Technological and Educational Institute of Central Macedonia

School of Technological Applications
Department of Engineering Informatics

Master's thesis on

Medium Access Control (MAC) Standards for Wireless Body Area Networks (WBANs) and Security Considerations

Kiriakos Gavouchidis

In partial fulfillment of the requirements for the degree of
Master of Science
in
Communication and Information Systems

Supervisor: Dr. Dimitrios Efstathiou

March, 2016

Acknowledgment

A big Efxaristo (Thank you) to my supervisor, Assistant Prof. Efstathiou for the chance he gave me to write this Master Thesis in this very interesting and exciting area. He is always there, for help, for advice, for criticism, and feedback. With patience, and insightful. With encouragement, enthusiasm and many ideas. Thank you.

Abstract

WBANs are a key element to the ubiquitous healthcare revolution. From the communication point of view, they are one of the most challenging elements for this application and also other application areas such as military, sport, or entertainment. New applications and requirements force the development of the WBAN technology, e.g. the MAC sublayer protocol and its existing and future standards. Every standard described in this Master Thesis represents an evolution of the previous standard according to the application needs with the goal to find solutions for the existing challenges in WBANs. One main issue in WBANs is to minimize energy consumption due to the fact that the nodes may be implanted in the human body, so batteries can not be replaced after a small time period. Minimal energy consumption is a critical factor for the survive of WBAN technology.

This work consists of two parts. The first part describes the MAC sublayer standards for WBANs. The second part of the work analyzes the security of WBANs.

The first part starts with the description of the different types of existing WBANs, we present the main application areas of WBANs and analyze their manifold requirements. Some of these requirements, mentioned here as an example, are: Long battery life, power consumption, scalability, network topology to be implemented, and WBAN co-existence. Then we refer to the services and the functionality of the MAC sublayer protocol for WBANs and to the different channel access methods such as TDMA and CSMA/CA. The analysis and description of the existing MAC sublayer protocol standards follows. The MAC sublayer is part of the Data Link Layer of the ISO-OSI standard. The MAC protocol is mainly responsible and regulates the WBAN access to the channel. We study the IEEE 802.15.1, the Bluetooth LE, the IEEE 802.15.4, the IEEE 802.15.4a, the IEEE 802.14.4j, the IEEE 802.15.6, and the SmartBAN standard. After their detailed description, especially of the IEEE 802.15.6 standard, we compare them with each other, and emphasize their advantages and disadvantages. The explanation of more than thirty MAC sublayer protocol implementations for WBANs are the next part of the work. Implementations like H-MAC, BodyMAC, TRAMA, LEACH, STEM, P-MAC, and also RuBee, and ANT+, complete the picture. The last section of the first part is dedicated to the challenges of this exciting technology.

Security and privacy for WBANs are defined at the second part of this Master Thesis. We analyze three different types of WBAN attacks, the DoS attack type, attacks on secrecy and authentication, and attacks on service integrity. For the first and second type of attacks we describe concrete attacks from the WBAN praxis. Some of the presented attacks are the Flooding attack, the De-synchronization attack, the Sinkhole attack, the Misdirection attack, the Homing attack, the Collision attack, and the Unfairness attack. After every attack description we discuss the countermeasures against them and the weakness if any, to act against them successful. We analyze the differences between Wireless Sensor Networks (WSN) and WBANs having security in focus. At the end of part two we present the security characteristics of the MAC sublayer standards, with reference to their advantages, their disadvantages, and the challenges.

A summary of the MAC sublayer protocol standards and the WBAN security concludes the Master Thesis.

Περίληψη

Η τεχνολογία των WBANs είναι μία τεχνολογία που εξελίσσεται με γοργούς ρυθμούς. Οι εφαρμογές της σε τομείς όπως η υγεία, τα σπορ, ή οι ένοπλες δυνάμεις, δίνουν ώθηση στην ανάπτυξή τους. Η εξέλιξη της τεχνολογίας WBAN είναι αλληλένδετη με τα standards που υπάρχουν. Το κάθε standard που ορίζεται σε αυτή την εργασία αποτελεί εξέλιξη του προηγούμενου standard με στόχο την καλύτερη κάλυψη των αναγκών στα WBANs. Μια βασική ανάγκη των WBANs είναι η εξοικονόμηση ενέργειας της μπαταρίας των αισθητήρων (nodes) λόγω της χρήσης τους εκτός των άλλων και μέσα στο ανθρώπινο σώμα, κάτι που σημαίνει ότι η εξοικονόμηση ενέργειας είναι καθοριστική για την επιβίωση και ανάπτυξη αυτής της τεχνολογίας.

Η εργασία αυτή αποτελείται από δύο μέρη. Το πρώτο μέρος περιγράφει τα MAC sublayer standards για WBANs. Το δεύτερο μέρος της αναλύει την ασφάλεια των WBANs.

Στην αρχή του πρώτου μέρους αναλύουμε τα διάφορα είδη WBANs που υπάρχουν, περιγράφουμε τις διάφορες εφαρμογές των WBANs και τις προϋποθέσεις που επιβάλλονται για την λειτουργία τους. Μερικές από αυτές τις προϋποθέσεις έχουν ως αντικείμενο το μέγεθος της ενέργειας που καταναλώνεται, την συνύπαρξη περισσοτέρων WBANs μεταξύ τους, η την τοπολογία δικτύου που πρέπει να χρησιμοποιηθεί. Μετά αναφέρουμε στις λειτουργίες και υπηρεσίες που προσφέρει το MAC πρωτόκολλο και στις διάφορες τεχνικές πρόσβασης στο κανάλι που μπορούν να χρησιμοποιηθούν σε WBANs, όπως είναι η CSMA/CA και η TDMA. Κατόπιν αναλύουμε τα διάφορα standards τα οποία έχουν ως αντικείμενό τους το MAC sublayer πρωτόκολλο των WBANs. Αυτό βρίσκεται στο προτελευταίο layer του ISO-OSI πρωτοκόλλου, στο Data Link Layer. Το MAC πρωτόκολλο είναι κυρίως υπεύθυνο για την ρύθμιση της πρόσβασης στο μέσο διάδοσης. Αναλύουμε τα standards IEEE 802.15.1, Bluetooth LE, IEEE 802.15.4, IEEE 802.15.4a, IEEE 802.14.4j, IEEE 802.15.6, και το SmartBAN standard. Μετά την εκτενή περιγραφή τους συγκρίνουμε τα standards μεταξύ τους περιγράφοντας τα πλεονεκτήματα και τα μειονεκτήματά τους. Επίσης περιγράφουμε πάνω από τριάντα διαφορετικές εφαρμογές MAC sublayer πρωτόκολλα για WBANs, όπως το H-MAC, το BodyMAC, το TRAMA, το LEACH, το STEM, το P-MAC, καθώς επίσης το RuBee, το ANT+, και διάφορα άλλα. Στο τέλος του πρώτου μέρους κάνουμε αναφορά στις προκλήσεις που αντιμετωπίζει αυτή η συναρπαστική τεχνολογία.

Στο δεύτερο μέρος της εργασίας περιγράφουμε τούς όρους της ασφάλειας (security) και της ιδιωτικότητας (privacy) στα WBANs. Αναλύουμε τα διάφορα είδη επιθέσεων κατά των WBANs όπως τις επιθέσεις κατά της διαθεσιμότητας του δικτύου (DoS), επιθέσεις κατά της μυστικότητας και της authentication καθώς και επιθέσεις κατά του service integrity. Για κάθε ένα από αυτά τα είδη επιθέσεων παρουσιάζουμε και περιγράφουμε συγκεκριμένες επιθέσεις, όπως την Flooding, την De-synchronization, την Sinkhole attack, την Misdirection, την Homing attack, την Collision attack, ή την Unfairness attack. Επίσης παρουσιάζουμε και τον τρόπο που αντιμετωπίζονται επιτυχώς αλλά και οι αδυναμίες αντιμετώπισης των επιθέσεων. Αναλύουμε τις διαφορές μεταξύ Wireless Sensor Networks (WSN) και των WBANs από την οπτική γωνία της ασφάλειας. Στο τέλος της εργασίας αναλύουμε τα MAC sublayer standards εξετάζοντας τις λύσεις που δίνουν για το θέμα της ασφάλειας, αναφέρουμε τα πλεονεκτήματα τους, τα μειονεκτήματα τους και κάνουμε αναφορά στις προκλήσεις που πρέπει να αντιμετωπιστούν.

Η εργασία τελειώνει με μία γενική επισκόπηση για τα MAC sublayer standards για τα WBANs και την ασφάλειά τους.

Contents

List of figures

List of tables

Abbreviations

AAA	Abdominal Aortic Aneurysm
ACK	Acknowledgement
ADC	Analog-to-digital Converter
AGBA	Adaptive Guard Band Algorithm
AgCI	Silver Chloride
AMT	Aeronautical Mobile Telemetry
ANT	Advanced and adaptive Network Technology
AP	Access point
AWGN	Additive white Gaussian noise
B-Ack	Block acknowledgment
B-MAC	Berkeley MAC
BAN	Body Area Network
BNC	Body network controller
BP	Beacon Period
BT BR	Bluetooth basic rate
BT EDR	Bluetooth Enhanced Data Rate
BT LE	Bluetooth Low Energy
C-Ass	Connection Assignment
C-Rec	Connection Request
C-RICER	cognitive-receiver initiated cycled receiver
CA	Congestion Avoidance
CAP	Contention Access Period
CBC	Cipher Block Chaining
CCA	Clear Channel Assessment
CCAP	Configurable Contention Access Period
CCH	Control Channel
CE	Consumer Electronics
CFP	Contention-free period
CP	Contention Probability
CR	Cognitive radio
CRBAN	Cognitive radio body area network
CRC	Cognitive Radio Controller
CRC	Cyclical Redundancy Check
CS	Compressed Sensing
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention window
D-Beacon	Data Beacon
D-MAC	Data Gathering MAC
D-Req	Disconnection Request
DAA	Detect and avoid
DAF	Drift Adjustment Factor
DCAAC-MAC	Dynamic channel adjustable asynchronous cognitive radio MAC
DCC MAC	Dynamic Channel Coding MAC
DCH	Data channel
DoE	U.S. Department of Energy
DoS	Denial-of-Service
DRP	Distributed reservation protocol
EAP	Exclusive access phase
ECC	Elliptic Curve Cryptography

ECG	Wireless electrocardiogram
EEC	Electroencephalogram
EIRP	Effective Isotropically Radiated Power
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ER MAC	Exclusion Regions MAC
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FFD	Full-function device
FDMA	Frequency Division Multiple Access
FLAMA	Flow-Aware Medium Access
FRTS	Future Request-to-Send
GFSK	Gaussian frequency shift keying
GTK	Group Temporal Key
GTS	Guaranteed time slot
H-MAC	Heartbeat Driven MAC Protocol
HERO	Hazards of Electromagnetic Radiation to Ordnance
HID	Hub id
HME	Hub management entity
I-Ack	Immediate acknowledgment
IBE	Identity-based encryption
IE	Information element
IMD	Implantable Medical Device
IR	Impulse radio
IR-UWB	Impulse radio ultra-wideband
ISM	Industrial scientific medical
EIFS	Extended Inter Frame Space
FCS	Frame check sequence
FDA	Food and Drug Administration
FFD	Full function device
FM-UWB	Wideband frequency modulation
G-Ack	Group acknowledgment
HBC	Human Body Communication
HEED	Hybrid Energy-Efficient Distributed Clustering
HME	Hub management entity
ISM	Industrial scientific medical
ITU	International Telecommunication Union
L-Ack	Late Acknowledgement
LBT	Listen-before-transmit
LC	Link Control
LE	Link Establishment
LEACH	Low-Energy Adaptive Clustering Hierarchy
LLC	Logical Link Control
LPL	Low-Power Listening
LR-WPAN	Ultra-low-power Wireless Personal Area Network
LSB	Least significant bit
MAC	Medium access control
MAC	Message Authentication Code
MAP	Managed access phase
MB-OFDM	Multiband orthogonal frequency-division multiplexing
MBAN	Medical body area network
MC WBAN	Molecular WBAN

MCU	Microcontroller Unit
MEC	Micro energy cell
MEMS	Micro-Electro Mechanical Systems
MFR	MAC Footer
MIC	Message integrity code
MICS	Medical implant communications service
MIFS	Minimum interframe space
MK	Master Key
MN	Master Node
MPDU	Medium access control protocol data unit
MS	Monitoring Station
MSB	Most significant bit
MSDU	Media access control service data unit
NAV	Network allocation vector
N-Ack	No acknowledgment
NACK	Negative Acknowledgment
NB	Narrowband
NCTS	Not Clear to Send
NID	Node identifier
NME	Node management entity
NPDU	Network Layer Protocol Data Unit
NSR	Non-Significant Risk
OSI	Open System Interconnection
P-MAC	Pattern-MAC
PAP	Public applications profiles
PCA	Prioritized Contention Access
PCA	Priority Channel Access
PCF	Point coordination function
PD	Personal Device
PDU	Protocol Data Unit
PHHC	Personal Home & Hospital Care
PHR	Physical Header
PHY	Physical Layer
PLCP	Physical Layer Convergence Procedure
PoC	Point-of-Care
PPDU	Physical protocol data unit
PPM-UWB	Pulse Position Modulation UWB
PSDU	PHY Service Data Unit
PSIFS	Short Interframe Space
PSMA	Preamble Sense Multiple Access
PTK	Pairwise Temporal Key
PU	Primary user
QoS	Quality of service
RAP	Random access phase
RCA	Re-use Channel Access
RCPC	Rate Compatible Punctured Convolution
RDEV	Ranging Capable Device
RF	Radio Frequency
RFD	Reduced-function device
RFID	Radio frequency identification
RSSI	Received signal strength indicator

