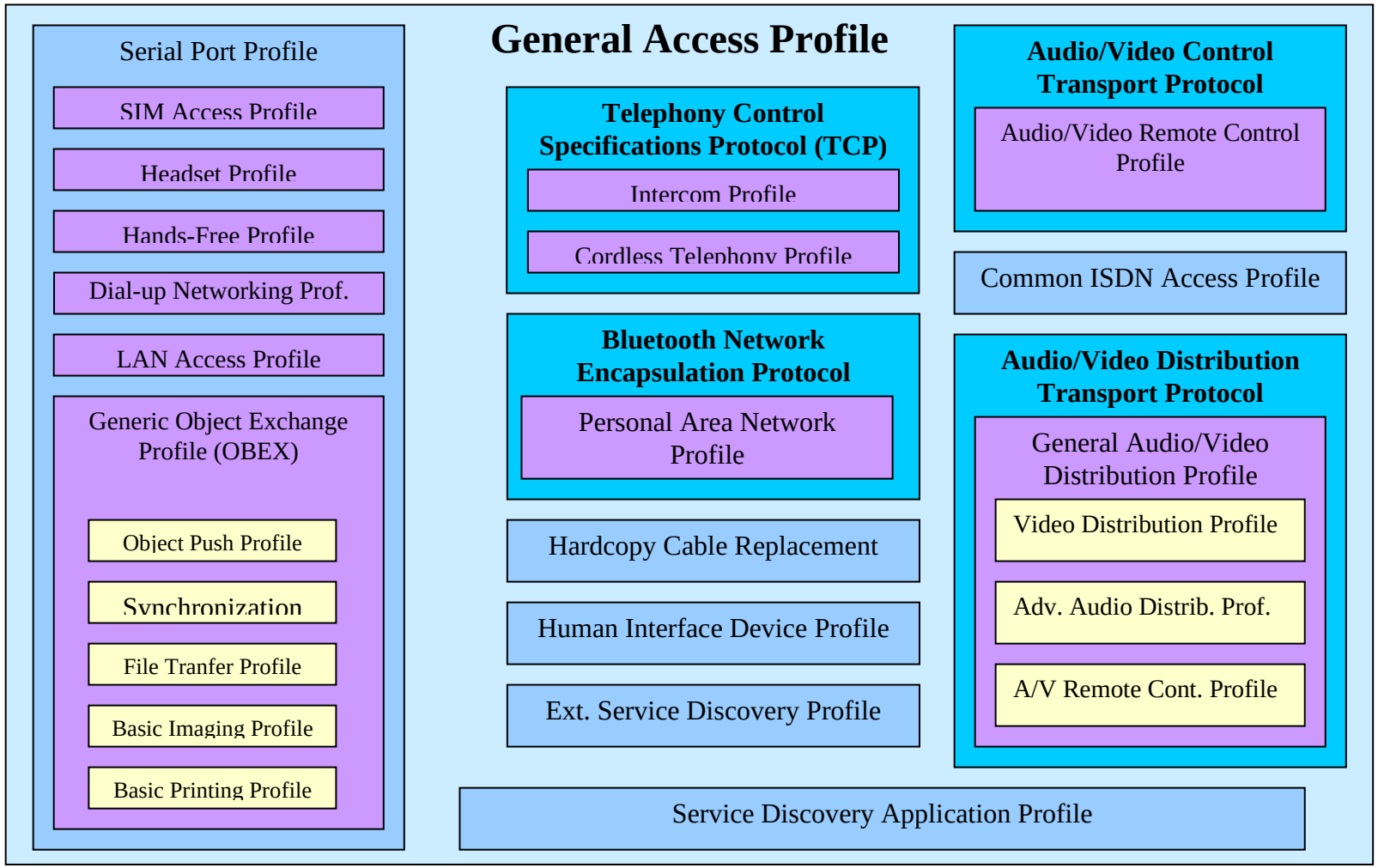

Figure 4.10: Bluetooth Profiles [3]

Current Bluetooth Application Profiles:

1. *Generic Access Profile* (GAP) – is a basic profile, which main intention is describe using of lower layers of Bluetooth protocols so that not have to do separately. GAP defines also functions to device search, link management and security levels. GAP has to be identical in all Bluetooth Devices.
2. *Serial Port Profile* (SPP) – defines protocols and operations to Bluetooth devices which are used serial-port emulation. It is based on the ETSI T07.10 specification and uses RFCOMM protocol. SPP is for foundation to many profiles; like LAN Access, Headset and Fax profiles.
3. *SIM Access Profile* (SAP) – which controls the wireless access to the data on the SIM card in the mobile phone.
4. *Headset Profile* (HSP) – defines how Bluetooth communication can be used between headset and a mobile phone or PC. Headset profile can act remote device's audio input and output interface, which means that you can use it for headset with microphone.
5. *Fax Profile* (FAX) – defines how Bluetooth communication can be used with Fax gateway devices. For example between mobile phone and PC with Fax.
6. *Hands-Free Profile* (HFP) – defines how Bluetooth device can receive calls from a hand-free device. A typical example is hands-free set in our car which works via car's own stereo system.
7. *Dial-up Networking Profile* (DUN) – defines how Bluetooth device can form phone contact to other device. The most common scenario is accessing the Internet form a laptop by dialling up (wirelessly) a mobile phone. DUN can only used in point-to-point links.
8. *Local Area Network Access Profile* (LAP) – defines using of point-to-point protocol (PPP) in above of RFCOMM serial-port emulation. It is usually used in Bluetooth base stations. It has three defined situations: 1. local area network of single device, 2. local area network of many devices, and 3. communication between two devices.
9. *Generic Object Exchange Profile* (OBEX) – is a transfer profile, which defines data objects and a communication devices can use to exchange those objects. Only connection-oriented OBEX is supported to Bluetooth devices. OBEX has 6 different profiles which are using it.

