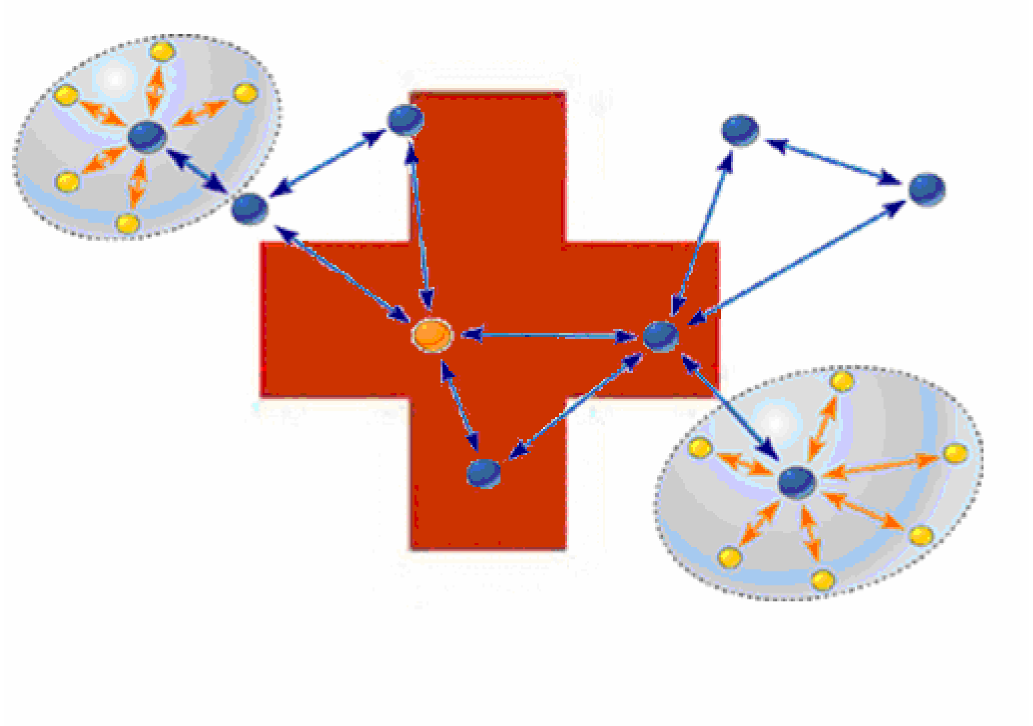
HØGSKOLEN I AGDER
Agder University College

THE UNIVERSITY OF
NEW SOUTH WALES

Master Thesis in
Information and Communication Technology



The Impact of ZigBee in a BioMedical Environment

By
Bård M. Thraning

Agder University College
Grimstad, July 2005

Abstract

The next generation of older people worldwide is predicted to reach 761 million by 2025, more than double what it was in 1990. During this century, for the very first time in human history the old will outnumber the young. The care demand for this generation will be enormous. Sensor networks have the potential to help reduce the workload of medical care. By introducing Body Area Networks of wireless vital sign sensors the collection of physiological data can be greatly simplified. The Body Area Network will be worn by patients who need 24 hours surveillance due to a chronic illness, and it will report any abnormalities to a physician. A good quality of life can be maintained for patients who can function in their everyday activities while being monitored.

The Body Area Network needs a wireless technology to transmit the vital signs data. Today many proprietary solutions have been developed, but the need for a globally standardized technology is absolutely present. This thesis investigates three IEEE standards and their upper specifications, and evaluates them up against a proprietary solution to see which will be the best fit for a Body Area Network. ZigBee, based on the IEEE 802.15.4 standard, is further explored to investigate its possibilities and weaknesses in a biomedical environment. Four scenarios are described to unveil its limitations. Those are later discussed and possible solutions are proposed.

In the evaluation of the wireless technologies ZigBee is found superior mainly because it is a standard, even though proprietary solutions can be better fitted to special uses. ZigBee being a global standard is a fact of cardinal importance in this case.

It is also found that ZigBee has what it takes to be the single technology in a complete monitoring scenario with multiple patients. It can perform adequately with its security properties, scalability, and power consumption, even though the relatively low data rate was anticipated to be an issue. Synchronization will still need some more work.

The impact of ZigBee would be that more companies could focus on increased product innovation since they do not need to develop proprietary solutions from scratch.

Preface

This master thesis is written in collaboration with the University of New South Wales (UNSW), school of Electrical Engineering and Telecommunications, and Agder University College, faculty of Engineering and Science. It is the final stage in the Master of Science degree in Information and Communication Technology at the Faculty of Engineering and Science at Agder University College.

The thesis is given by WPRmedical and Kitron Development and is carried out under the supervision of Ass.Prof Rune Fensli. It has been conducted as an important part of the research project "A Wearable Cardiac Alarm System using Wireless ECG, Continuous Event Recording and Communication with a Clinical Alarm Station" which is executed by Ass.Prof Rune Fensli, Agder University College in close co-operation with University of Aalborg.

I would like to thank Professor Branko Celler at UNSW for inspirational conversations in the initial face. And special thanks to Ass.Prof Rune Fensli for substantial guidance throughout the project.

Grimstad, July 2005.
Bård M. Thraning

Table of contents

ABSTRACT .... **I**

PREFACE .... **II**

TABLE OF CONTENTS .... **III**

TABLE OF FIGURES .... **VI**

LIST OF TABLES .... **VII**

ACRONYMS AND ABBREVATIONS .... **VIII**

1 INTRODUCTION **1**

1.1 BACKGROUND/MOTIVATION 1
1.2 THESIS DEFINITION 1
1.3 GOAL OF THE WORK 2
1.4 STATUS IN RELATED WORK 2
1.5 REPORT OUTLINE 2

2 BODY AREA NETWORKS **4**

2.1 COMPONENTS AND SYSTEM OVERVIEW 4
2.2 RESEARCH PROJECTS 6
2.2.1 Body Area Network Project 6
2.2.2 Human++ project 7
2.2.3 A WBAN of intelligent motion sensors for computer assisted physical rehabilitation 7
2.2.4 Noninvasive Wireless Body Area Network 8
2.2.5 Body Area Network – A "Healthy aims" project 9
2.2.6 MobiHealth 9
2.2.7 CodeBlue: Wireless Sensor Networks for Medical Care 11
2.2.8 Proactive health 11
2.2.9 TelemediCare 13
2.2.10 UbiMon 14
2.2.11 WsHC 15
2.3 POTENTIAL AREAS FOR BAN APPLICATIONS 16
2.4 IMPORTANT CHALLENGES IN CONSTRUCTION OF WIRELESS SENSOR NETWORKS 16
2.4.1 Battery capacity 17
2.4.2 Scalability 17
2.4.3 Data rate capacity 17
2.4.4 Fail-safety 17
2.4.5 Real time synchronization 17
2.4.6 Association 17
2.4.7 Security 17
2.4.8 Cost 18

3 SHORT RANGE WIRELESS TECHNOLOGIES **18**

3.1 IEEE 802.15.1 / BLUETOOTH 18
3.1.1 Overview 18
3.1.2 Network topology 20
3.1.3 Protocol stack 21
3.1.4 Security 22
3.1.5 Cost 23
3.1.6 Prospects 23
3.2 IEEE 802.15.3 HIGH-RATE WPAN / ULTRA WIDEBAND (UWB) 24

3.2.1 General overview ... 24
3.2.2 Technical overview of UWB ... 24
3.2.3 Technical overview of IEEE 802.15.3 ... 27
3.2.4 Association ... 29
3.2.5 Security ... 29
3.2.6 Cost ... 29
3.2.7 Prospects ... 30
3.3 IEEE 802.15.4 LOW-RATE WPAN ... 30
3.3.1 Components of the IEEE 802.15.4 WPAN ... 31
3.3.2 Network topologies ... 31
3.3.3 Architecture ... 32
3.3.4 Superframe and frame structure ... 33
3.3.5 Robustness ... 35
3.3.6 Security ... 35
3.4 ZIGBEE ... 36
3.4.1 Overview ... 36
3.4.2 Architecture ... 36
3.4.3 Association ... 39
3.4.4 Power consumption ... 39
3.4.5 Security ... 40
3.4.6 Cost ... 40
3.4.7 Prospects ... 41
3.5 PROPRIETARY SOLUTION - NORDIC NRF24AP1 ... 41
3.5.1 Overview ... 41
3.5.2 Architecture ... 42
3.5.3 Network topology ... 43
3.5.4 Pairing (Association) ... 45
3.5.5 Data types ... 45
3.5.6 Security ... 46
3.5.7 Cost ... 46
3.6 COEXISTENCE ... 46
3.6.1 ZigBee ... 47
3.6.2 UWB ... 48
3.6.3 Bluetooth ... 48
3.6.4 Proprietary solution – Nordic nRF24xx ... 49

4 EVALUATION OF BAN COMPATIBILITY ... 50

4.1 BLUETOOTH IN BAN ... 50
4.1.1 Battery capacity ... 50
4.1.2 Scalability ... 50
4.1.3 Data rate capacity ... 50
4.1.4 Fail-safety ... 51
4.1.5 Real time synchronization ... 51
4.1.6 Association ... 51
4.1.7 Security ... 51
4.1.8 Cost ... 51
4.2 UWB IN BAN ... 52
4.2.1 Battery capacity ... 52
4.2.2 Scalability ... 52
4.2.3 Data rate capacity ... 52
4.2.4 Fail-safety ... 52
4.2.5 Real time synchronization ... 52
4.2.6 Association ... 52
4.2.7 Security ... 52
4.2.8 Cost ... 53
4.3 802.15.4 / ZIGBEE IN BAN ... 53

4.3.1 Battery capacity 53
4.3.2 Scalability 53
4.3.3 Data rate capacity 53
4.3.4 Fail-safety 53
4.3.5 Real time synchronization 54
4.3.6 Association 54
4.3.7 Security 54
4.3.8 Cost 54
4.4 PROPRIETARY SOLUTION / NORDIC NRF24AP1 IN BAN 54
4.4.1 Battery capacity 54
4.4.2 Scalability 55
4.4.3 Data rate capacity 55
4.4.4 Fail-safety 55
4.4.5 Real time synchronization 55
4.4.6 Association 55
4.4.7 Security 55
4.4.8 Cost 55
4.5 SUMMARY 56

5 PATIENT MONITORING WITH ZIGBEE – POSSIBILITIES AND LIMITATIONS 57

5.1 SCENARIO #1 - MONITORING ONE PATIENT IN HOSPITAL 58
5.1.1 Power consumption 60
5.1.2 Data rate 61
5.1.3 Time delay 61
5.1.4 Association 61
5.1.5 Synchronization 62
5.2 SCENARIO #2 - MONITORING TWO PATIENTS IN HOSPITAL 62
5.3 SCENARIO #3 - MONITORING N PATIENTS IN HOSPITAL 65
5.3.1 Mobility 66
5.4 SCENARIO #4 - MONITORING ONE PATIENT IN THE HOME 67

6 MAKING ZIGBEE WORK IN A BIOMEDICAL ENVIRONMENT – PROPOSED SOLUTIONS 69

6.1 MENDING THE DEFICIENCIES 69
6.1.1 Increasing battery lifetime 69
6.1.2 Time delay 70
6.1.3 Increasing the number of patients in the network 71
6.1.4 Synchronization 71
6.2 PROPOSED COMPLETE ZIGBEE PATIENT MONITORING NETWORK 72
6.2.1 Sensor perspective 74
6.2.2 NWK CO perspective 75
6.2.3 Application layer issues 75
6.2.4 Security 75
6.2.5 Coexistence 76

7 DISCUSSION 77

7.1 BEST SUITED TECHNOLOGY FOR BAN 77
7.2 THE SCENARIOS – OPTIMAL SOLUTIONS 78

8 CONCLUSION AND FURTHER WORK 80

8.1 CONCLUSION 80
8.2 FURTHER WORK 80

9 REFERENCES 82

Table of figures

Figure 1. The architecture of a wireless body area network [5] [25]................................ 5
Figure 2. The core of a wireless body area network.. 5
Figure 3. Examples of piconet formations [11] 20
Figure 4. The Bluetooth protocol stack [11]... 21
Figure 5. Diagram of the UWB common platform [8].. 25
Figure 6. The MultiBand OFDM frequency band plan [8]... 26
Figure 7. The components of an 802.15.3 piconet [9]... 27
Figure 8. Examples of star and peer-to-peer Topology [1].. 32
Figure 9. LR-WPAN device architecture [1]... 33
Figure 10. Superframe structure without GTSs [1] 34
Figure 11. Superframe structure with GTSs [1].. 34
Figure 12. ZigBee stack architecture [2].. 37
Figure 13. ZigBee network formations [2] 38
Figure 14. The architecture of the nRF24AP1 with external components [19]............... 43
Figure 15. Channel based communication using ANT [18] 43
Figure 16. Examples of ANT network configurations [18]... 44
Figure 17. One patient being monitored with mesh topology 58
Figure 18. Monitoring one patient (Star topology).. 59
Figure 20. Queuing packets in scenario 1 62
Figure 21. Examples of ECG and blood pressure curves [49]... 62
Figure 22. Two patients being monitored (Mesh) 63
Figure 23. Monitoring two patients (Cluster tree) 63
Figure 24. Association in scenario 2... 64
Figure 25. Monitoring N beds (Cluster tree) 65
Figure 26. Monitoring a patient in the home [50] (Modified by author)......................... 67
Figure 19. Graphical presentation showing the packet size/ data rate relation [2]........... 70
Figure 27. Complete ZigBee patient monitoring network... 73
Figure 28. The sensors live their own lives pretty much unaffected of what happens outside of the BAN 74
Figure 29. The NWK CO should only see the BCUs 74

List of tables

Table 1. Modulation, coding and data rates for the 2.4 GHz PHY [9] 28
Table 2. Table of frequency, data rate, and number of channels in the ISM bands [40] .. 30
Table 3. Bluetooth power classes [12]. 50
Table 4. Comparison of short range low power wireless technologies 56

Acronyms and abbrevations

ACK – Acknowledgement
ACL - Access Control List
AES – Advanced Encryption Standard
Ah - Ampere hours
APS - Asynchronous Power Save
ARQ - Automatic Retransmission Request
BAN – Body Area Network
BCU – Body Central Unit
BER – Bit Error Rate
BSU – Body Sensor Unit
CAP - Contention Access Period
CFP – Contention Free Period
CIP-node - Central Information Processing node
CRC - Cyclic Redundancy Check
CSM - Common Signalling Mode
CSMA/CA – Carrier Sense Multiple Access / Collision Avoidance
CTAP - Channel Time Allocation Period
DECT – Digital Enhanced Cordless Telecommunications
DEV - Device
DEVID – Device Identification
DLL - Data Link Layer
DQPSK – Differential Quadrature Phase-Shift Keying
DSN – Data Sequence Number
DSSS – Direct Sequence Spread Spectrum
EDR - Enhanced Data Rate
ECG – Electrocardiogram
ETH - Eidgenössische Technische Hochschule
FCC - Federal Communications Commission
FEC - Forward Error Correction
FFD – Full Function Device
FHSS - Frequency Hop Spread Spectrum
FOKUS - Fraunhofer Institute for Open Communication Systems
FSK - Frequency Shift Keying
GPRS – General Packet Radio Service
GPS – Global Positioning System
GSM – Global System for Mobile communications
HCI - Host Controller Interface
ICU - Intensive Care Units
IEEE – Institute of Electrical and Electronics Engineers
IMEC – Interuniversity MicroElectronics Center
Imm-ACK – Immediate Acknowledgement
ISM - Industrial, Scientific and Medical

IST - Information Society Technologies
L2CAP - Logical Link Control and Adaptation Protocol
LC or LCP – Link Controller (Protocol)
LM or LMP – Link Manager (Protocol)
LPC - Local Patient Computer
MAC - Medium Access Layer
MBOA - MultiBand OFDM Alliance
MCPS - MAC Common Part Sublayer
MCU - Microcontroller
MLME - MAC layer Management Entity
NWK – Network
NWK CO - Network Coordinator
OBEX - Object Exchange Protocol
OEM - Original Equipment Manufacturers
OSI - Open System Interconnection
PDA – Personal Digital Assistant
PHY - Physical layer
PNC - Piconet Coordinator
POS – Personal Operating Space
PPP - Point-to-Point Protocol
PSPS - Piconet-Synchronized Power Save
QAM – Quadrature Amplitude Modulation
QoS - Quality of Service
R&D – Research and Development
RF – Radio Frequency
RFD – Reduced Function Device
RX – Receiver
RSSI - Received Signal Strength Indication
SAP - Service Access Points
SH – Smart Home
SIG – Special Interest Group
SME - Small and Medium-sized Enterprises
SpO2 – Pulse Oximeter
SSCS - Service-Specific Convergence Sublayer
TCM –Trellis Coded Modulation
TX – Transmitter
UART – Universal Asynchronous Receiver Transmitter
UbiMon - Ubiquitous Monitoring Environment for Wearable and Implantable Sensors
UMTS – Universal Mobile Telecommunications System
U-NII - Unlicensed-National Information Infrastructure
UPnP - Universal Plug and Play
USD – United States Dollar
UWB - Ultra wideband
VPN - Virtual Private Network
WAP - Wireless Application Protocol
WBAN – Wireless Body Area Network

WLAN – Wireless Local Area Network
WPAN – Wireless Personal Area Network
WPRmedical – Wireless Patient Recording medical
WsHC - Wireless Health and Care
WSN – Wireless Sensor Network
WUSB - Wireless Universal Serial Bus
ZDO - ZigBee Device Object

1 Introduction

1.1 Background/Motivation

Vital signs monitoring of patients in hospitals has been an important part of the treatment and care for many years. Hence it has been subject for several research projects over the years, resulting in further and further improvements of the technology. In the recent years the time too get rid of the wiring have come, making the monitoring more comfortable for the patient. By introducing wireless monitoring the doors for remote monitoring in the home as well as the hospital, are pushed wide open. Now, more than ever, the importance of remote monitoring is on the agenda. The next generation of older people (>65) worldwide is predicted to reach 761 million by 2025, more than double what it was in 1990. If these trends continue, this century will see the first time in human history that the old outnumber the young [50]. Providing care for these will be a major challenge, hence it will be important in the coming years to develop technology which can reduce the workload on the caregivers.

To prevent overloads of the hospitals a key issue will be to provide care and safety to the patients in their own homes. This can be solved with the use of so called Body Area Networks (BANs). These BANs can obtain vital signs from the patient and inform the caregiver when unfortunate incidents occur.

1.2 Thesis definition

Wireless Patient Recording Medical (WPRmedical) and Kitron Development are working on a system for wireless monitoring of biomedical signals. With the use of a radio network based on ZigBee technology it can possibly be implemented favourable solutions compared to Bluetooth and RF-radio communication principles. It is desirable to be able to monitor reliably on-line measurements from a patient with the use of several wireless sensors communication within a BAN to a Central Information Processing node (CIP-node), where the signals are processed and later on forwarded to a clinical alarm station using wireless technologies like WLAN and GSM/GPRS.

The thesis will focus on evaluation of possible technologies and solutions for communication between several wireless sensors and a CIP-node, with respect to battery capacity, scalability, fail-safety, security and cost in the design of new applications and communication principles. Especially the ZigBee protocol stack shall be investigated in order to evaluate possible solutions for suitable application layer protocols that can be used in a scenario of biomedical signals communicating within a BAN framework.

A study shall be conducted regarding protocol principles with respect to effective data rate and time delays in order to estimate optimal solutions, where necessary precautions are taken in order to obtain a reliable and safe data transfer in a multi-unit wireless environment.

1.3 Goal of the work

A paramount objective apart from what is described in the thesis definition is to find whether ZigBee is an adequate technology for patient monitoring or not.

1.4 Status in related work

Because of its importance there are currently many projects researching patient monitoring. Some of these are listed and described in section 2.2. Research on wireless monitoring has grown the last few years, and some proprietary solutions have scratched the surface recently. This thesis investigates the use of standardized solutions in wireless monitoring. It has been carried out as an important part of the research project "A Wearable Cardiac Alarm System using Wireless ECG, Continuous Event Recording and Communication with a Clinical Alarm Station".

1.5 Report outline

Chapter 1 is the introduction including background of the project, its definition and the status in related work.

Chapter 2 gives an overview of BAN, research projects concerning the topic and areas where BAN can be of importance. Challenges when implementing sensors in a BAN configuration are listed in the last section.

Chapter 3 presents different short range wireless technologies which could be used in a BAN. The chapter gives an introduction to three IEEE standards, 802.15.1, 802.15.3, 802.15.4 as well as ZigBee and a proprietary solution from Nordic semiconductors called nRF24AP1. Coexistence issues with these technologies are also inspected.

Chapter 4 evaluates the technologies presented in chapter 3 for best compatibility with BAN. The criteria are battery capacity, scalability, data rate capacity, fail-safety, real time synchronization, association, security and cost.

Chapter 5 takes a look at the possibilities and limitations with using ZigBee in four patient monitoring scenarios.

Chapter 6 presents solutions to problems found in chapter 5. A full scaled patient monitoring network using ZigBee is presented as well.

Chapter 7 includes a discussion of the theoretical analysis performed throughout the report, and identifies future work.

Chapter 8 presents the conclusions which can be drawn from the work.

2 Body Area Networks

To supervise patients suffering from chronic diseases, such as diabetes and asthma, permanent logging of vital signs is an essential part. Cardiology is the most prominent area of application for long-term logging of patient data, where long-term-Electrocardiograms (ECGs) are required as early indicators for impending heart attacks and for therapy control. In general there is an increasing demand for continuous patient monitoring. Body Area Networks (BANs) are expected to be a basic infrastructure element for electronic health care. In most cases medical monitoring require more than one sensor to be attached to the human body, e.g. stroke patients should observe blood pressure values, parameters related to blood oxygen saturation, temperature and weight on a long-term basis. Patients with high blood pressure are facing an increased risk of serious cardiac diseases without any symptoms of pain - continuous monitoring of related parameters enables efficient early warning mechanisms and prevention measures [5].

Current monitoring technology requires "cabling" of patients wearing a set of wired sensor elements, linked to one or several devices for processing and visualisation of the sensor signals. Using wireless multi-parameter monitoring technology, a wide range of diseases could be prevented, treated and managed more effectively. Existing wireless transmission schemes do not meet the requirements in terms of minimising radiation and transmission power consumption to just match the range of human body dimensions [5].

2.1 Components and system overview

As shown in figure 1 the BAN concept enables wireless communication between several miniaturised, intelligent Body Sensor Units (BSU) and a single Body Central Unit (BCU) worn at the human body. The BAN data can be accessed online through a separate wireless transmission link from the BCU to a network access point, using different technology, (e.g. WLAN, GPRS etc). This way a patient wearing a BAN can be monitored externally at all times. Measurement data can regularly be stored in a medical server, a physician can check up on a patient whenever needed, and in case of an emergency an immediate response unit will be alerted. Alerts can be triggered by the patient himself or by highly irregular measurement data. A caregiver can also be contacted in less dramatic circumstances. A patient can also receive information from a physician or even receive the weather forecast for the day.

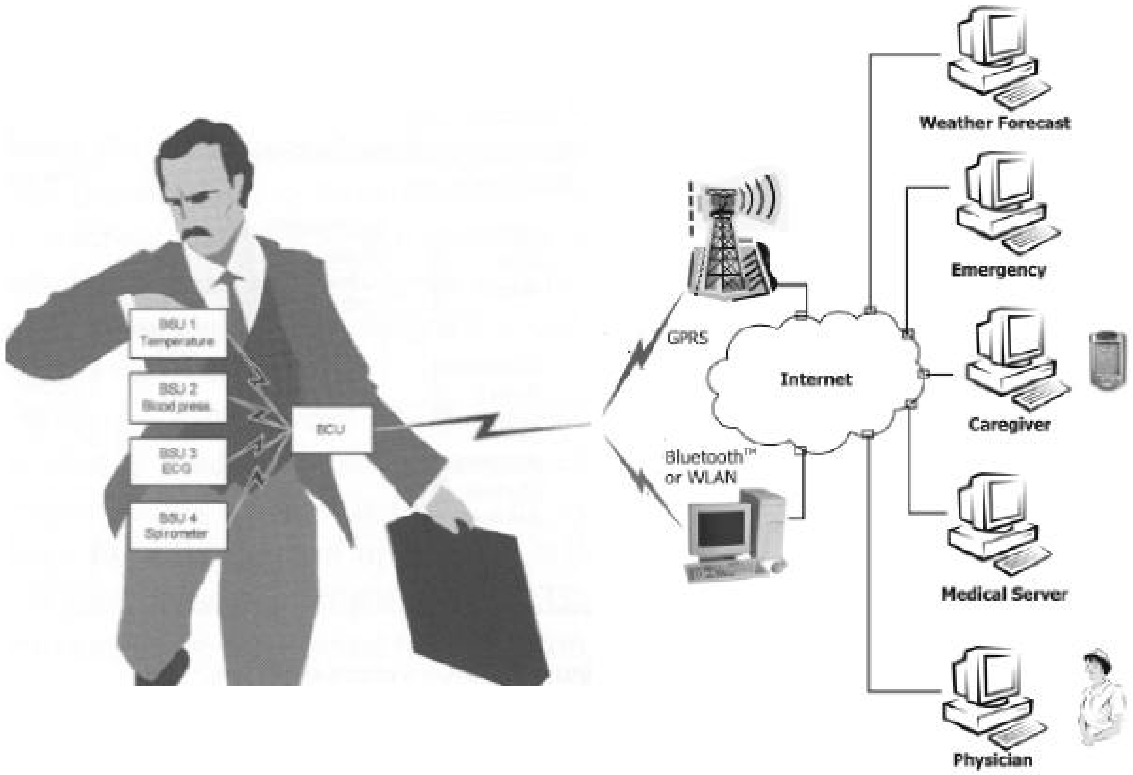


Figure 1. The architecture of a wireless body area network [5] [25]

The core functionality of a BAN provides wireless interconnection between several BSU units and a single BCU via an air interface which is unlicensed (see figure 2).