RTS	Request To Send
RX	Receive or reception
S-MAC	Sensor MAC
S-Ras	Slot-Reassignment
SACA	Slotted aloha channel access
SAP	Service Access Point
SAR	Specific absorption rate
SDU	Service data unit
SNR	Signal-to-noise ratio
SoC	System-on-chip
SSD	Safe Separation Distance
STEM	Sparse Topology and Energy Management
SU	Secondary user
T-MAC	Timeout MAC
TDMA	Time Division Multiple Access
TH-code	Time Hopping Code
TRAMA	Traffic-Adaptive Medium Access
TSRB	Time Slot Reserved for Bursty Traffic
TSRP	Time Slot Reserved for Period Traffic
TX	Transmit or transmission
U-MAC	Ultra-wide band MAC
UP	User Priority
UWB	Ultra-wideband
WBAN	Wireless Body Area Network
WBASN	Wireless body area sensor network
WFT	Wakeup Fallback Time
WiseMAC	Wireless Sensor MAC
WMTS	Wireless medical telemetry system
WPAN	Wireless personal area network
WSN	Wireless Sensor Network

Definitions

bilink: a communications link for transfer of management and data traffic from a hub to a node and vice versa.

downlink: A communications link for transfer of management and data traffic from a hub to a node.

downlink allocation: An allocation with allocation interval(s) in which a hub initiates one or more frame transactions to transmit management and data traffic to a node and the node returns acknowledgment if required.

duty cycle: The duty cycle is the ratio between the pulse duration and the period of a rectangular waveform.

LR-WPAN: low-rate wireless personal area network.

Octet: An octet is a unit of digital information in computing and telecommunications that consists of eight bits. The term is often used when the term byte might be ambiguous [1].

poll: A control type frame or its variant sent by a hub to grant an immediate polled allocation to the addressed node or to inform the node of a future poll or post.

polled allocation: A non-reoccurring time interval that a hub grants to a node using polling access for initiating one or more frame transactions by the node. A polled allocation is an uplink allocation interval, suitable for servicing “ordinary,” “unexpected,” or “extra” uplink traffic (for example, due to data rate variations and/or channel impairments). A polled allocation is also called a *polled allocation interval.*

polling access: An access method, based on impromptu or scheduled polling by a hub, whereby a hub grants to a node a polled allocation for initiating one or more frame transactions by the node.

post: A management or data type frame sent by a hub to a node within its body area network (BAN). A post starts a posted allocation.

posted allocation: A non-reoccurring time interval that a hub grants to itself using posting access for initiating a frame transaction. A posted allocation is a downlink allocation interval, suitable for servicing “unexpected” or “extra” downlink traffic (for example, due to network management needs, data rate variations, and/or channel impairments).

posting access: An access method, based on impromptu or scheduled posting by a hub, whereby a hub grants to itself a posted allocation, typically outside scheduled uplink allocations, for initiating one or more frame transactions by the hub.

scheduled access: An access method, based on advance reservation and committed scheduling, whereby a node and a hub obtain scheduled reoccurring time intervals for initiating frame transactions.

scheduled allocation: One or more scheduled reoccurring time intervals that a node and a hub obtains using scheduled access for initiating frame transactions. A scheduled allocation is an uplink allocation, a downlink allocation, or a bilink allocation, suitable for servicing high or low duty cycle periodic or quasiperiodic traffic on a committed schedule.

type-I polled allocation: A polled allocation the length of which is specified in terms of the duration of time granted for transmission.

type-I polling access: Polling access that provides type-I polled allocations.

type-II polled allocation: A polled allocation the length of which is specified in terms of the number of frames granted for transmission.

type-II polling access: Polling access that provides type-II polled allocations.

uplink allocation: An allocation with allocation interval(s) in which a node initiates one or more frame transactions to transmit management and data traffic to a hub and the hub returns acknowledgment if required.

uplink: A communications link for transfer of management and data traffic from a node to a hub.

wpan: wireless personal area network.

1 INTRODUCTION

New drugs, medicine progress through new technology and healthy nutrition are some of the factors which todays lead to an increase of life expectancy. Longer live also means growth of aging population and more costs for health care. The total health care expenditure in 2013 in Germany reached 314,9 billion Euros, an increase of 4% [2]. This and other statistics from different countries necessitate to reduce the costs and to make medicine more affordable. Early disease detection is an additionally factor helping people which suffer on cancer, diabetes, cardiovascular disease and many other dangerous diseases. Early disease detection helps treating it in an early stadium and also helps in saving costs. A way early disease detection and disease prevention can be reached is proactive wellness management. Proactive wellness management should be in the future an inherent part of health care systems. A key to succeed that are wearable monitoring systems based on *wireless body area networks* and techniques like *sensing*.

1.1 WIRELESS BODY AREA NETWORKS

Sensing is a technique to gather information about physical objects or areas. A *sensor* or *transducer* is an object performing a sensing task, converting one form of energy in the physical world into electrical energy. The human body consists of several physical sensors. For example, the eyes, which capture optical information (light) or the ears which capture acoustic information (sound). Sensors capture phenomena in the physical world.

Sensors can be classified according to the criteria physical property, power supply and electrical phenomenon. We list the most important sensor types taking into account the sensor class.

Sensor classification according to its physical property:

- Temperature like Thermistors or thermocouples
- Pressure like Pressure gauges, barometers, or ionization gauges
- Optical like Photodiodes, phototransistors, infrared sensors, or CCD sensors
- Acoustic like Piezoelectric resonators, or microphones
- Mechanical like strain gauges, tactile sensors, capacitive diaphragms, or piezo resistive cells
- Motion, Vibration like Accelerometers, or mass air flow sensors
- Position like GPS, ultrasound-based sensors, infrared-based sensors, or inclinometers
- Electromagnetic like Hall-effect sensors, or magnetometers
- Chemical like pH sensors, electrochemical sensors, or infrared gas sensors
- Humidity like Capacitive and resistive sensors, hygrometers, or MEMS-based humidity sensors
- Radiation like Ionization detectors, or Geiger-Mueller counters

Sensor classification according to power supply:

- *active* sensors require external power to detect change in energy of transmitted signal
- *passive* sensors detect energy in the operating environment and obtain their power from this energy input (e.g., passive infrared sensor)

Sensor classification according to electrical phenomenon:

- *resistive* sensors use changes in *electrical resistivity (ρ)* based on physical properties such as temperature (resistance $R = \rho * l/A$). Electrical resistivity is an intrinsic property that quantifies how strongly a given material opposes the flow of electric current.

- *capacitive* sensors use changes in capacitor dimensions or *permittivity* (ε) based on physical properties (capacitance C = ε*A/d). The permittivity of a medium describes how much electric field (flux) is 'generated' per unit charge in that medium.
- *inductive* sensors rely on the principle of inductance, where electromagnetic force is induced by fluctuating current.
- *piezoelectric* sensors rely on materials such crystals or ceramics that generate a displacement of charges in response to mechanical deformation.

Wearable monitoring systems record e.g. electrocardiographic and electromyographic data, thoracic or abdominal signals. The field of applications is wide: Health & wellness monitoring, safety monitoring, home rehabilitation, assessment of treatment efficacy, and early detection of disorders are some of them. From the technical point of view wearable monitoring systems use a network consisting of intelligent low transmit-power and short-range sensors and actuators implanted in the human body or placed on the body. Such networks are commonly referred to as *Wireless Body Area Networks*. Terms such as *Low-Rate Wireless Personal Area Network (LR-WPAN)*, *Wireless Sensor Network (WSN)* or *Wireless Body Area Network (WBAN)* are often referred and discussed in this work, we define them at the beginning.

A *Low-Rate Wireless Personal Area Network 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 an LR-WPAN are ease of installation, reliable data transfer, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol [3].

A *Wireless Sensor Network (WSN)* consists of a LR-WPAN and a sensor application (Figure 1).

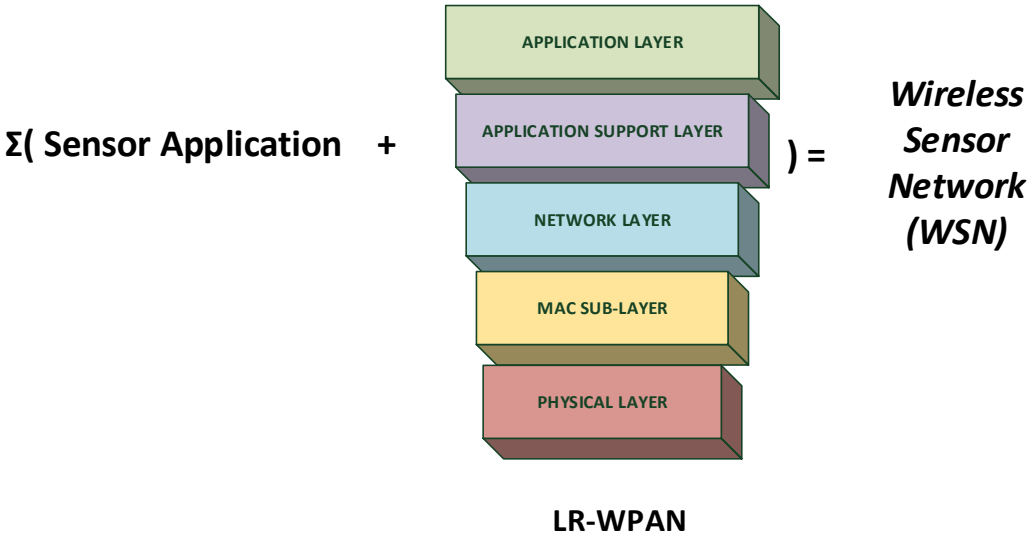


Figure 1 Definition of Wireless Sensor Networks

Wireless Body Area Network (WBAN) is a collection of low-power, miniaturized, invasive or non-invasive, lightweight devices with wireless communication capabilities that operate in the proximity of the human body. This special-purpose sensor network designed to operate autonomously. These devices can be placed in, on or around the body, and are often wireless sensor nodes that can monitor the human body functions and characteristics of the surrounding environment for a long-term period [4].

A comparison of the WBAN and WSN characteristics is given in the Table 1.

Comparison criteria	Wireless Sensor Network	Wireless Body Area Network
Network Dimensions	Few to several thousand nodes over an area from meters to kilometers	Dense distribution limited by body size
Topology	Random, Fixed/Static	One-hop or two-hop star topology
Node Size	Small size preferred (no major limitation in most cases)	Miniaturization required
Node Accuracy	Accuracy outweighs large number of nodes and allows for result validation	Each of the nodes have to be accurate and robust
Node Replacement	Easily performed (some nodes are disposable)	Difficulty in replacement of implanted nodes
Bio-compatibility	Not a concern in most applications	Essential for implants and some external sensors
Power Supply and Battery	Accessible, capable of changing more frequently and easily	Difficulty in replacement and accessibility of implanted settings
Node Lifetime	Several years/months/weeks (application dependent)	Several years/months (application dependent)
Power Demand	Easier power supply, hence greater demand	Energy power supply more difficult, hence lower demand
Energy Scavenging	Wind and solar power as candidates	Thermal body heat and motion as candidates
Data Rate	More frequently homogenous	More frequently heterogeneous
Data loss impact	Data loss over wireless transfer is compensated by the large number of nodes	Data loss is considered more significant
Security Level	Low (application-dependent)	Higher security level
Traffic	Application specific, modest data rate, cyclic/sporadic	Application specific, modest data rate, cyclic/sporadic
Wireless Technology	WLAN, GPRS, ZigBee, Bluetooth, RF	802.15.6, ZigBee, Bluetooth, UWB
Context Awareness	Insignificant with static sensors in a well-defined environment	Very significant due to sensitive context exchange of body physiology
Overall Design Goals	Self-operability, cost optimization, energy efficiency	Energy efficiency, eliminate electromagnetic exposure

Table 1 Comparison of WBANs and WSNs

1.1.1 Taxonomy of WBANs

WBANs are differed in relation to the wireless communication technology employed. Four types of WBANs exist:

1. Radio frequency (RF) WBANs
2. Human Body Communication (HBC) WBANs
3. Ultrasound WBANs
4. Molecular WBANs

The radio frequency (RF) WBANs are divided in

- Medical implant communications service (MICS)
- Wireless medical telemetry system (WMTS)
- Industrial scientific medical (ISM)
- Medical body area network (MBAN)
- Ultra-wide band (UWB)

Figure 2 shows the WBAN frequency bands.