10. *File Transfer Profile* (FTP) – is used to browse of files, file convention and transferring from other Bluetooth devices.
11. *Object Push Profile* (OPP) – is used by sending of pictures, vCards and vCal-files to other devices.
12. *Synchronization Profile* (SYNC) – defines how files will synchronize between many Bluetooth devices.
13. *Basic Printing Profile* (PBP) – defines settings of Bluetooth printing.
14. *Basic Imaging Profile* (BIP) – defines duties of photo transferring.
15. *Telephony Control Specification Protocol* (TCP) – is a bit oriented protocol which defines how Bluetooth device can be used as wireless phone. It runs directly over L2CAP.
16. *Intercom Profile* (ICP) – is TCP based profile which defines how two Bluetooth phones can communicate directly to each others in same network without using public network.
17. *Cordless Telephony Profile* (CTP) – defines how a cordless phone or mobile phone can be implemented over Bluetooth wireless link.
18. *Common ISDN Access Profile* (CIP) – defines how ISDN signalling can be transferred via Bluetooth technology.
19. *Extended Service Discovery Profile* (ESDP) – defines how universal plug and play works over Bluetooth connection.
20. *Human Interface Device Profile* (HID) – defines protocols, procedures and features how different Bluetooth units can work with different programs, like how Bluetooth keyboard work with Windows.
21. *Hardcopy Cable Replacement Profile* (HCRP) – defines how driver-based printing is accomplished over Bluetooth wireless link. This is a simple alternative to a cable connection between a device and a printer.
22. *Service Discovery Application Profile* (SDAP) – works via SDP and defines how Bluetooth devices can search services in other devices and also how devices can list types of found services.
23. *Bluetooth Network Encapsulation Protocol* (BNEP) – defines basic protocols to common networking over Bluetooth media and is used by PAN profile.
24. *Personal Area Networking Profile* (PAN) – defines personal Bluetooth-network which is based to Internet Protocol. It describes how two or more Bluetooth devices can form an ad-hoc network.

25. *Audio/Video Distribution Transport Protocol* (AVDTP) – defines A/V stream negation, establishment and transmission procedures in Bluetooth technology.
26. *General Audio/Video Distribution Profile* (GAVDP) – defines how audio and video streams are distributed and used in Bluetooth technology. It has two roles, initiator and an acceptor. Typical example is mp3-player with wireless head-set, where device is used as the initiator and headset is used as the acceptor.
27. *Advanced Audio Distribution Profile* (A2DP) – defines how Bluetooth device can send stereo quality audio to other device using for Bluetooth technology.
28. *Video Distribution Profile* (VDP) – defines how video Bluetooth devise streams video over Bluetooth technology.
29. *Audio/Video Remote Control Profile* (AVRCP) – defines how Bluetooth can be used on remote controls. It may be used with A2DP or VDP. [3]

More information of Bluetooth Profiles can be found on Bluetooth SIG's web-pages.

With these profiles Bluetooth technology has many possibilities to work on different kind of applications. Furthermore, since Bluetooth is very fast-growing standard, it will get new profiles soon. With new profiles Bluetooth get a new application changes.

5 SECURITY OF BLUETOOTH

Because primary idea of Bluetooth technology was cable replacement, the overall goal for Bluetooth security is to make the wireless connection at least as secure as cables would be. Since Bluetooth is a wireless communication type, there is a big risk that someone could to eavesdrop the data transferring or data will send to wrong person without permission of user (for instance when two Bluetooth devices meet on supermarket). The Bluetooth specification defines security at link level. These mechanisms are in MAC level and these must be implemented in same way within each Bluetooth device. Application-level security is not specified, which leaves to developer possibility of choose security mechanism that is most suitable for each application. If user needs more security it is most desirable to use encryption of higher layers. On the other hand, low transmission-power of Bluetooth devices prevent broadcast from carrying very far. [11]

Each Bluetooth device has four different entities of security at the link level. First, every unit has unique 48-bit Bluetooth device address (BD_ADDR) which is defined by Institute of Electrical an Electronics Engineers (IEEE). With this address the user can have some faith. Secondly, devices have private 128-bit authentication key which is random number and used for authentication purposes. Third is private encryption key witch is user-defined and can have a size between 8 – 128 bits. That key is used for encryption. Fourth entity is a Bluetooth device's itself made random number (RAND), which is a frequently changing 128-bit or pseudo-random number. All these features have to be implemented in silicon. In addition with before mentioned two keys is used PIN-code, which is used to identify between two devices. Regularly PIN-code is fed manually to devices which are wanted to contact each other. The code is chose by user and its size is 1 – 16 bytes. [3]

Starting points of Bluetooth security are defined in Generic Access profile. The Bluetooth security can have tree different modes. These modes are:

- Security Mode 1: is non-secure mode.
- Security Mode 2: Service level enforced security (service procedure begins at L2CAP layer).
- Security Mode 3: Link level enforced security (service procedure before than connection is formed in LMP layer).

The main different between Security mode 2 and Security mode 3 is that in Security mode 3 all security activities will do before channel opening while Security mode 2 is open for all upper layers during security activities. All these security activities occur in link layer. Devices are divided for two levels; “trusted devices” and “untrusted devices”. This dividing into two groups controls how devices will get to services. One device can operate only for one security mode at a time, for instance a device in Security mode 3 authenticates all else devices witch are contacting to it. Security mode 3 is *stationary* witch means that device works same in the same way with all other devices witch are contacting to it. While security mode 2 is *flexible*; witch enables device and service directs into security measures. These differences are produced in next figure.

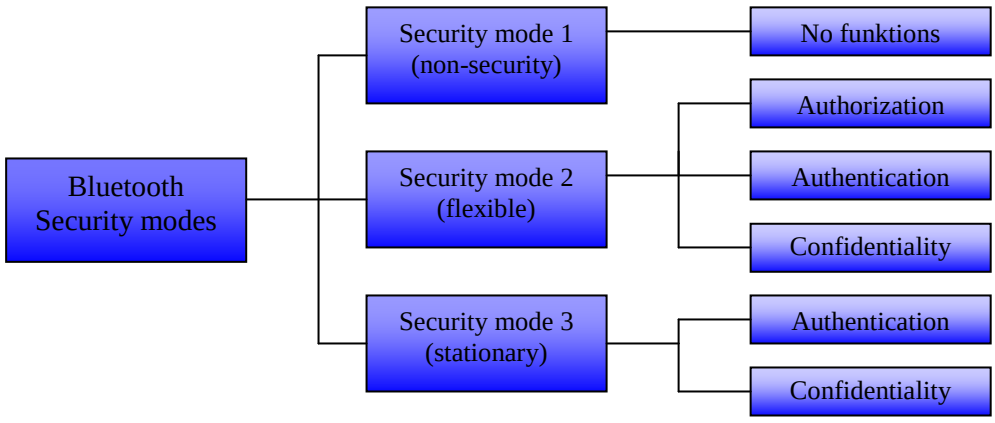

Figure 5.10: Security modes of Bluetooth

The GAP defines also different classes to devices and services. Devices are divided to 2 class; trusted devices and untrusted devices. The levels for services are: Services which requires authorization and authentication, services which requires authentication only and services which are open to all devices. [3]