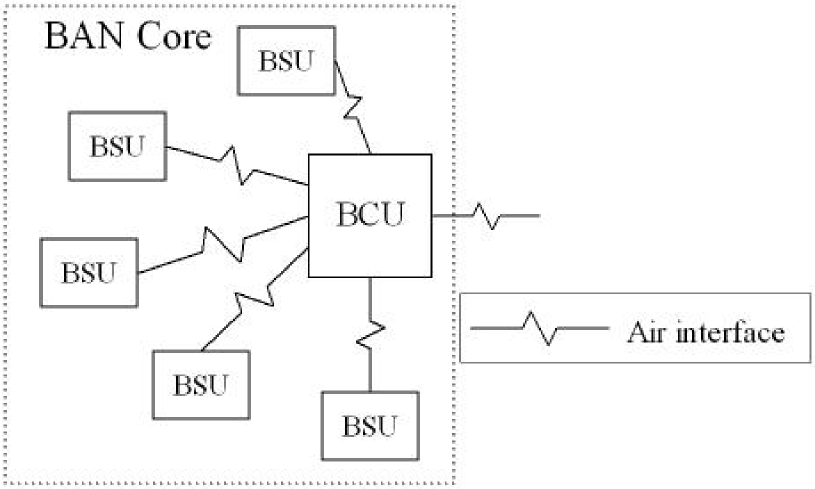


Figure 2. The core of a wireless body area network

The air interface between the BSU and the BCU is characterised by the 2m maximum distance typical for human body dimensions.

A BCU concentrates the data streams from multiple attached BSUs and performs the communication to the outside world. This is conducted by standard wireless communication technology like DECT, WLAN, Bluetooth, etc (see figure 1) [5].

2.2 Research projects

2.2.1 Body Area Network Project

A project conducted by the Fraunhofer Institute.

Information about the project is from [30].

With its BAN project the Fraunhofer Institute for Open Communication Systems (FOKUS) has engineered the integration of body sensors in an Internet environment. Sensors attached to the body of the patient are interconnected via a wireless network thus making them components in an Internet network. Transmitted data can then be easily downloaded on any Internet-compatible end device.

With the technologies of the BAN elderly people and patients enjoy a much greater degree of freedom and can now remain much longer in their familiar home surroundings, whilst the permanent availability of current patient health status data allows medical personnel much tighter control of their planning operations. And mobile communication technologies also enable emergency physicians to prepare themselves by accessing patients' files online via PDA or notebook whilst being driven to the point-of-care.

Fraunhofer FOKUS developments in the medical and healthcare sector are suitable for

- hospitals
- home care services
- healthcare centers
- sports medicine

FOKUS researches and develops mobile communication systems for wireless and wired networks. FOKUS develops the building blocks needed both for end-to-end seamless integration of technologies and end devices, and for the deployment of open flexible communication services and applications. The medical and healthcare sector is a domain in which the rich and diversified range of FOKUS solutions are actively deployed – for instance the IPcom project from the Smart Environments division, the I-Net project from the 3G beyond division or solutions for interactive TV and vehicles.

2.2.2 Human++ project

A project conducted by IMEC.

Information is picked up from the project’s website [24]

Human++ research tackles a number of challenges to realize this smart technology for body and mind:

- Increase the lifetime of battery-powered devices
- Increase the interaction between sensors and actuators
- add intelligence to the devices
- extend devices with chemical and biological features
- integrate and package heterogeneous components
- fundamentally understand measuring medical phenomena
- develop biocompatible systems

IMEC's Human++ research program develops generic technologies to improve the functionality of therapeutic and diagnostic devices, answering the abovementioned challenges. Building blocks for the body area network will be able to provide medical, sports and entertainment functions to the user.

A cornerstone in this research is the realization of a body area network, consisting of sensors/actuators communicating with a personal digital assistant to monitor a person's health.

2.2.3 A WBAN of intelligent motion sensors for computer assisted physical rehabilitation

A project conducted by the Electrical and Computer Engineering Department, University of Alabama.

Information about this project is from [25].

Recent technological advances in integrated circuits, wireless communications, and physiological sensing allow miniature, lightweight, ultra-low power, intelligent monitoring devices. A number of these devices can be integrated into a WBAN, a new enabling technology for health monitoring.

Using off-the-shelf wireless sensors they have designed a prototype WBAN which features a standard ZigBee compliant radio and a common set of physiological, kinetic, and environmental sensors.

They introduce a multi-tier telemedicine system and describe how they optimized our prototype WBAN implementation for computer-assisted physical rehabilitation applications and ambulatory monitoring. The system performs real-time analysis of sensors' data, provides guidance and feedback to the user, and can generate warnings based on the user's state, level of activity, and environmental conditions. In addition, all recorded information can be transferred to medical servers via the Internet and seamlessly integrated into the user's electronic medical record and research databases.

WBANs promise inexpensive, unobtrusive, and unsupervised ambulatory monitoring during normal daily activities for prolonged periods of time. To make this technology ubiquitous and affordable, a number of challenging issues should be resolved, such as system design, configuration and customization, seamless integration, standardization, further utilization of common off-the-shelf components, security and privacy, and social issues.

2.2.4 Noninvasive Wireless Body Area Network

A project by the Eidgenössische Technische Hochschule (ETH), Institute of Technology Zurich.

The principle research goal of the project is the design, optimization and demonstration of a non-invasive WBAN with unprecedented energy efficiency, unobtrusiveness, scalability, and cost structure.

A BAN connects independent nodes (e.g. sensors) dispersed in the clothing. It is an indispensable element of Wearable Computing and has rich applications in home/health care, sports, defence, ambient intelligence, pervasive computing and many other areas. Major characteristics/challenges of our design are:

- An extremely low transmit power per node (non-invasive) to minimize interference and cope with health concerns. The targeted transmit power is below the spurious emission level of electronic equipment like personal computers and portable CD players. This is the key for the user acceptance of a wireless network so close to the body.

- An efficient support of a high density of heterogeneous nodes (about 50 per body) with data rates ranging from several hundred to several million bits per second.

- An optimal network energy efficiency (node autonomy). We target an energy consumption which is an order of magnitude below the current state of the art.

Some immediate consequences of these requirements are:

(i) The use of a broadband signalling scheme (possibly Ultra Wideband),
(ii) Frequency range below 6 GHz and

(iii) The support of heterogeneous multihop links to cope with the high path loss through the human body.

These requirements are extremely hard to satisfy and are not met by known wireless network technologies and wireless BAN designs [23].

2.2.5 Body Area Network – A "Healthy aims" project

A project under Healthy Aims led by Zarlink semiconductor Inc.

Healthy Aims is an EU Framework VI project including 26 partners, including 6 SMEs (Small and Medium-sized Enterprises), across 9 EU countries. These partners will develop a range of medical implants to help the aging population and those with disabilities. The project is funded under the Information Society Technologies (IST) Microsystem programme and combines experts from a wide range of disciplines [27].

As a partner in the "Healthy Aims" project, Zarlink is developing novel in-body antenna designs and ultra low-power communications systems for BANs [28].

2.2.6 MobiHealth

A project led by the University of Twente & Ericsson GmbH.

MobiHealth aims at developing and trialling new mobile value-added services in the area of healthcare, thus bringing healthcare to the patient. The MobiHealth system allows patients to be fully mobile whilst undergoing health monitoring.

The patient wears a lightweight monitoring system – the MobiHealth BAN – which is customized to their individual health needs. Physical measurements such as blood pressure or ECG are measured by the MobiHealth BAN and transmitted wirelessly from the BAN to their doctor, the hospital or their health call centre.
Therefore, a patient who requires monitoring for short or long periods of time does not have to stay in hospital for monitoring but with their MobiHealth BAN can be free to pursue daily life activities.

MobiHealth significantly contributes to addressing the healthcare sector's increasing problems of resource management and is expected to decrease disease and care related costs. Moreover, it helps to satisfy patients' growing need for mobility and personalized care [31].

The MobiHealth project started in May 2002 and was completed in February 2004. It has developed innovative mobile health services, based on 2.5 (GPRS) and 3G (UMTS) networks. MobiHealth has developed a mobile health BAN and a generic service platform for BAN services for patients and health professionals. Remote (patient) monitoring services are just one of the kinds of services that can be provided. This is achieved with the integration of sensors to a wireless BAN. The BAN connected sensors continuously measure and transmit vital constants to health service providers and brokers. This way the BAN facilitates remote monitoring of patients' vital signs and therefore enables proactive disease prevention and management by continuous monitoring of patients' health condition 'anytime and everywhere'.

The use of health BANs together with advanced wireless communications enables remote management of chronic conditions and detection of health emergencies whilst maximising patient mobility. MobiHealth has developed a generic BAN for healthcare and an m-health service platform. The BAN incorporates a set of body-worn devices and handles communication amongst those devices. It also handles external communication with a remote location. During the MobiHealth project the main devices used are medical sensors and positioning (GPS) devices and the remote healthcare location is a healthcare provider (a hospital or medical call center). Biosignals measured by sensors connected to the BAN are transmitted to the remote healthcare location over wireless telephony services.

The results of the project include architecture for, and a prototype of, a generic service platform for provision of ubiquitous healthcare services based on BANs. The MobiHealth BAN and service platform are trialed in four European countries with a variety of patient groups. The MobiHealth System can support not only sensors, but potentially any body worn device; hence the system has potentially many applications in healthcare which allow healthcare services to be delivered in the community.

In the last months of the project 9 different trials scenarios were implemented for different types of patients. These trials allowed us to identify problems and issues in the development of mobile e-health services and identify limitations and shortcomings of the existing and forthcoming public network infrastructure.

First results indicate that several issues need to be resolved by both network operators and hardware manufacturers for a better support to mobile health services. Ambulatory monitoring is more successful for some biosignals than others, for example some measurements are severely disrupted by movement artifacts. Some monitoring equipment is still too cumbersome for ambulatory use, because of the nature of the equipment or because of power requirements, while even with 2.5 and 3G we still suffer from limited bandwidth for applications that serve many simultaneous users. Other challenges relate to security, integrity and privacy of data during transmission to both local transmission (e.g. intra-BAN) and long range (e.g. extra-BAN) communications. Powering always on devices and continuous transmission will continue to raise technical challenges. Business models for healthcare and accounting and billing models for network services need to evolve if technical innovations are to be exploited fully. Standardisation at all levels is essential for open solutions to prevail. At the same time specialization, customisation and personalisation are widely considered to be success criteria for innovative services [32].

2.2.7 CodeBlue: Wireless Sensor Networks for Medical Care

A project led by the Division of Engineering and Applied Sciences, Harvard University.

The information is taken from the project website [29].

The CodeBlue project is exploring applications of wireless sensor network technology to a range of medical applications, including pre-hospital and in-hospital emergency care, disaster response, and stroke patient rehabilitation.

Recent advances in embedded computing systems have led to the emergence of wireless sensor networks, consisting of small, battery-powered "motes" with limited computation and radio communication capabilities. Sensor networks permit data gathering and computation to be deeply embedded in the physical environment. This technology has the potential to impact the delivery and study of resuscitative care by allowing vital signs to be automatically collected and fully integrated into the patient care record and used for real-time triage, correlation with hospital records, and long-term observation.

The CodeBlue system is currently under development and a source code release is anticipated soon (April 2005).

The research focuses on the following areas:

- Integration of medical sensors with low-power wireless networks
- Wireless ad-hoc routing protocols for critical care; security, robustness, prioritization
- Hardware architectures for ultra-low-power sensing, computation, and communication
- Interoperation with hospital information systems; privacy and reliability issues
- 3D location tracking using radio signal information
- Adaptive resource management, congestion control, and bandwidth allocation in wireless networks

The project is supported by the National Science Foundation, National Institutes of Health, U.S. Army, Sun Microsystems, and Microsoft Corporation.

2.2.8 Proactive health

A project led by Intel.

Information about this project is found at the project’s website [26].

Intel's Proactive Health lab employs both social scientists who study the needs of seniors dealing with cognitive decline, cancer, and cardiovascular disease, and engineers who build home health technology prototypes to test with real families.

Intel's Proactive Health Research is exploring the ways in which ubiquitous computing can support the daily health and wellness needs of people in their homes and everyday lives. Can proactive systems, that anticipate a patient's needs, improve the quality of life for both the patients and their caregivers?

The project, launched in April 2002, consists of three phases:

- Phase One: Focus on physical and cognitive decline, especially on technologies that will help tomorrow's elderly population to age in place from wherever they and their families choose
- Phase Two: Address the needs of those with common chronic conditions like cancer and cardiovascular disease.
- Phase Three: Focus on wellness, including nutrition, physical fitness, and mental health.

Across all three phases, Intel is seeking to understand how technology can support behaviors that help prevent disease, foster independence, and improve quality of life.

Each phase of the project consists of three types of research. First, ethnographic field research is conducted in people's homes to identify their needs, through observation and interviews. Second, field results are then applied to develop and test early prototypes of future home systems that could help to meet the health needs of the entire household. Third, outcome studies are conducted of more developed prototype systems to determine whether or not such systems lead to positive outcomes.

The complex problems being addressed in the Proactive Health Strategic Research Project are beyond the capability of any one organization to solve. In conducting this research, the objective is to catalyze a research ecosystem of universities, industry labs, and government agencies to assist in this effort. Key collaborators include Intel Research Seattle, the University of Washington, the Oregon Health and Science University, the University of Rochester, and Georgia Tech. In addition, ideas are being exchanged and knowledge shared with other university, industry, and government researchers through conferences, workshops, and articles.

The goal of the research is to develop technology to assist these people in continuing to live meaningful lives at home.

Digital Home Technologies for Aging in Place: How can we deliver quality care to a rapidly growing population of older adults--historically the most expensive demographic to treat--while reducing the nation's healthcare costs? This solution can be enabled by a range of proactive computing technologies in the digital home enabling seniors to "age in place," maintaining their independence and deferring more costly institutional care as long as possible.

The Promise of Wireless Sensor Networks: The combination of social isolation, inactivity and failing nutrition is alarmingly common among today's aging population, but information technology may offer the means to counteract a harmful outcome. Intel has taken the initiative to invest in research and development of these sensor networks, recognizing this technology as crucial to addressing the pending global age wave and public health crisis.

Aging in Place Case Study: Helping the elderly age gracefully at home case study.
This study focuses on approximately 60 households in four cities across the U.S. that are dealing with everything from mild cognitive impairment to the advanced stages of Alzheimer's disease.

2.2.9 TelemediCare

A project conducted by SINTEF.

Information is found at the IST website [33].

The TelemediCare system will improve the quality of home-based care and medical treatment, through the development of a new generation of open platform telemedicine solutions. The project will introduce Medical Net Instruments, which implies that patients will receive 24-hour real-time medical monitoring in their own home. Advanced and reliable sensors on the body will supply high quality medical data. These data are sent to the patient’s computer through wireless communication. The computer will analyse and store the data. Intelligent software will trigger medical supervision, treatment or care by establishing two-way communication over the Internet with remote, "arrive-on-call" treatment/care providers. The system’s functionality is based on profound knowledge and understanding of the health care system throughout Europe. Development and demonstration is done in close co-operation with experienced telemedicine users in Sweden, Norway and Greece.

Work description:
The TelemediCare project involves several areas of research and development in the field of telemedicine: Four, miniaturised, non-intrusive medical sensors on the patient’s body will provide high quality real-time data on ECG, blood pressure, oxymetry and temperature. All (or some) of these parameters are of relevance to the monitoring of several medical conditions. The technological platform for these sensors will be open for later development of a wider range/family of medical sensors. Reliable wireless communication between sensors and the Local Patient Computer (LPC) improves well-being and mobility of monitored patients. The LPC will be the bridge between each patient and the surrounding treatment and care infrastructure. The computer will store high-resolution data in a Local Patient Record. Software services enable integration of binary objects, such as raw/analysed data, images etc., into the remote health care information system. The LPC will comprise an artificial intelligence that is able to trigger services from the treatment/care infrastructure on the basis of the evaluation of single or multiple elements in the patient’s medical status. The project will develop a secure web-based interface between the LPC and the monitoring treatment/care providing infrastructure. This will also allow for seamless integration with existing Hospital

Information Systems. The functionality of each component - as well as the entire system - will be developed, tested, validated and evaluated in realistic settings and in close co-operation with treatment and care providers with long experience from telemedicine. Medical experts and practitioners from Karolinska Hospital and municipal health care providers in rural areas of Norway and Greece will take part in establishing the functional and non-functional requirements for both single components and the entire system. The TelemediCare system will have an open technological platform.

The project was completed mid 2002. The main result of the 1-year assessment is, as planned, the prototype of a state-of-the-art tool for the analysis of protocols for e-commerce and other security-sensitive IT-applications. The project results demonstrate the success of the assessment phase: the prototype tool is better than all other existing analysis tools worldwide, in that it has either better coverage or better performance, or both. In particular, the prototype tool can detect many subtle attacks (e.g. based on typing ambiguities) that are missed by most other tools.

2.2.10 UbiMon

The UbiMon (Ubiquitous Monitoring Environment for Wearable and Implantable Sensors) project, funded by DTI, aims to provide a continuous and unobtrusive monitoring system for patients in order to capture transient but life threatening events. The project is conducted by the department of Computing, Imperial College London, UK [20].

The following information is picked up from UbiMon's website [21].

UbiMon is aimed at addressing general issues related to using wearable and implantable sensors for distributed mobile monitoring. As an exemplar, the value of the research is to be demonstrated in the management of patients with arrhythmic heart disease. This is motivated by the fact that cardiovascular disease remains the major cause of mortality and morbidity in the industrialised world despite significant progress in its prevention and treatment. Clinically, there is a growing need for continuous monitoring under natural physiological states of the patient so that transient but life threatening abnormalities to be detected or predicted. We will also investigate in parallel the use of implantable sensors for post surgical care, especially in conjunction with minimal access surgery. UbiMon represents a coherent cross-disciplinary integration of different expertise of the consortium, bringing together computing, electronics, bioengineering and medicine.

The objectives of the project are to develop:

- Techniques for portable communicator interactions with implantable sensors and interventional devices.
- A wearable communicator performing multi-sensor interfacing.
- Automated techniques for integrating multi-sensory data leading to an intervention strategy.

- A preliminary clinical evaluation for management of patients with ischaemic and arrhythmic heart disease.

The primary deliverables are:

- Novel micro-power circulatory for fully integrated sensory processing.
- Incorporation of ambient sensors, context awareness for improved sensing and episode detection
- Intelligent data fusion and mining for reliable prediction of critical events

The technical innovations are:

- Low power sensor coupling and telemetry suitable for long term implants
- Context aware and adapt to environment changes
- Integrated local processing with remote long term trend analysis
- Multi-sensory fusion and data mining with prediction for critical events [21]

With the current UbiMon structure, a number of wireless biosensors including 3-leads ECG, 2-leads ECG strip, and SpO2 sensors have been developed [20].

2.2.11 WsHC

The information about this project is picked up from the WsHC website [22].

Wireless Health and Care (WsHC) is a multi-disciplinary, collaborative research and development (R&D) project. Its aim is to develop prototype products and services within the health services based on wireless communication: Collection of sensor data via Bluetooth, ZigBee or specially designed radio protocols; data transfer to and from implantable probes; distribution of data to health personnel; and communication between health personnel.

The demonstrators of WsHC are built around an example scenario where a male person with a chronic disease (diabetes type I) is victim to a serious accident. This person is followed through several phases: Caring to his chronic disease; at the scene of the accident and during hospitalization; during his reconvalescence at home. Several demonstrators are developed that show how wireless technology can assist our friend throughout the scenario.

The needs and requirements of the health personnel for wireless technology are also considered. This comprises the accident scene, the operation room, the post-operative surveillance, and the home care personnel.

2.3 Potential areas for BAN applications

A wide range of future applications is expected since BAN can be used in many scenarios. In intensive care units (ICU), typical monitoring of vital parameters like blood pressure, body temperature, or ECG currently requires extensive wired instrumentation. Patients regardless of medical indications are not only bound to bed, but fixed by numerous cables and wires, unable to turn or just even move in bed. A BAN can eliminate the risk of unintentional disruption caused by moving patients and the uncomfortable handling of cables and wires. Practicability of monitoring in non-ICU clinical wards could also be enhanced using BAN as a platform for the acquisition of most vital signs data. Due to both economical and medical considerations, reducing the duration of stay at ICUs is desirable. The BAN BCU can be implemented as a wrist watch or a small belt-worn box. This can provide or support identification, authorisation and authentication procedures. In future pervasive clinical communication environments, nearly all services used and interactions performed by patients during hospital stays could be guided by a permanently worn personal BAN system. Typical areas covered could be admission and discharge, interactions with medical workflow, patient feedback and supervision, confirmation and acceptance of diagnostic or therapeutic measures, billing and quality control etc [5].

Patient monitoring in home environments is one of the most attractive areas of BAN applications. Due to cost saving aspects, hospitals try to minimise the duration of in-patient stays. BAN enables seamless connectivity in both hospital and home. The BAN BCU is able to interconnect with home network access points via wireless indoor communication systems like for example WLAN, DECT or Bluetooth. Wireless BAN-based monitoring is most desirable for patients with chronic diseases such as diabetes, asthma and cardiovascular diseases. When employing wireless BAN in the home of the patient it is also useful for rehabilitation measures and post operational care. A BAN BCU with modules for accessing global wireless networks like GSM or UMTS can provide potentially world-wide mobility for BAN users. Quality of life can be significantly improved in particular for patients suffering from chronic diseases which require permanent monitoring of vital signs [5].

BAN can also be useful in the areas of personal health support and medical process evaluation [5].

2.4 Important challenges in construction of wireless sensor networks

When constructing a wireless sensor network (WSN) there are many factors that need to be taken under consideration. In this project the following are considered essential.

2.4.1 Battery capacity

Power consumption in a WSN is important since most or all devices are battery powered. Replacing or recharging in short intervals will be impractical, so power consumption is of significant concern.

2.4.2 Scalability

The capability of a system to increase performance under an increased load when nodes are added needs to be considered.

2.4.3 Data rate capacity

How much it is possible to transfer per a unit of time between the nodes in a sensor network is of importance.

2.4.4 Fail-safety

Different mechanisms to ensure robustness needs to be in place. This to make sure the data frames gets through to the correct receiver without collisions or other errors.

2.4.5 Real time synchronization

The ability of the network to transmit data in real time, without error, is important in this project. Time synchronization between two sensors in one BAN needs to work seamlessly.

2.4.6 Association

The service used to establish a device’s membership in a WPAN. How a WPAN adds a new node is of interest in this project. As well as how one sensor is associated with the correct output at the monitor side.

2.4.7 Security

The security in wireless networks is always of great importance. In sensor networks it is especially important to have integrity and authentication. Integrity means that it is critical that the data at the receiver is the same as at the sender and has not been accidentally or maliciously modified, altered, or destroyed. Authentication is a concept within computer security that means to make absolute sure that the sender really is who it claims to be.

2.4.8 Cost

To be able to compete in the international market it is essential that the components are at lowest possible price. This is very important when the product shall be mass-produced.

3 Short range wireless technologies

3.1 IEEE 802.15.1 / Bluetooth

3.1.1 Overview

The Institute of Electrical and Electronics Engineers (IEEE) 802.15.1 standard is derived from the Bluetooth specification (version 1.1). In fact they have just added two clauses to the existing specification; WPAN architecture overview and Service access points (SAPs). In other words, the 802.15.1 standard presents a wireless personal area network (WPAN) that utilizes the Bluetooth wireless technology [11]. A PAN is defined as a computer network used for communication among computer devices close to one person.

Ericsson Mobile Communications started the development of the Bluetooth technology in 1994. In 1998 a group of companies formed the Bluetooth Special Interest Group (SIG) that would work to define and promote the Bluetooth specification. To exploit Bluetooth commercially the company must become a member of the SIG organization. Version 1.0 of the Bluetooth specification was released in 1999. The Bluetooth SIG later wanted to have the IEEE adopt the Bluetooth specifications and make them a formal IEEE 802 standard, the final agreement was achieved in 2000. The name Bluetooth is from Harald Blåtand, King of Denmark and Norway from 935 and 936 respectively, to 940 known for his unification of the warring tribes from Denmark, Norway and Sweden. Bluetooth likewise was intended to unify different technologies like computers and mobile phones [7].