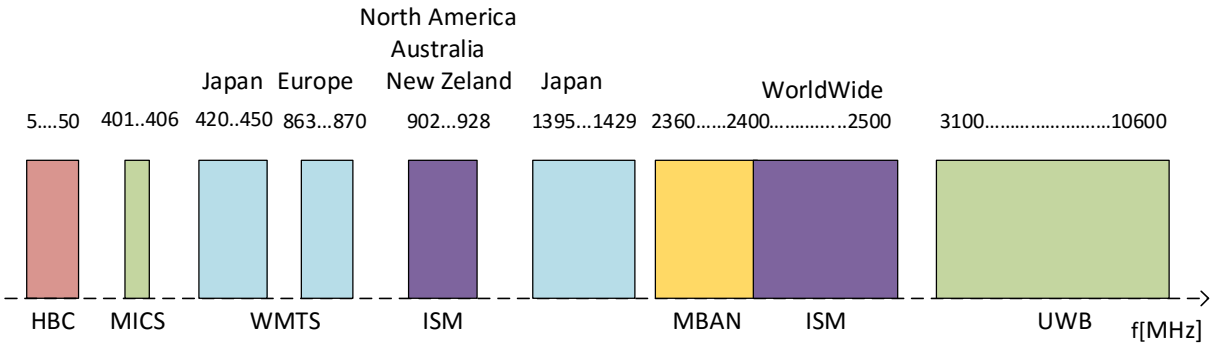


Figure 2 WBAN frequency bands

MICS and WMTS are used for medical in-body communication. MICS and WMTS bands introduced to overcome bit rate and reliability limitations derived by the magnetic coupling communication technology used in the early wireless medical devices. Within the MICS band a bit rate of 400 kbps can be achieved and a communication range about 2 meters. A shallowable camera pill is an example of a WMTS application. It requires 1 Mbps bit rate which can be achieved in the WMTS band. WMTS fulfills also the function requirements for devices such cardiac pacemakers, implanted defibrillators and neurostimulators. WMTS and MICS bands are in use exclusively for body-worn and implanted medical applications which require point-to-point communication.

The intention defining the unlicensed ISM bands by the International Telecommunication Union (ITU) wasn't the use of them in telecommunication. Due to their unlicensed status they are prone to coexistence issues that must be taken into account. The band between 2400 and 2500 MHz is in great demand because of its worldwide availability.

The *medical body area network (MBAN)* is described in the section 2.4.6. 40 MHz of protected spectrum is allocated between 2.36 and 2.40 GHz. The 2.36 – 2.39 GHz frequency range is available on a secondary basis. This helps to mitigate the interference by devices working in the adjacent ISM unlicensed band.

Any signal that employs more than 500 MHz of spectrum is defined by ITU as an *ultra-wide Band (UWB)* signal. ITU presuppose that the power spectral density shall not exceed 41.25 dBm/MHz. This is 30 dB below the maximum allowed in the 2.4-2.5 GHz ISM band. The use of UWB in WBANs has the follow advantages:

a. low susceptibility to multipath fading making indoor systems performant
b. no interference
c. bit rate up to 500 Mbps
d. simplicity of the transceiver architecture
e. low energy consumption

Human body communication WBANs use the human body as communication medium. Signals can be propagated through the human body in two ways:

- by capacitive coupling of the human body to the surrounding environment
- by galvanic coupling. This works through coupling alternate current into the human body

The noticeable benefits of the use of HBC are intrinsic security, low energy consumption and the possibility for coexistence with other HCB WBANs.

Ultrasound WBANs are a good alternative to the radio frequency WBANs and are based on the use of ultrasound. These can be acoustic waves at non-hearable frequencies. High attenuation, a limit of RF propagation, can be overcome by ultrasonic waves. This technology has been used for several years for underwater communications and they are considered as an appropriate communications method inside the human body which is mostly made up of water.

Molecular WBANs (MC WBANs) are also a good alternative to the radio frequency WBANs if we consider the in-body use case. They use molecules as messages. Molecules transferred between a transmitter and a receiver applying nanotechnology. Channel characteristics like noise, propagation delay, applicable modulations, and achievable capacity differ significantly from those of RF medium. Due to their intrinsic biocompatibility, diffusion-based molecular communications are promising for nanomedicine applications. An information-theoretic approach of a diffusion-based MC system is shown in the Figure 3. Transmitter, channel and receiver are part of the physical system. The nature of the molecular movement which is based on Brownian motion must be considered when designing MAC solutions. Such solutions should be kept simple due to very low memory and processing capabilities of nanomachines. This Master Thesis is focused on RF WBANs.

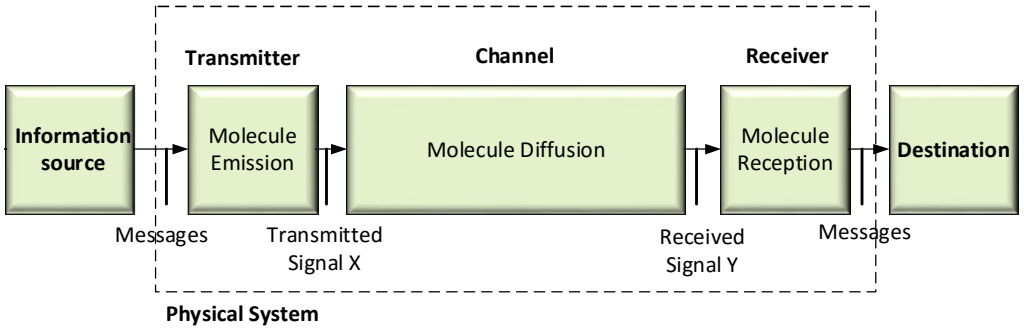


Figure 3 Information-theoretic diagram of a diffusion-based MC system

1.1.2 WBAN applications and Requirements

Every WBAN application has its own requirements. In general terms the most significant of them are:

- data rate
- reliability
- energy efficiency

We will describe the different application fields of WBANs and the corresponding requirements.

1.1.2.1 WBAN applications

The state-of-the art literature mentions three types of applications where WBANs are in use: Healthcare, sport and entertainment, and military and defense.

1.1.2.1.1 Healthcare

This is the most important and promising application field of WBANs (Figure 4). The following is a non-exhaustive list of applications of WBANs.

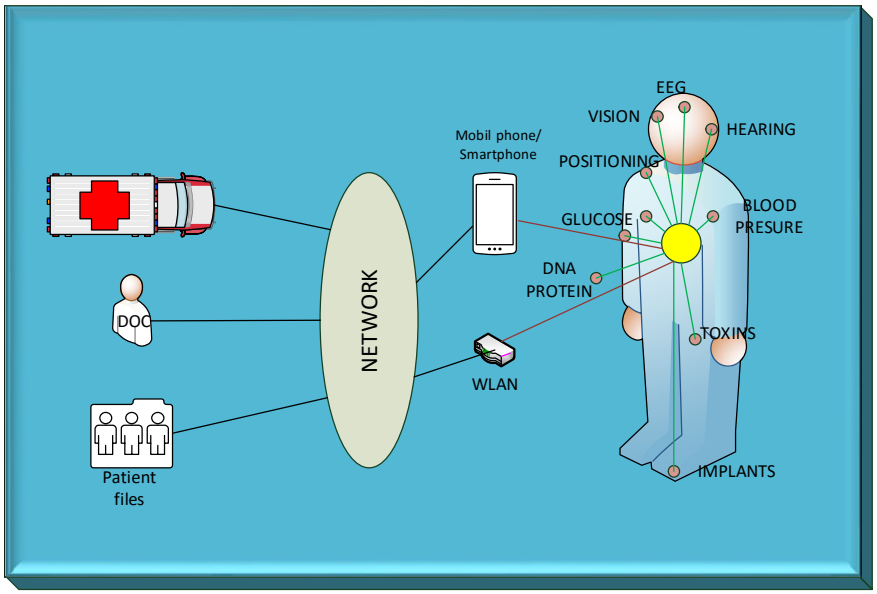


Figure 4 WBAN use for healthcare

1.1.2.1.1.1 Monitoring of parameters

Monitoring of parameters includes

- Monitoring Glucose for patients with diabetes using a wearable WBAN
- Monitoring and proper dosing of insulin as an implant WBAN reduces the risk of fainting and eliminates risks of loss of circulation, later life blindness and more complications
- Monitoring Toxins
- Monitoring allergic agents in the air via wearable WBAN helping asthma patients
- Sleep Analysis (Figure 5)

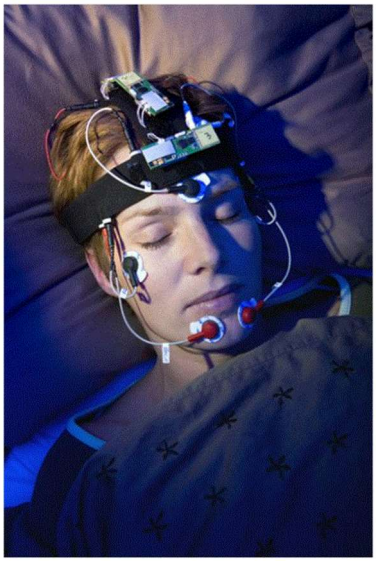


Figure 5 WBAN use for sleep Analysis

1.1.2.1.1.2 Biofeedback

Existing wearable sensing technologies make possible the detection of emotions. This happens through the induction of physical manifestations throughout the body. Fear for example increases respiration rate and heart-beat, which leads in palm sweating. Humans emotional status can be monitored through the monitoring of emotion-related physiological signals.

Some other biofeedback applications are wireless autonomous electroencephalogram (EEG) monitoring to detect epileptic seizure, wireless electrocardiogram (ECG) patch, automated arrhythmia detection, cochlear implant, artificial retina, pulse oximetry, drugs delivery, post-operative monitoring, body temperature monitoring and blood pressure monitoring.

A polysomnography test can be used to realize sleep disorders. This test requires analysis of a number of bio potentials recorded overnight. These measurements require a lot of cables. In the area of wireless sleep staging wearable WBANs are capable of delocalization of intelligence and instruments. This means no more disruption to the patient's motion and no more interruption if patient falling sleep.

Through implant WBAN technology myocardial infarction can be reduced by monitoring episodic events. Also WBAN based sensors (implanted) are capable to monitor cancer cells in the human body enabling physicians to continually diagnose tumors without biopsy.

1.1.2.1.2 Sport and Entertainment

In this area of application WBANs deal with physiological analysis (e.g. heartbeat, blood oximetry, posture), control of rehabilitation efficiency and motion capture where users gather information concerning their sport activity. Tuning of the training schedules of athletes, performance improvement and prevention of injuries related to incorrect training are some other applications in this area.

An entertainment application is the tracking of the position of different parts of the body. The real-time information gathered in this way allows users to use its body as a controller in videogames. Motion capture is also used by film industry to realize highly realistic digital movies.

1.1.2.1.3 Military and defense

Monitoring vital parameters, providing of information about the surrounding environment due to threats avoidance, collection of information at squad level to make able better coordination of the squad actions and tasks, battle readiness or assessing soldier fatigue are some military and defense applications of wearable WBANs. Inter-WBAN communication, means communication between WBANs, spatial localization techniques, and a secure communication channel in order to prevent ambushes are important issues for this application area. Policemen and fire-fighters can also use wearable WBANs to reduce the probability of injury on the one hand and on the other hand to improve monitoring and care in case of injury.

1.1.2.2 WBAN application requirements

The development of a WBAN is a quite challenging task because of the wide range of requirements by the applications they use them. In this section we describe the main requirements from the application point of view. Requirements with reference to a concrete standard (e.g. IEEE 802.15.1, IEEE 802.15.4, and IEEE 802.15.6) are described in the corresponding section of this work.

1.1.2.2.1 Power Consumption

Power consumption depends on the kind of application. Due to the fact that WBANs are battery-powered, the battery lifetime must be up to several years in particular for implanted devices. Requirements like power-wise MAC protocol design and ultra-low-power design for radio transceivers is essential. A technique to save power consumption is lowering the duty cycle. The devices fall then the most time in sleeping mode. This is the right technique for applications with no need of frequent transmissions. Despite of that a tradeoff between power consumption and delay must be found. Energy harvesting is an additional way to reduce the need of batteries.

Energy harvesting uses unconventional energy sources to power circuitry. Typically, a tiny energy source is converted to electricity and stored in a durable storage cell such as a capacitor, super capacitor, or micro energy cell (MEC), which is a form of lithium solid-state battery. The system generally includes circuitry to manage the power and protect the storage device and other circuitry. Sources of energy include light, captured by photovoltaic cells; vibration or pressure, captured by a piezoelectric element; temperature differentials, captured by a thermoelectric generator; radio energy (RF); and even biochemically produced energy, such as cells that extract energy from blood sugar [5]. In our case, in WBANs, body heat or human movements contribute to energy production.