5.1 Security architecture of Bluetooth

The security operations of Bluetooth begin from input of the PIN-code (Figure 5.11). First thing is to create Initialization key that length is 128 bits. This first step is called *pairing.* It is necessary when two Bluetooth devices meet first time. To set trust these two devices can enter a secret PIN code to both devices. Unfortunately, most of Bluetooth devices limit the length to four digits which makes whole security of Bluetooth questionable at least. Next is to create 128 bits Link key which is based to PIN, the device address and random numbers. This link key is used for *authentication*. The authentication is challenge-response process based on link key. In challenge-response process device who requests authentication generates a random number and send it to other device. After that it gets a response, which has been calculated from a random number using the Link key, from the other device. [12]

Next step is encryption. In Bluetooth technology every outgoing packet's payload will encrypted. Encryption has tree modes:

- Encryption mode 1: non-encryption
- Encryption mode 2: spread messages are not encrypted, all others are.
- Encryption mode 3: All data traffic is encrypted.

During the *encryption* stage of the security architecture is generated encryption key. That is based on link key, values generated during the authentication and again a random number. This keys maximum size is 128 bits and it can be indivially creates for each transmission. The next step is to generate payload key. The payload key based on the encryption key, a device address and the current clock and it is made for ciphering user data. The payload key is a stream of pseudo-random bits. The *ciphering* process is a simple XOR of the user data and the payload key. [12]

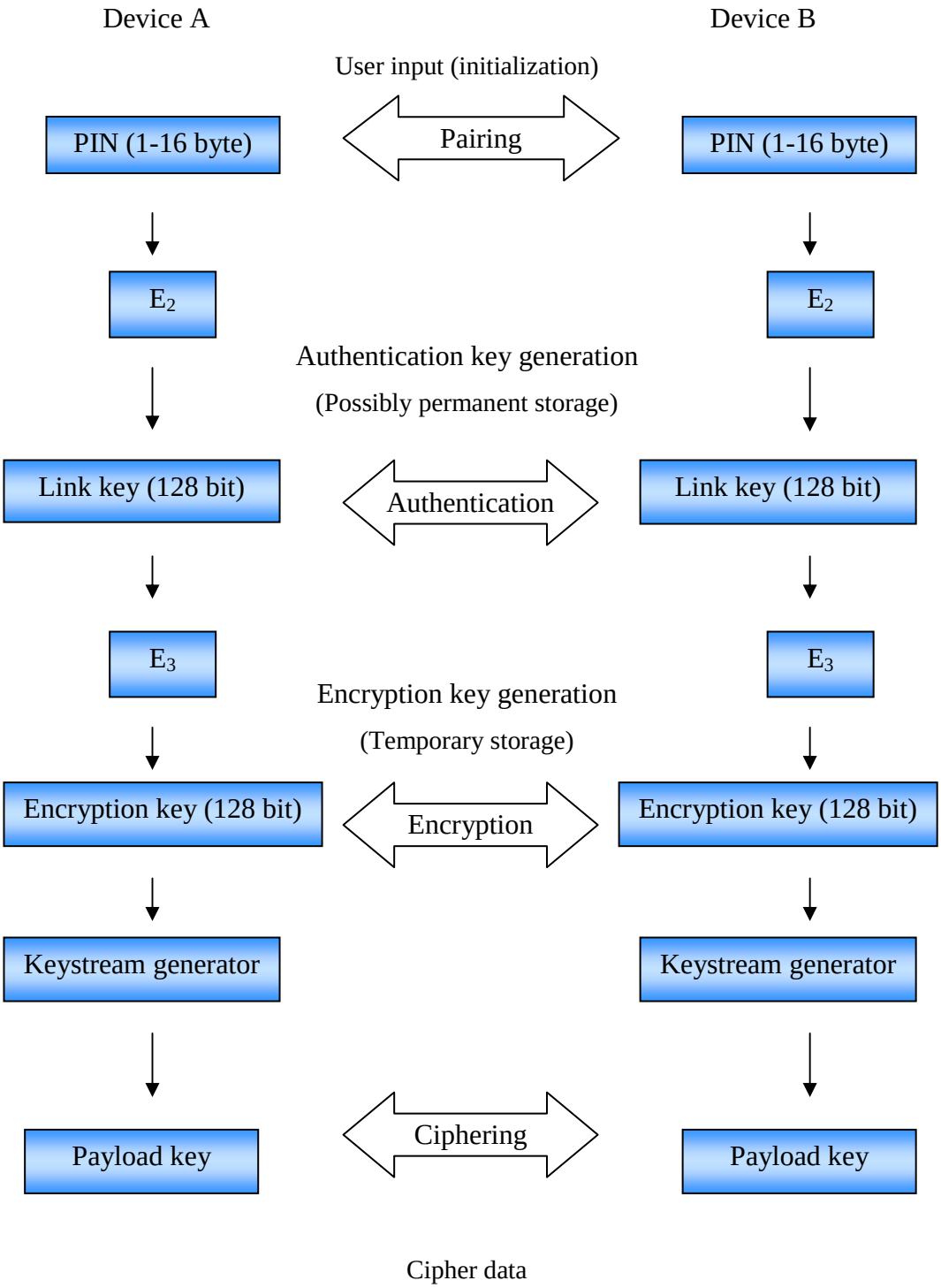

Figure 5.11: Security architecture of Bluetooth [12]

5.2 Bluetooth Security Problems

Opinions of Bluetooth security are variables. Generally opinions it that Bluetooth is not very unprotected protocol, but it causes some conflicts, for instance looks: [13]. Because Bluetooth is tried to do very flexible and wide available, it leads to complicated protocols. Same like Bluetooth security architecture, which is nowadays very complicated. These complications are the enemy of data security, because simple mechanism is easier to rule and not cause any surprises. But the Bluetooth SIG makes every time hard work that these problems get away. The recourse takes all the time new steps to get better security of Bluetooth technology.

6 BLUETOOTH APPLICATIONS

The Bluetooth Technology is designed to between of mobile phones and computers. It is a wireless technology which makes possible to transfer data without cables.