The Bluetooth wireless technology uses a short-range radio link that is optimized for power-conscious, battery-operated, small size, lightweight personal devices. A Bluetooth WPAN supports both synchronous communication channels for telephony-grade voice communication and asynchronous communications channels for data communications. These facilities enable a rich set of devices and applications to participate in the Bluetooth WPAN. For example, a cellular phone may use the circuit-switched channels to carry audio to and from a headset while concurrently using a packet-switched channel to exchange data with a notebook computer [11].

A Bluetooth WPAN has a limited life span. It is created in an ad hoc manner whenever an application in a device desires to exchange data with matching applications in other devices. The Bluetooth WPAN may cease to exist when the applications involved have completed their tasks and no longer need to continue exchanging data.

The Bluetooth WPAN operates in the unlicensed 2.4 GHz industrial, scientific and medical (ISM) band. It avoids interference and noise from other devices operating in the same frequency band by using the spread spectrum technique called frequency hopping (FHSS). The communication changes the transmitting/receiving frequency 1600 times per second across 79 different frequencies. Information is exchanged through packets, and each packet is transmitted on a different frequency in the hopping sequence. Bluetooth supports both voice and data. The voice channels operate with 64 kbit/s. The Bluetooth 1.0 data rates include an asymmetric data rate (one way) of 721 kbit/s (while permitting 57.6 kbit/s in the return direction); and a symmetric data rate of 432.6 kbit/s. Bluetooth 2.0 has been designed to be backward compatible with existing Bluetooth devices, and will offer data transmission rates up to 10 Mbps. In general the main features of the Bluetooth Core Specification Version 2.0 + Enhanced Data Rate (EDR) are:

- 3 times faster transmission speed (up to 10 times in certain cases)
- Lower power consumption through reduced duty cycle
- Simplification of multi-link scenarios due to more available bandwidth
- Backwards compatible to earlier versions
- Further improved BER (Bit Error Rate) performance [13]

The jitter for the voice traffic is kept low by using small transmission slots. And a Gaussian-shaped, binary frequency shift keying (FSK) with a symbol rate of 1 Msymbols/s minimizes transceiver complexity.

Each device is classified into 3 power classes:

Power Class 1: is designed for long range (up to 100m) devices, with a max output power of 20 dBm,
Power Class 2: for ordinary range devices (up to 10m) devices, with a max output power of 4 dBm,
Power Class 3: for short range devices (up to 10cm) devices, with a max output power of 0 dBm.

The Bluetooth radio interface is based on a nominal antenna power of 0dBm. Each device can optionally vary its transmitted power.

A packet transmitted over the air in a Bluetooth WPAN, comprises a fixed-size access code, which is used, among other things, to distinguish one Bluetooth WPAN from another. It also contains a fixed-size packet header, which is used for managing the transmission of the packet in a Bluetooth WPAN, and a variable-size payload, which carries upper layer data. Due to the small size of these packets, large upper-layer packets need to be segmented prior to transmission over the air [11].

3.1.2 Network topology

The piconet is the simplest form of network configuration for Bluetooth devices. A piconet can comprise of one master device and one or more (up to seven active) slave devices. Each Bluetooth device is capable of assuming the master or slave role, depending on its configuration. The role of each device is determined upon initial connection, usually with the connection requesting device as the master (i.e. the device that initializes the formation of the piconet). Bluetooth provides both point-to-point (see Figure 3 a) and point-to-multipoint connections (Figure 3 b). Several piconets can network together to form scatternets (see Figure 3 c). In a scatternet, one or more devices participate in more than one piconet. However, they can only send and receive data in one piconet at a time. A master in one piconet can be a slave in another piconet.

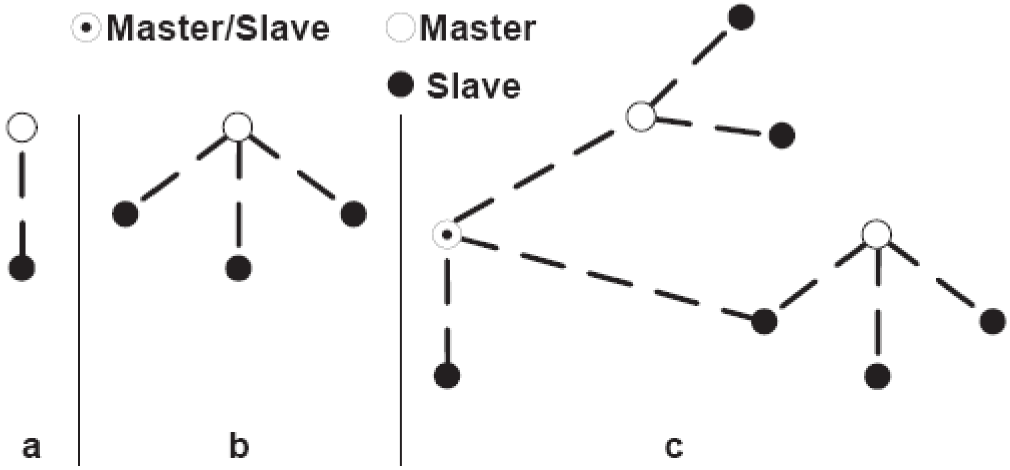


Figure 3. Examples of piconet formations [11]

The piconet is synchronized by the system clock of the master. The master never adjusts its system clock during the existence of the piconet. The slaves adapt their native clocks with a timing offset in order to match the master clock. This offset is updated each time a packet is received from the master. By comparing the exact RX timing of the received packet with the estimated RX timing, the slaves correct the offset for any timing misalignments [11].

3.1.3 Protocol stack

The Bluetooth protocol stack includes both Bluetooth-specific protocols (e.g., LMP, L2CAP) and non-Bluetooth-specific protocols like the Object Exchange Protocol (OBEX), the Point-to-Point Protocol (PPP), and the Wireless Application Protocol (WAP) etc.

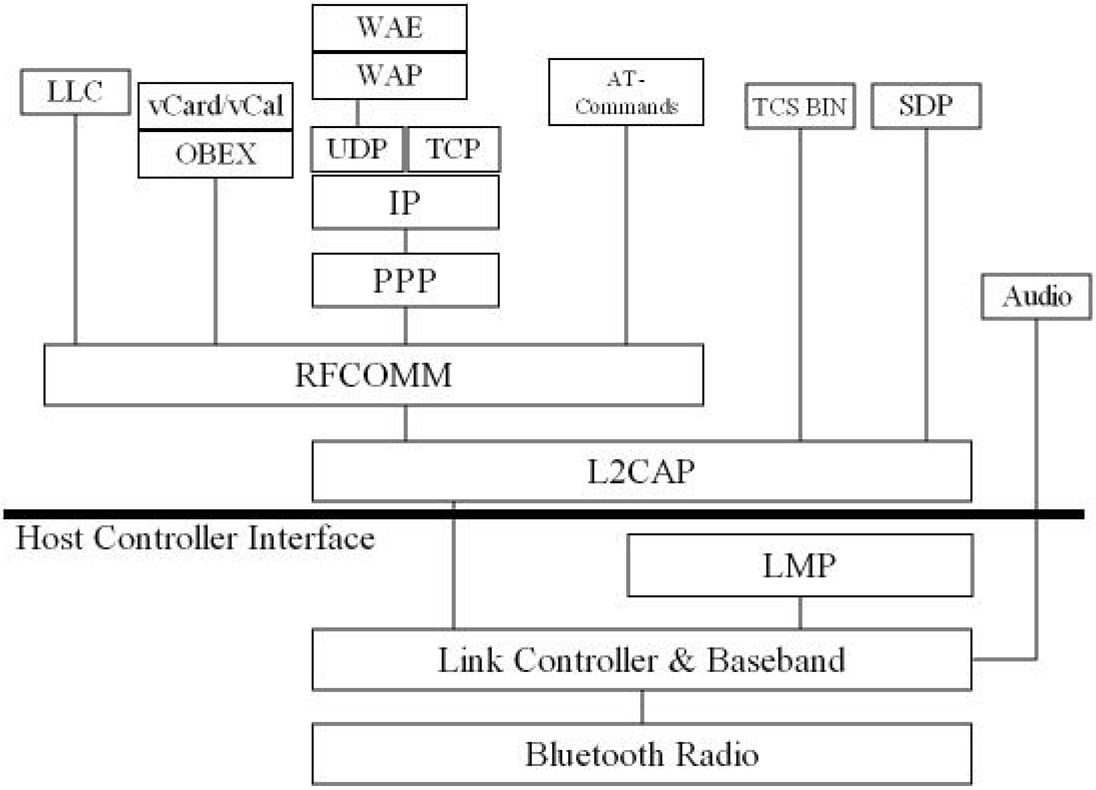


Figure 4. The Bluetooth protocol stack [11]

The RFCOMM layer is a serial port emulation layer for enabling legacy applications over Bluetooth links. This way existing protocols at the higher layers can be used, hence existing applications can work with Bluetooth. The TCS is a telephony control and signalling layer for advanced telephony applications. The SDP is a service discovery layer allowing Bluetooth devices to ask other devices for the services that they can provide.

The IEEE 802.15.1 standard only includes the layers from L2CAP and below. The Bluetooth radio has two objects: It receives a bit stream from the MAC sublayer and transmits the bit stream via radio waves to an associated station; and it receives radio waves from an associated station and converts them to a bit stream that is passed to the MAC. This reflects the limited scope of the physical radio portion of the IEEE 802.15.1 architecture. Bits and radio waves are transmitted, but this layer does not do any interpretation [11].

The baseband layer lies on top of the Bluetooth radio layer in the Bluetooth stack. The baseband protocol is implemented as a Link Controller (LC), which works with the link manager for carrying out link level routines like link connection and power control. The LC is responsible for the encoding and decoding of Bluetooth packets and managing the Link Control Protocol (LCP) signalling.

The Link Module is also responsible for performing the three error correction schemes that are defined for Bluetooth:

- 1/3 rate FEC
- 2/3 rate FEC
- ARQ scheme for the data

The purpose of the two FEC (forward error correction) schemes is to reduce the number of retransmissions. The ARQ (automatic retransmission request) scheme will cause the data to be retransmitted until an acknowledgement is received indicating a successful transmission (or until a pre-defined time-out occurs). A CRC (cyclic redundancy check) code is added to each packet and used by the receiver to decide whether or not the packet has arrived error free. The ARQ scheme is only used for data packets, not synchronous payloads such as voice.

The link manager (LM) is responsible for the creation, modification and releasing of logical links. The LM carries out link setup, authentication, link configuration and other protocols. It discovers other remote LMs and communicates with them via the Link Manager Protocol (LMP). To perform its service provider role, the LM uses the services of the underlying LC.

The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the Baseband Protocol and resides in the data link layer. L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions.

The host controller interface (HCI) provides a command interface to the baseband controller and link manager, and access to hardware status and control registers. This interface provides a uniform method of accessing the Bluetooth baseband capabilities. The HCI section has two functions in the Bluetooth Specification. It defines a basis for a physical interface for a Bluetooth external module and it defines the control functions necessary for all Bluetooth implementations [12].

3.1.4 Security

In every Bluetooth device, there are four entities used for maintaining the security at the link level. First Bluetooth uses IEEE defined device addresses, which is a 48-bit address that is unique for each Bluetooth device. Second it uses a private authentication key, which is a 128-bit random number used for authentication purposes. Third, a private encryption key is used, 8-128 bits in length that is used for encryption. And forth a random number (RAND) is used, which is a frequently changing 128-bit random or pseudo-random number that is made by the Bluetooth device itself.

In Bluetooth Generic Access Profile, the Bluetooth security is divided into three modes:

Security Mode 1: non-secure
Security Mode 2: service level enforced security
Security Mode 3: link level enforced security

The difference between Security Mode 2 and Security Mode 3 is that in Security Mode 3 the Bluetooth device initiates security procedures before the channel is established. [12]

There are also different security levels for devices and services. For devices, there are two levels, "trusted device" and "untrusted device". A trusted device, having been paired with one's other device, has unrestricted access to all services. For services, three security levels are defined: services that require authorization and authentication, services that require authentication only and services that are open to all devices [13].

The transmission scheme (FHSS) provides another level of security in itself. Instead of transmitting over one frequency within the 2.4 GHz band, Bluetooth radios use a fast frequency-hopping technique, allowing only synchronized receivers to access the transmitted data [11].

3.1.5 Cost

In Taiwan, Bluetooth chip prices for entry-level products were under $4 in Q3 2004, with chips for audio solutions at $6 apiece [44].

3.1.6 Prospects

When Ericsson stopped the Bluetooth production in mid 2004, many said it was the end for Bluetooth. But new actors came in to play and new improved Bluetooth versions are on the way. Bluetooth 2.0 a.k.a. Bluetooth 2.0+EDR offers a 3 times faster data transfer than Bluetooth v1.2., this with almost no rise in power consumption making it more power efficient than its predecessor. This of course translates to longer battery life and makes it more competitive in the sensor market.

And recently the Bluetooth SIG formally chose ultra wideband (see section 3.2) as the foundation for future versions of its technology, making Bluetooth's future very interesting [13].

3.2 IEEE 802.15.3 High-Rate WPAN / Ultra wideband (UWB)

3.2.1 General overview

802.15.3 is the IEEE standard for high data rate WPAN designed to provide Quality of Service (QoS) for real time distribution of multimedia content like video and music. It is initially intended for a home multimedia wireless network. The original standard uses a "traditional" carrier-based 2.4 GHz radio as the physical layer (PHY). But a sister standard, 802.15.3a, is on the way. It will define an alternative PHY, based on UWB, which will provide in excess of 110 Mbps at a 10m distance and 480 Mbps at 2m [6]. There are currently two proposals remaining in the competition, the MultiBand OFDM Alliance (MBOA) led by Intel and Texas Instruments, and the DS-CDMA group led by Freescale (a Motorola spinoff) and XtremeSpectrum. They have argued for several years and it does not seem like they will ever agree since they now are going to the market with separate designs [10].

3.2.2 Technical overview of UWB

Ultra-wideband usually refers to a radio modulation technique based on transmitting very-short-duration pulses, often of duration of only nanoseconds or less, whereby the occupied bandwidth goes to very large values [7]. In the U.S., the Federal Communications Commission (FCC) has mandated that UWB radio transmission can legally operate in the range from 3.1 GHz to 10.6 GHz, at a transmit power of -41 dBm/MHz. The FCC has restricted UWB to 10 meter range. The concept of a UWB radio includes many different applications and industries and has been called the "common UWB radio platform". The UWB radio, along with the convergence layer, becomes the underlying transport mechanism for different applications, some of which are currently only wired. Some of the more notable applications that is most likely to operate on top of the common UWB platform would be wireless universal serial bus (WUSB), IEEE 1394, the next generation of Bluetooth, and Universal Plug and Play (UPnP). Figure 5 shows a diagram of this vision.

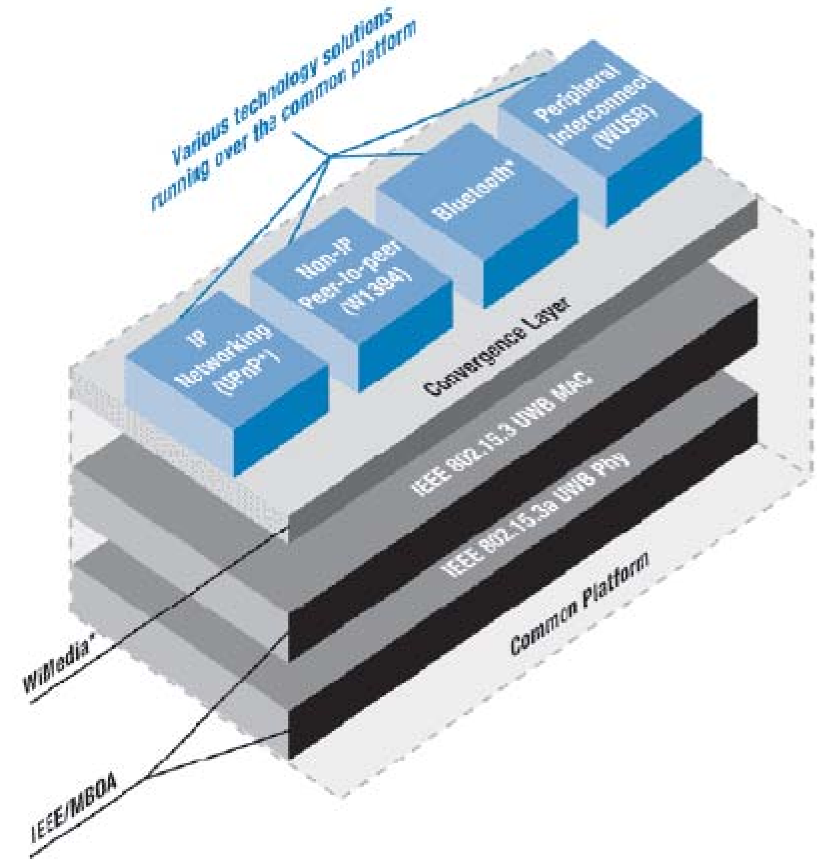


Figure 5. Diagram of the UWB common platform [8]

A traditional UWB transmitter works by sending billions of pulses across a very wide spectrum of a frequency several GHz in bandwidth. The corresponding receiver then translates the pulses into data by listening for a familiar pulse sequence sent by the transmitter. Specifically, UWB is defined as any radio technology having a spectrum that occupies a bandwidth greater than 20 percent of the center frequency, or a bandwidth of at least 500 MHz [8].

Modern UWB systems use other modulation techniques, such as Orthogonal Frequency Division Multiplexing (OFDM), to occupy these extremely wide bandwidths (this is Intel and TI's proposal). In addition, the use of multiple bands in combination with OFDM modulation can provide significant advantages to traditional UWB systems. The MultiBand OFDM approach allows for good coexistence with narrowband systems such as 802.11a, adaptation to different regulatory environments, future scalability and backward compatibility. This design allows the technology to comply with local regulations by dynamically turning off subbands and individual OFDM tones to comply with local rules of operation on allocated spectrum [8].

With the formation of the MBOA in June 2003, OFDM for each subband was added to the initial multiband approach in order to develop the best technical solution for UWB.

To date, the MultiBand OFDM Alliance has more than 170 participants (and growing) that support a single technical proposal for UWB. It recently joined forces with the WiMedia alliance (March 2005), which makes the MBOA group very strong in the battle of the 802.15.3a standard.

In the MultiBand OFDM approach, the available spectrum of 7.5 GHz is divided into several 528-MHz bands. This allows the selective implementation of bands at certain frequency ranges while leaving other parts of the spectrum unused. The dynamic ability of the radio to operate in certain areas of the spectrum is important because it can adapt to regulatory constraints imposed by governments around the world.

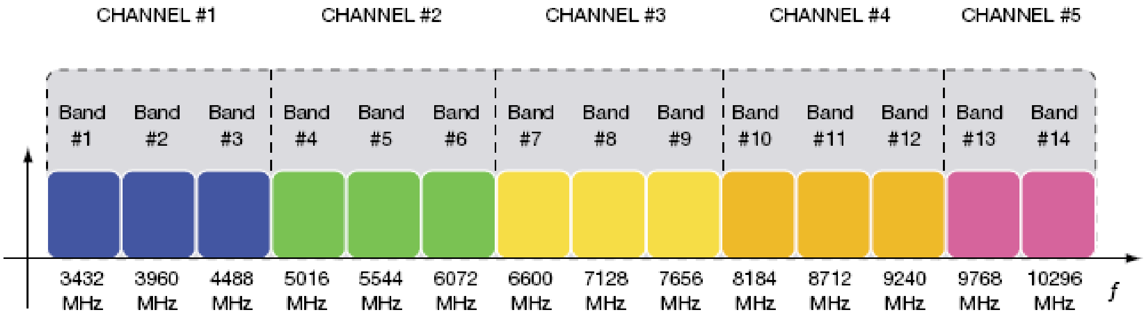


Figure 6. The MultiBand OFDM frequency band plan [8].

The band plan for the MBOA proposal has five logical channels (see figure 2). Channel 1, which contains the first three bands, is mandatory for all UWB devices and radios. Multiple groups of bands enable multiple modes of operation for MultiBand OFDM devices. In the current MultiBand OFDM Alliance's proposal, bands 1–3 are used for Mode 1 devices (mandatory mode), while the other remaining channels (2–5) are optional. There are up to four time-frequency codes per channel, thus allowing for a total of 20 piconets with the current MBOA proposal. In addition, the proposal also allows flexibility to avoid channel 2 if a U-NII (Unlicensed-National Information Infrastructure) interference is present, e.g. from 802.11a [8].

3.2.2.1 OFDM Modulation

The information transmitted on each band is modulated using OFDM. OFDM distributes the data over a large number of carriers that are spaced apart at precise frequencies. This spacing provides the orthogonality in this technique, which prevents the demodulators from seeing frequencies other than their own. The benefits of OFDM are high-spectral efficiency, resiliency to RF interference, and lower multipath distortion.

By using OFDM modulation techniques coupled with multibanding, it becomes easier to collect multipath energy using a single RF chain and allows the receiver to deal with narrowband interference without having to sacrifice subbands or data rate. These advantages relate to the ability to turn off individual tones and also easily recover damaged tones through the use of forward error-correction coding [8].

3.2.3 Technical overview of IEEE 802.15.3

A piconet is a wireless ad hoc data communications system which allows a number of independent data devices (DEVs) to communicate with each other. A piconet is distinguished from other types of data networks in that communications are normally confined to a small area around a person or object that typically covers at least 10 m in all directions whether the person or object is stationary or in motion.

Figure 1 shows the different components that form the 802.15.3 piconet. The basic component is the DEV, one of which is required to assume the role of the piconet coordinator (PNC). The PNC provides the basic timing for the piconet with the beacon. Additionally, the PNC manages the QoS requirements, power save modes and access control to the piconet.

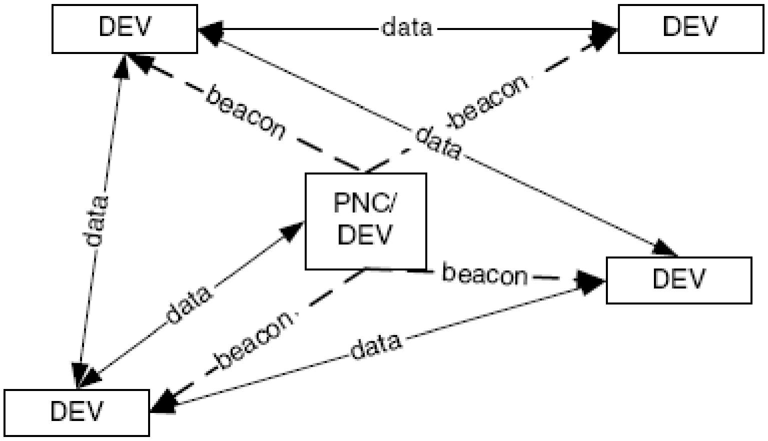
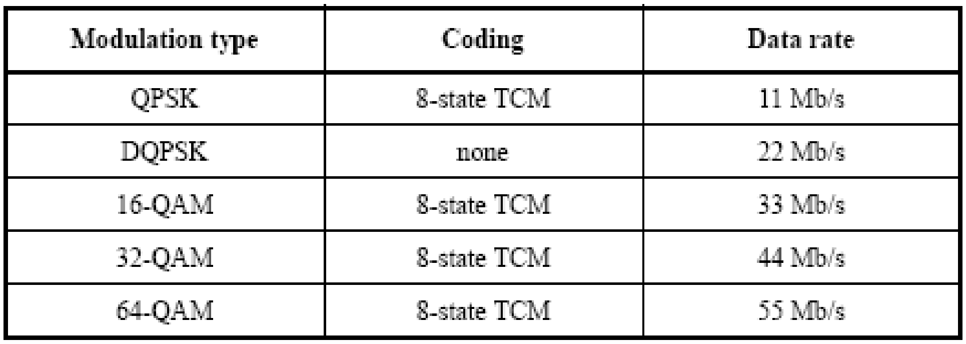


Figure 7. The components of an 802.15.3 piconet [9]

A DEV can also request the formation of a subsidiary piconet, referred to as either a child or neighbour piconet, depending on the method the DEV used to associate with the parent PNC. Child and neighbour piconets are also referred to as dependent piconets since they rely on the parent PNC to allocate channel time for the operation of the dependent piconet [9].

An 802.15.3-compliant DEV shall, at a minimum, support DQPSK modulation. In addition, if an 802.15.3 DEV supports a given modulation format other than DQPSK, it shall also support all of the lower modulation formats. For example, if an 802.15.3 implementation supports 32-QAM, it shall also support 16-QAM and QPSK-TCM as well as the DQPSK modulation formats.



Modulation type	Coding	Data rate
QPSK	8-state TCM	11 Mb/s
DQPSK	none	22 Mb/s
16-QAM	8-state TCM	33 Mb/s
32-QAM	8-state TCM	44 Mb/s
64-QAM	8-state TCM	55 Mb/s

Table 1. Modulation, coding and data rates for the 2.4 GHz PHY [9]

The symbol rate for all modulations is 11 Mbaud. Based on this symbol rate and the coding, the raw physical layer data rates supported are 11, 22, 33, 44, 55 Mb/s as shown in table 1.

802.15.3 piconets use two access methods in the superframe; CSMA/CA during the contention access period (CAP) and TDMA during the channel time allocation period (CTAP). To ensure robustness it supports three types of acknowledgement, no, immediate, and delayed.