1.1.2.2.2 Coexistence

The most WBANs operate in the license-free ISM band at 2.45 GHz which is a really overcrowded frequency band if we take into account that in fact Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15.1), IEEE 802.15.4/ZigBee and other standards operate with the same frequency band. This is a strong indication regarding challenges and chances. The challenge here is to take into account interference and to offer a WBAN system which will operate in a reliable way especially if applied in medical applications. The chance would be to use other nearby networks as relay networks to forward the information especially for delay-tolerant applications.

1.1.2.2.3 Antenna and radio channel

An important issue is the trade-off between the size of the antenna and its efficiency. Antenna design can be a very critical issue. Factors like the antenna body position could have immediate influence to

antenna's radiation and polarization characteristics. In order to design an antenna with proper radiation properties the choice of radio channel is crucial.

1.1.2.2.4 Security and privacy

Security, privacy and their implementation in WBANs are part of this work and they are considered in the second section of this work. At this point we want to underline that except privacy there are three factors security can be addressed to. These are confidentiality, authorization and integrity. An important reason for that is the use of WBANs in medical and military applications. Another important statement here is that due to the limited processing power of WBANs no conventional data encryption or authentication methods are suitable. Resource-efficient and novel lightweight methods are in demand like biometric identification based mechanisms.

1.1.2.2.5 Range and topology

The communication range of a WBAN is limited to a few meters. In detail topology considerations will be made in the single standard description parts of this work. A simple star topology is usually enough. In cases of implanted nodes where the human body act as an obstacle for radio propagation, multi-hop communication must be established. Association and disassociation procedures allow nodes to join or leave the network as required by the application.

1.1.2.2.6 Bit rate and quality of service

The bit rate in WBANs varies from 1 kbps to 10 Mbps depending on the data to be send and on the application. Interference avoidance and error correction should be implemented at medium access control (MAC) and physical (PHY) layer. Some other QoS issues are:

- end-to-end delay
- delay variation
- capacity to provide reliable reaction in case of emergency
- network traffic handling using priority levels

1.1.2.2.7 Device form

To fit the antenna and the battery into the device providing a good radiation property and lifetime is a critical aspect. Depending on the WBAN application device flexibility and strechability may also be relevant especially in military, sport and fitness.

1.1.2.2.8 Safety for the human body

Heating is the only issue regarding health-related effects for WBANs. General restrictions which guarantee health safety when the human body is exposed in electromagnetic fields are specified from ICNIRP, the International Commission on Non-Ionizing Radiation Protection. This restriction is concretized using the *Specific Absorption Rate (SAR)*. Specific absorption rate (SAR) is a measure of the rate at which energy is absorbed by the human body when exposed to a radio frequency (RF) electromagnetic field. Although, it can also refer to absorption of other forms of energy by tissue, including ultrasound. It is defined as the power absorbed per mass of tissue and has units of watts per kilogram (W/kg) [6]. Because low-power devices as WBANs do not radiate enough power for the whole-body only local SAR contemplation has to apply, measuring the SAR only in parts of the body most exposed to RF fields. Compliance with international or regional regulations must be taken into account.

1.1.2.2.9 Signal processing

Power efficient signal processing techniques can help to keep under control the power consumption in the whole process of biological signal acquisition and processing. *Compressed sensing (CS)* for example is a technique allowing to sample a sparse analogue signal at a sub-Nyquist rate, having as result energy saving without loss of information contained in it. The Nyquist rate is a lower bound for the sample rate for alias-free signal sampling [7]. WBANs for EEG, ECG and EMG apply CS and have low-power consumption by reducing the amount of data to be transmitted. CS can compress the data up to the factor 16.

2 MEDIUM ACCESS CONTROL (MAC) STANDARDS FOR WIRELESS BODY AREA NETWORKS

The medium access control (MAC) protocol is implemented in the data link layer of the ISO-OSI protocol layer model (Figure 6) and it is primarily responsible for regulating access to the shared medium.

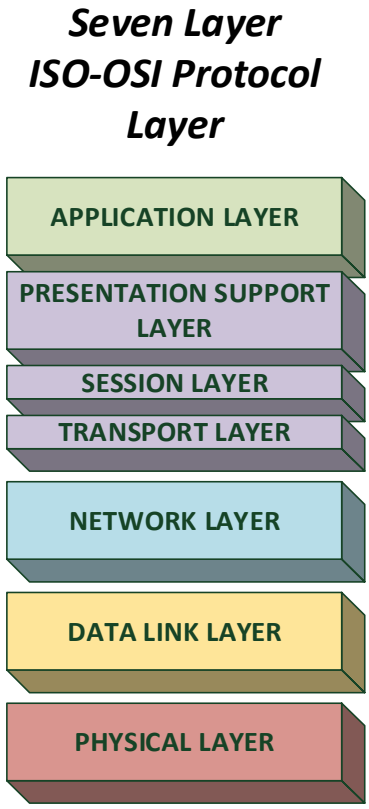


Figure 6 Seven layer ISO-OSI protocol layer

In chapter two of this work we describe the existing MAC standards for wireless body area networks. Chapter two is the biggest chapter of the work and we give an outline of what will be presented. In section 2.1 we present the MAC functionality and MAC services in a WBAN. In section 2.2 we analyze the Multiple Access Techniques are used in WBAN technology e.g. TDMA and CSMA/CA. In section 2.3 we start we the standards description with the first proposed standard for WBANs, the IEEE 802.15.1 standard or Bluetooth. After that we describe the Bluetooth Low Energy (BT LE), that is a special configuration - the ultra-low-power consumption configuration - of Bluetooth technology. [8] In section 2.4 we present the next standard defined for LR-WPANs, the IEEE 802.15.4 standard. The IEEE 802.15.4 standard published in 2006 and specifies the physical (PHY) and medium access control (MAC) layers for short-range wireless communications having as goal to support low-power, low cost and low bit rate networks. Nowadays IEEE 802.15.4 is the de-facto standard for WSNs. Section 2.5 analyzes the IEEE 802.15.4a standard, the most adopted standard for UWB-based MAC implementations. In section 2.6 we describe the IEEE 802.15.6 standard. We treat it in detail and consider it as our focus, the

centerpiece of the work. The IEEE 802.15.6 standard published in 2012 designed for wireless communications in the vicinity of, or inside a human body. The 802.15.6 task group recognized that existing standards did not fully fulfill existing medical and communication regulations and WBAN application requirements. Section 2.6 describes inter alia the defined MAC frame formats and the MAC functions. Section 2.7 examines MAC protocols for Cognitive Radio Body Area Networks. In section 2.8 we explore a new and very exciting area for MAC standards for WBANs, the Smart Body Area Network MAC. In section 2.9 we see into some MAC protocols defined in the scientific community or are in use in WBAN applications. One of them is the IEEE 1902.1 (RuBee) standard that applies in modern military applications. In section 2.10 we refer to the existing industrial hardware and devices (nodes and hubs) which could be used to implement various applications. In section 2.11 we compare the described standards together. In section 2.12 we refer to the MAC challenges for WBAN networks.

2.1 MAC Functionality and Services in a WBAN

Traditional MAC protocols can be broadly classified into

- *scheduled-* or *reservation-based MAC protocols* and
- *contention-based MAC protocols*

Schedule- or reservation-based MAC protocols arrange an assignment that devices with wireless communication capabilities (e.g. nodes/hubs) can follow for accessing the physical medium to avoid collision. Schedule based MAC protocols are divided into

- *synchronous schedule based MAC protocols*
- *asynchronous schedule based MAC protocols*
- *hybrid schedule based MAC protocols*

Synchronous schedule based MAC protocols need network topology information and time synchronization to guarantee communication of nodes/hubs which are active simultaneously.

Duty cycling is a technique where active nodes/hubs periodically turn their radio off and go to sleep.

Asynchronous schedule based MAC protocols trigger or initiate communication between nodes/hubs in different active cycles.

Contention-based MAC protocols do not need an assignment to be followed for collision avoidance. They define a backoff algorithm for devices to follow, when a collision occurs by access of the physical medium. They eliminate the overhead of time synchronization or network topology information. Data send immediately and retransmitted in case of collision. An additional approach here is to sense the physical medium and if it is idle to transmit the data.

2.2 Multiple Access Techniques

Before starting with the analysis of the MAC protocol standards for WBANs we will provide a short introduction into multiple access techniques. Channel access mechanisms provided by MAC sublayer are also expressed as multiple access techniques. These enable several stations connected to the same physical medium to share it. There are two important techniques used in WBANs. The *Time Division Multiple Access (TDMA)* and the *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)*. A comprehensive overview to this accessing techniques is given in Table 2. *Frequency Division Multiple Access (FDMA)* is not used because of the complexity of its hardware. *Pure ALOHA* and *SLOTTED Aloha*

are not used (with some exceptions as we see later) because of high packet drop rates, high rate of collisions and low energy efficiency.

Technique	Features	Advantages	Disadvantages	Application	Synchroni-zation required	Modulation scheme /technique	Probability of collision
TDMA	Divides radio spectrum in time slots	Flexible bit rate	Wide timing synchronization	Analog and digital systems	Yes	DQPSK, GMSK and GFSK	Low
FDMA	Transmit simultaneously and continuously	Reduced information bit rate	Precise filtering	Analog systems	Yes	FSK and FM	Low
CSMA/CA	Carrier sensing with collision avoidance	Avoids data collision	Inappropriate for large/active networks	802.15.4 (WPAN)	No	DSSS and FHSS	Interme-diate
Pure ALOHA	Sends data without sensing medium	Adaptive to varying number of stations	Requires queuing buffers for retransmission	Ethernet standard based on the ALOHA network/UMTS	No	N/A	Very high
S-ALOHA	Divided into time slots	Doubles the efficiency of ALOHA	Requires synchronization and queuing buffers	It is used in different frequen-cies with the same radio front-end	No	GMSK	High

Table 2 Multiple access techniques

2.2.1 Frequency division multiple access (FDMA)

In FDMA each channel is assigned only to one user at a time. FDMA can be used with digital and analog signals. FDMA is usually implemented in narrowband systems and it is a basic technology in the analog Advanced Mobile Phone Service (AMPS) where a FDMA bandwidth of 30 KHz is implemented. AMPS is the most widely-installed cellular phone system in North America.

2.2.2 Time Division Multiple Access (TDMA)

In TDMA the time frame is divided in dedicated time slots. Each device, e.g. node, transmits its data in rapid succession in its own time slot sharing the same frequency channel. After the transmission the node falls into an inactive state, this lead to the complete avoidance of idle listening as well to less collisions. This means less energy use than other techniques. For the same reasons as before TDMA protocols are more power efficient than other multiple access protocols (nodes in inactive state). Figure 7 shows a flow chart for TDMA and FDMA. The synchronization showed on the right part of the flow chart is done between the node and the hub. The node checks for its own time slot and it sends its data packets only during this time slot. Otherwise, it waits till its time slot comes. If no data is there to transmit, communication terminates.