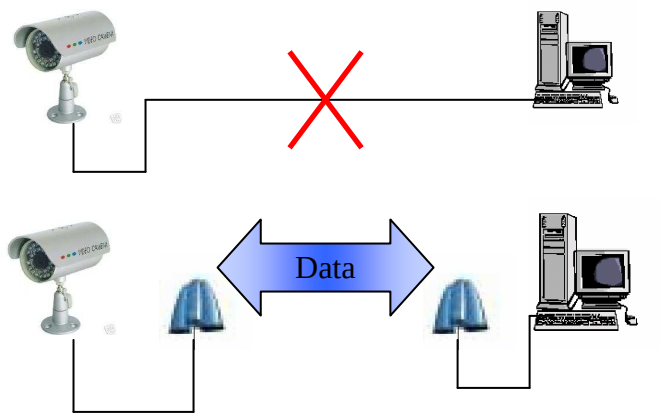

Figure 6.10: Bluetooth release cables

That cable releasing offers to Bluetooth many alternatives where it can be used. Bluetooth technology develops all the time and new protocols and profiles are coming. Bluetooth's data capacity set some limits for transferring data. Nowadays Bluetooth applications can also be used with other wireless communications like GSM and GPRS. This gives much more possibilities to use Bluetooth. The Bluetooth technology is also gained ground in automation field. It can be used for monitoring, transferring and logging of data or operator communication. Thanks to many companies who are working on developing Bluetooth technology the cost of Bluetooth are decreased. Bluetooth is not as its best when it is used to real-time applications, because it is not designed for it. This limits a little for using of it. At its best Bluetooth is with little files transferring. Maximum bit rate of Bluetooth version 1.2 limits also quality of video files.

Bluetooth SIG has also special Automation Study Group. This group's duty is design and develops Bluetooth Industrial Automation applications, especially controlling and automation. [2]

6.1 Requirements of automation technology

Bluetooth technology fits to many current automation applications already, but there are still some applications where it can not use. As it is mentioned in earlier chapters, Bluetooth was originally designed to communications between mobile phones and computers. For that reason messages are normally quite short, but have a very robust security and fast transfer. That is suitable for some automation applications, like using with simple sensors. [4]

In Automation field is always free market area for new contacting types, especially wireless ones. In these days economy and efficiency are main points of automation applications. So, new connection type has consumed loss power and that is one of Bluetooth's strengths. Other significant matter is security, because nowadays there is lot of different kind of viruses and other dangers like electro magnetic disturbances. Connection in automation technology has to be robust and reliable. It is said that Bluetooth's security level is a good level, thanks for its many security functions. And Bluetooth SIG is all the time developing these security operations better.

Since, Automation technology has really wide action operation area is very important that connection can also be used in different temperatures. In these days Bluetooth can be used temperatures between –40 to +85 ºC, which meet normally automation application's needs. Distances are ordinally quite short, so Bluetooth's range is enough. But in some places can be some barrier, like pillars and walls, which take some power of Bluetooth transmission. As it seems, Automation field is not the easiest one to apply a new technology. But also Automation technology is going on, sooner or later new technologies, like wireless, have to come into use.

6.2 Why to choose Bluetooth?

When Bluetooth developed, it was originally meant to release cables between devices. Starting point of Bluetooth specification has been cheap prize, low power

consumption, simply structure and good tolerance of environmental conditions. In other hand Bluetooth has to be easy to use. For instance, system can form data transmission nets by itself, without that user have to carry about forming. These easily, little size and inexpensive prize makes it very interesting target to automation and industry field. [15]

Already this inexpensive prize of Bluetooth is very alluring feature, which may run companies to try that new technology. Because nowadays every company try to achieve as good results as they can and one demand for that are low-costs. Little size is not very important feature in every application, but there is also some places where size of unit is really important. For example, whit little size is possible to develop some new applications which can work in a confined space. [15]

Because automation concept is very wide and versatile, that easily to use is quite important thing. Thanks for Bluetooth many protocols and profiles, same device can be used in many fields. Actually that is not so important, because originally applications in automation are specialized only for a particular purpose. But this feature gives also some benefits which are remarkable in some situations. [15]

6.3 Bluetooth's possibilities in automation

Nowadays wireless transmitters and components are able to do same duties than their comparable cable versions. This is a big benefit for wireless systems, because there does not need marshalling points, control room cabinets, cabling systems and all kind of cost to installing and maintenance these cabling systems. For instance, the big saving of money become already in planning phase. Since the designers do not have to plan where the cables can put and how much they can cost. Using wireless network makes also the job of mechanics easier, because these days plants and factories have so much different devices that the cabling could be very difficult to do. In fact, many of today's plants are not perfectly and compromises in building are inevitable. In other hand, nowadays technology involves so fast that some older cables are come to end of their life-cycle. This makes requirements to install new

cables or fix older ones. In this situation more cheaper is release cables with wireless connection if it is possible. [20]

Another key advantage of wireless contacting is that these are mobile. In this situation is good to remind about quite short transmission distance of Bluetooth technology. But in other hand, that wireless gives some benefits for Bluetooth what cabled connections not have. It will work in same way, though temperature will change. A good example of this is oil refinery, where temperature can change quite lot and conditions are also very difficult. It is very difficult, but not impossible, to make cable connections there. Of course there are a lot of cable connections, but using of wireless connections gives more security against fire. Because, cables can, for one reason or other, cause some risk of fire and there is a lot of very highly inflammable liquid and material. [20]

The using of Bluetooth devices in Automation technology can be divided in three different areas:

- Bluetooth device to connect with other Bluetooth device
- Bluetooth device in middleman (act as an intermediary)
- Bluetooth device linked to other connection type

6.3.1 Bluetooth device with other Bluetooth device

Nowadays the main trend of communication between devices is wireless. Regularly, in normal factory or other fixed workplace, the distances are so short (maybe under 20 m) that the wireless connection advisable to release from cables. On key difficult in this area is that today we have a number of different device and service discovery technologies that are designed for specific networking protocols, specific link and connectivity technologies or event operating environments. So that Bluetooth can be used in different applications it needed a protocol which is suitable for that application in question. For example if you want to use Bluetooth for transfer to data between computer and fax, you need to use fax protocol to this. So today this is normal problem, because the Bluetooth technology is so developed that it has some

protocol for almost every application and Bluetooth SIG is all the time trying to develop it much better than it is.

In automation field is lot of different devices which have to communicate each other that whole system works well. This communicating can also made with Bluetooth technology. We can call this network “Blue Web”, which means a piconet between two or several Bluetooth devices. The Bluetooth technology is suited for this task very well. It is simple, robust and reliable way to transfer data. For instance if you want to establish own piconet between your computer and some other units like camera or some sensor, it is possible. There are existed many situations where the cable connection is not possible to build, like some spinning wheels. For instance, Nokia Tyres will use this Bluetooth technology on their new wheels.