All DEVs within a piconet is synchronized to the PNC's clock. In addition, child or neighbor PNCs shall synchronize their piconet's time usage to the parent PNC's beacon and their CTA. The beacon sent at the beginning of every superframe contains the information necessary to time-synchronize the DEVs in the piconet [9].

3.2.3.1 Power management

An important goal of the 802.15.3 standard is to enable long operation time for battery powered DEVs. The best method for extending battery life is to enable DEVs to turn off completely or reduce power for long periods of time, where a long period is relative to the superframe duration. This standard provides three techniques to enable DEVs to turn off for one or more superframes: device synchronized power save (DSPS) mode, piconet-synchronized power save (PSPS) mode and asynchronous power save (APS) mode. In the piconet, DEVs operate in one of four power management modes; ACTIVE mode, DSPS mode, PSPS mode or APS mode. Regardless of the DEV's power management mode, every DEV in the piconet is allowed to power down during parts of the superframe when the DEV is not scheduled to transmit or receive data [9].

It is also possible to control transmit power in the piconet, this enables DEVs to minimize interference with other wireless networks that share the same channel as well as to decrease the power usage in some PHY implementations [9]. Actually, UWB transmit power is less than what a standard PC is allowed to radiate unintentionally. It then spreads the power over an extremely wide swath of radio spectrum. This makes the UWB signal at any one frequency extremely small. Because of their low power spectrum density, unlicensed UWB radios will cause no interference to other radio systems operating in dedicated bands [6].

3.2.4 Association

An unassociated DEV initiates the association process by sending an association request to the piconet coordinator. The PNC acknowledge all correct received association request commands by sending an immediate acknowledgement frame (Imm-ACK). The coordinator then takes some time to ensure that the DEV should be allowed in the piconet and that there are enough resources for another DEV. If permission is granted it sends an association response back to the DEV, including an assigned DEVID, letting it know that connecting is allowed. That DEVID will then be used for all future communications. The PNC needs to do this within 262.14 µs. The connecting DEV then needs to send a second associate request including its new DEVID to the PNC. The PNC then sets the DEV as associated and responds with an Imm-ACK, upon receiving this ACK the DEV consider itself associated. All other DEVs in the piconet also receive information about their new neighbor from the PNC [9].

3.2.5 Security

UWB was designed with security in mind. Its signal is supposedly indistinguishable from regular RF noise due to its pulse sequencing technology. It communicates in very short bursts (measure in picoseconds or trillionths of a second), so a receiver has to know exactly when to listen in order to pickup the signal - something that, at least for now, cannot be easily performed using "outside" equipment. It also has interference and jamming protection built-in with the way it transmits signals across a broad frequency spectrum. In addition, it has built-in encryption and physical security through its location sensing technology.

The 802.15.3 standard supports two different modes of security, no security and the use of strong cryptography. The standard supports the protection of command, beacon and data frames using a 128-bit AES security suite, and the distribution of keys for command and data frame protection [9].

3.2.6 Cost

One of the fundamental advantages of UWB is that it eliminates many of the analog and mixed signal components of traditional carrier wave based radios. It is an "all digital" radio and can take advantage of Moore's Law scaling. Once it is fully developed, it is destined to become a low cost solution, particularly considering the data rates it can support [6]. An ABI research study has predicted that the price will be somewhere close to 14 dollar [42].

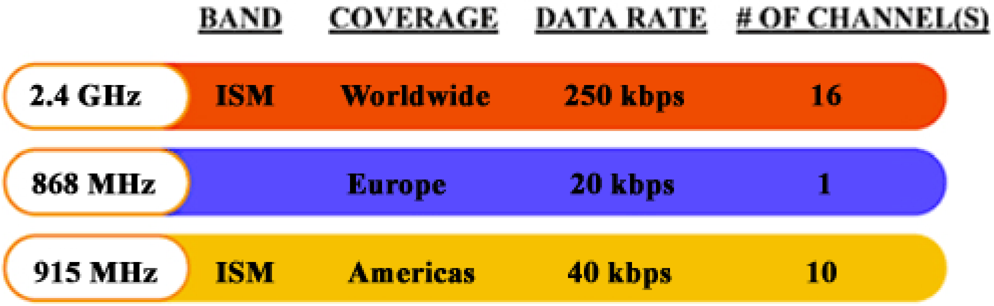
3.2.7 Prospects

It does not seem like the two camps, MBOA and DS-CDMA, will agree any time soon. Especially not now when they have started going to the market with separate designs. However a compromise has been introduced called Common Signalling Mode (CSM), using this technology both solutions can coexist. But as of today MBOA has still not agreed on the compromise.

Joining forces with Bluetooth is as lucrative for UWB as it is for Bluetooth. UWB is a new player in the marked and needs the help of a big player like Bluetooth to be accepted.

3.3 IEEE 802.15.4 Low-Rate WPAN

IEEE 802.15.4 is a standard defined by the IEEE for low-rate (LR) WPANs. A LR-WPAN is a simple, low cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of a LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life [1]. Like all IEEE 802 standards, the IEEE 802.15.4 standard encompasses only those layers up to and including portions of the data link layer (DLL). I.e. the standard defines the PHY and the medium access layer (MAC). In particular it defines two PHYs representing three license-free frequency bands that include sixteen channels at 2.4 GHz, ten channels at 902 to 928 MHz, and one channel at 868 to 870 MHz. The maximum data rates for each band are 250 kbps, 40 kbps and 20 kbps, respectively.



	BAND	COVERAGE	DATA RATE	# OF CHANNEL(S)
2.4 GHz	ISM	Worldwide	250 kbps	16
868 MHz		Europe	20 kbps	1
915 MHz	ISM	Americas	40 kbps	10

Table 2. Table of frequency, data rate, and number of channels in the ISM bands [40]

The 2.4 GHz band operates worldwide while the sub-1 GHz band operates in North America, Europe, and Australia/New Zealand (see Table 2). The IEEE standard is intended to conform to established regulations in Europe, Japan, Canada and the United States [2].

3.3.1 Components of the IEEE 802.15.4 WPAN

A WPAN consists of several components; the most basic is the device. There are two different device types which can participate in an LR-WPAN; a full-function device (FFD) and a reduced-function device (RFD). A FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD. A RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; they do not have the need to send large amounts of data and may only associate with a single FFD at a time. Because of that, the RFD can be implemented using minimal resources and memory capacity.

Two or more devices within a personal operating space (POS) communicating on the same physical channel constitute a WPAN. But a network shall include at least one FFD, operating as the PAN coordinator.

An IEEE 802.15.4 network is part of the WPAN family of standards although the coverage of an LR-WPAN may extend beyond the POS, which typically defines the WPAN.

Propagation characteristics for wireless media are dynamic and uncertain, thus a well-defined coverage area does not exist. Small changes in position or direction may result in drastic differences in the signal strength or quality of the communication link. These effects occur whether a device is stationary or mobile as moving objects may impact station-to-station propagation [1].

3.3.2 Network topologies

The formation of the network is performed by the network layer, which is not a part of the IEEE 802.15.4 standard. Still a brief overview of the possibilities is worth mentioning.

In both wired and wireless networks, the network layer is responsible for topology construction and maintenance, as well as naming and binding services, which incorporate the necessary tasks of addressing, routing, and security [3]. But this is far more challenging to implement for wireless services because of the premium placed on energy conservation. In fact, it is important for any network layer implementation built on the already energy conscious IEEE 802.15.4 standard to be equally conservative. Network layers built on the standard are expected to be self-organizing and self-maintaining, to minimize total cost to the consumer user [4].

The IEEE 802.15.4 standard supports multiple network topologies, including both star and peer-to-peer networks (see figure 8). The topology is an application design choice; some applications may require the low-latency connection of the star network, e.g. PC peripherals, toys and games, and personal health care. Others may require the large-area coverage of peer-to-peer networking, e.g. perimeter security [4].

The basic structure of a star network can be seen in figure 8. After an FFD is activated for the first time, it may establish its own network and become the PAN coordinator. All star networks operate independently from all other star networks currently in operation. This is achieved by choosing a PAN identifier, which is not currently used by any other network within the radio sphere of influence. Once the PAN identifier is chosen, the PAN coordinator can allow other devices to join its network; both FFDs and RFDs may join the network [1].

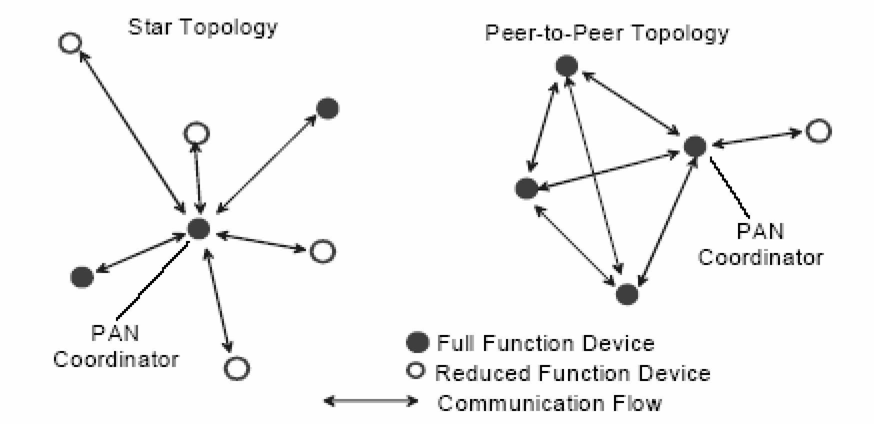


Figure 8. Examples of star and peer-to-peer Topology [1]

Each independent PAN will select a unique identifier. This PAN identifier allows communication between devices within a network using short addresses and enables transmissions between devices across independent networks.

3.3.3 Architecture

The LR-WPAN architecture is defined in terms of layers defined by the open system interconnection (OSI) model (see figure 9). A LR-WPAN device comprises a PHY, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sublayer that provides access to the physical channel for all types of transfer [1].

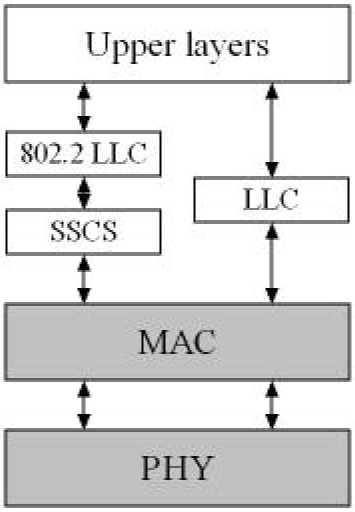


Figure 9. LR-WPAN device architecture [1]

IEEE 802 splits the data link layer (DLL) into two sublayers, the MAC and logical link control (LLC) sublayers. The IEEE 802.15.4 MAC provides services to an IEEE 802.2 type 1 LLC through the service-specific convergence sublayer (SSCS), or a proprietary LLC can access the MAC services directly without going through the SSCS. The SSCS ensures compatibility between different LLC sublayers and allows the MAC to be accessed through a single set of access points. Using this model, the 802.15.4 MAC provides features not utilized by 802.2, and therefore allows the more complex network topologies mentioned above.

The features of the IEEE 802.15.4 MAC are association and disassociation, acknowledged frame delivery, channel access mechanism, frame validation, guaranteed time slot management, and beacon management.

The MAC sublayer provides two services to higher layers that can be accessed through two service access points (SAPs). The MAC data service is accessed through the MAC common part sublayer (MCPS-SAP), and the MAC management services are accessed through the MAC layer management entity (MLME-SAP). These two services provide an interface between the SSCS or another LLC and the PHY layer [1].

3.3.4 Superframe and frame structure

The LR-WPAN standard allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator. The superframe is bounded by network beacons, is sent by the coordinator (see Figure 10), and is divided into 16 equally sized slots. The beacon frame is transmitted in the first slot of each superframe. If a coordinator does not wish to use a superframe structure, it may turn off the beacon transmissions. The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the structure of the superframes. Any device wishing to communicate during the contention access period between two beacons will compete with other devices using a slotted CSMA-CA mechanism. All transactions will be completed by the time of the next network beacon. The superframe can have an active and an inactive portion. During the inactive portion, the coordinator will not interact with its PAN and may enter a low-power mode [1].

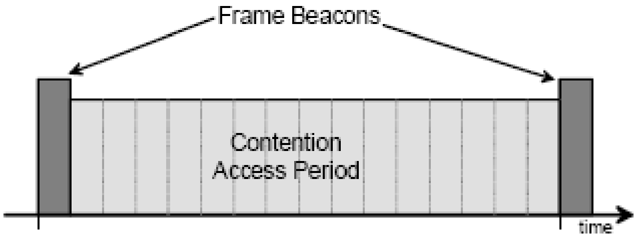


Figure 10. Superframe structure without GTSs [1]

For low-latency applications or applications requiring specific data bandwidth, the PAN coordinator may dedicate portions of the active superframe to that application. These portions are called guaranteed time slots (GTSs). The GTSs form the contention-free period (CFP), which always appears at the end of the active superframe starting at a slot boundary immediately following the CAP, as shown in Figure 5. The PAN coordinator may allocate up to seven of these GTSs, and a GTS may occupy more than one slot period. However, a sufficient portion of the CAP shall remain for contention-based access of other networked devices or new devices wishing to join the network. All contention-based transactions shall be complete before the CFP begins. Also each device transmitting in a GTS shall ensure that its transaction is complete before the time of the next GTS or the end of the CFP.

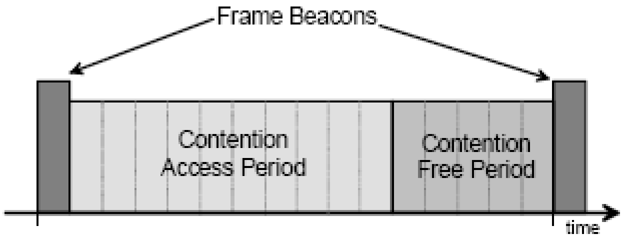


Figure 11. Superframe structure with GTSs [1]

The frame structures have been designed to keep the complexity to a minimum while at the same time making them sufficiently robust for transmission on a noisy channel. The LR-WPAN defines four frame structures [1]:

- A beacon frame, used by a coordinator to transmit beacons
- A data frame, used for all transfers of data
- An acknowledgment frame, used for confirming successful frame reception
- A MAC command frame, used for handling all MAC peer entity control transfers

3.3.5 Robustness

The LR-WPAN employs different mechanisms to ensure robustness in the data transmission. These mechanisms are the Carrier Sense Multiple Access – Collision Avoidance (CSMA-CA) mechanism, frame acknowledgment, and data verification [1].

3.3.6 Security

The security mechanisms in this standard are symmetric-key based using keys provided by higher layer processes. The management and establishment of these keys is the responsibility of the implementer. The security provided by these mechanisms assumes the keys are generated, transmitted, and stored in a secure manner.

The IEEE 802.15.4 MAC sublayer specifies four security services. Access control is a security service that provides the ability for a device to select the other devices with which it is willing to communicate. Each device maintains a list of trusted devices within the network called an access control list (ACL). Data encryption uses symmetric key 128-bit advanced encryption standard (AES). Frame integrity is used to protect data from being modified by parties without cryptographic keys. And sequential freshness to reject data frames that have been replayed, the network controller compares the freshness value with the last known value from the device and rejects it if the freshness value has not been updated to a new value.

The MAC sublayer provides different security services depending on which of two security modes it is in. There is unsecured mode, which basically means no security is provided at all, and there is ACL mode. Devices operating in ACL mode provide limited security services for communications with other devices. While in ACL mode, the higher layer may choose to reject frames based on whether the MAC sublayer indicates that a frame is purported to originate from a specific device. Because cryptographic protection is not provided in the MAC sublayer in this mode, the higher layer should implement other mechanisms to ensure the identity of the sending device. Access control is the only service which is provided in ACL mode [1].

3.4 ZigBee

3.4.1 Overview

The standard gets its name from the domestic honeybee, which are individually simple organisms that work together to tackle complex tasks [14]. The ZigBee Alliance is a consortium of leading semiconductor manufacturers, technology providers, original equipment manufacturers (OEMs) and end-users worldwide that have developed a common standard for wireless networking of sensors and controllers. The alliance has of Q1 2005 over 150 members including eight promoters (Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Philips, and Samsung) [14]. While other wireless standards are concerned with exchanging large amounts of data, ZigBee is built for devices that have smaller throughput needs. The other driving factors are low cost, high reliability, high security, low battery usage, simplicity and interoperability with other ZigBee devices [14]. As a culmination of two years of worldwide development and interoperability testing by more than 100 member companies within the ZigBee Alliance, the ZigBee specification was ratified in Q4 2004. The general characteristics of the specification include typical range of 50 meters (5-500 m based on environment), fully hand-shaked protocol for transfer reliability, 64-bit IEEE and 16-bit short addressing, supporting over 65,000 nodes per network, and optimization for low duty-cycle applications. It is also a self-organising and self-healing technology, meaning that ZigBee networks should be essentially plug-and-play, they won't need configuring by the user and can adapt to network changes automatically [14].

3.4.2 Architecture

When engineers first started working with ZigBee in 1998 [7] it was targeted towards automation and remote control applications. ZigBee was created to address a market need for an industry standard to support these applications, as opposed to proprietary solutions. The IEEE 802.15.4 committee started working on a low data rate standard a short while later. The ZigBee Alliance and the IEEE decided to join forces and ZigBee became the commercial name for the technology. The way the partnership works, is that the ZigBee technology is build on the PHY and MAC layers defined by the IEEE 802.15.4 standard (see section 3.3). The IEEE standard defines the Physical hardware and Media Access Control layers of the network, while the ZigBee Alliance defines the upper layers (see figure 12).

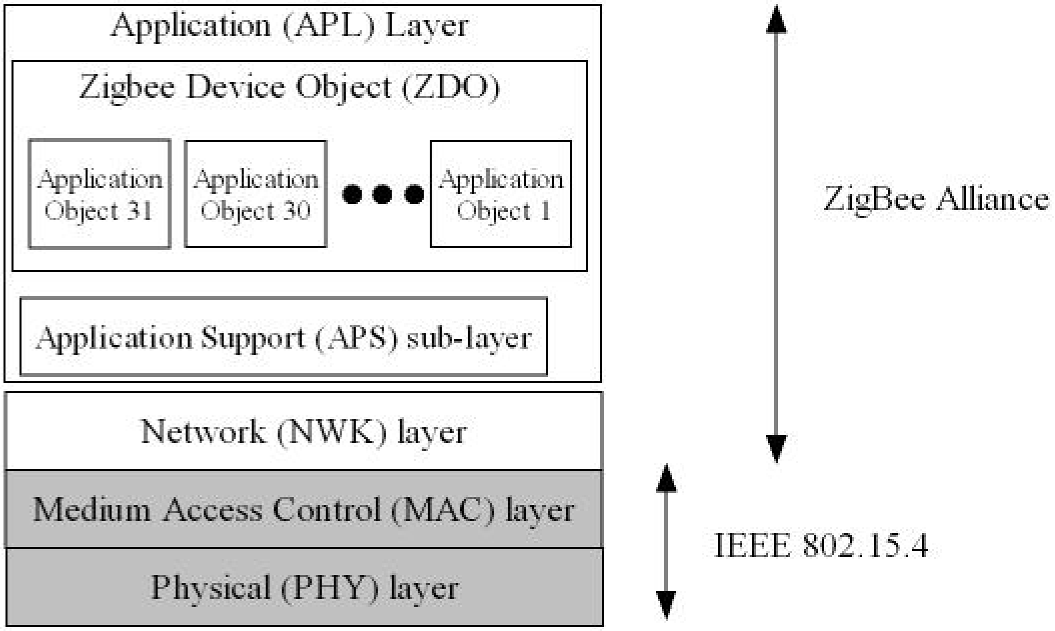


Figure 12. ZigBee stack architecture [2]

The fact that ZigBee rides on top of the IEEE 802.15.4 standard means that ZigBee can take full advantage of the standards qualities which is presented in the previous section (3.3). But it also suffers from its limitations, e.g. low data rate.

The NWK layer has three main objectives; association or dissociation of devices using the network coordinator, security implementation, and routing of frames to their intended destination. In addition, the NWK layer of the network coordinator is responsible for starting a new network and assigning an address to newly associated devices [2].

The ZigBee NWK layer supports multiple network topologies including star, cluster tree, and mesh, all illustrated in figure 13. In star topology one of the FFD-type (the device types are the same as the one described in section 3.3.1) devices assumes the role of network coordinator. It is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the coordinator. A mesh network allows for continuous connections and reconfiguration around blocked paths by "hopping" from node to node until a connection can be established. Mesh networks are self-healing, meaning that the network can still operate even when a node breaks down or a connection goes bad. As a result, a very reliable network is formed. Cluster tree is a mix of star and mesh formations as illustrated in figure 13 [2].

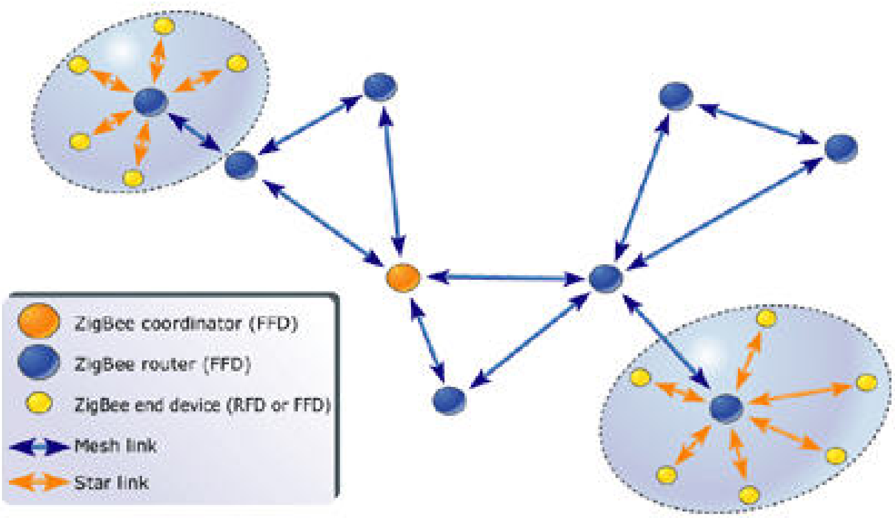


Figure 13. ZigBee network formations [2]

For WPANs supporting beacons, synchronization is performed by receiving and decoding the beacon frames. For WPANs not supporting beacons, synchronization is performed by polling the coordinator for data. Beacons are primarily used to reduce a system's power consumption; it simply tells the devices when to communicate with each other. Beacon mode is recommended when the devices are battery powered [1].

The application layer consists of the application support layer (APS), the ZigBee device object (ZDO) and the manufacturer-defined application objects. The APS is responsible for maintaining tables for binding and forwarding messages between bound devices. A binding is the ability to match two devices together based on their services and their needs. The layer is also responsible for device discovery, which is the procedure to discover other devices that are operating in the local area. The ZDO defines the role of the device in the ZigBee network (ZigBee network coordinator, ZigBee coordinator, or ZigBee end device). The ZigBee device object is also responsible for initiating and responding to binding requests. The application objects are defined by the manufacturer that implements the application. The ZigBee protocol stack supports up to 30 distinct application objects to be implemented at the same time [2].

Compared to other wireless standards the ZigBee stack is small. For network-edge devices with limited capabilities, the stack requires about 4Kb of the memory. Full implementation of the protocol stack takes less than 32Kb of memory. The network coordinator may require extra RAM for a node device database, for transaction tables and for pairing tables. The 802.15.4 standard defines 26 primitives for the PHY and MAC layers. Those numbers are modest compared to 131 primitives defined for Bluetooth. Such a compact footprint enables the opportunity to run ZigBee on a simple 8-bit microcontroller [15].

3.4.3 Association

When a new device want to join an existing WPAN a parent-child relationship is formed. The new device becomes the child, while the first device becomes the parent. Only a coordinator or a router can permit a device to join. A child can be added to a network in two ways: the child can join the network using the MAC layer association procedure or the child can be added to the network directly by a previously designated parent device. Typical joining time is 30 ms.

The MAC layer association procedure involves first of all the joining device (the child) to scan for nearby WPANs. When it finds a suitable WPAN, one that allows new members, it sends a join request to that network. If allowed to join, the child receives a 16 bit logical address unique to that network to use for future transmissions.

When joining a network directly the parent device need to be preconfigured with the 64-bit address of the child device. When joining is initiated the parent searches its registers to check whether the device is already connected. If it is not found the parent allocate a unique 16-bit network address for the new device. Joining directly does not require any over-the-air transmissions. However, once the parent has added the child to its network it is still necessary for the child to make contact to establish the connection. This is done with a procedure called orphaning, which is usually used when a device looses contact with the network and tries to reconnect. In short terms it makes sure it is the right parent-child coupling and then retransmits the network address to the child [43].

3.4.4 Power consumption

ZigBee has been designed with ultra low power consumption in mind from day one. There are many features which help reduce the power consumption. First there is the data rate. As a contrast to Wi-Fi and Bluetooth, ZigBee won't be sending email, large documents and audio. Sensor readings, which are typically a few tens of bytes, do not require a high bandwidth, and ZigBee's low bandwidth helps it fulfil its goals of low power, low cost, and robustness. Because of ZigBee applications' low bandwidth requirements, a ZigBee node sleeps most of the time saving battery power, and then wake up, send data quickly, and go back to sleep again. Even sleeping nodes can achieve suitably low latency, because ZigBee can transition from sleep mode to active mode in 15 msec or less. In contrast, wake-up delays for Bluetooth are typically around three seconds.