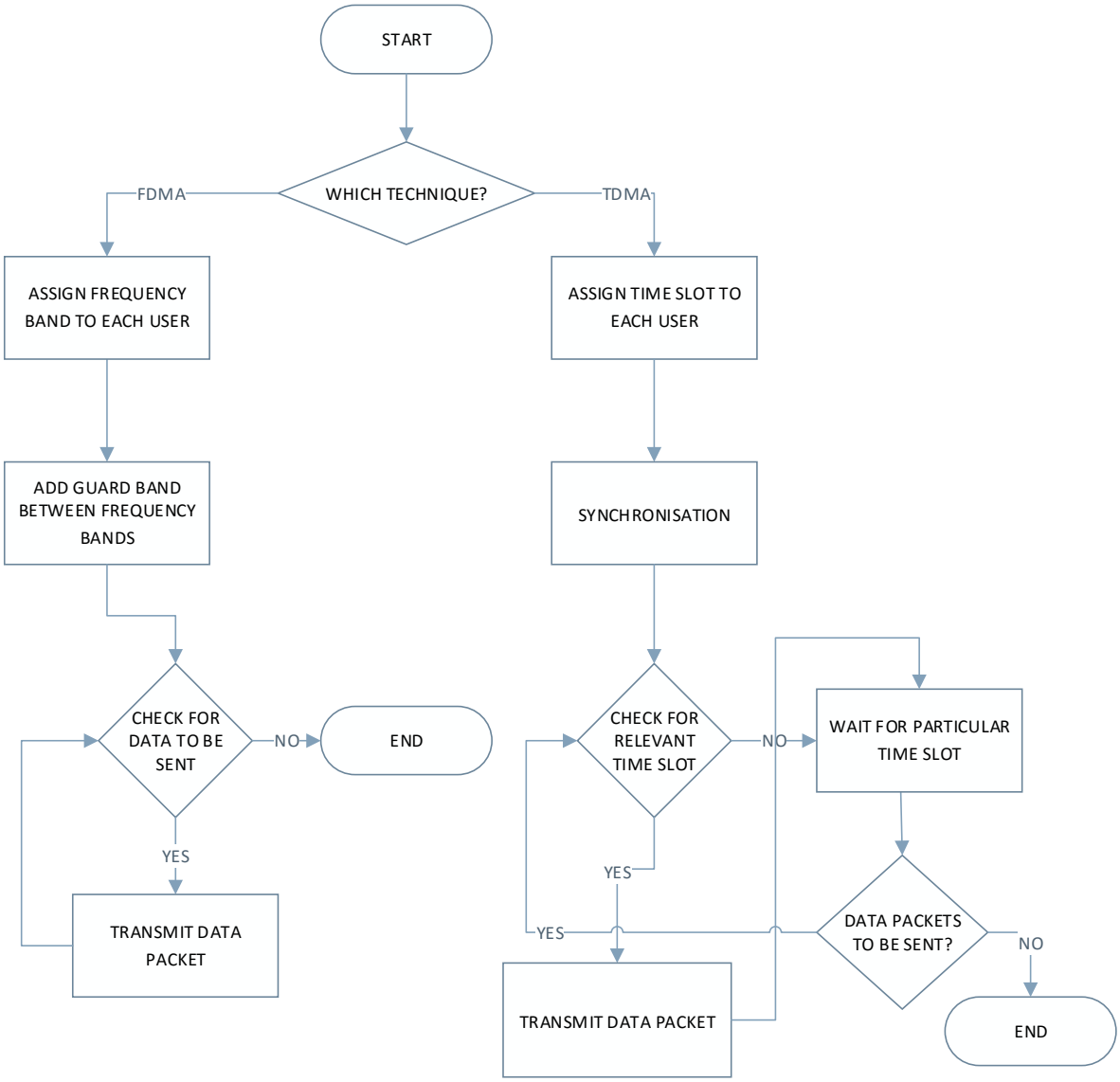


Figure 7 FDMA and TDMA flow chart

2.2.3 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

In the simple CSMA version if a node wishes to transmit a data packet it senses the medium if it is idle. If the medium is idle for a given period, the node transmits the data without to consider if any other nodes transmit already their data. This leads in collision. CSMA/CA improves the probability of collision. CA is the abbreviation for collision avoidance. CSMA/CA is an extension of CSMA. CA provides performance to CSMA through disabling the transfer of data for a specific node if other nodes are transmitting. CSMA/CA tries to avoid collisions.

Within the CSMA/CA protocol, MAC has two operation modes, the *Distributed coordination function (DCF)*, which allows multiple access, and the *Point coordination function (PCF)* which characterized by polling-based priority access. PCF is not used in practice and we will not mention it further. We will describe the DCF operation mode which consists of a basic access mode described by the basic CSMA/CA access algorithm and an optional RTS/CTS access mode, described by the CSMA/CA RTS/CTS access algorithm. CSMA/CA consists of:

a) Basic CSMA/CA access algorithm
b) Hidden station problem
c) Exposed station problem
d) A CSMA/CA RTS/CTS access algorithm (with congestion avoidance (CA))

2.2.3.1 Basic CSMA/CA access algorithm

The basic CSMA/CA algorithm consists of three parts, the sender, the receiver and the backoff part. Before we describe the algorithm we will address some declarations:

- The *contention window (CW)* is in units of slot time
- *DIFS* is the *Distributed Inter Frame Space*
- *SIFS* is the *Short Inter Frame Space*, which is used to give priority access to ACK packets (receiver)
- *BO* is the *Back-Off* variable within one CW
- *ACK is an acknowledgment*, which confirms the correct reception of the packet
- The *extended Inter Frame Space (EIFS)* interval is used if the sender node does not receive an ACK due to collision or transmission errors. In this case the sender node reactivates the backoff algorithm after the channel remains idle for an EIFS interval

The algorithm flow is as follows:

sender

- MAC (the firmware in NIC) receives a frame from an upper network layer
- go to backoff function
- transmit the frame (backoff is 0) /* this is the return point of backoff */
- wait for the ACK of the receiver
- if timeout, go to backoff function

receiver

- is the received frame OK?
- if yes, wait for SIFS time
- transmit ACK

backoff

- if due to a timeout, double CW
- else wait until channel is idle plus an additional DIFS /* channel is idle at minimum for DIFS */
- select a random waiting time between [1, CW]
- decrement CW by 1 when channel is idle
- return if CW = 0 /* next task is the immediately transmit of the frame */

The next Figure 8 shows the timeline for sender and receiver without collision.

Timeline without Collision:

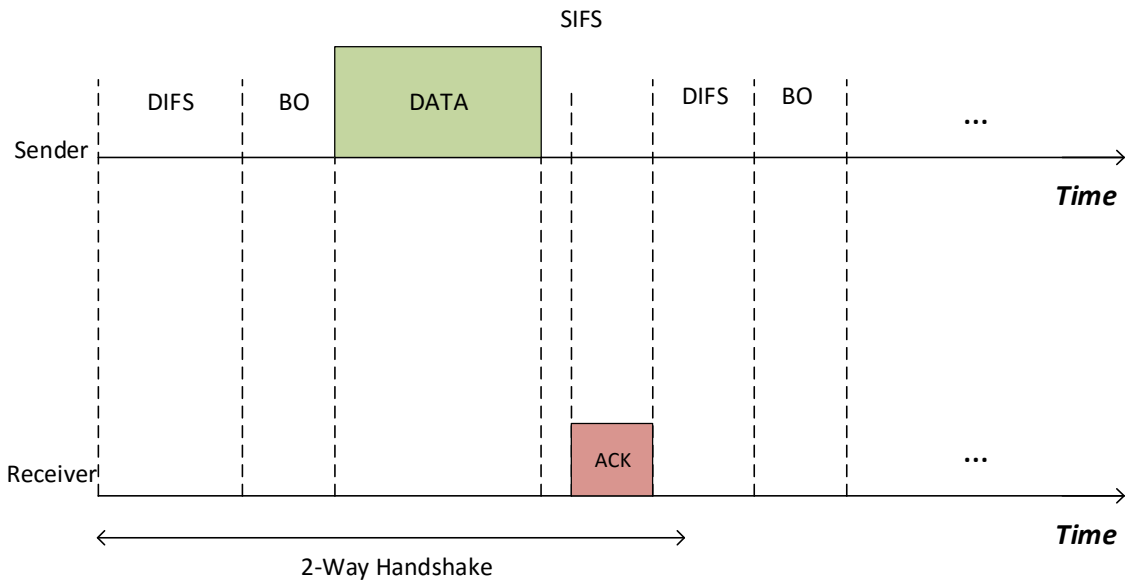


Figure 8 Example of a basic CSMA/CA access without collision

For the first attempt to transmit the frame the CW equals the initial contention window size CW_{min}. If the transmission was not successful, CW is doubled. The maximum allowed value for CW is the maximum contention window size CW_{max}. If the transmission was successful or if the retransmission number of the frame reaches the limit L_{retry}, CW would be reset to $CW_{min.}$ In the backoff function, if the channel becomes busy again, the node freezes its backoff countdown process and begin again if the channel is idle for DIFS time.

In the following Figure 9 we see a time snapshot with collision. The collision exists between the transmitters Sue and Mira.

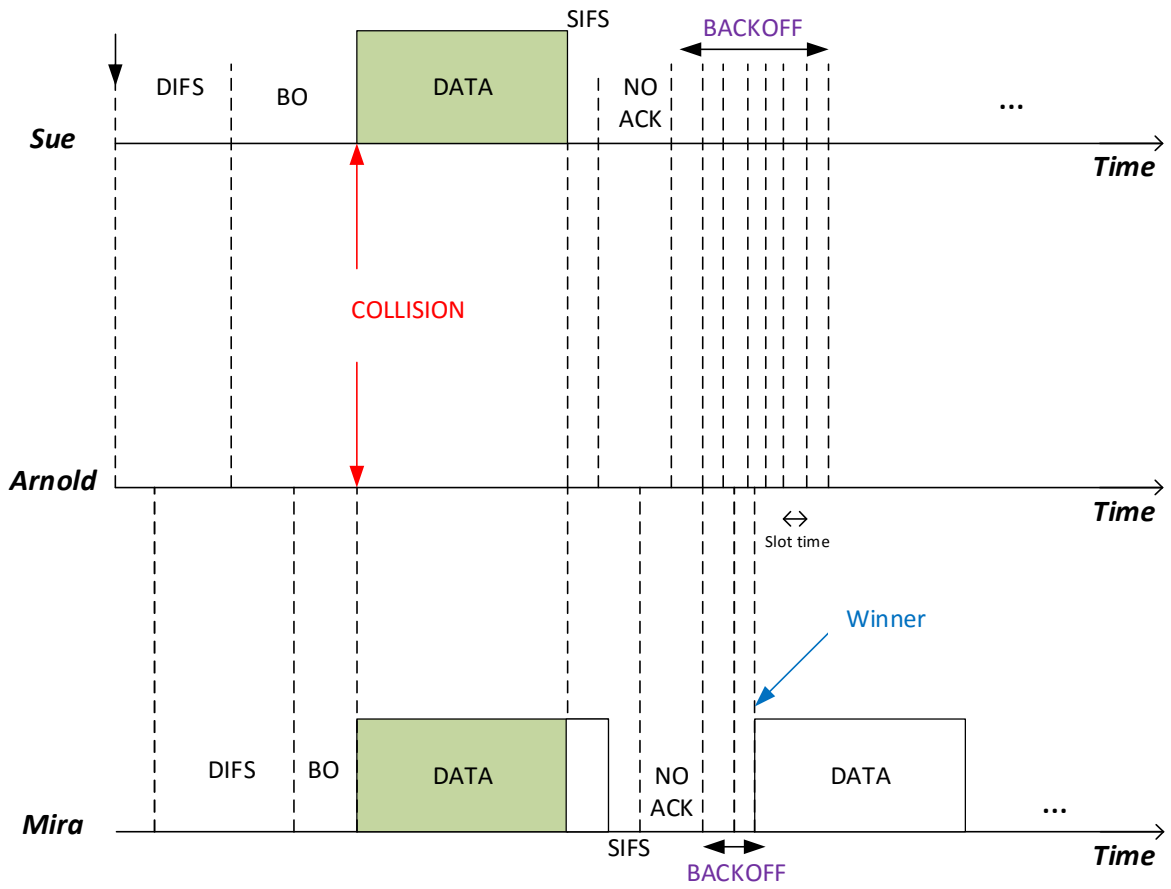


Figure 9 CSMA/CA Collision use case

2.2.3.2 Hidden station problem

The hidden station problem is described as follows (Figure 10):

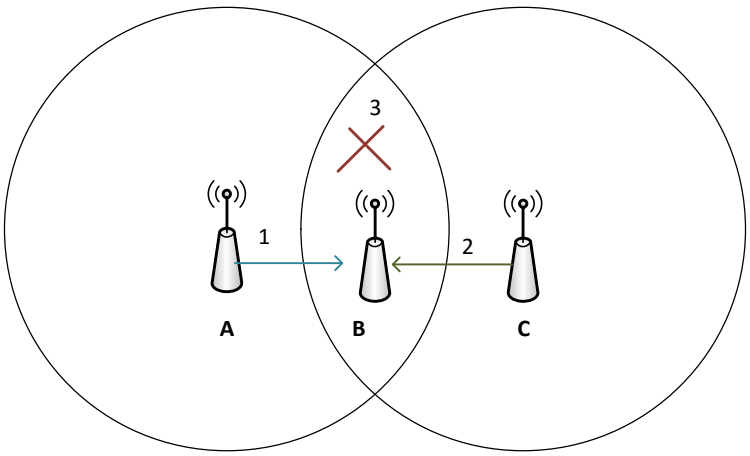


Figure 10 Hidden station problem

- Transmitter A transmits data to B
- Transmitter C does not sense transmitter A
- Transmitter C transmits to B
- At transmitter B occurs interference

The solution to this problem is described in the section 2.2.3.4 (A CSMA/CA RTS/CTS access algorithm).

2.2.3.3 Exposed station problem

The exposed station problem is described as follows (Figure 11):

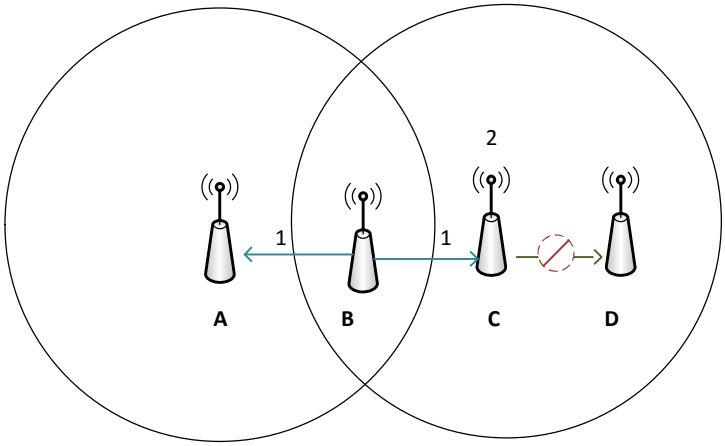


Figure 11 Exposed station problem

- Transmitter B transmits data to transmitter A
- Transmitter C would like to transmit to D but senses B
- Transmitter C refrains from transmitting to D

The solution of this problem is described in the next section.