The name of that smart tyre system is Road Snoop Safety System. Each smart tyre has one Bluetooth chips inside of it. That little Bluetooth chip is planning to send real-time messages to mobile-phone of users. These messages will give information about tire wear. In the beginning the chip is used to monitor temperature and pressure of tyre. But it is also developed that later it can be used to monitor about hydroplaning. In other hand the smart tyre can also warn to user if somebody is going to steal it. [15][16]

Bluetooth is very suitable to this task, because is very easy to use and it is wireless. In other hand, the second problem is power consumption. But this is not a problem to Bluetooth device, because its power consumption is not very high. There is designed that with Bluetooth chip can be installed little battery, but this battery might not needed. The power for the Bluetooth chip will get from the transformation power of tyre. This energy producing will adjusted with electronic steering control. Is calculated that when car make 80 km an hour, one 64 square centimetres area of that smart tyre, can produce 0.001 W power. That is enough for Bluetooth device. [18]

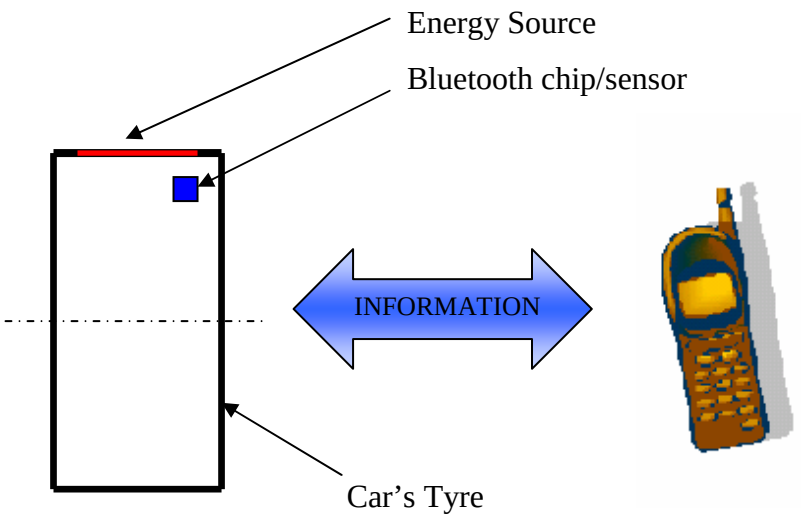

Figure 6.30: Road Snoop Safety System

Bluetooth in special care demanding situations

As I above mentioned Bluetooth technology's best use subject is monitoring. Since, Bluetooth is wireless connection; it is very hygienic because it not has cables with attract dust and bacteria. This offers also the Bluetooth technology for Pharmaceutical and life sciences. Another noteworthy, place where wireless technology can be used is systems where, for one reason or other, is wanted to keep closed or tightly sealed, like tanks. Inside the tank can be installed for instance a sensor with Bluetooth contact. That sensor transmits information, like temperature, to other Bluetooth receiver. Figure 6.31 shows a simply example for this. Bluetooth contact is suitable for this task, because its transmission will not care about surface of tank and it does not consume a lot of power. It is also good to notice that Bluetooth technology needs some power to work. This situation can be settled for install a little source of energy with Bluetooth core. This source of energy can be change when power will end. [20]

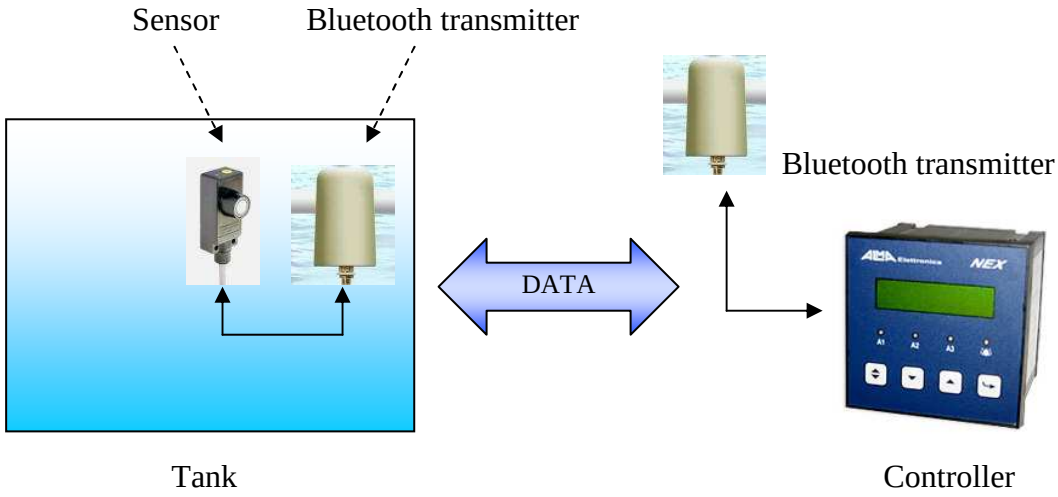

Figure 6.31: Bluetooth transmission

Wireless technology makes possible to monitor easily many tanks at same time. In Bluetooth technology this is possible with piconet and scatternet. Via these scatternets the data can be collected from many devices (Figure 6.32).