A big part of ZigBee's power savings come from the radio technology of 802.15.4, which itself was designed for low power. For example 802.15.4 uses DSSS technology because the alternative FHSS, which Bluetooth uses, would have used too much power just in keeping its frequency hops synchronized.

To save as much power as possible, ZigBee can employ a talk-when-ready communication strategy, simply sending data when it has data ready to send and then waiting for an automatic acknowledgement. If it does not get an ACK, it just means it got clobbered, so it sends the package again. This solution has much better power management than if you listen and determine if it's quiet before you talk. However, this is not always true. In a network of thousands of tiny sensors large numbers of packet collisions and retransmissions could waste power and significantly shorten sensor node battery life.

ZigBee also reduces power consumption in its components by providing for power saving RFDs in addition to more capable FFDs (see section 3.3.1). Each ZigBee network needs at least one FFD as a controller, but most network nodes can be RFDs. RFDs contain less circuitry than FFDs, and little or no power-consuming memory.

ZigBee conserves still more power by reducing the need for associated processing. Simple 8-bit processors can handle ZigBee chores easily, and ZigBee protocol stacks occupy very little memory. An FFD stack, as mentioned in the previous section, needs about 32 Kb, and an RFD stack needs only about 4 Kb. Those numbers compare with about 250 Kb for the far more complex Bluetooth technology [40].

3.4.5 Security

ZigBee takes advantage of the security model of the IEEE 802.15.4 MAC sublayer (section 3.3.6), however the 802.15.4 standard does not provide a mechanism for moving security keys around a network; this is where ZigBee comes in. To ensure reliable and secure wireless networks, ZigBee offers a security toolbox including access control lists, data freshness timer and 128-bit encryption. Integrity is kept with the use of a message integrity code (MIC). The security toolbox consists of key management features that let you safely manage a network remotely. The actual security implementation is specified by the implementer using this standardized toolbox of ZigBee security software. This way the developer can choose the security necessary for the application, providing a manageable trade-off against data volume, battery life, and system processing power requirements [43].

3.4.6 Cost

ZigBee's low cost is due to its relatively simple implementations. RFDs reduce ZigBee component costs by omitting memory and other circuitry, and simple 8-bit processors and small protocol stacks help keep system costs down. Often, an application's main processor can easily bear the small additional load of ZigBee processing, making a separate processor for ZigBee functions unnecessary [15].

A single chip 2.4 GHz IEEE 802.15.4/Zigbee transceiver, Chipcon CC2420, costs 3.98 USD for one and 3.74 each if you buy 500 [45].

3.4.7 Prospects

ZigBee is predicted to have a bright future by many. It is clear that a full stack standard for LR – WPANs has it place in the market, especially in home automation for which it is intended. New ways to use ZigBee is currently being researched, e.g. the first mobile phone using ZigBee is produced, and in some time my guess is that we will see many ZigBee profiles. However, it is important to be careful with such predictions. Similar technologies with bright forecasts have crashed and burned before.

ZigBee's future is still uncertain since it has not really hit the market, but with its massive backing from its Alliance members it has every chance in the world to make it big.

3.5 Proprietary solution - Nordic nRF24AP1

3.5.1 Overview

Today there are numerous proprietary solutions operating in the 2.4 GHz ISM band. Chipcon and Nordic Semiconductors are two of the leading companies producing RF technology in that band. Especially Nordic Semiconductors has taken an interesting approach producing their latest chip, teaming up with Dynastream Innovations Inc. The result embeds Dynastream's ANT wireless protocol with Nordic's 2.4GHz RF transceiver and is called nRF24AP1.

The nRF24AP1 is an ultra-low power single-chip radio transceiver with embedded ANT protocol for personal area networks. ANT is a 2.4GHz bidirectional wireless PAN communications technology optimized for transferring low data-rate, low latency data between multiple ANT-enabled devices. The ultra-low power consumption of the ANT chipset makes it possible to have extended battery life even from low capacity supplies like coin cell batteries, such as are required for e.g. heart rate monitors. The small size and low-cost implementation of ANT allows effortless integration into small devices like PDAs, and mobile phones.

The ANT – Host interface has been designed with simplicity in mind so that it can be easily and quickly implemented into new devices and applications. The encapsulation of the wireless protocol complexity within the ANT chipset vastly reduces the burden on the application host controller, allowing a low-cost 4-bit or 8-bit Microcontroller (MCU) to establish and maintain complex wireless networks with remote devices. Data transfers can be scheduled in a deterministic or ad-hoc fashion, and a burst mode allows for the efficient transfer of large amounts of stored data to and from a PC or other computing devices. The ANT system balances functionality, cost, size, and power consumption within the constraints of a mobile Personal Area Network. Typical applications include sensor integration, tagging systems, remote monitoring, Personal Area Networks, etc.

It is designed to run on a coin cell battery; hence the current consumption of the device is extremely low. A typical sensor application can operate on approximately 40μA average current consumption. Short, low peak current transitions are battery friendly.

Maximum data rate over the air is 1000 kbps. But the maximum true data throughput (all data – no overhead) is 20 kbps, with a range up to 30 metres. The nRF24AP1 defines 125 RF channels [19].

3.5.2 Architecture

The ANT protocol stack is stored on-chip and is executed by the nRF24AP1's internal MCU core. The nRF24AP1 is composed of 4 main building blocks as shown in Figure 14, together they form the drop-in RF and protocol solution. As shown, the 4 main blocks are the serial interface, the timing interface, the ANT protocol engine, and the RF transceiver. Both the ANT protocol engine and the RF transceiver are embedded within the device and interact with the external host environment through a Universal Asynchronous Receiver Transmitter (UART) or synchronous serial interface. This approach allows system and application developers to interact with the nRF24AP1 as a black box wireless solution. Integration of an RF protocol with the RF physical layer is not required. All information from application developers, like channel configuration and message data information, is passed through the serial interface. The nRF24AP1 executes the configuration and sends/receives the message data packets over the air to other waiting devices.

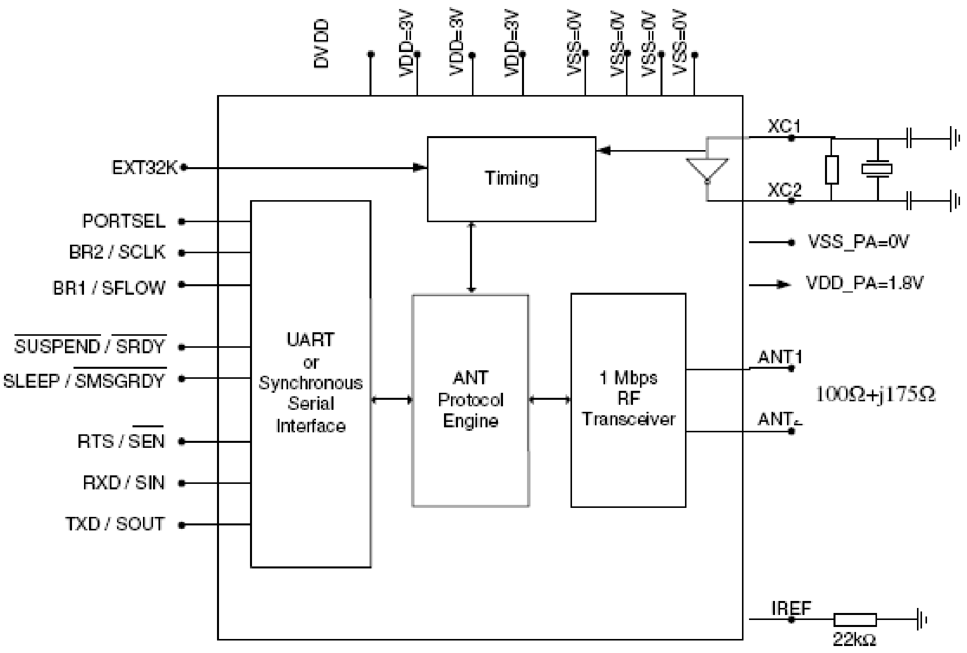


Figure 14. The architecture of the nRF24AP1 with external components [19]

The ANT protocol implements layers 1-4 of the OSI networking stack as well as automatically providing session authentication of network devices [19].

3.5.3 Network topology

The ANT protocol has been designed to support a large range of scalable network topologies, from simple 2-node unidirectional connections, to complex multi-transceiver systems with full point-to-multipoint communication capabilities.

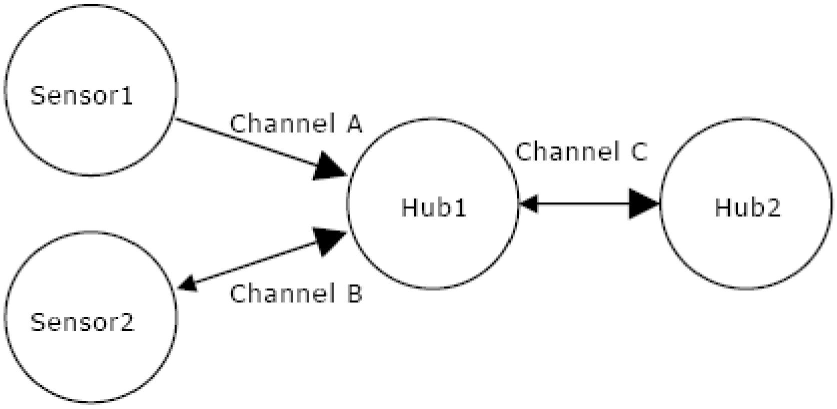


Figure 15. Channel based communication using ANT [18]

ANT usage and configuration is primarily channel-based. Figure 15 shows a simple network of ANT nodes, represented by circles. ANT nodes can connect to other ANT nodes via dedicated channels. Each channel generally connects two nodes together; however a single channel can in fact connect multiple nodes. There is a minimum one single master and one single slave participant in each channel. The master functions as the primary transmitter; and the slave the primary receiver. In Figure 1, large arrows indicate the primary data flow from master to slave, with small arrows indicating reverse message flow (e.g. Channel B, C). A channel with single arrow (e.g. Channel A) is used to represent a one-way link, which supports the use of lower-cost transmit-only nodes. An ANT node can act as both a slave (e.g. Hub1 channel A,B) and a master (e.g. Hub1 channel C) simultaneously.

The simple serial interface (asynchronous or synchronous) to the device allows for flexibility and scalability from ultra-low power sensors (40µA) through to higher data rate (20kbps) applications implemented in a multitude of network configurations (see figure 16). Networks can be scaled from as little as two nodes to thousands. Numerous network configurations and applications are possible due to 2^{32} unique IDs, multiple radio frequencies, public and private network management and scalable data rates [18].

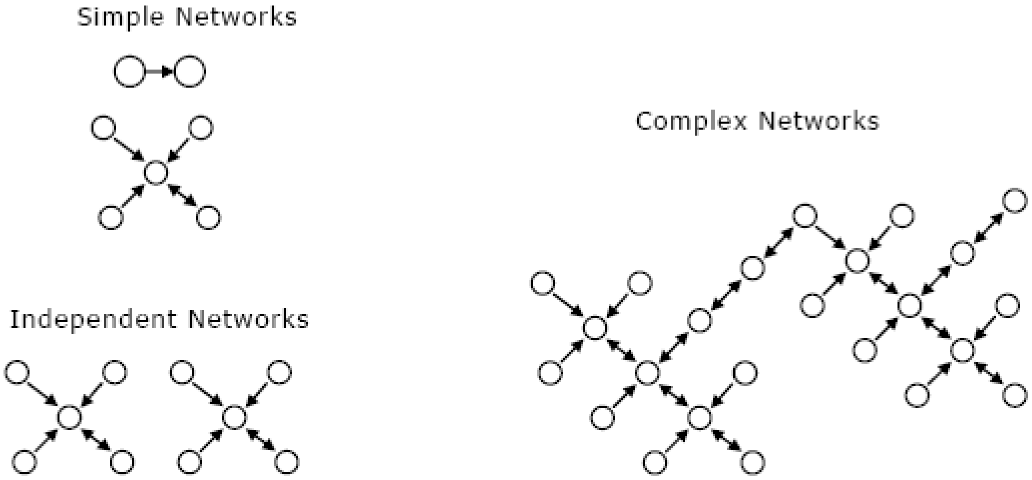


Figure 16. Examples of ANT network configurations [18]

Each node in an ANT network consists of an ANT protocol engine and a host controller. The ANT engine encapsulates the complexity of establishing and maintaining ANT connections and channel operation within its firmware. The host controller is thus free to handle the particulars of an application with only a limited burden in initiating ANT communications to other nodes, which it does via a simple serial interface between host and ANT engine [18].

3.5.4 Pairing (Association)

The act of pairing two devices (master with slave) involves establishing a relationship between two nodes that wish to communicate with one another in future communications sessions. This relationship can be permanent, semi-permanent or transitory. The pairing relationship can be one-to-one or one-to-many.

A pairing operation consists of a slave device acquiring the unique ID of the master device. If permanent pairing is desired, the slave node stores the master's ID to be used to open a channel with this ID in all subsequent communication sessions. In a semi-permanent situation, the slave may wish to occasionally purge any stored ID and pair with a new master. In a transitory situation, the slave may pair with a master on a temporary basis only. If a master uses only broadcast messaging, or if it uses the MAC (multiple access channel) feature, multiple slaves may pair and communicate with the same master. Establishing a channel involves the broadcasting of a unique ID by the master, and a search and acquisition of this ID by a slave. In the case where a slave does not have knowledge of a specific master ID, a pairing mechanism is available. The slave can search for a master of a specific device type, and upon a successful search result, the specific ID of the master can be stored and used in the same manner as previously described for all future communications [18].

Several mechanisms protect against inter-channel interference including adaptive channel synchronization as well as protocol error detection. Its resilience against data corruption and radio blackouts results in a robust and stable communications system for critical data [41].

3.5.5 Data types

Data messages are transmitted from the master to slave on every channel timeslot. At the end of every channel timeslot, the slave may optionally send data to the master. Three basic data types are supported, broadcast data, acknowledged data and burst data.

Broadcast data is the most basic data type, and is the system default. This form of data is never acknowledged, and so the channel master will be unaware in the case of lost data packets. In the case of a one-way transmission link (transmit-only node communicating to a receiver), broadcast data is the only available data type due to the inability of an acknowledgement. Broadcast data consumes the least amount of RF bandwidth and system power consumption.

For acknowledged data the slave will respond to the data packet with an acknowledgment message back to the master. The master's host controller will be notified of each acknowledged data packet's success or failure. Acknowledged data packets use more RF bandwidth and consume more power. It is ideally suited for the transmission of critical control data where 100% data transmission integrity is required.

Burst data transmission provides a mechanism for the master to send large amounts of data to the slave. A burst transaction begins at the next scheduled timeslot, and consists of a series of continuous acknowledged data messages from master to slave. Any lost messages are automatically retransmitted. A burst transaction takes precedence over all other channels on both participating nodes [18].

3.5.6 Security

nRF24AP1 supports confidentiality, authentication and integrity. Data can be encoded with an ID and encrypted, providing both security and immunity from user crosstalk [41]. To ensure integrity sequence numbers are used [18].

3.5.7 Cost

Samples of the nRF24AP1 will be available April 2005, with volume production scheduled for end Q2 2005. The nRF24AP1 is priced at USD3.95 in quantities of 10K [17].

3.6 Coexistence

Operation in the 2.4 GHz ISM band provides the convenience of an unlicensed band with availability almost worldwide. Wireless devices based on the IEEE 802.11b and the IEEE 802.15 standards have been widely deployed and among numerous proprietary solutions they coexist in the ISM band. Unlike other bands where interference is avoided by different wireless services being regulated to operate at separate frequencies or separate physical locations, in the ISM band access to the medium by different services is typically not coordinated. Therefore coexistence between services in the 2.4 GHz ISM band is a concern.

A system can use one of two methods to transmit in this band; both are spread-spectrum techniques. FHSS enables a device to transmit high energy in a relatively narrow band, but for a limited time. DSSS allows a device to occupy a wider bandwidth with relatively low energy in a given segment of the band, and it does not hop.

For example Bluetooth deploys FHSS, using 1-MHz-wide channels and a hop rate of 1600 hops/sec (625 microseconds in every frequency channel). Bluetooth uses 79 different channels in the United States and most of the rest of the world. IEEE 802.11b (Wi-Fi) opted for DSSS, using 22 MHz of bandwidth to transmit data with speeds of up to 11 Mb/sec. A Wi-Fi system can use any of 11 22-MHz-wide subchannels across the allocated 83.5 MHz of the 2.4 GHz frequency band. A maximum of three Wi-Fi networks can coexist without interfering with one another. Geographies outside of the United States may support more or fewer than 11 selectable subchannels. However, regardless of the portion of the band in which Wi-Fi operates, sharing with Bluetooth is inevitable. Two wireless systems using the same frequency band would have a high propensity to interfere with each other.

There are a number of industry led activities focused on coexistence in the 2.4 GHz band. The IEEE 802.15.2 Coexistence Task Group was formed in order to evaluate the performance of Bluetooth devices interfering with WLAN devices and develop a model for coexistence which will consist of a set of recommended practices and possibly modifications to the Bluetooth and the IEEE 802.11 standard specifications that allow the proper operation of these protocols in a cooperating way. At the same time, the Bluetooth SIG formed its own task group on Coexistence. Both the Bluetooth and the IEEE working groups maintain liaison relations and are looking at similar techniques for alleviating the impact of interference. The proposals considered by the groups range from collaborative schemes intended for Bluetooth and IEEE 802.11 protocols to be implemented in the same device to fully independent solutions that rely on interference detection and estimation [5].

3.6.1 ZigBee

ZigBee employs a talk when ready communication strategy, meaning that it sends data when it has data to send and then awaits an automatic acknowledgement. If it does not get an acknowledgement it means the package failed and it simply sends it again. This strategy leads to very little RF interference. That is mainly because ZigBee nodes have very low duty cycles, transmitting only occasionally and sending only small amounts of data. Other ZigBee nodes, as well as Wi-Fi and Bluetooth modules, can easily deal with such small, infrequent bursts [14].

ZigBee-based products can access up to 16 separate, 5MHz channels in the 2.4GHz band, several of which do not overlap with US and European versions of IEEE 802.11 or Wi-Fi. ZigBee incorporates an IEEE 802.15.4 defined CSMA-CA protocol that reduces the probability of interfering with other users and automatic retransmission of data ensures robustness [14].

Chipcon has performed several ad-hoc coexistence tests using its CC2420 chip with promising results. In one test, two CC2420DBs passed data back and forth, while an 18-dBm, frequency-hopping, 2.4 -GHz transmitter receiver pair using 15 channels operated approximately 1m away from both CC2420s. Neither system exhibited any performance degradation. Similarly, two CC2420DBs placed close to a laptop transferring a file across a 2.4-GHz IEEE 802.11b connection exhibited no performance drop [34].

3.6.2 UWB

When it comes to UWB the levels of interference are low. This is due to the low power limitations set by the FCC [35]. However, the level also depends on the type of UWB. The signals of most Ultra-wideband impulse radios generally appears as white noise to other radios in operation in lower spectrums. Other types of UWB, such as gated, or frequency hopped signals, can cause more noise, depending on the nature of the victim receiver. It is interesting to note that most UWB systems transmit power is lower than what a standard PC is allowed to radiate unintentionally. It then spreads the power over an extremely wide swath of radio spectrum. A UWB transmitter can distribute its energy over the equivalent of 1000 TV channels, or 30,000 FM channels, or a-half-million walkie-talkie frequencies. This makes the UWB signal at any one frequency extremely small. Because of their low power spectrum density, unlicensed UWB radios will cause no interference to other radio systems operating in dedicated bands [36].

The IEEE 802.15.3 standard offers a variety of techniques to enhance the coexistence with other users in the band. The methods provided by the standard include [9]:

- passive scanning
- dynamic channel selection
- the ability to request channel quality information
- link quality and received signal strength indication (RSSI)
- a channel plan that minimizes channel overlap
- lower transmit power
- transmit power control
- neighbor piconet capability

See C2 in the specification for more information [9].

3.6.3 Bluetooth

The severity of interference is a function of the system designs and the distance between the devices. Since the strength of a radio signal varies approximately with the "inverse square" of the distance, a small increase in separation can reduce the level of interference significantly. Studies by a number of companies indicate that if the separation is more than 2 meters, in most cases there is no perceptible degradation transmitting data in either device. From two meters to about a half-meter, there is a graceful degradation. As the devices are brought in very close proximity and collocated, the degradation can be quite noticeable. Fortunately, this scenario only happens when the two systems are in the same device, and in those cases, Bluetooth hardware and Wi-Fi hardware can collaborate to dramatically improve performance [37].

If a Bluetooth device encounters interference on a channel, it deals with the problem by hopping to the next channel and trying again. In this manner it can attempt to avoid interference from a Wi-Fi network [38].

3.6.4 Proprietary solution – Nordic nRF24xx

The nRF24xx can coexist with Bluetooth, which jumps among 79 channels, but only stays on one channel for 625 us. If a collision occurs at the channel used by the nRF24xx system, we know that the channel will be free again for the nrF2402 to re-transmit the package within 625 us. The longest one has to wait is when a Bluetooth device starts to transmit just as one nRF2402 packet is finishing, then the channel will be occupied for up to ~625us. If we wait beyond this before retransmitting the channel is likely to be vacant again. So, by sending each package from the nRF2402 2 times > 625 us apart one of them will get across.

If the collision occurs with a different nRF24xx device we know that it will be off the air within 262 us (max length ShockBurst package), which enables you to re-transmit even faster. By sending each packet twice, you will avoid interference with Bluetooth and other frequency jumping devices [39].

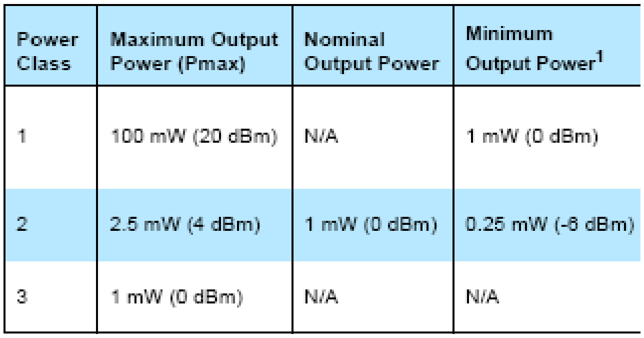
4 Evaluation of BAN compatibility

4.1 Bluetooth in BAN

4.1.1 Battery capacity

The Bluetooth radio interface is based on a nominal antenna power of 0dBm. Each device can optionally vary its transmitted power [12].

Each Bluetooth device is classified into 3 power classes:



Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1]
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)
3	1 mW (0 dBm)	N/A	N/A

Table 3. Bluetooth power classes [12].

1. Minimum output power at maximum power setting.

The range of a Bluetooth device is from 10 to 100 meters depending on the power class. Basically, the rule is the longer range the higher power consumption.

4.1.2 Scalability

A Bluetooth piconet is formed by one master device and one or more (up to seven active) slave devices. Several piconets can network together to form scatternets (see Figure 3 c). However, they can only send and receive data in one piconet at a time.

4.1.3 Data rate capacity

Bluetooth supports both voice and data. The voice channels support 64 kbit/s. The Bluetooth 1.0 data rates include an asymmetric data rate (one way) of 721 kbit/s (while permitting 57.6 kbit/s in the return direction); and a symmetric data rate of 432.6 kbit/s. Bluetooth 2.0 has been designed to be backward compatible with existing Bluetooth devices, and offers data transmission rates up to 10 Mbps (see section 3.1.1).

4.1.4 Fail-safety

Three error correction schemes defined for Bluetooth:

1/3 rate FEC
2/3 rate FEC
ARQ scheme for the data

The purpose of the two FEC schemes is to reduce the number of retransmissions. The ARQ scheme will cause the data to be retransmitted until an acknowledgement is received indicating a successful transmission (or until a pre-defined time-out occurs).

4.1.5 Real time synchronization

Synchronization of a piconet is performed by the master, which updates its slaves regularly with clock information to correct any misalignments (see section 3.1.2).

4.1.6 Association

The Link Manager layer takes care of the association of new slaves in Bluetooth.

4.1.7 Security

In each Bluetooth unit, the authentication and encryption routines are implemented in the same way. Four different entities are used for maintaining security at the link layer: a public address which is unique for each user, two secret keys, and a random number which is different for each new transaction (see section 3.1.4). The current Bluetooth specification defines security at the link level; application level security is up to the application developers. So they can select the most appropriate security mechanisms for their particular application (see section 3.1.4).

4.1.8 Cost

In Taiwan, Bluetooth chip prices for entry-level products were under $4 in Q3 2004, with chips for audio solutions at $6 apiece (see section 3.1.5).

4.2 UWB in BAN

4.2.1 Battery capacity

The devices in a UWB piconet are able to employ power saving techniques to reduce their power consumption. A device can enable three different modes of power saving. It basically constrains the device's awake-time (see section 3.2.3.1).