2.2.3.4 A CSMA/CA RTS/CTS access algorithm (with congestion avoidance (CA))

The solution to the hidden station problem and the exposed station problem is *congestion avoidance*. Congestion avoidance includes a *Request To Send (RTS) / Clear To Send (CTS)* reservation handshake. Before the data transmit a RTS/CTS handshake is performed. Figure 12 shows the timeline for a transmission and receipt using CSMA/CA RTS/CTS.

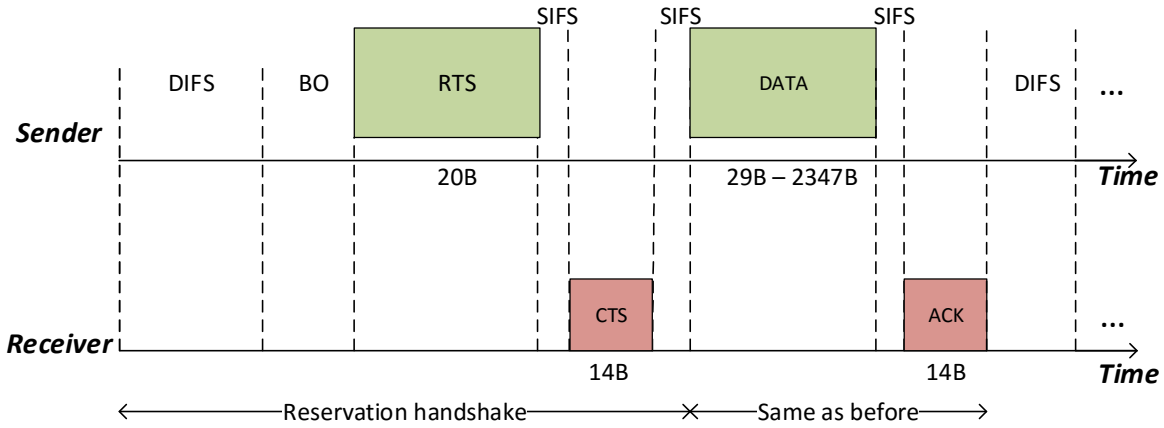


Figure 12 An example for transmitting and receiving with CSMA/CA RTS/CTS

Carrier sensing is done in the following two ways:

- *Physical carrier sensing* which detects the activity on the radio interface
- *Virtual carrier sensing* which is used by the DCF RTS/CTS access mode

The virtual carrier sensing is implemented through transmission of duration information in the header of the RTS and CTS packets. This duration information is the indication of the amount of time the medium is reserved for data transmitting and acknowledgement. Every node or station in the same *basic service set* uses this information to update its *network allocation vector (NAV)*. A *basic service set* are a collection of nodes that have recognized each other. For this period of time every other node which does not use the medium, must defer in accessing the medium. Using virtual carrier sensing all nodes of the same basic service set learn how long the channel will be in use for data transmission. NAV is decremented by clock. If NAV > 0, then do not access even if the physical carrier sensing says channel is idle.

Figure 13 shows a flow chart for CSMA/CA.

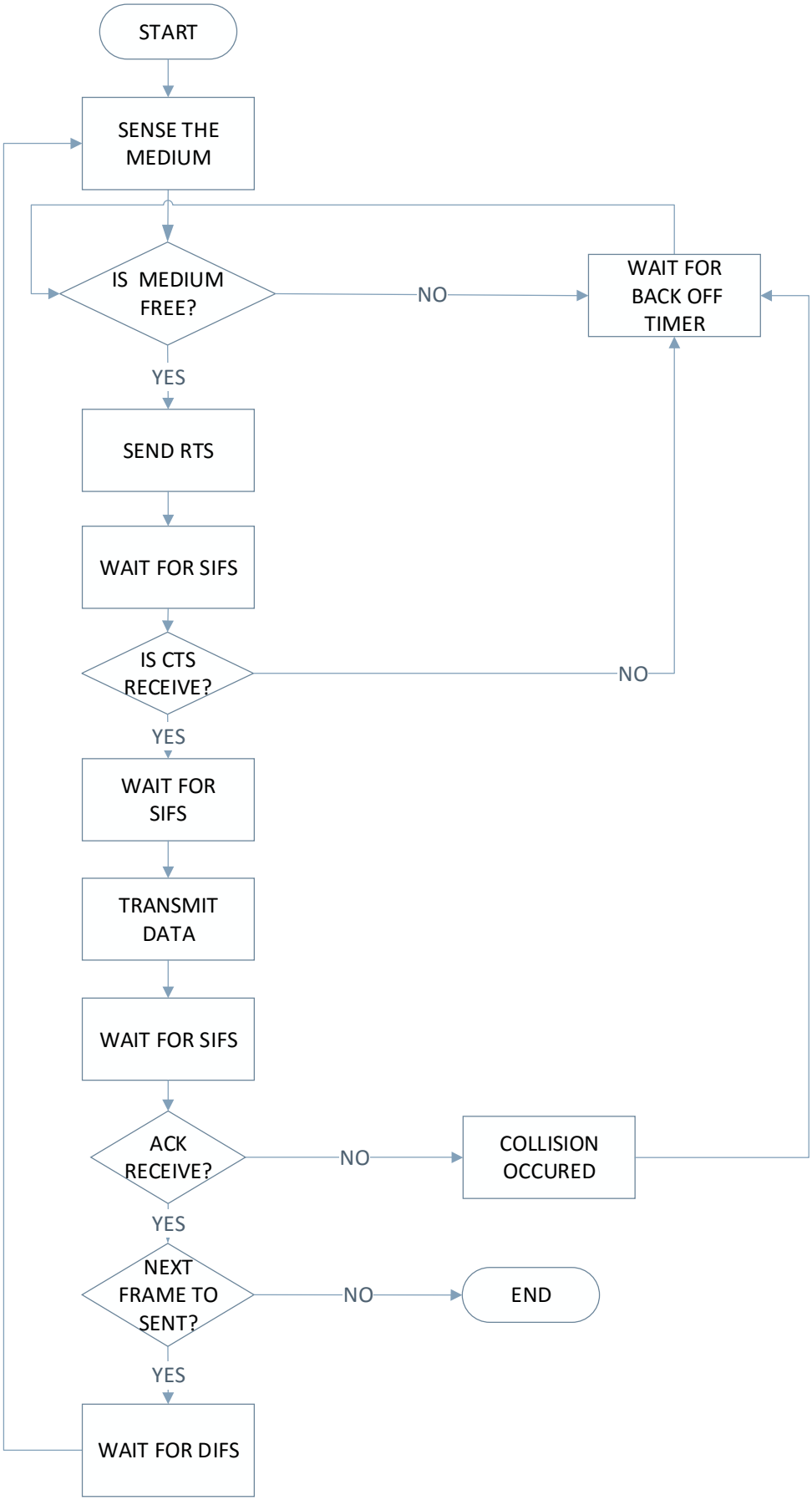


Figure 13 CSMA/CA flow chart

As mentioned above CSMA/CA RTS/CTS solves the hidden station problem. The RTS/CTS handshake "clears" the hidden area. As shown in Figure 14 the node C may not be able to receive the RTS from the sending node A, will hear the CTS from the receiving node B and in this way the channel will be reserved for the transmission from node A to node B.

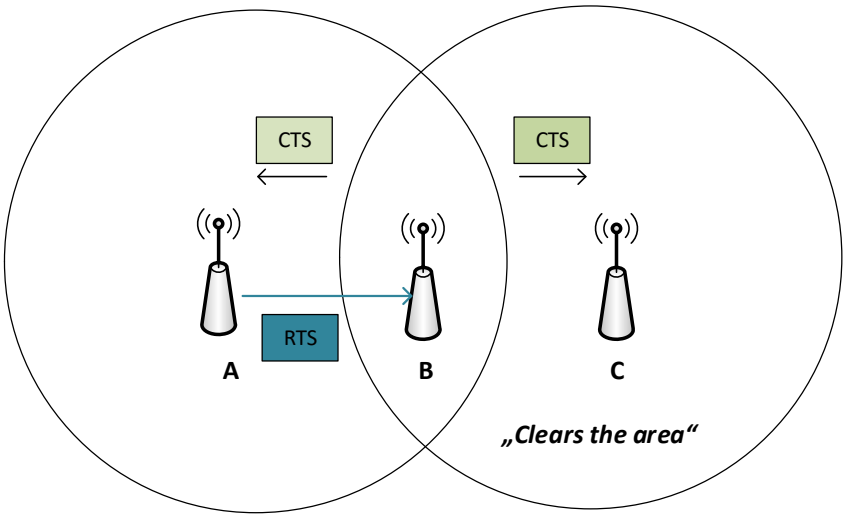


Figure 14 RTS/CTS handshake

Prior to the data transmission, the sending node A will send a RTS packet as announcement of the upcoming transmission. After the destination node B receives this RTS packet, it will send a CTS packet after a SIFS time interval. Both packets, the RTS and CTS, are short control packets. The sender A is allowed to transmit its data only after it has successfully received the CTS packet. The RTS/CTS handshake helps avoiding long collisions.

2.2.4 Pure ALOHA

Pure ALOHA is a contention-based protocol. It does not guarantee a successful transmission and uses a random access method to transmit data. Without delay after the generation of a frame, the frame is transmitted. The transmission is successful or otherwise a collision occurred. In case of collision the transmission of the frame was unsuccessful. The sender node can always find out if its frame was destroyed by listening to channel. After a random period of time the sender re-transmits its frame.

2.2.5 Slotted ALOHA

Slotted ALOHA is a variant of pure ALOHA. The channel is divided into time slots of equal length greater or equal to average frame duration. The frame transmission is allowed to start at the beginning of a time slot. Figure 15 shows a flow chart of pure ALOHA and slotted ALOHA. ALOHA is simple to implement but the efficiency is low.