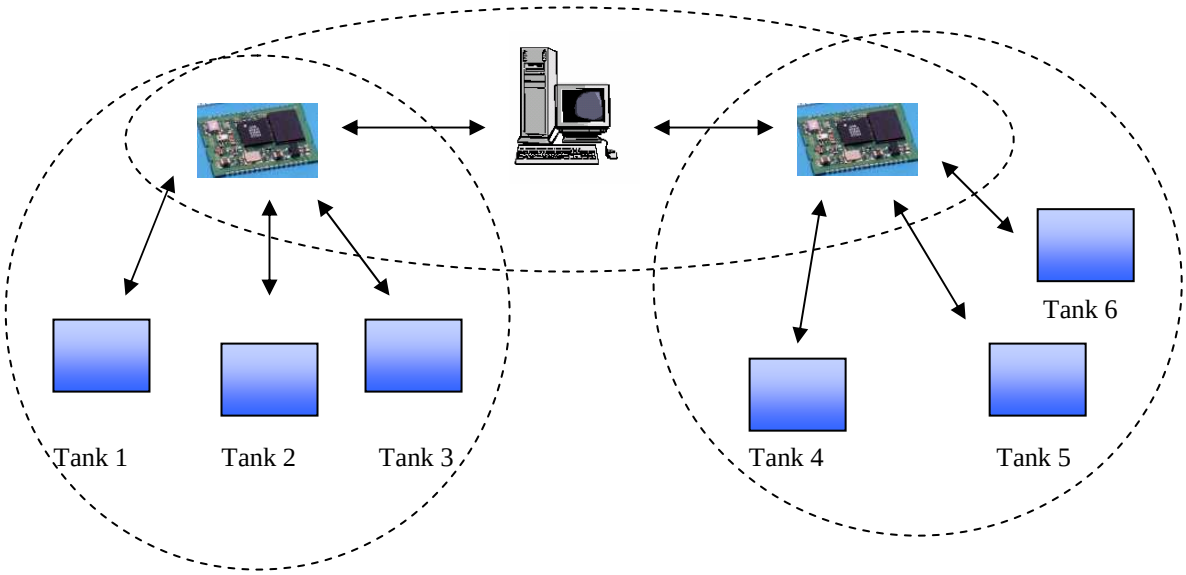

Figure 6.32 Bluetooth scatternet use to monitoring

These were only the one kind of examples for using of Bluetooth to monitoring. This kind of applications can be used also in manufacturing automation to monitor different things. Bluetooth is not only good communication feature to difficult or

special places, but it can also use in basically applications, like in automation line to transfer sensors data to computer.

6.3.2 Bluetooth device on middleman

Sometimes, when distances are too large or there is some matter (for example wall) in the way of Bluetooth signal, then must to found another solve. One solve for this situation is use Bluetooth device in middleman. That means one Bluetooth device transmits radio signal to another Bluetooth device. Like this way, Bluetooth systems range can be raised. Ordinally this system needs scatternet to work.

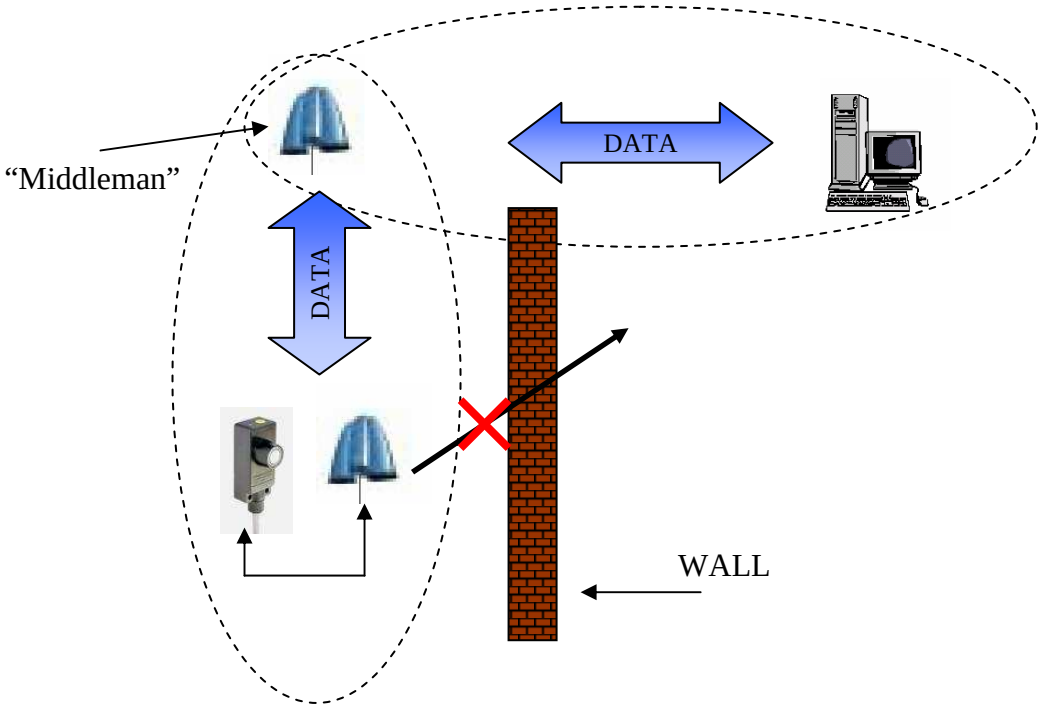

Figure 6.33: Bluetooth device on middleman

6.3.3 Bluetooth with other networks

If Bluetooth's own range for a reason or other is not enough there is another way. Bluetooth is also easy to connect with other common communication types, like WAP or LAN. This is very good quality, because Bluetooth is only short-distance connection. When Bluetooth is connected to other communication type, it can get wider range to work. Bluetooth's advanced protocol and profile structure makes this possible.

Bluetooth can be used to make connect computer of controller to LAN. This makes possible to monitor big area in same workstation. Also with this feature can be utilized the characteristics of Internet. To make this connection Bluetooth uses its IP profile (look Chapter 4: profiles). This is viable feature which helps to control devices from farther away.

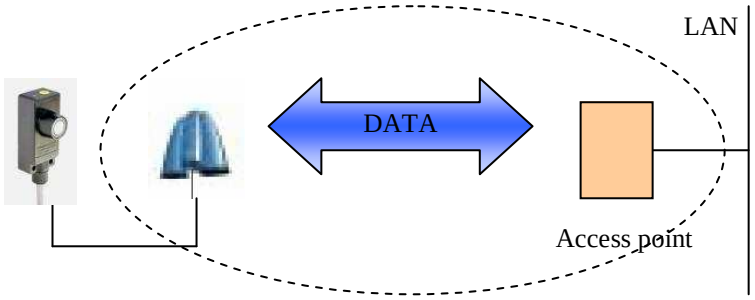

Figure 6.34: Bluetooth with other communication type [4]

Previous example shows how Bluetooth can be connected to stationary internet connection, but wireless internet connection is also possible. Commonly this happens by use mobile phone. So, this event demands Bluetooth enable laptop and mobile phone with Bluetooth core. First mobile phone and laptop have to contact together and after that via mobile phone will be former contact to Internet. With this feature you can work almost anywhere in word where is possible to enable internet. For instance, this can be used when you are somewhere to service or install new programs to your customer's terminal and you have to download some files on your company's computer to your laptop. This makes possible to get any time newest files and information almost everywhere. This feature is possible to make with WAP.

6.4 Bluetooth’s major problems in Automation

Although Bluetooth sounds nice technology to use everywhere, there founds still some problems. Usually problems comes because conditions in automation field are not same than in normal consumer use. Biggest problems are heat, vibration and moisture. It is also possible that all these features can be on same situation. Since in automation field is also many other electric devices there is also danger of electric interferences.