4.2.2 Scalability

An UWB piconet can form child piconets and neighbor piconets (see section 3.2.3).

4.2.3 Data rate capacity

The raw physical layer data rates supported in the IEEE 802.15.3 standard are 11, 22, 33, 44, 55 Mb/s (see section 3.2.3). 802.15.3a supports 110 – 480 Mbit/s.

4.2.4 Fail-safety

802.15.3 uses a hybrid CSMA/CA and TDMA. It also supports different types of acknowledgment (see section 3.2.3).

4.2.5 Real time synchronization

All DEVs in a piconet is synchronized to the PNC's clock. All child and neighbor piconets synchronize themselves to their parents' PNCs (see section 3.2.3).

4.2.6 Association

When a new node associate with a UWB piconet the coordinator gives it a identification called DEVID, which is used for all future transmissions in that piconet (see section 3.2.4).

4.2.7 Security

The 802.15.3 standard supports two different modes of security, no security and the use of strong cryptography. The standard supports the protection of command, beacon and data frames using a 128-bit AES security suite, and the distribution of keys for command and data frame protection (see section 3.2.4).

Additional security services need to be provided by the higher layers to ensure proper management and establishment of the symmetric keys used in this standard.

4.2.8 Cost

UWB is not yet on the marked, but according to an ABI Research study the price will somewhere close to 14 dollars (see section 3.2.4).

4.3 802.15.4 / ZigBee in BAN

4.3.1 Battery capacity

ZigBee has been designed with ultra low power consumption in mind and there are many features which help reduce the power consumption. For example it has a relatively low data rate and it uses DSSS, which consumes less power than FHSS. But the main reason for its ultra low power consumption is its sleep management; a ZigBee node sleeps most of the time saving battery power (see section 3.4.3).

4.3.2 Scalability

A ZigBee network has enough addresses to support 65,000 nodes, but a coordinator can only manage 255 active nodes at a time (see section 3.4.2).

4.3.3 Data rate capacity

The maximum data rates are 250 kbps in the 2.4 GHz band, 40 kbps in the 915 MHz band and 20 kbps in the 868 MHz band (see section 3.3). These apply within a range of 50 metres.

4.3.4 Fail-safety

The IEEE 802.15.4 standard employs various mechanisms to ensure robustness in the data transmission. These mechanisms are a CSMA-CA mechanism, frame acknowledgment, and data verification (see section 3.3.5).

4.3.5 Real time synchronization

For WPANs supporting beacons, synchronization is performed by receiving and decoding the beacon frames. For WPANs not supporting beacons, synchronization is performed by polling the coordinator for data. Time stamps is not default, but may be included by the implementer (see section 3.4.2).

4.3.6 Association

ZigBee associates new nodes in two different ways, either by the MAC layer association procedure or by joining directly. In both the node is issued a unique network address (see section 3.4.3).

4.3.7 Security

The IEEE 802.15.4 MAC sublayer specifies four security services; access control, data encryption, frame integrity and sequential freshness (see section 3.3.6).
ZigBee's security toolbox ensures reliable and secure networks. Data transmissions are protected by access-control lists, packet-freshness timers, and 128-bit encryption (see section 3.4.4).

4.3.8 Cost

A single chip 2.4 GHz IEEE 802.15.4/Zigbee transceiver, Chipcon CC2420, costs 3.98 NOK for one and 3.74 each if you buy 500 [CHIPCON Single-Chip Transceivers May – July 2005].

4.4 Proprietary solution / Nordic nRF24AP1 in BAN

4.4.1 Battery capacity

Nordic’s 2.4 GHz transceivers, including the nRF24AP1, are designed to run on a coin cell battery; hence the current consumption of the device is extremely low. A typical sensor application can operate on approximately 40µA average current consumption. Its short, low peak current transitions are battery friendly (see section 3.5.1).

4.4.2 Scalability

Networks can be scaled from as little as two nodes to thousands. Numerous network configurations and applications are possible due to 2^{32} unique IDs, multiple radio frequencies, public and private network management, and scalable data rates.

4.4.3 Data rate capacity

Maximum data rate over the air is 1000 kbps. But the maximum true data throughput (all data – no overhead) is 20 kbps. Range up to 30 metres (see section 3.5.1).

4.4.4 Fail-safety

Three types of communication are supported, broadcast data, acknowledged data, and burst data. Acknowledged data is recommended where 100 % integrity is needed (see section 3.5.4). Several mechanisms protect against inter-channel interference including adaptive channel synchronization as well as protocol error detection. Its resilience against data corruption and radio blackouts result in a robust and stable communications system for critical data (see section 3.5.3).

4.4.5 Real time synchronization

Nordic nRF24AP1 uses adaptive channel communications – they automatically adjust and synchronize with each other to provide robust, non-destructive operation [41].

4.4.6 Association

A slave has the ability to search for a certain device as its master, meaning association of a new device can be initiated automatically. After successful association the slave will have been issued an ID called Device type.

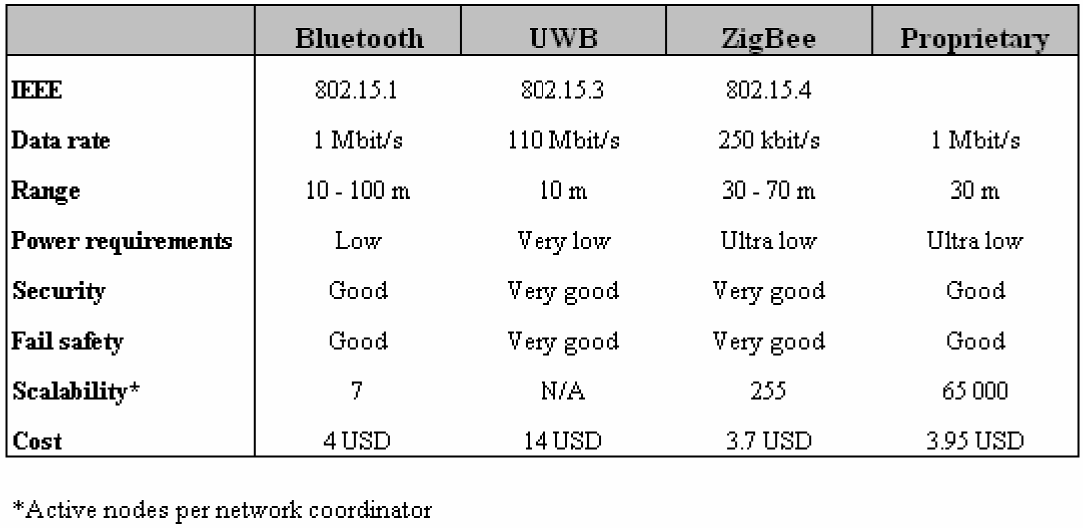
4.4.7 Security

Data can be encoded with an ID and encrypted, providing both security and immunity from user crosstalk. Sequence numbers are used to ensure integrity (see section 3.5.1).

4.4.8 Cost

The nRF24AP1 is priced at USD3.95 in quantities of 10K (see section 3.5.5).

4.5 Summary



	Bluetooth	UWB	ZigBee	Proprietary
IEEE	802.15.1	802.15.3	802.15.4	
Data rate	1 Mbit/s	110 Mbit/s	250 kbit/s	1 Mbit/s
Range	10 - 100 m	10 m	30 - 70 m	30 m
Power requirements	Low	Very low	Ultra low	Ultra low
Security	Good	Very good	Very good	Good
Fail safety	Good	Very good	Very good	Good
Scalability*	7	N/A	255	65 000
Cost	4 USD	14 USD	3.7 USD	3.95 USD

*Active nodes per network coordinator

Table 4. Comparison of short range low power wireless technologies

Each of the technologies built on the IEEE 802.15 standards were designed with different intentions in mind. Bluetooth was designed to replace cabling, UWB was designed for wireless multimedia transmission in the home, and ZigBee for home automation. Hence none of them were specifically designed to be used in a body area network. Despite that all of them could operate in a BAN, some more successful than others.

Bluetooth will struggle because its power requirements are not fitted for battery operated devices that can not be recharged or changed regularly. It is also heavily restricted by its scalability options; it can only have seven active nodes in one network.

UWB could work fine in a BAN with its amazing data rate opportunities. But it is struggling to reach the markets because of internal feuds, the predicted price is way to high as well.

ZigBee looks like a perfect fit, except for its low data rate (discussed closer in chapter 5 and 6). However, ZigBee’s excellent battery capacity is mainly a profit of its sleep management. It has such long battery life because the nodes sleep most of the time. But in a BAN nodes may need to transmit continuous real time data, how this affects ZigBee’s power consumption will be examined in chapter 5.1.1.

Nordic’s proprietary solution is ZigBee’s strongest contender. It has significantly higher data rate and it actually has lower power consumption. Security could be an issue though, it is hard to read from their specification what it does and does not support.

5 Patient Monitoring with ZigBee – Possibilities and Limitations

To investigate ZigBee's possible solutions in a BAN four scenarios are proposed. First are the cases of monitoring one, two, and N patients in a hospital environment. Finally the possibilities of ZigBee in a home network scenario are investigated.

In the following scenarios four types of sensors are taken into consideration:

- ECG sensors
- Blood pressure sensors
- Pulse oximetry sensors
- Respiration sensors

Each provides real time readings that need to be monitored. Unlike sensors that measure e.g. temperature and luminous intensity, these transmit data continuously, hence against ZigBee's sleep almost-all-the-time nature. This is an important part of ZigBee's power saving techniques, and could compromise its ultra low power consumption. To take full advantage of ZigBee's power management, beacon mode should be used in all the scenarios. That means the devices only transmits after receiving a beacon from their coordinator.

The sensors in this analysis have a 500 Hz sampling rate with 12 bit resolution, based on wishes from the employer.

Whether ZigBee's bitrate (250 Kbit/s) are adequate will be inspected in each scenario, as well as time delay and security.

Synchronization between sensors is an important aspect. Two sensors may need to be time synchronized at the monitoring unit, e.g. ECG and blood pressure.

5.1 Scenario #1 - Monitoring one patient in hospital

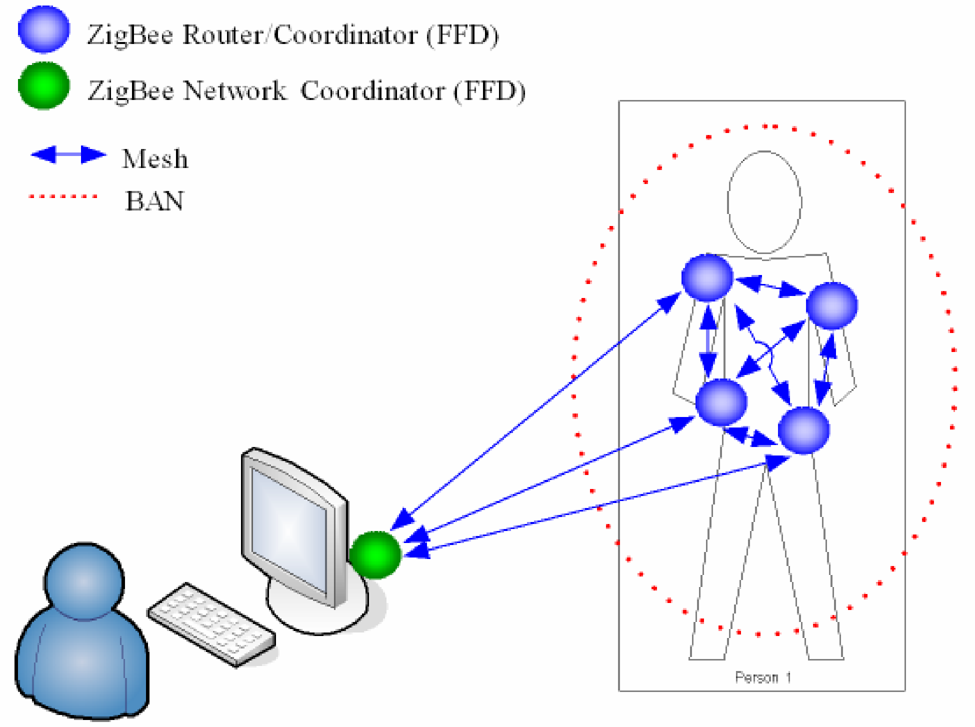

ZigBee Router/Coordinator (FFD)
ZigBee Network Coordinator (FFD)
Mesh
BAN
Person 1

Figure 17. One patient being monitored with mesh topology

Using mesh topology there is no master node in the BAN, every node/sensor communicates directly with the coordinator/monitor (see figure 17). In mesh networking each node acts as a router. This way a data flow from one node can take multiple routes to its destination, making it very resilient; if a node drops out the flow is simply redirected through other nodes. A routing algorithm is used to ensure that the data takes the fastest route.

Possible backsides to mesh networking are synchronization and authentication. Two (or more) data flows that need to be time synchronized at the receiver may take different routes, resulting in different time delays. If this delay difference is greater than what is possible to buffer, there is a problem which is not acceptable. To achieve near real time output it is possible to buffer the signals which need to be synchronized, that way they can be played out simultaneously. However, the size of the buffer can not be greater than what the human eye can register, since the signal output need to look like real time data to a person. It is fair to assume that the delay from the actual sensor reading to the monitor screen output should not be more than 500 ms in a medical environment.

Authentication needs to work flawlessly making sure the data comes from the correct sensor. When monitoring one single patient this is no problem since every packet each sensor sends contains a unique sender address.

To reduce cost and power consumption a cluster tree topology can be used (see figure 18). This combination of mesh and star topology allows the use of RFDs, which were designed to be battery powered. The BAN will use star formation with a coordinator as a BCU and the sensors will be RFDs. Between the BCU and the monitoring device mesh can still be used.

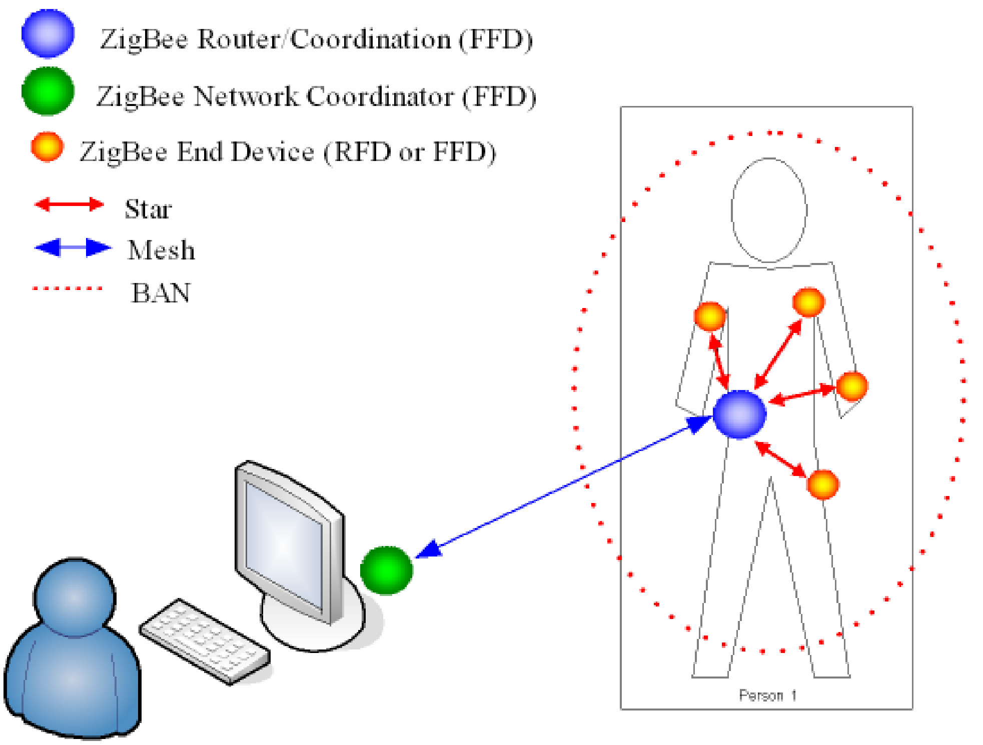

ZigBee Router/Coordination (FFD)
ZigBee Network Coordinator (FFD)
ZigBee End Device (RFD or FFD)
Star
Mesh
BAN
Person 1

Figure 18. Monitoring one patient (Star topology)

RFDs can only talk to routers or coordinators so every packet must go through the BCU. This way the transmit delay for each sensor will be more or less constant, making it easier to synchronize data from different sensors at the receiver.

If the monitoring device is connected directly to the BAN coordinator, making it the network coordinator and eliminating the extra hop, performance will be improved in every aspect discussed in this scenario. It is considered because of scalability, it is easier to add patients when you have an "external" network coordinator.

5.1.1 Power consumption

The power consumption is an important issue since ZigBee bases its low power operation on extremely low duty cycle, which is not the case in patient monitoring which require a continuous data stream. Here star network is considered since it is the most power saving topology. Routers and coordinators are designed to be mains powered or to use replaceable batteries, while it is the end devices (sensors) that need batteries with long lifetimes.

To keep the sensors unobtrusive it is important to keep the batteries small in physical size, thus coin cell batteries are required. Radio supply voltage for a CC2420 transceiver is 1.8V, so a 3V coin cell battery is sufficient. These are available with different Ampere hours (Ah), the higher Ah the longer lifetime, but higher price as well. It is all up to how much price matters, they can be found with 1800 mAh, but those are very expensive (21.4 USD each [46]). 1000 mAh versions are half the price, still expensive but anything less will not have the sufficient lifetime. Calculations using both values are performed next. To keep the power consumption as low as possible, it is considered that the sensor sends its packages to the BCU (marked blue in figure 18) and receives an ACK from the coordinator. From there it is the BCU's responsibility to send the package to the network coordinator (NWK CO) (marked green in figure 18). The power consumption of a potential additional microcontroller is not taken into account, neither is battery leakage. All transceiver details are from Chipcon's CC2420 data sheet [47].

---

*Battery lifetime calculation, capacity = **1800 mAh***
TX current drain = 17.4 mA
Duty cycle = 100 %

$$Lifetime = \frac{1.8Ah}{17.4 \cdot 10^{-3}} = 103.45h$$

Battery lifetime using an 1800 mAh battery and 100 % duty cycle is 103.45 hours.

---

*Battery lifetime calculation, capacity = **1000 mAh***

TX current drain = 17.4 mA
Duty cycle = 100 %

$$Lifetime = \frac{1Ah}{17.4 \cdot 10^{-3}} = 57.47h$$

Battery lifetime using a 1000 mAh battery and 100 % duty cycle is 57.47 hours.

Using the different batteries, lifetimes of respectively 4.3 days and 2.4 days are achieved. That is not very impressive for the ultra low power technology ZigBee.

5.1.2 Data rate

With a 500 Hz sampling rate and a 12 bit resolution 500 * 12 bits = 6000 bits needs to be transferred each second. With 104 bits in each packet there are 58 packets per second with 15 bytes overhead each. This sums up to 12960 bits (13 kbit) all together that needs to be transferred. That is no problem between each sensor and the BAN coordinator, where the effective data rate according to the ZigBee alliance is 250 kbit/s. Between the star coordinator and the network coordinator the traffic is more extensive, but 13 kbit*4 = 52 kbit per second should not be a problem either.

5.1.3 Time delay

In any dynamic routing, each node-to-node "hop" introduces latency. With ZigBee, that latency is typically several milliseconds per hop, so that a multi-hop path can introduce tens of milliseconds of latency as data travels to its destination. Routing algorithms are used to optimize the data path, but dynamic routing always introduces latency. Research done by Freescale semiconductor shows that each hop adds approximate 10 ms to the transmission time [48].

Each packet which is sent is 119 bytes, to transmit 119 bytes at 250 kbit/s takes 119*8/250 = 3.8 ms. In scenario 1 there is one hop for each sensor, meaning each packet will have additionally 10 ms delay resulting in 13.8 ms transmission time.

5.1.4 Association

To make sure each sensor is associated to the correct output on the monitor, each sensor shall use its unique 16 bit network address assigned by the network coordinator. Each output must have its own queue. When a packet arrives at the network coordinator the address should be checked and then be put in the correct queue.

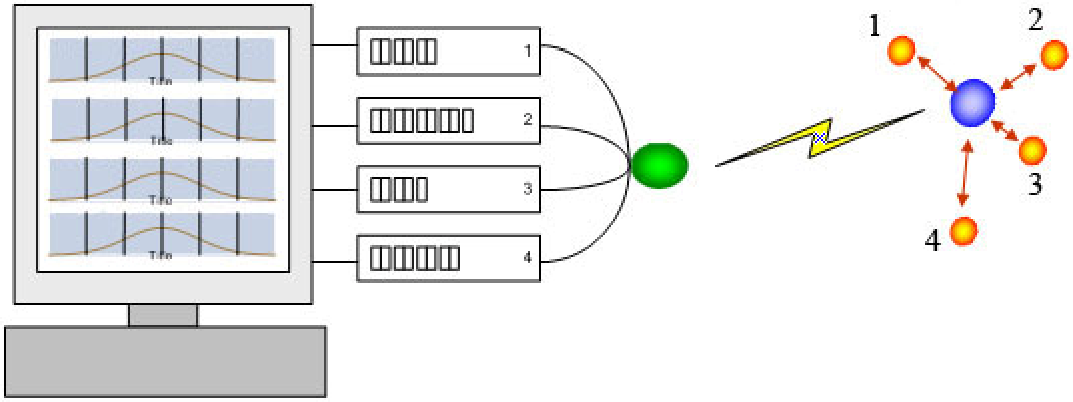


Figure 20. Queuing packets in scenario 1

5.1.5 Synchronization

With different latencies for two or more sensors it can be difficult to time synchronize their output on the monitor. For example it is preferable that the blood pressure curve is in sync with the ECG-curve like in figure 21.

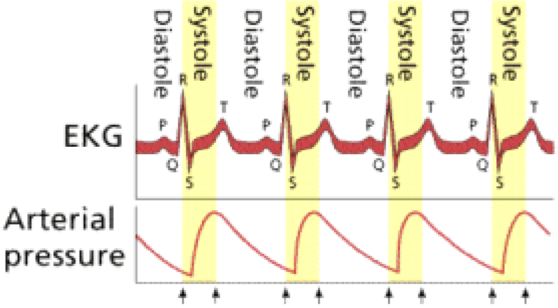


Figure 21. Examples of ECG and blood pressure curves [49]

There is no technique described in the standard how to achieve this. The synchronization problem will be examined further in chapter 6.

5.2 Scenario #2 - Monitoring two patients in hospital

In figure 22 only three sensors are used to describe the BANs, this is solely to keep the figure more tidy and organized.

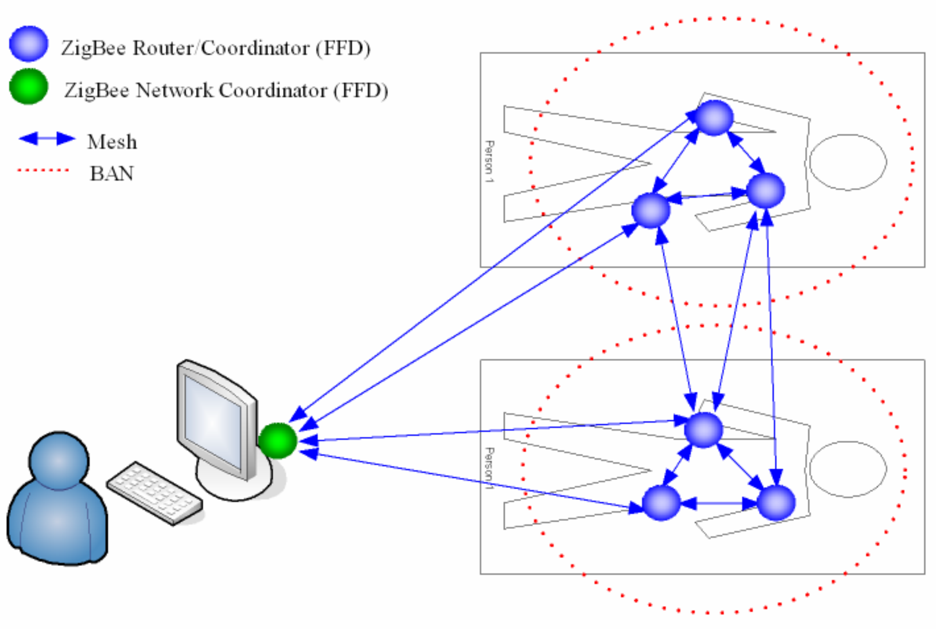

ZigBee Router/Coordinator (FFD)
ZigBee Network Coordinator (FFD)
Mesh
BAN
Person 1
Person 1

Figure 22. Two patients being monitored (Mesh)

The network depicted in figure 22 will result in varying latency; a sensor reading can have everything from one to three hops. On the other hand it is very robust (packets can be rerouted if a node goes down). Using this network it is not possible to take advantage of the power saving RFDs, which is important to keep the energy use to a minimum. Because of that a combination of mesh and star will be the better solution in this scenario as well (see figure 23).