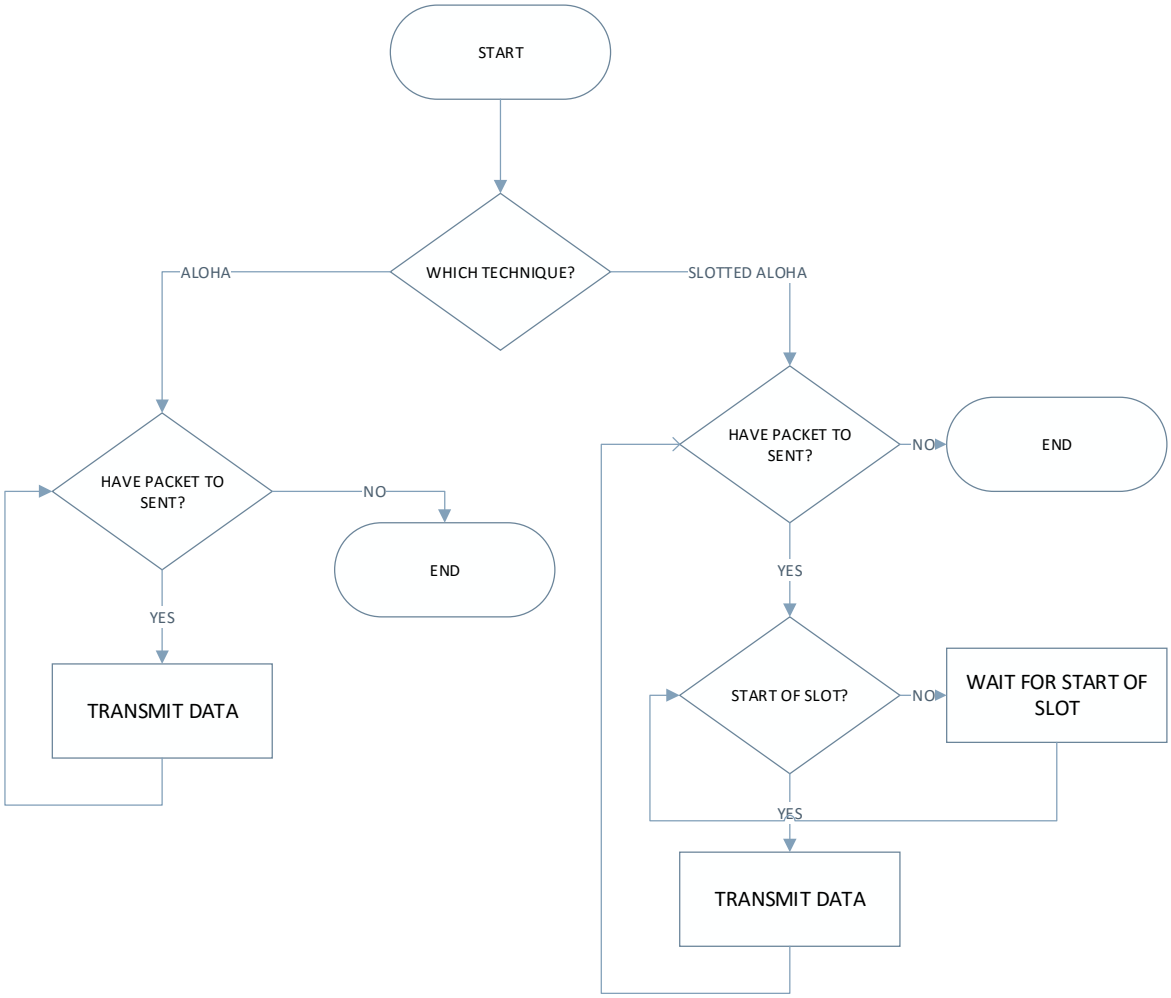


Figure 15 Flow diagram for Pure ALOHA and Slotted ALOHA

2.3 IEEE 802.15. 1 STANDARD (BLUETOOTH)

Bluetooth technology is a short range wireless communication standard. It is also known as IEEE 802.15.1 standard. Its key features are robustness, low-power consumption and low cost. Bluetooth is used for connecting a variety of personally carried devices supporting voice and data applications. Up to eight Bluetooth devices form a short-range network called piconet. In a piconet the involving devices are synchronized to a common clock and hopping sequence at the same physical channel. Piconet consists of a master device. All other devices are slave devices and are synchronized by using the master device clock which is identical with the Bluetooth clock. The described topology here is a star topology (Figure 18). Bluetooth devices operate in the 2.4 GHz ISM band. They utilize frequency hopping among 79 Bluetooth channels which are 1 MHz wide at a nominal rate of 1,600 hops/sec to reduce interference. The Bluetooth standard specifies three device classes. They differ in transmission power and corresponding coverage ranging from 1 to 100 meter.

There exist two main core configurations of Bluetooth technology systems: The *Bluetooth basic rate (BT BR)*, with optional *Bluetooth Enhanced Data Rate (BT EDR).* BT BR as the "classic" Bluetooth introduced a bit rate up to 3 Mbps with BT EDR.

Upcoming applications for the wireless and semiconductor markets led to new standardization activities. One of them is the ultra-low-power extension of Bluetooth. This is the second main core configuration, called the *Bluetooth low energy (BT LE)* configuration. BT LE belongs together with IEEE 802.15.4 and IEEE 802.15.6 to the main solutions considered as reference for the development of WBANs. BT LE was defined in the latest BT core configuration in June 2010. BT LE has as target applications for small and inexpensive devices powered by button-cell batteries, such as wireless sensors. These products characterized by lower current consumption, transmission range up to 30 meters, lower cost and lower complexity than BT BR and BT EDR. BT LE is also specified for applications with low duty cycles and bit rates.

Some of the applications of BT LE are:

- Automotive: parking assistant, keyless entry, tire pressure monitoring
- Home automation and entertainment: remote controls, home sensor and switches
- Watch/wrist wearable devices: proximity detection, mobile phones and music player remote controls
- Sports and fitness: speedometer, heart rate meter, pedometer, sport equipment and monitoring devices
- Healthcare and illness treatment: glucose meter, pulse oximeter, blood pressure monitor, weight scale

As is BT BR in BT LE the star topology is the only possible topology. Bluetooth LE specifications define the whole protocol stack. There are two implementation options defined for BT LE. The *single-mode* and the *dual-mode* option. The single-mode applies at applications which require low-power consumption and small size. The dual-mode applies at mobile phones and PCs.

BT LE uses the Gaussian frequency shift keying (GFSK) modulation. The supported bit rate is 1 Mbps and it operates in the 2.45 GHz band. There are defined 40 channels with a 2 MHz bandwidth for each of them.

Bluetooth is a well-known and widespread technology. For these reasons it could be useful for WBANs. Mobile phones and tablets are equipped with dual-mode BT radio and also some monitoring devices using BT LE (e.g., heart rate belts) are already in the market.

The main drawbacks of BT are:

- limited scalability due to the restriction to use only star topology
- the lack of multihop communication

2.4 IEEE 802.15.4 Standard for Wireless Personal Area Networks (LR-WPANs)

The IEEE 802.15.4 standard developed for the design and implementation of Low-Rate Wireless Personal Area Networks (LR-WPANs). It specifies the physical layer and medium access control (MAC) for LR-WPANs and it is maintained by the IEEE 802.15 working group [9]. Low cost, low-power consumption, low data (bit) rate transmissions and low complexity are its key features. These key features are supported or implemented by inexpensive fixed or mobile devices [4] [10]. The main application field of the technology defined with the IEEE 802.15.4 standard is the implementation of wireless sensor networks (WSNs) and the implementation of the first generation WBAN for medical and health monitoring applications [11].

On the left side of Figure 16 the diagram shows the Open System Interconnection (OSI) model which defines a networking conceptual framework to implement protocols in seven layers. The right side of the same figure shows the wireless networking protocol stack model.

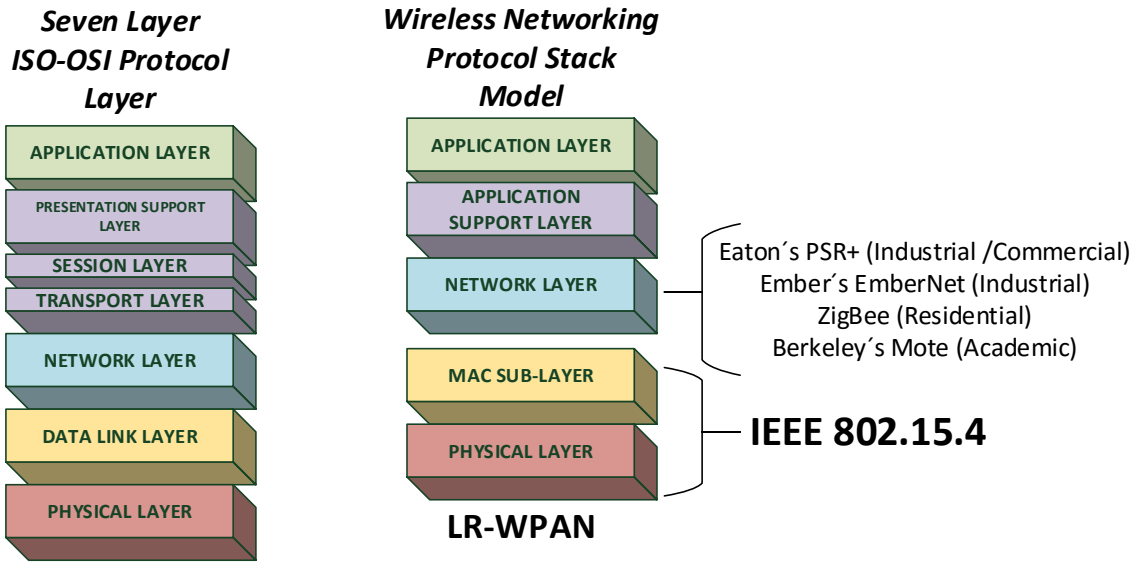


Figure 16 OSI protocol layer and wireless networking protocol stack model

Figure 17 shows the protocol architecture of IEEE 802.15.4. Its parts are the PHY layer for 868/915 MHz and 2400 MHz, the MAC sublayer, the IEEE 802.2 Logical Link Control (LLC), and other LLCs.

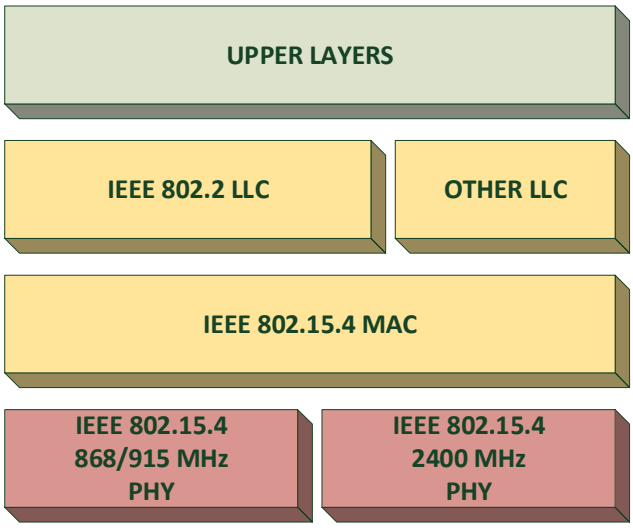


Figure 17 IEEE 802.15.4 protocol architecture

IEEE 802.15.4 defines two device types. The *full-function device (FFD)* and the *reduced-function device (RFD)*. FFDs are all the devices which take the role of the *coordinator* (hub), the *PAN coordinator* or a router. FFD is equivalent to a dual mode chip.

A *coordinator* is an FFD with network device functionality that provides coordination and other services to the network.

A *PAN coordinator* is a coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator. In a WBAN a hub can take the role of a PAN coordinator.

RFD are devices implemented with minimal memory capacity, minimal resources and for extremely simple applications. RFD can only act as an end device. It is equivalent to the standalone chip in Bluetooth Low Energy.

2.4.1 Topology

Two topologies are supported from IEEE 802.15.4. The star topology and the peer-to-peer topology (Figure 18).

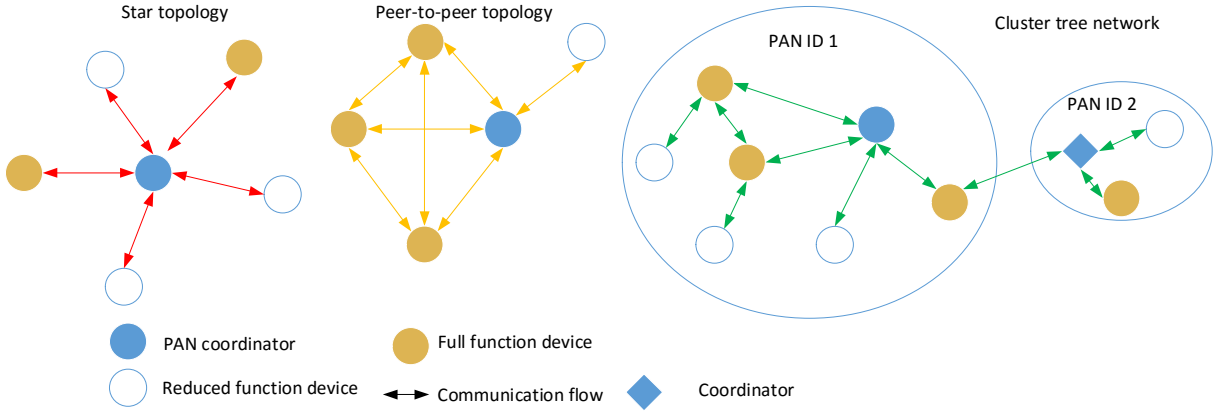


Figure 18 IEEE 802.15.4 topologies and their use

The star topology, which will typically operate in a WPAN configuration, consists of FFDs and RFDs. One of the FFD takes the role of the PAN coordinator which is the central controller of the LR-WPAN and all communication goes through this central controller.

As the name suggests in the peer-to-peer topology, which can support a multi-hop network, each device can communicate with each other device if there are in the communication range of one another. The range can be extended by incorporating the mesh network architecture using the configuration. In contrast to the typical peer-to-peer model in which the interconnected nodes (peers) share resources amongst each other without the use of a centralized administrative system the IEEE 802.15.4 standard specifies the use of a PAN coordinator for choosing the PAN identifier and manage the network.

Out of the peer-to-peer topology more complex network structures can be constructed. An example can be seen in the figure above. In this example, we see a multicluster tree where the PAN coordinator can advise a device to become the coordinator of the new cluster adjacent to the first one. In this way, new devices can connect the network and extend the coverage area of the network.

2.4.2 Communication methods

IEEE 802.15.4 defines two modes of operation. The *beacon-enabled mode* and the *nonbeacon-enabled mode*, which corresponds to two different channel access mechanisms.

In the nonbeacon-enabled star topology, the coordinator or the PAN coordinator remains awake and does not transmit any beacon. Connected devices e.g. nodes do not need to be synchronized. They communicate with the PAN coordinator (send or request data) in a contention-based way using the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Contention is a media access method that is used to share a broadcast medium. In contention, any instance in the network (e.g. computer) can transmit data at any time (first come-first served) [12]. The advantage of the non-beacon mode is that the nodes do not need to regularly power-up to receive a beacon. The disadvantage is that the coordinator cannot start communication with the nodes, but the nodes must poll the coordinator.

In the nonbeacon-enabled peer-to-peer topology, the communication devices must keep permanently their radio on or otherwise some communication mechanisms must be applied.