That temperature is Bluetooth’s problem only in special positions, where temperature is really high or low. In these days Bluetooth can work well in temperatures between -40 and +85 ºC. For example Bluegigas Module 2022-1-B2B is working in this area. [19]

As we all know vibration and moisture are never good matter to automation devices, especially to electrical devices. In additional to this, that frequency of 2,4 GHz can absorb to water very well. That mean if humidity is high is possible that a part of radiation can absorbent to air and lose. Some of these problems what environment causes can decide with traditional methods. Like if air is too cold, it can warm up and if humidity is too high the device can be cased. Bluetooth device can also protect for vibration by use some normal methods. These additional activities takes off Bluetooth originally benefits, because size will grown, prize will rise. Also power consumption will increase, because transmission has to be more powerful. [15]

This power consumption is not a problem in automation field, because usually there founds a lot of power points where Bluetooth unit can connect up. Only some special applications, like that Nokia Smart Tyre, power consumption is important because there have to install battery with Bluetooth chip. Bigger problem than these above cases are electricity interferences. Especially very big electric operators produce strong electricity interferences, which makes transmission difficult. In automation field is used many electricity motors and inventers which may cause strong interferences. This problem comes, because ISM-band maximum power is only 100mW. [15]

Connection problems

With the above environment conditions, also range, contact forming time and widespread nets causes some problems to short-range radio links. Bluetooth's biggest range in free space is 100m. That is enough in normal conditions to automation technology, but some situations, for instance in industry hall where machines and structures can prevent contact forming. This range problem can be solved with scatternets (look Chapter 6.3.2). That is possible because one Bluetooth unit can be member of two different piconet. This works perfectly in theory, but in reality it causes new problems. If device is slave in two different piconets, it is possible than data transmission overlap with other transmission from another piconet. In this situation is possible that data packet will destroy or will not reach its destination. [15]

Contact forming time may also cause some problems. Usually automation applications depends knowledge about maximum contact forming time. For instance, if how long automation program will wait that connection, until it moves to next measure. These above mentioned interferences in environment usually caused problems in connections, thus is difficult to say maximum contact forming time but you have to suppose it. The contact forming times are mostly long in Bluetooth technology and that is a little problem. In ideal situation this contacting from standby-mode to active-mode (look Chapter 3.2.5) takes 2,56 seconds and maximum time is 5,12 second. This connection forming time is not a problem if all devices are kept in ACTIVE- or HOLD-mode. In this case connecting takes only some milliseconds. [15]

In other hand Bluetooth's security can be counted to one problem. Since, Bluetooth is wireless connection it is possible that data can lose in the middle of transfer or someone can snatch it without permission of user. In additional, some problems can come if Bluetooth devices for one reason or other lose contact to each other. This may be very dangerous especially in monitoring situations.

In Bluetooth specification is fixed a lot of attention on compatibility of devices. The specification is sometimes really complicated and it is possible that some devices

used different usage models which caused that devices can not communicate each other. This problem can be solved to use only devices which are known to work among themselves.

6.5 Bluetooth's future

Bluetooth version 2.0 + EDR

After Bluetooth's version 1.2 Bluetooth SIG has released version 2.0 + EDR (Enhanged Data Rate) in end of year 2004. As earlier was mentioned, that new version brought some new characteristic for Bluetooth. These new features are:

- 3 times faster (up to 3MB/s) transmission speed (up to 10 times in certain cases)
- Lower power consumption through reduced duty cycle (faster connection takes less time)
- Simplification of multi-link scenarios due to more available bandwidth
- Backward compatible to earlier versions
- Further improved BER (Bit Error Rate) performance

Most important of these features is that transmission speed rising. That speed raising gives for Bluetooth much more application alternatives, because earlier this was a little problem. Especially video quality make gains at the expense of transmission speed, because with EDR is possible send more bigger video file in same time than with older one. With these above characteristics Bluetooth version 2.0 makes possible data transmission to several devices at same time. This was earlier one of Bluetooth's weakness. [21]

Next target for Bluetooth SIG is to develop satisfactory QoS, Bluetooth security and dramatically improve power consumption, enabling Bluetooth sensors last on single battery for multiple years. The plan for 2006 version, according to Bluetooth's SIG

advance board, is to improve performance, develop multi-cast capabilities, make better security and try to raise the range of low battery sensors to about 100m.

In year 2003, Ericsson Technology Licensing research group considered developing Bluetooth standard witch would compete against ZigBee specification in industrial control and automation applications, in ZigBee's target market. According that plan they would keep the Bluetooth radio, but optimize the media-access controller. The name of new development would be Bluetooth Lite, but it is still at an investigate stage, because the board of SIG has not been introduced it yet. Following table touch briefly on characteristics of Bluetooth Lite. ZigBee technology, Bluetooth 2.0 and Bluetooth Lite are compared in APPENDIX 2. [3]

Bluetooth's new applications

Nowadays Bluetooth is developed especially in multimedia field. There is came many different kind of applications, like wireless head sets and wireless game pads. Also home automation field has got some applications, like Bluetooth remote control for garage doors.

In the medicine field is also many situations where is possible to enable Bluetooth communication, for instance to patient monitoring things. In these days is commonly to use cables for monitoring patient, but in future may be possible to release these cables with Bluetooth technology. Bluetooth can also utilize in medical testing and dosage. [22]

Bluetooth will become more common in travelling field. There Bluetooth can use for recognize people, for instance in hotels. Also in airport Bluetooth can be utilized, because "electric tickets" are nowadays very common. With electric ticket and Bluetooth enable mobile phone, person can walk through the port, without visiting on desk. [22]

Bluetooth enables new partner

Actually Bluetooth's future seems very bright. Bluetooth technology takes a big step in wireless field in 03/2006, when Bluetooth SIG chose UWB-technology (ultra-wide band) for its future fast data transmissions. In UWB-technology data will transfer in wide frequency band but low transmission power. According to Bluetooth SIG UWB-technology can offer up to 100 Mbit/s wireless connections in range of 15 meter. First contacting cores between Bluetooth- and UWB-technology are coming after one year. [23]

7 CONCLUSION

The goal of this thesis was to examine and find out Bluetooth technology's utilization and possibilities in automation technology. Nowadays PLC is very important feature in automation technology and Bluetooth might be one of its data transmission ways on future.

At first Bluetooth feels really good communication method, but on closer examination there founds some significance points. Since Bluetooth is wireless connection type it gives some benefits for it, but in other hand wireless brings some drawbacks. Firstly, most of automation applications desire real-time data delivery and wireless connections, especially Bluetooth, are not best choice into these applications. For instance Bluetooth connection time can cause some problems in some applications and worst of all it can produce some dangerous situations. In additional it is always possible that, for one reason or other, the connection between Bluetooth devices may cut of or data can be snatched without permission of user. Reliable is one of Automation technology's main demands. It causes sometimes big problems for wireless connection, but on other hand Bluetooth has good security, which improves its characteristics.