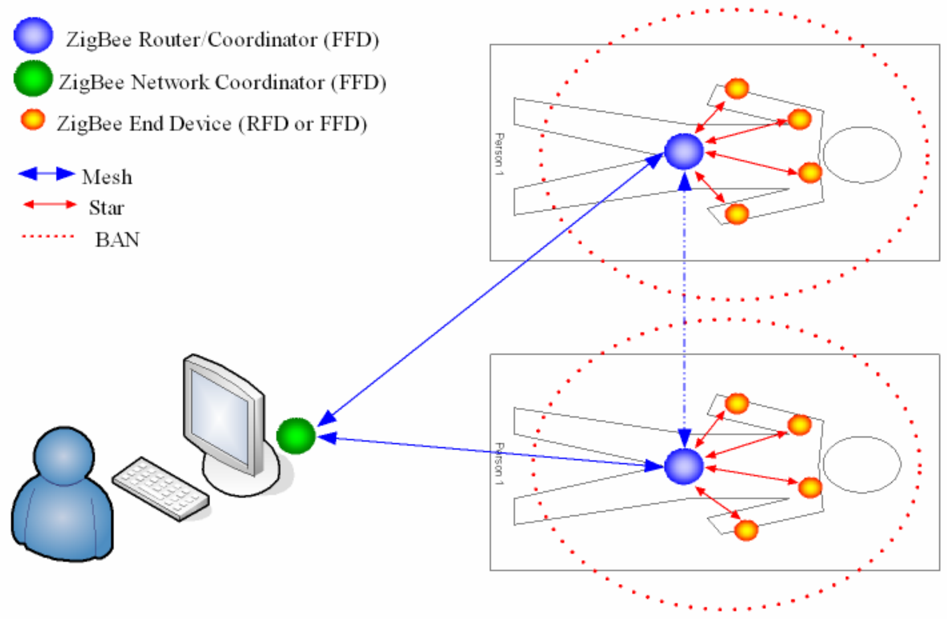

ZigBee Router/Coordinator (FFD)
ZigBee Network Coordinator (FFD)
ZigBee End Device (RFD or FFD)
Mesh
Star
BAN
Person 1
Person 1

Figure 23. Monitoring two patients (Cluster tree)

The data rate will still be sufficient, since the two BANs will use separate links to the monitoring device. In theory it is possible to route the data from one BAN through the others' coordinator, but there is no point in this case to do so. The only things that can go wrong are if either the network coordinator or one or both of the other coordinators go down. In either situation it does not help to route packages any other way. Therefore it is best to deny communication between the two BAN coordinators. Time delay will have the same effect as in scenario 1.

Additional routers can be added in the mesh network if the physical distance between the patients and the monitor is greater than the ZigBee alliance recommends.

A new problem which arises when another patient is added is authentication of the sensors. When a BAN coordinator receives a data packet from a sensor it should be 100 % certain that it is from one of its own sensors and not from the neighbor BAN. This is solved by the BAN coordinator creating an ACL. Only devices listed are authorized to communicate in that BAN. Every BAN should have its own ACL, that way crosstalk between the BANs will never occur.

Another issue is that the different BANs need to be distinguished at the monitoring side. In this scenario all the network coordinator needs to know, is from which router it received the data packet. But for scalability purposes it is possible to select a suitable BAN identifier. When packets arrive at the network coordinator they should first be checked for BAN identifiers, and then be put in the correct BAN queue (see figure 24), and then be split up in the different queues.

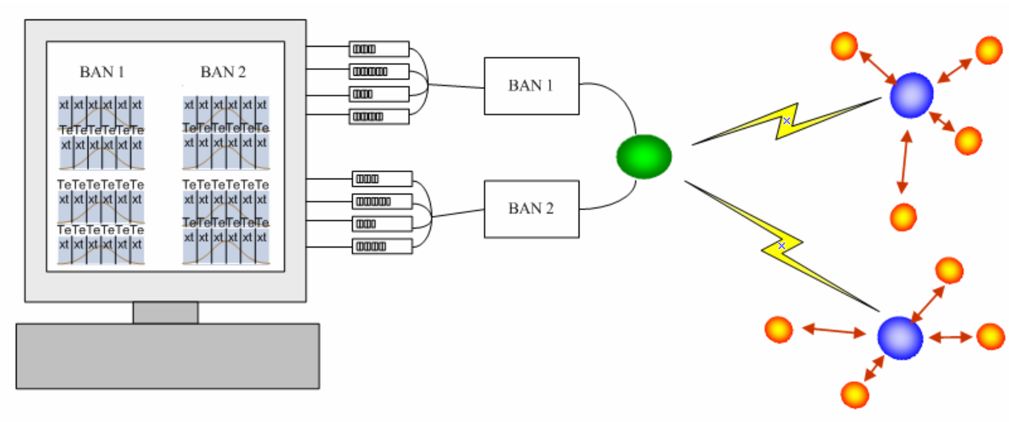


Figure 24. Association in scenario 2

5.3 Scenario #3 - Monitoring N patients in hospital

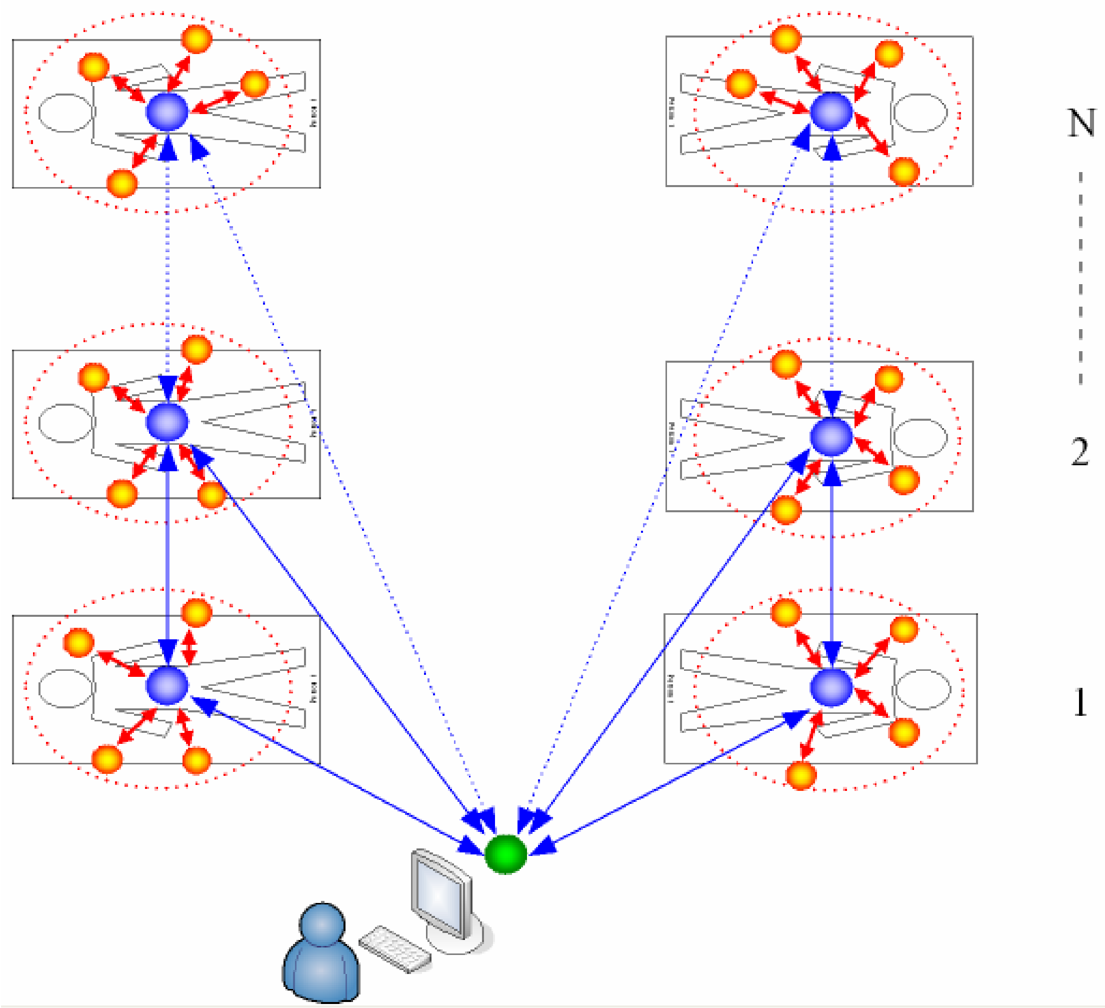


Figure 25. Monitoring N beds (Cluster tree)

An interesting part in this scenario is to see how many patients that can be monitored in the same network. A ZigBee network can have 255 active nodes at the same time; this will be the actual number of nodes since every node in this scenario is active all the time. Each BAN employs five nodes, four sensors and one coordinator. One node has to act as the network coordinator, so without taking anything else under consideration it is possible to monitor exactly 50 patients with four additional nodes acting like routers. But there are several problem areas that need to be considered, like effective data rate, time delay, and synchronization. The power consumption and association solutions can work as described in scenario 1 and 2.

First of all I would recommend not allowing routing through the BAN coordinators to reduce the power use in the coordinators as much as possible. This is important in a scenario of roaming (see section 5.3.1), the BAN coordinator, or BCU, can be mains powered when the patient is in the bed and battery powered when the patient is out for a walk. Another restriction is that the network coordinator can only receive data from 16 users at the time (16 channels), and only 7 of them are GTSs. 50 * 4 = 200 sensors transmit every 138 ms for at least 13 ms depending on the latency. That is simply not possible.

Each BCU needs one channel to transmit its data to the NWK CO every 138 ms. That means 16 BCUs can transmit at the same time. A burst with 4 packets of 119 bytes takes 15.2 ms to transmit. The last ACK will be received (in case of no error) 0.35 ms after the last packet is sent (see 5.1.1.1). Channel access time is 15 ms. This gives a transmit time of 15.2 + 15 + 0.35 = 30.55 ms. Each packet is sent in a GTS. The channels can then be re-allocated to new BCUs. A BCU needs to transmit every 138 ms, in that period 4 sets of 16 nodes can in theory transmit. However allowing only three sets gives better time for re-transmission and re-allocation of the channels, enhancing robustness. This way (3 * 16 =) 48 patients can be monitored at once.

No additional routers are needed if all the patients are in the same room, 48 patients can be put within 50 meters range (in a big hall). Using this solution the time delay will be constant except for possible collisions since there are no alternative routes.

Another possibility is to let the sensors transmit every 138/4 = 34.5 ms so the BCU can fit the data from the four different sensors in one packet and send it to the NWK CO. This way every BCU will need a channel every 34.5 ms, with 34.15 ms transmit time the BCU would transmit continuously leaving no margin for error (no time to retransmit). This solution allows 16 users. It would solve the synchronization problem, but how would the NWK CO distinguish the different sensors with all the data in one packet with one sender address? Another problem is that the sensors will not have any sleep time, thus have a 100 % duty cycle, shortening the battery lifetime severely.

5.3.1 Mobility

For a patient to be able to move around the hospital is a welcome freedom. If ZigBee routers are purposely placed around the hospital within reach of each other this should be possible, at least in theory. ZigBee is self-healing and self-forming, meaning it automatically finds new routes if a node goes down. This makes roaming possible as long as the BAN is within reach of a ZigBee router, either in its own ZigBee network or another ZigBee network. It takes 30 ms for a ZigBee node to connect to a new router. Handover is a subject for worry, since mobility is not supported in the current specification (v1.0), and no handover techniques are described. But in my opinion it should not be a problem. If it is transmitting when the handover occurs it will simply be a faulty transmission and retransmission through the new router is commenced. Anyways, a patient will be able to move freely around in the room and to the bathroom next door for example without handover, as long it is within reach of the NWK CO.

5.4 Scenario #4 - Monitoring one patient in the home

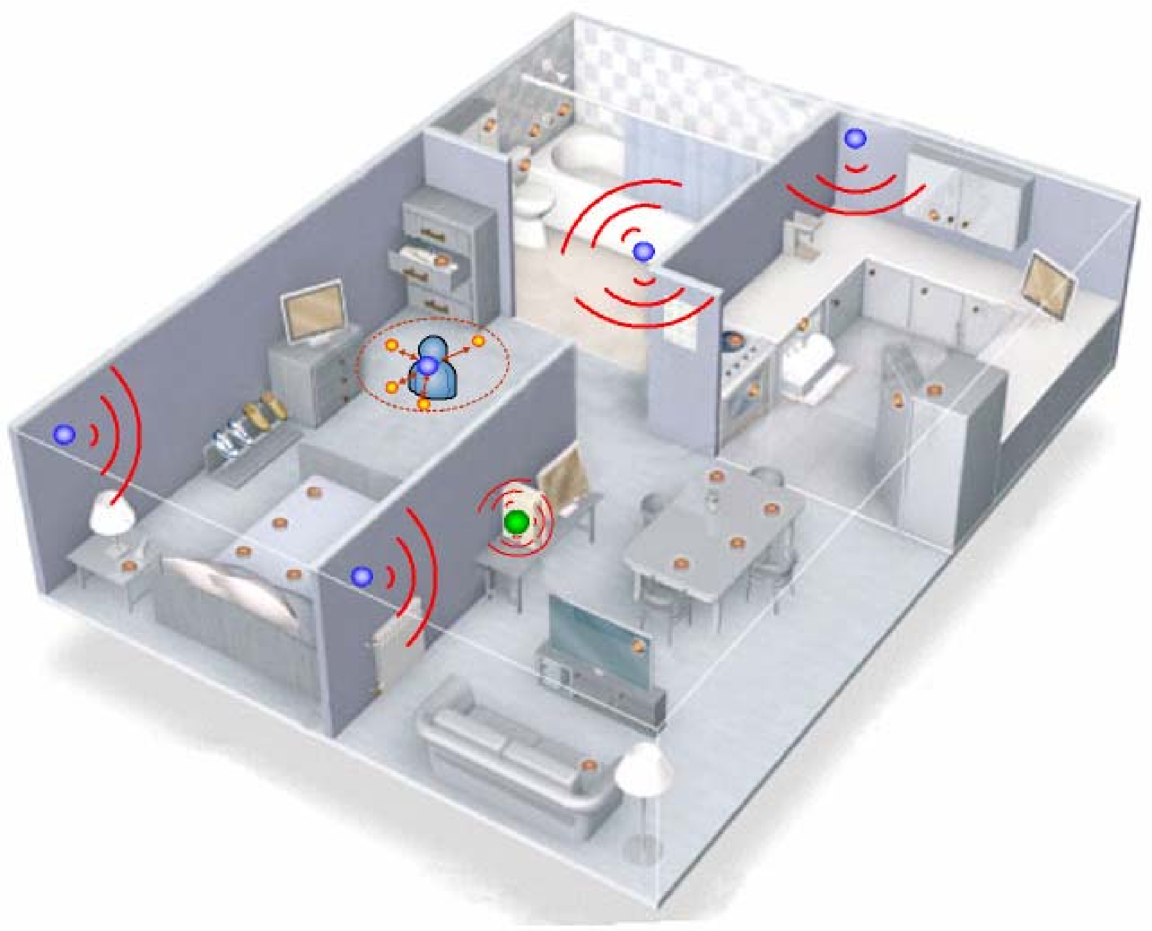


Figure 26. Monitoring a patient in the home [50] (Modified by author)

Patient monitoring can be integrated with a Smart Home (SH) network. Figure 26 shows a patient surrounded by his BAN doing his daily chores while being monitored. The small orange circles indicate sensors in the smart home network (except those encircled in the BAN); their readings can tell whether they are watching TV, sleeping, using the toilet, making food and a lot more (see [50] for more information on Smart Home). The sensors in the SH network will be tied together in the same ZigBee network as the BAN.

This system can let e.g. a physician or a family member etc. know what the patient is up to, making sure everything is alright, if not action is taken. Many will think this is a invasion of privacy, but it is in fact a price many will pay to spend their lives in the comfort of their own home in stead of an institution.

The BAN will transmit sensor readings to the NWK CO the same way as in the other scenarios. NWK CO is shown in the figure as a green circle connected to the PC in the living room. That PC can be connected to the internet, preferably with a Virtual Private Network (VPN) to a database which gathers the incoming data, to a physician, to a family member, and an alert central. Readings from the sensors will be processed in the PC and if everything is in order the readings will quietly be stored on the PC and the database on the other end of the VPN. If anything goes wrong, depending on the degree of seriousness, either or both a family member and a physician will be notified. In case of an immediate emergency the alert will sound and an ambulance will be sent. At the same time readings from the last minutes will be sent to the physician for special analysis.

The BAN will behave much like scenario 1. To save power it could use the same transmit cycles. I suggest the BAN will use the GTSs and the other SH nodes will compete for slots in the CAP. SH nodes will have extremely low duty cycle (<1%), e.g. the sensor on the TV only sends when it is either turned on or off, and it is not critical if a collision occurs. Coexistence between the BAN and the SH nodes should therefore not be a problem. The time delay could vary a bit, using the results from Freescale [48] it will be n*10 ms, n being number of hops. In figure 26 the maximum number of hops is two. Time delay is closer investigated in chapter 6.

In this scenario it is important to note that the patient will be moving around more than in a hospital scene. This means the BCU will need to be battery powered for longer periods of time. This poses a problem since the BCU is a FFD which has a high duty cycle. But the BCU device will have to be bigger in size and can therefore fit two AA batteries (maybe mobile batteries can be used?). Two rechargeable AA batteries with 2300 mAh can be bought for 2.50 USD each [51]. With 100 % duty cycle the battery lifetime will be:

$$\frac{4.6Ah}{18 \cdot 10^{-3} A} = 255.5h$$

$18 \cdot 10^{-3} A$ is an average of the RX and TX current consumption [47].

255.5 hours (10.6 days) is a satisfactory lifetime for a rechargeable device. A docking station can be placed on the bed table, recharging the BCU every night.

6 Making ZigBee work in a biomedical environment – proposed solutions

Possibilities when using ZigBee in different scenarios of medical monitoring is shown in the previous chapter. But it introduces some problems as well. The battery life of the sensors is too low, the number of patients ZigBee can monitor could be higher, and the synchronization issue needs to be worked out. Solutions to these problems are presented in this chapter along with a proposal for a completely feasible fully scaled non-invasive ZigBee patient monitoring network.

6.1 Mending the deficiencies

6.1.1 Increasing battery lifetime

The calculations in section 5.1.1 apply if 100 % duty cycle is assumed. The duty cycle could be a lot less in an actual sensor network.

The question is how often do the sensors need to transmit? First of all, to achieve best possible effective data rate the general trend is that at larger packet sizes the effective data rate approaches the raw data rate (see figure 19). The biggest packets ZigBee can send are 128 bytes with a maximum payload of 104 bytes. If 4 bytes addressing is used (sufficient in this scenario) total size is 119 bytes. Each sample has 12 bit resolution, this means that 69 samples fit in each packet (104*8/12=69.33) (possible application layer header is not taken into account). The sensor, using 500 Hz sampling rate, samples every 2 ms (1/500 Hz). And the sensor does not transmit until the packet is full (69 samples), this means that the sensor transmits every 69*2 ms = 138 ms. To transmit 119 bytes at 250 kbit/s takes 3.8 ms. To wake up from sleep mode takes 15 ms and to access the channel the same. It then awaits an ACK frame of 11 bytes which takes 0.35 ms to transmit at 250 kbit/s. This gives 15 ms + 15 ms + 3.8 ms + 0.35 ms = 34.15 ms radio activity time. If the samples are gathered and stored in the application layer, the radio can sleep when it is not in use. And it is in use 34.15 ms per 138 ms which gives a duty cycle of 0.247, if no errors occur.

Receiving beacon frames from the coordinator, for time synchronization, is not taken into account here.

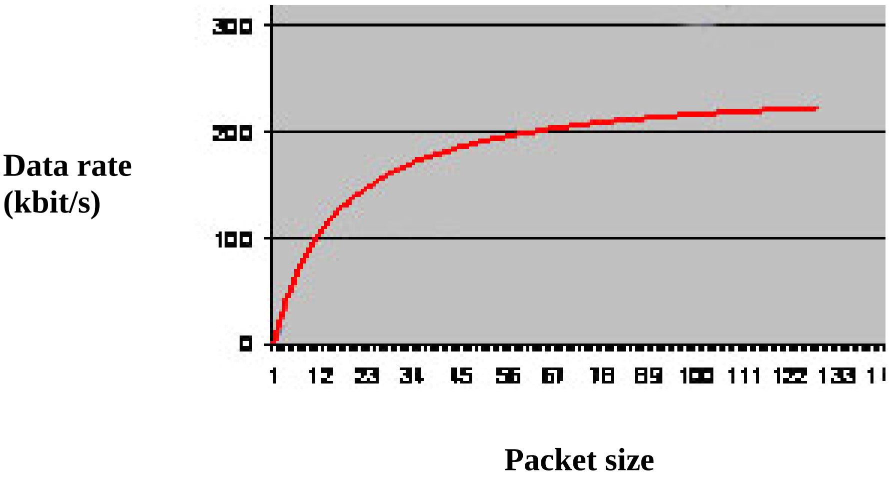


Figure 19. Graphical presentation showing the packet size/ data rate relation [2]

With this duty cycle the new calculations will be:

For a 1800 mAh battery

$$Lifetime = \frac{1.8Ah}{17.4 \cdot 10^{-3} \cdot 0.247} = 418.82h$$

For a 1000 mAh battery

$$Lifetime = \frac{1Ah}{17.4 \cdot 10^{-3} \cdot 0.247} = 232.68h$$

The new battery lifetimes are, respectively, 17.5 days and 9.7 days. These are best case results and actual lifetimes will most likely be somewhat below this. Also note that sleep mode current is not taken into account since it is approx. 2 uA and will have no impact on the battery life.

6.1.2 Time delay

To save power the sensor transmits packets containing 69 samples every 138 ms, this means the monitoring device receives a packet every 151.8 ms (138 ms + 13.8 ms transfer time). That gives a 13.8 ms delay from packet n has been fully played out until packet n+1 is received. A delay of 13.8 ms is not noticeable for the human eye; e.g. movies use 24 images per second which is an update every 41.67 ms. However, if an error occurs re-transmission gives a bigger delay. The sender expects an ACK within e.g. 15 ms (it takes 10.35 ms to send an ACK), if it does not receive one, it re-transmits the package, this gives an re-transmission time of 15 ms + 13.8 ms = 28.8 ms. To be sure it is a good idea to add a buffer delay in the queues (see figure 20 and 24). If the packets are held in the buffer e.g. 200 ms before they are played that gives suitable time for possible re-transmissions.

6.1.3 Increasing the number of patients in the network

When it comes to the number of patients in the network the restriction is not the relative low data rate as anticipated; it is actually the gateway to the monitoring device (the NWK CO) not being able to receive such frequent data frames from the sensors. One solution could be to reduce the sampling rate. Experiments carried out by the coalition of Ass.Prof. Rune Fensli at Agder University College and the University of Aalborg shows that a sampling rate of 250 Hz is sufficient for ECG readings [52]. The effect of this bisected sampling rate is analyzed next.

There is still room for 69 samples in each package, but with the new sampling frequency it only samples every 1/250 Hz = 4 ms. Because of that the sensor would only need to transmit every 69 * 4 ms = 276 ms, increasing the battery lifetime as well. Sensor radios will then only be active 34.15 ms every 276 ms, giving a duty cycle of 0.12. This will increase battery life to 862 hours (35.9 days) for 1800 mAh batteries and to 478.9 (19.95 days) for 1000 mAh batteries. With intervals of 276 ms it is now possible to fit 6 cycles, which gives room for 6*16 = 96 patients. It turns out reducing the sampling frequency kills two birds with one stone; the number of patients in the network can be doubled and the battery lifetime is doubled as well.

6.1.4 Synchronization

One way the synchronization problem could be solved is to use the optional superframe structure supported by the IEEE 802.15.4 standard. The BAN coordinator will then issue a beacon for time synchronization, PAN identification, and description of the superframe structure, followed by 15 equally sized time slots, the superframe is ended by another beacon frame (see section 3.3.4). The time slots are either CAPs or CFPs. In this case contention free periods will be used to ensure low latency. Up to seven time slots can be allocated to contention free access.

The sensor radios wake up to receive the beacon frames at regular intervals, since they need them to transmit in such a beacon enabled network. The beacon frame should tell the sensors to restart their data sequence number (DSN) counting every now and then, especially if suspicion of lost synchronization is present. The sequence number field in an outgoing frame is filled with the value of *macDSN*, which is then incremented. *macDSN* is an 8 bit value and it starts at zero every time it reaches 255. It is initially a random number created by an algorithm which is outside the scope of the IEEE 802.15.4 standard. If the beacon frame could carry instructions to set the DSN value to 0, this technique would work. It is important to note that the DSN value should not be reset in every beacon transmission, to make sure it does not inflict with the play out order. The sensors then transmit in their allocated time slots and go back to sleep, ergo every sensor should be synchronized and the power consumption is not affected. The monitoring device then needs to make the buffers cooperate and play out the equal DSNs at the same time.

Another way the synchronization problem could be solved is by using timestamps. If the network coordinator transmits beacon frames synchronizing the sensor clocks regularly, the sensors can stamp all their outgoing frames with the time it was transmitted. This solution demands interoperation between the buffers as well. As the frames enter the different buffers they should be checked for timestamps as well as sequence numbers, to make sure they get played in the correct order. Here as well the buffers should cooperate with each other and play out the packages with the same timestamp simultaneously.

To make this compatible with the power consumption restrictions, the network coordinator should transmit the synchronize information in the start beacons of the superframes initiating the data gathering. Thus, the awake-time of the sensor radios is not affected. However, this might require some modifications of the ZigBee protocol, since the current version of the specification does not say anything about time stamping the outgoing data frames. But research conducted by Emil Jovanov implies that MAC layer time stamping can be done [16].

6.2 Proposed complete ZigBee patient monitoring network

The proposed ZigBee solution is based on scenario 3, with 96 patients and a 250 Hz sampling rate as proposed in the previous section (see figure 27). This means the same techniques for power saving and association will be used. As in the other scenarios the time delay will be approximate constant due to no extra hops. 96 patients in one room is of course an extreme case scenario, this is simply to show what is possible.

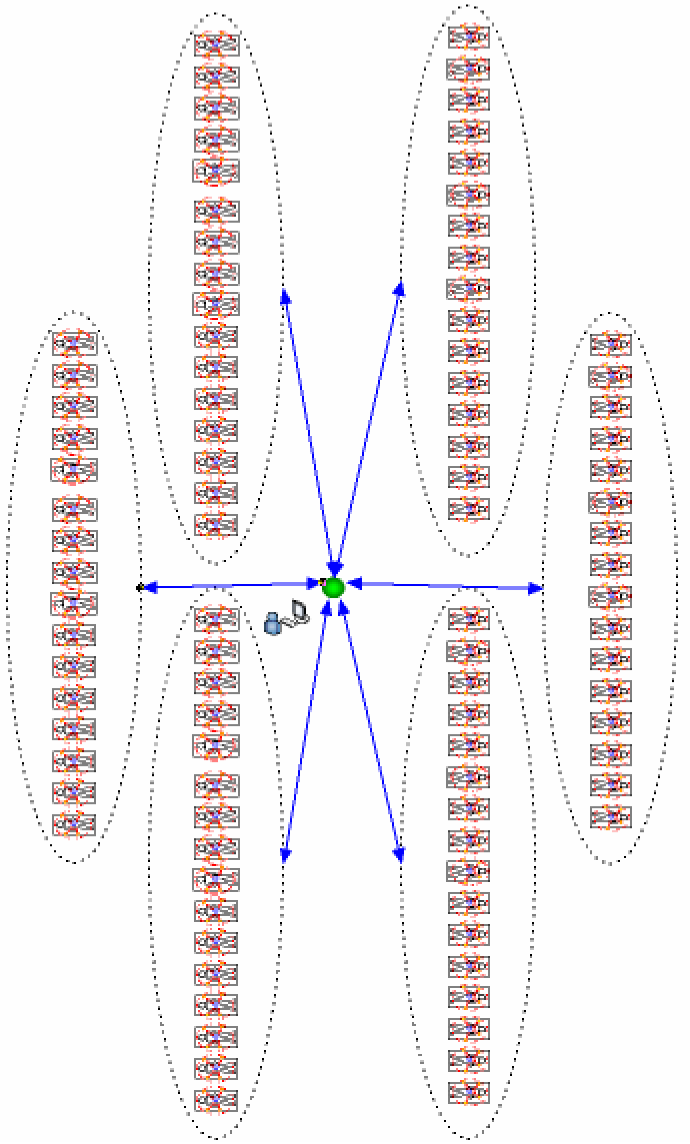


Figure 27. Complete ZigBee patient monitoring network

The network is illustrative split in two parts; the BANs (see figure 28) and the coordinators (see figure 29). In their daily work they will operate almost independently. In the forming phase the sensors will be given a unique address from the NWK CO, after that they only relate to their BAN coordinator, also called BCU. The sensors send their readings to their coordinator and goes to sleep to save power; it is the BCU's responsibility to get the data to the NWK CO. This way the NWK CO could consider only the BCUs as its network, making it a star topology suitable for superframe structure (see figure 29). In fact this way there are only multiple star networks within the network.

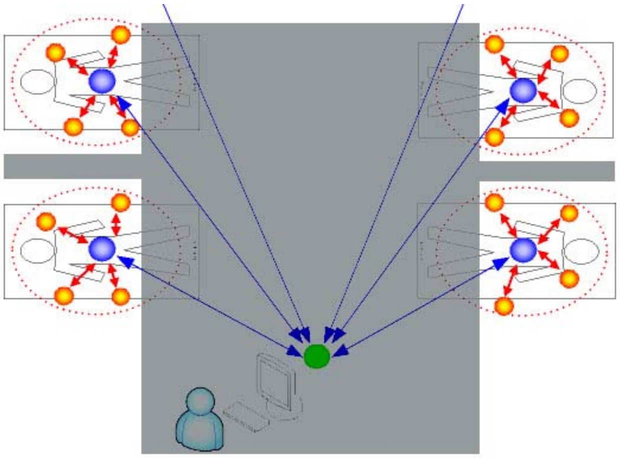


Figure 28. The sensors live their own lives pretty much unaffected of what happens outside of the BAN

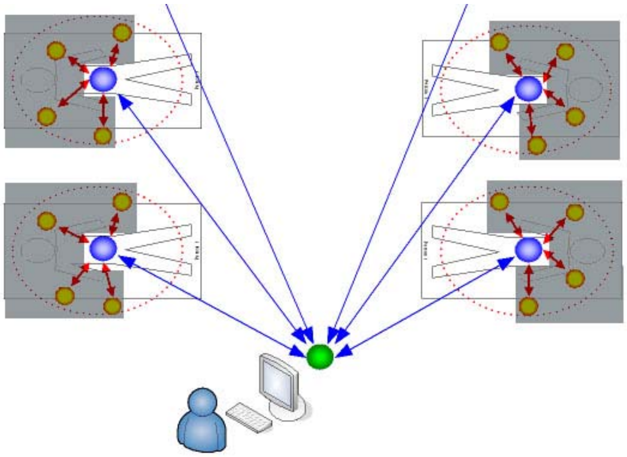


Figure 29. The NWK CO should only see the BCUs

6.2.1 Sensor perspective

The BAN can function like described in the previous scenarios with reduced sampling frequency to increase battery life and number of patients. All traffic is sent in guaranteed time slots, hence no collisions will occur.

The radio wakes up when it is ready to send and listens for the beacon initiating the superframe which should be sent in constant intervals of 276 ms. It is only awake when it transmits and not during the entire superframe. This is achieved by setting the *BatteryLifeExtension* option to TRUE.

6.2.2 NWK CO perspective

As mentioned the NWK CO should only "see" and deal with the BCUs making a star network within the network, this makes it possible for the coordinators (the BCUs) to transmit to the NWK CO in the same manner as the sensors transmits to them.

The NWK CO sends beacons to 16 BCUs at the time and allows them to transmit the readings they have obtained from the sensors. Then the NWK CO will move to another 16 BCUs and repeat the procedure till everybody has transmitted their readings, it will then start over again. The patients must be put in groups of three and be asked for data in constant intervals (see figure 30). Transmission time for the BCUs is 30.55 ms. Six sets of three transmitting gives:

$$30,55 \cdot 6 = 183.3ms$$

It takes 183.3 ms to obtain the readings from all the patients (if no errors occur). That means it is more than enough time for all BCUs to transmit before the next round, which gives room for retransmissions and channel reallocation. Optionally more patients can be added.

To commence monitoring, the NWK CO should send out beacons containing instructions to activate the sensors to the groups one at a time, with 276 ms / 6 = 46 ms delay between each group starting with "group 1". When all the groups are activated group 1 receives the first beacon to transmit the first readings and so on. This way the BCUs gets permit to transmit shortly after receiving the data from the sensors. Now even the BCUs can take advantage of sleep mode, saving power.

6.2.3 Application layer issues

The solution presented in section 6.2 is in principle application layer independent. It can work unaffected of what is going on in the APL, which will be responsible for handling the sensor readings and storing them in suitable package lengths. In a system where only one type of data is transmitted in a constant interval no APL protocol header needs to be added in my opinion. The application on the other side are aware of what type of data it receives since it only should accept sensor readings, it will not need any additional information to play the sample stream out on the monitor. Responsibilities of the APL protocol are moved to lower layers making the solution more flexible. E.g. synchronization and error handling are primarily solved in the MAC layer.

6.2.4 Security

The security in the presented scenario will be good enough for sensitive medical data. Integrity can be applied to avoid tampering with the data by using a MIC, authentication is kept with unique addresses for each device, a 64 bit IEEE address to identify each device and a 16 bit unique network address used for communication. ACLs are used to avoid cross talking and encryption can be added if needed.

6.2.5 Coexistence

Coexistence is always an issue when it comes to devices that operate in the 2.4 GHz band. In a hospital environment other devices which use the mentioned ISM band would most likely be of course other ZigBee nodes and IEEE 802.11 WLAN. Some occasional Bluetooth devices could enter the area as well. Interference between ZigBee nodes is not a factor; this is solved in the manner described above (transmits only when permitted). How ZigBee handles coexistence with WLAN and/or Bluetooth is explained in section 3.6.1 and 3.6.3.

7 Discussion

7.1 Best suited technology for BAN

The different technologies presented in chapter 3 is evaluated in chapter 4, based on their properties when it comes to battery lifetime, scalability, data rate, fail-safety, real-time synchronization, association, security and cost.

Of the standard based technologies Bluetooth is the most mature; it has already been on the marked for some years and is today the most common system in the 2.4 GHz space. Thus many of its childhood diseases have been cured. It has good throughput and range, and acceptable security and fail-safety (it lacks authenticity and freshness check). But its power requirements and scalability will be a problem in a BAN. Bluetooth can only have seven active nodes per coordinator, meaning that using Bluetooth a BAN has to restrict itself to seven sensors. However, the biggest problem with Bluetooth is its power requirements. It is designed to use cyclic power sources (e.g. rechargeable batteries) or to be mains powered, i.e. it has relatively high power consumption. This is not compatible with BAN which requires very low consumption.

UWB based on 802.15.3a is a new technology which is now starting to enter the marked. It has an extremely good data rate and an acceptable range of ten meters, which is sufficient in a BAN. UWB technology has low power requirements and good security and fail-safety. The specification does not state exactly how many active nodes a coordinator can have, but it is fair to assume that it is a sufficient number. The drawbacks are the price and the fact that it is such a new technology. More research needs to be done and the predicted pricing of 14 USD per component is too high. My advice would be to give it a year or two and see how it develops.

ZigBee emerges as a very good solution with its extremely low cost and power consumption. It has very good scalability, fail-safety and security. However, the backside is that it has limited data rate with its 250 kbit/s, which could be a problem depending on the requirements of the BAN. As shown in chapter 5 and 6 it is possible to make it work.

Nordic’s nRF24AP1 is a proprietary solution which seems to be a good fit for BAN. It shares the same basic radio architecture as Bluetooth. The difference is that Bluetooth’s need for a complex protocol engine increases the power consumption and cost dramatically. Nordic’s solution supports a good data rate and range, as well as it is very competitive when it comes to price and scalability. It also has very low power consumption, in fact the lowest of the four. But it has some shortcomings when it comes to fail-safety; it lacks access control mechanisms. Still, nRF24AP1 would function just fine in a BAN.

The biggest drawback for the solution from Nordic is the fact that it is a proprietary solution. The other technologies examined in this project are globally standardized. That gives them the advantage of providing product interoperability and vendor independence. But standardization is a double edged sword, since ZigBee is designed to fit for many applications it will never be the perfect fit for one special device. A proprietary solution can be designed to fit perfectly for one use. But it is my opinion that standardization of BAN technology will be the better solution in the long run.

7.2 The Scenarios – Optimal solutions

Four different scenarios are presented where three of them are situated in a hospital and one in the home. All scenarios assume the use of four sensors on the patient.

When monitoring patients in a hospital environment using a star topology between the sensors and the BCU will be a power saving approach. Sensors can then be RFDs with low complexity since they do not need to perform any complicated processing. Power consumption is of high priority in the end devices since they need to be battery powered and are impractical to change or recharge in short intervals. Since ZigBee's power management relies on low duty cycles and long sleep intervals, a technique trying to exploit this is proposed. The solution is that the sensor only transmits when it absolutely has to, thus use the largest data frames supported in the standard. This gives the highest sleep rate for the radio which again gives the best power management. All the scenarios will benefit from the technique. Another part of the solution is to make the sensors to only communicate with the BCUs, accordingly send the readings to the BCU, get an ACK from it and then go to sleep. By not waiting until the packet reaches the NWK CO it saves important sleep time, to get the sensor readings to the NWK CO is solely the BCU's responsibility. Using this "bursty transfer technique" battery lifetimes are 17.5 days and 9.7 days, depending on the battery's mAh value. Whether or not that is sufficient in a patient monitoring case depends on how you look at it. 17.5 days could be tolerable in a hospital since the patient is at any time accessible, and the batteries can be changed, even if it would be preferable to keep the amount of battery changes to a minimum. In a home scenario 17.5 days probably would be too short, since the patient either has to come to the clinic or someone from the clinic has to make a housecall every time a battery change is needed.

To achieve better battery lifetime it was found that reducing the sampling rate from 500 to 250 Hz was very effective. Now the batteries could last up to approximate 36 and 20 days, depending on the size. 36 days is acceptable in both hospital and home cases. In the home monitoring scenario, a monthly visit from a nurse or any other trained caregiver to check up on a patient is recommended anyways, since technology never will replace human interaction. If price is an important issue 20 days of battery life is still a decent result. But it is important to remember that these results are based on theoretical best case scenarios, the actual battery life will be a little lower.

By allocating channels between three groups of 16 patients the number of patients is respectable 48. And if the sampling rate is reduced as proposed, 98 patients can be monitored in one ZigBee network. That will be adequate in many clinical wards, in hospitals or institutions. Bigger hospitals and institutions could try to use multiple ZigBee networks, but that is outside the scope of this thesis. ZigBee's scalability is especially a good match with home monitoring, where the BAN is integrated in a smart home network. The BAN use just 5 nodes leaving 250 for SH tasks, which gives room for a lot of opportunities (see [50]).

Two different solutions are proposed to achieve time synchronization between two or more sensors in the same BAN. One includes regular resets of the DSN counting, while the other suggests the use of timestamps. Both are simple suggestions and need more work to be operational.

The time delay issue is solved by adding a 200 ms delay in the buffer, the delay can optionally be longer to achieve better fail-safety in dense environments. Even though all the data in the proposed system use guaranteed time slots, there is never a 100 percent guarantee that your wireless transmission will be successful, e.g. conflicts with other ISM band technologies may occur as well as fading of the signal due to obstacles. The time delay due to router hops is not present in the proposed solution, but could easily be levelled by the buffer delay since each hop adds merely 10 ms.

Transferring medical data requires a high degree of security; integrity, authentication, and confidentiality are especially essential. ZigBee employs extensive security solutions, and offers a level of security suitable for medical scenarios. E.g. in a home scenario it is extremely important to use cryptography so no one outside can sniff packages and tell where in the house you are and what is wrong with you. ZigBee supports 128 bit AES (see section 3.4.5).

The thesis definition says the ZigBee protocol stack shall be investigated in order to evaluate possible solutions for suitable application layer protocols that can be used in a scenario of biomedical signals communicating within a BAN framework. The proposed solution is APL independent, making it more flexible. The data being transferred would require only a very simple APL protocol, if any (see section 6.2.3). All the APL functionality is proposed moved to lower layers, e.g. synchronization can be solved by timestamping in the MAC layer rather in the APL. This makes an APL protocol redundant.

8 Conclusion and further work

8.1 Conclusion

In this thesis different short range wireless technologies has been evaluated for use in a Body Area Network. One of those technologies called ZigBee has been investigated more thoroughly in different patient monitoring scenarios, exploring its limitations and possibilities.

Although all the wireless technologies presented can be used in a Body Area Network, ZigBee and Nordic's proprietary solution stands out. Technically, Nordic's solution is the best fit, but ZigBee has the advantage of being a global standard. In my opinion it is important to try to standardize a technology for acquiring medical sensor readings, hence I would endorse ZigBee.

When studying ZigBee in the different monitoring scenarios it is clear that the use of star topology in the Body Area Networks will be more energy sufficient than mesh topology. Stars can take advantage of reduced function devices which is designed to be battery powered, hence they use less power. In the scenarios limitations like battery life, scalability of patients, and proper synchronization of sensors in the same Body Area Network are revealed. However solutions to those weaknesses are proposed along with an example on how a ZigBee monitoring network could be realized. It is an even better fit in a home monitoring scenario combined with a smart home network. Monitoring just one patient leaves lots of resources for the smart home nodes which act more like applications ZigBee was intended for (low duty cycle operation). This shows ZigBee has a future in biomedical environments.

Patient monitoring is an area where the technological progress goes relatively fast. The impact of ZigBee could result in e.g. increased product innovation as a result of the industry standardization. Companies can focus their energies on innovation in stead of developing a proprietary solution from scratch every time. Other advantages are that ZigBee offers interoperability and vendor independence as well.

Based on data rate, power consumption, security, and scalability ZigBee *can* be used in a patient monitoring network. Based on price and the benefits of standardization, it *should* be used.

8.2 Further work

With the benefits of ZigBee in mind it would be important to take a look at different aspects of a biomedical environment where ZigBee can be exploited.

In case of monitoring in a big hospital the possibilities of employing multiple ZigBee networks should be examined. Further, mesh networking between hospital-rooms should be investigated, since the patients, most likely, will not be placed in groups of 96 in one room as depicted in chapter 6.2.

It will be necessary to develop functionality at the NWK CO side which is able to put the incoming data in the correct buffers based on the address fields of the packets (see section 5.2). In the proposed solutions for synchronization there must be done further research to see how this can be implemented as well. A technique to reset the DSN would need to be developed and ZigBee's timestamp handling needs to be checked out.

9 References

[1] IEEE Standard 802.15.4-2003, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)"

[2] Patrick Kinney, "ZigBee Technology: Wireless Control that Simply Works"
Kinney Consulting LLC, Chair of IEEE 802.15.4 Task Group
Secretary of ZigBee BoD, Chair of ZigBee Building Automation Profile WG

[3] J. Elson and D. Estrin, "An Address-Free Architecture for Dynamic Sensor Networks" Tech. rep. 00-724, Comp. Sci. Dept., USC, Jan. 2000.

[4] Ed Callaway, Venkat Bahl, Paul Gorday, Jose A. Gutierrez, Lance Hester, Marco Naeve, and Bob Heile, "Home Networking with IEEE 802.15.4, a Developing Standard for Low-Rate Wireless Personal Area Networks," IEEE Communications Magazine, special issue on Home Networking, v. 40, n. 8, August 2002, pp. 70-77.

[5] Thomas Norgall, Robert Schmidt, Thomas von der Grün, **“**Body Area Network – A key Infrastructure Element for Patient Centred Telemedicine”.

[6] Freescale Semiconductor’s Ultra Wideband FAQ
http://www.freescale.com/webapp/sps/site/overview.jsp?nodeId=02XPgQhHPR02204720, checked 17.07.2005

[7] Wikipedia

[8] Rafael Kolic, “Ultra Wideband-the Next-Generation Wireless Connection”, Technology@Intel Magazine, February/March 2004.

[9] IEEE Standard 802.15.3-2003, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High-Rate Wireless Personal Area Networks (WPANs)"

[10] Ashok Bindra, “Do we really need a unified ultra-wideband (UWB) standard?”, RFDESIGN magazine, Nov 2004.

[11] IEEE Standard 802.15.1-2002, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)"

[12] The Bluetooth SIG. The Bluetooth Specification version 1.2, Technical report, The Bluetooth SIG, 2003. Available online at https://www.bluetooth.org/spec/, checked 17.07.2005

[13] Bluetooth Homepage. http://www.bluetooth.com

[14] The ZigBee Alliance. http://www.zigbee.org

[15] John Adams, "A primer to ZigBee and 802.15.4", presentation at CES, Q1 2004

[16] Emil Jovanov, Dennis Cox, Aleksandar Milenkovic, "Time synchronization in ZigBee networks", IEEE spectrum, May 2005

[17] Nordic semiconductor homepage. http://www.nvlsi.no/index.cfm?obj=document&act=display&doc=245

[18] ANT Message Protocol and Usage, D00000652 Rev1.31 PRELIMINARY, Dynastream Innovations Inc., April 26, 2005

[19] nRF24AP1 Datasheet Rev 2.0, Single chip 2.4 GHz Transceiver with Embedded ANT protocol, April 2005

[20] Benny P L Lo and Guang-Zhong Yang, "Key Technical Challenges and Current Implementations of Body Sensor Networks", the 2nd International Workshop on Body Sensor Networks (BSN 2005), April 2005

[21] UbiMon website, http://www.doc.ic.ac.uk/vip/ubimon/home/index.html, checked 17.07.2005

[22] WsHC website, http://www.wshc.no/index.php, checked 17.07.2005

[23] The Non-invasive WBAN project at ETH, Zurich, website, http://www.nari.ee.ethz.ch/wireless/research/projects/ban.html, checked 17.07.2005

[24] The IMEC Human++ project website, http://www.imec.be/ovinter/static_research/human.shtml, checked 17.07.2005

[25] Emil Jovanov, Aleksandar Milenkovic, Chris Otto and Piet C de Groen," A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation", 01 March 2005

[26] Intel's Prohealth project website. http://www.intel.com/research/prohealth/, checked 17.07.2005

[27] Healthy Aims project website, http://www.healthyaims.org/, checked 17.07.2005

[28] Zarlink's BAN project website, http://ulp.zarlink.com/ban.htm, checked 17.07.2005

[29] CodeBlue project website, http://www.eecs.harvard.edu/~mdw/proj/codeblue/, checked 17.07.2005

[30] "Body-Sensor Wireless Networks - Monitoring Patients' Health with BAN", Information flyer from FOKUS, http://www.fokus.gmd.de/web-dokumente/Flyer_engl/BAN_E.pdf, checked 17.07.2005

[31] MobiHealth project website, http://www.mobihealth.org/, checked 17.07.2005

[32] Dimitri Konstantas, Aart Van Halteren, Richard Bults, Nikolai Dokovsky, George Koprinkov, Katarzyna Wac, Val Jones, Ing Widya, Rainer Herzog, "Mobile Patient Monitoring: THE MOBIHEALTH SYSTEM", International Congress on Medical and Care Compunetics NCC, The Hague, 2-4 June, 2004

[33] IST project fact sheet on TelemediCare, http://dbs.cordis.lu/fep-cgi/srchidadb?ACTION=D&CALLER=PROJ_IST&QF_EP_RPG=IST-1999-10754, checked 17.07.2005

[34] Dag Grini, "Crowd control: short-range devices in the 2.4-GHz ISM band", Chipcon

[35] FCC, First Report and Order 02-48. Feb 2002, http://www.fcc.gov/Bureaus/Engineering_Technology/News_Releases/2002/nret0203.html, checked 17.07.2005

[36] UWB forum website, http://www.UWBforum.org, checked 17.07.2005

[37] Bluetooth.org – The Official Bluetooth Membership Site, http://www.bluetooth.org, checked 17.07.2005

[38] IEEE Standard 802.15.2-2002, "IEEE Recommended Practice for information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands"

[39] nRF24xx Link Integrity, Nordic VLSI, white paper, April 2004

[40] Gary Legg, “ZigBee: Wireless Technology for Low-Power Sensor Networks”, TechOnline, May 2004, http://www.techonline.com/community/tech_topic/bluetooth/36561, checked 17.07.2005

[41] This is ANT website, http://www.thisisant.com, checked 17.07.2005

[42] ABI research, “Ultrawideband? 'Show Me the Money'”, Nov 2004, http://www.abiresearch.com/abiprdisplay.jsp?pressid=361, checked 17.07.2005

[43] ZigBee Document 053474r05, Version 1.0, specification, Dec 2004

[44] Telecom products, “Production up, prices down for 2005”, article, Dec 2004 http://www.telecom.globalsources.com/gsol/I/Bluetooth-handsfree/a/9000000057461.htm checked 17.07.2005

[45] Mouser Electronics, CHIPCON Single-Chip Transceivers, May – July 2005, http://www.mouser.com, checked 17.07.2005

[46] Panasonic batteries, http://www.apexbattery.com/lithium-batteries.html, checked 17.07.2005

[47] Chipcon SmartRF CC2420 2.4 GHz IEEE 802.15.4/ZigBee-ready RF Transceiver data sheet.

[48] Dr. –Ing. Gerald Kupris, Prof. Dr. Werner Buff, “Performance Investigations of Wireless Sensor Networks based on IEEE 802.15.4 / ZigBee”, Wireless M2M congress, Freescale semiconductor, June 2005

[49] Partners in Assistive Technology Training and Services web site, http://webschoolsolutions.com/patts/systems/heart.htm, checked 17.07.2005

[50] Philip E. Ross, “Managing Care Through the Air”, IEEE Spectrum, Dec 2004

[51] Battery shop web site, http://www.nimhbattery.com/mahapowerex-nimhbatteries-2300mAh-aa.htm, checked 17.07.2005

[52] Personal information, mail from Rune Fensli, 13.07-2005

[53] Jim Lansford, Ron Nevo, and Brett Monello, “Wi-Fi and Bluetooth: Enabling Coexistence”, Compliance Engineering, May 2001, http://www.ce-mag.com/archive/01/05/lansford.html, checked 17.07.2005