If Bluetooth wants to hold ones own in nowadays tight competition it has to play with its own strengths. These strengths are for instance low cost, low power consumption, easy contacting and good security. In addition wireless is also one of its benefits comparing to normal cable contact and consequently it have to strike applications where is not possible to use cable contact. One of Bluetooth strength is also its suitability for many different applications, thanks for its protocol structure. In future Bluetooth SIG has to fix them attention to improve Bluetooth's data transmission speed. Version 2.0 + EDR have to be only first step on this field, because Bluetooth's speed is not enough to compete with its competitors.

My opinion is that Bluetooth's future seems very bright, especially now when they establish new association with fast UBW-technology. I have strong belief, that Bluetooth will be one of future's communicating methods in Automation technology.

It is always good to remember, that only a good basic knowledge of Bluetooth technology is not enough. You also have to know operation of the automation application where you are designed to use Bluetooth data transmission. In right target of usage Bluetooth is certainly magnificent decision.

REFERENCES

[1] Wang, H., ”Overview of Bluetooth Technology”, http://www.pori.tut.fi/~mm/BT/Bluetooth_Overview.pdf, 05/2006

[2] Palo Wireless, ”Bluetooth Tutorial”, education web page, http://www.palowireless.com/infotooth/tutorial.asp, 05/2006

[3] Bluetooth SIG, Inc, “The Official Bluetooth Wireless info site”, http://www.bluetooth.com/Bluetooth/, 05/2006

[4] Lucan, V., “Bluetooth with industrial computers”, Master of Science Thesis, Tampere University of Technology, 05/2006 http://ae.tut.fi/research/AIN/Publications//Lucan%20Vladimir%20-%20Bluetooth%20in%20automation.pdf

[5] Stalling,W., “Wireless Communications and Networks”, 2002, ISBN: 0-13-040864-6, Pretince-Hall, Inc., pages 479-519

[6] “International Radio Frequency Allocation”, http://www.jeremysag.com/images/irfa.jpg, 05/2006

[7] Haartsen, J., “Bluetooth – The universal radio interface for ad-hoc”, Wireless connectivity, Ericsson Review No. 3 of 1998, http://www.ericsson.com/ericsson/corpinfo/publications/review/1998_03/ files/1998031.pdf, 05/2006

[8] Edtingger, N., ”Bluetooth”, study material, http://alpha.rrs.at/docs/bluetooth/folien.html, 05/2006

[9] Mikeska, Z., ”Radio Specification of the Bluetooth system”, Bluetooth student material, http://www.elektrorevue.cz/clanky/04003/english.htm, 05/2006

[10] Ketola, Krats, Lahti, ”Mikä ihmeen Bluetooth”, exercise job, http://www.cc.jyu.fi/~akrats/harkat/tli/Bluetooth.htm, 06/2006

[11] Mallick, M., “Mobile and Wireless Design Essentials”, 2003, ISBN: 0-471-21419-1, Wiley Publishing, Inc., pages 48-51

[12] Schiller, J., “Mobile Communications”, 2003, ISBN: 0-321-12381-6, Pearson Education limited, pages 269-293

[13] Vainio, J., ”Bluetooth Security”, Helsinki University, teaching material, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html, 06/2006

[14] Hac, A., “Mobile telecommunications protocols for data network”, 2003, ISBN: 0-470-85056-6, John Wiley & Sons, Ltd, pages 146-157

[15] Karasti, O., “Bluetooth teollisuudessa – Langattomasti vaativissa oloissa”, article of Professori magazine, May of 2000, http://www.prosessori.fi/es00/arkisto/PDF/BLUETOOT.PDF, 06/2006

[16] Tekes, Älyrengas lisää kuljettajan turvallisuutta”, Clients outcomes, http://www.tekes.fi/ajankohtaista/asiakkaiden_tuloksia/menestystarina_tiedot.asp?id=4076&paluu=, 06/2006

[17] Nokia Tyres, ” Road snoop to develop and commercialise intelligent tyre technology”, Press release 02/2001, http://www.nokiantyres.com/release_en?id=631044, 06/2006

[18] Suomen Kansallisverkko Oy, “Älyrengas louhii energian antureihinsa”, News release, 11/2004, ISSN: 1458–4441, http://www.verkkouutiset.fi/arkistojuttu.php?id=62486, 06/2006

[19] Bluegiga Technologies, ”Bluegiga’s Bluetooth Modules in a Nutshell”, product catalogue, http://www.bluegiga.com/default.asp?file=212, 06/2006

[20] Hankey, N., “Welcome to wireless”, magazine review, Process Engineering, 01/2006, pages 27-29, 06/2006

[21] Savonia ammattikorkeakoulu, “Wireless Platform – Bluetooth”, http://wirelessplatform.savonia-amk.fi/index.php?sivu=bluetooth&nayta=bluetooth20, 06/2006

[22] Miller, B., ”Future Applications for Bluetooth Wireless Technology”, Pretience Hall PTR, Article review, http://www.phptr.com/articles/article.asp?p=24243&rl=1 , 06/2006

[23] Staff, “Bluetooth, UWB to play together”, Electronic News, http://www.ferret.com.au/articles/fc/0c02f7fc.asp , 06/2006

[24] Wikipedia, “Bluetooth”, The Free Encyclopedia, http://en.wikipedia.org/wiki/Bluetooth, 07/2006

Packet Type	Lenght	Content	Use
ID	68 bits	Access code	Inquiry, page and response routines
NULL	126 bits	Access code + header	ARQ acknowledgement, flow control
POLL	126 bits	Access code + header	Regular polling of slaves
FHS	366 bits	Bluetooth device Address sender clock	Synchronization

Table 3.1.2.3 Types of control packets

Name	Bluetooth 2.0 + EDR	Bluetooth Lite (working name)	ZigBee
Standards body	Bluetooth SIG	Bluetooth SIG	IEE802.15.4 ZigBee Alliance
Specification date	Nov 2004	Planned for end of 2006	Dec 2004
Data rate (peak)	108kb/s to 1Mt/s, 1Mb/s to 3Mb/s in EDR transfere	Unknown	250kb/s
Range	About 10m	About 100m	About 75m
Connection nodes	8	256	65,536
Xmit current/power consumption	0,01 mW	Unknown	0,5mW (target value, physical layer only)

Table 8.2: Different technologies compared among themselves