The beacon-enabled mode provides a superframe structure. The access to the channel is managed through the superframe. This aims to facilitate low-power operation. In the communication process the PAN coordinator transmits beacons periodically. The transmitted beacons identify the PAN. A PAN is identified by a 16-bit PAN identifier. In this way all devices associated with the PAN coordinator are synchronized (by the beacons). The beacon frame contains a list of outstanding frames and other system parameters. The time period between two consecutive beacons is constant. Its value can be parameterized by the user as a multiple of 15.38 ms with maximum value 252 ms. Figure 19 is showing the IEEE 802.15.4 superframe structure. A superframe is separated by 16 time slots. All 16 slots have the same size. The superframe comprises an active and an inactive part. The active part consists of the *contention access period (CAP)* and the *contention-free period (CFP)*. Contention-based transactions must take place and completed in the CAP. CFP is reserved for applications which require specific data bandwidth, for low-latency applications or high priority data traffic. If a device wants to communicate with the PAN coordinator it requests a *guaranteed time slot (GTS)*. The PAN coordinator can allocate up to seven GTSs. A GTS can occupy more than one slot period. The inactive part of the superframe allows the nodes to go into the sleep state.

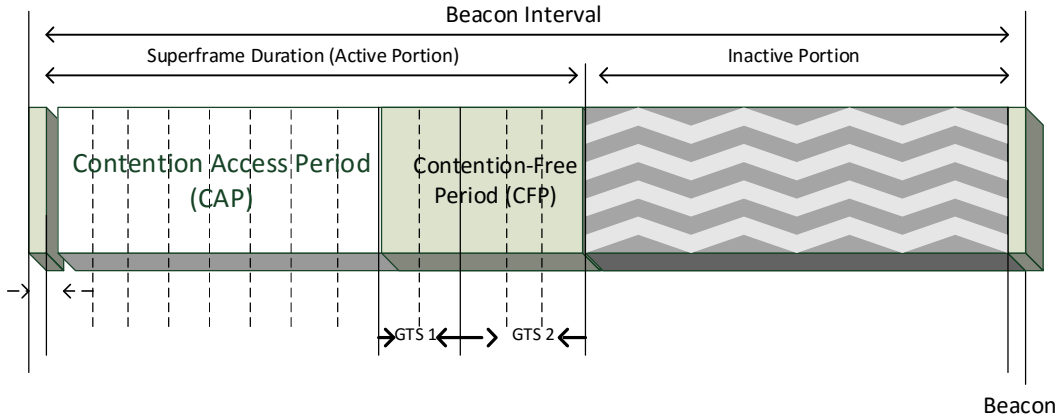


Figure 19 An example of an 802.15.4 superframe structure

The length of the active and inactive part is configurable. This flexibility allows the accommodation of different types of applications. The CAP slots are accessed using CSMA/CA. The GTS slots can be accessed if they are allocated by the coordinator after a node request. The request contains information (a flag) that indicates if the slot will be used to receive or to transmit. By receiving a slot request the coordinator will allocate a GTS slot when resources are free. If the GTS slots are used for transmission a node can schedule its sleep cycle and wakes up just before the slot starts and sends (the node) the packet. The node must wake up in advance if a CAP slot is used. The reason is that the node must perform carrier sensing or another collision avoidance procedure before it can start the transmission. Regardless of whether the data source is periodic or not (e.g. pulse or irregular heart), CAP slots can be used and support both kind of data sources. If high priority data from critical patients must be transmitted, GTS slots can be used. The use of the GTS slots guaranties the data transfer. Reliability can be improved using acknowledgment based connections. The IEEE 802.15.4 standard allows both access modes (access mode of the CAP slots and access mode of the GTS slots), to be configured using acknowledgment based connections.

Some key MAC sublayer features are shown in the Table 3.

Feature	Description
MAC protocol	CSMA/CA
Address	16-bit (short) or 64-bit (extended)
Transmission mode	Fully acknowledged mode
Energy detection	Yes, with the cooperation of the physical layer
Link quality indication	Yes, with the cooperation of the physical layer

Table 3 Key MAC sublayer features

There are some limitations of IEEE 802.15.4 regarding its GTS allocation:

- If nodes use a small piece of the allocated GTS, the major part of it will remain unused
- The protocol supports explicitly at maximum seven GTSs. In the case that different applications are active and if we take in consideration that one application can involve tens of sensor nodes (e.g. ECG), these applications may face a bandwidth scarcity problem
- A single node can request for all seven GTSs. This could result to an unbalanced slot distribution and other needful nodes in the same moment will be blocked
- The CAP size in the superframe is fixed. A WBAN needs specially for urgent scenarios a flexible size CAP
- The non-beacon mode is prone to collision and delay due to the fact that only random access is adopted for medium sharing

2.4.3 MAC Frames

Figure 20 shows the IEEE 802.15.4 MAC frame structure. Its main parts are the MAC header, the MAC service data unit, and the MAC footer. There are four types of MAC frames defined in the IEEE 802.15.4 standard:

- Data frame
- Beacon frame
- Acknowledgment frame

- MAC command frame

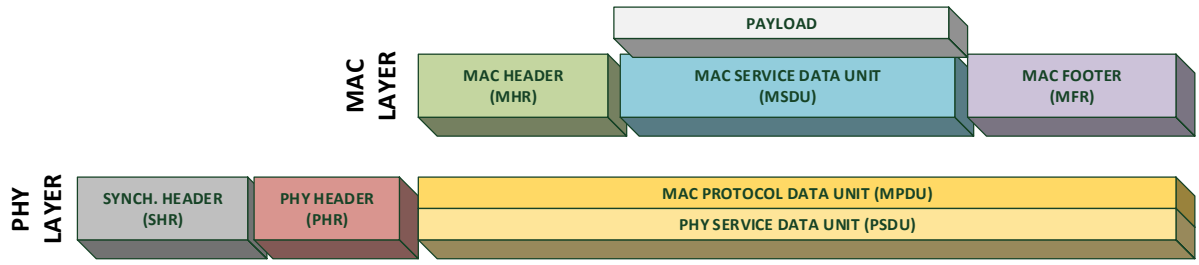


Figure 20 The IEEE 802.15.4 MAC frame structure

The IEEE 802.15.4 MAC sublayer handles the access to the physical radio channel. Its responsibilities are the follows:

1. beacon generation through the coordinator
2. node synchronization to the network beacons
3. supporting PAN association and disassociation
4. supporting coordinator and node security
5. handling channel access with either slotted or unslotted CSMA/CA
6. handling and managing GTS
7. defines the requirements for building a reliable link between two peer MAC entities

Data transfer can take place in three different ways.

- from a coordinator to a node
- from a node to a coordinator
- between two peer nodes

The control of the data transfer is incumbent on the nodes rather than by the coordinator. A node either polls the coordinator to receive data or transfers data to the coordinator. Both tasks happen with the application-defined rate.

2.4.4 IEEE 802.15.4 PHY Layer

Figure 20 in the previous section shows also the structure of the PHY layer. IEEE 802.15.4 specifies a total of 27 half-duplex channels across three frequency bands. A half-duplex system consists of two clearly defined channels and each party can communicate with the other but not simultaneously. Table 4 shows some of the key PHY layer futures of the IEEE 802.15.4 standard.

Frequency	868 – 868.6 MHz (Europe)	901 – 928 MHz (North America)	2.4 – 2.4835 GHz (World Wide)
Channel Bandwidth	0.3 MHz	0.6 MHz	2 MHz
No. of RF channels	1	10 (separation 2 MHz)	16 (separation 5 MHz)
Maximum data rate	20 kbs	40 kbs	250 kbs
Modulation technique	BPSK	BPSK	O-QPSK
Transmission power	1 mw (min)	1 mw (min)	1 mw (min)
BER requirements	< 1 %	< 1 %	< 1 %

Table 4 Key PHY layer futures of the IEEE 802.15.4 standard

2.4.5 ZigBee and IEEE 802.15.4

The origin of the name *ZigBee* can be found in wider sense Biology and Sociology and it has to do with the honey bee. Using a communication system, whereby a bee dances in a zig-zag pattern, worker bees are able to share information such as the distance and direction of a newly discovered food source to fellow colony members.

The *ZigBee Alliance* defines itself as follow: “The ZigBee Alliance is a global ecosystem of companies creating wireless solutions for use in residential, commercial and industrial applications. The ZigBee Alliance companies work together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard. The ZigBee Alliance membership comprises technology providers and original equipment manufacturers worldwide. Membership is open to all.”

As referred the IEEE 802.15.4 standard defines the medium access control (MAC) sublayer and the physical layer (PHY) specifications. From the ISO/OSI protocol stack point of view ZigBee builds up the network layer and the application layer on top of the IEEE 802.15.4 physical and data link layers. ZigBee inherits the radio frequency (RF) characteristics of IEEE 802.15.4, the RF link budget and the current draw. ZigBee defines a full protocol stack for LR-WPANs. The ZigBee stack architecture is shown in Figure 21.

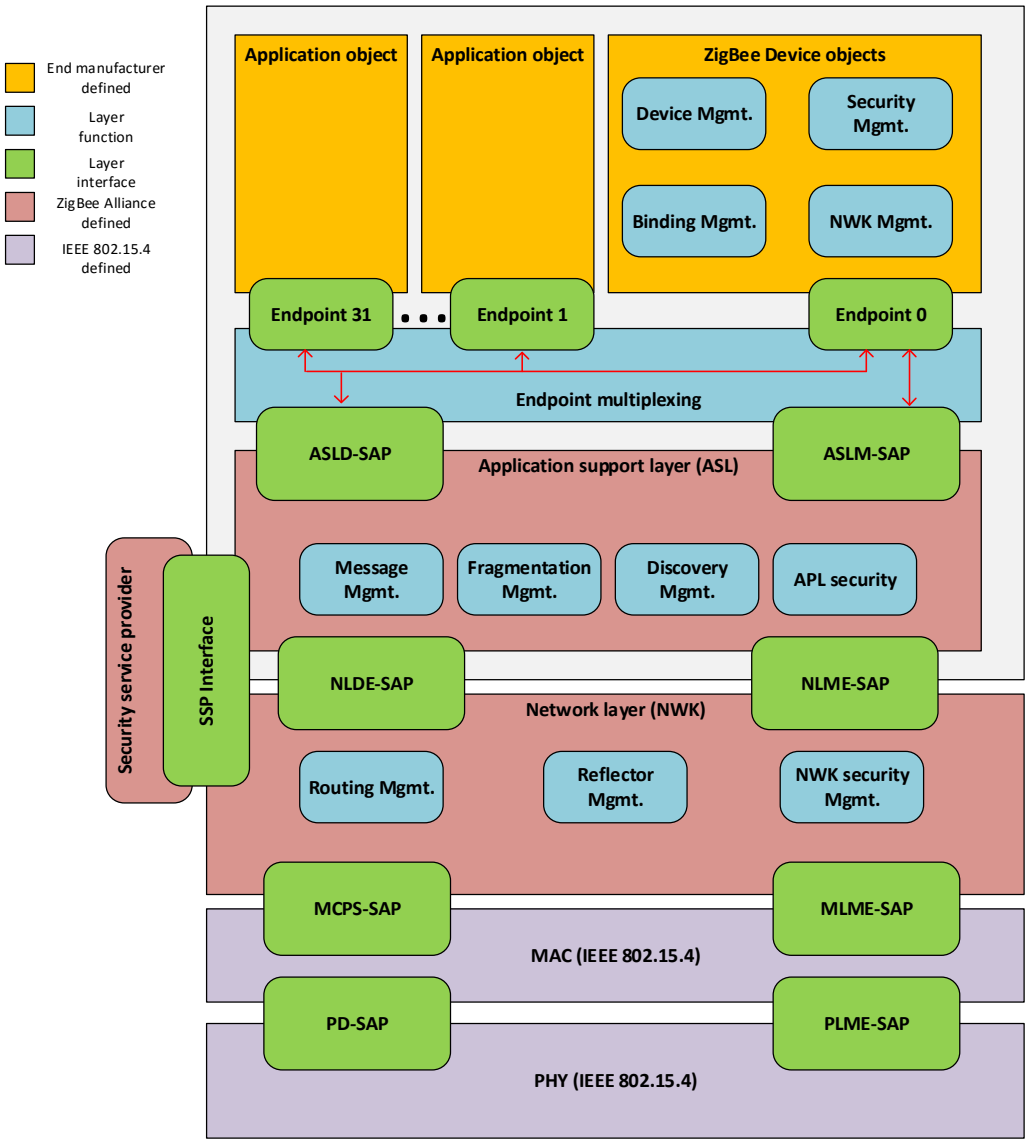


Figure 21 ZigBee stack architecture

It can be said that both technologies ZigBee and IEEE 802.15.4 are complementary and together they provide a complete set of operation principles for the implementation of distinct BAN applications. IEEE 802.15.4 is covering as standard the physical (PHY) layer and medium access control (MAC) sublayer targeting low-rate short-range radio-communications that is appropriate for BAN nodes. ZigBee enhances IEEE 802.15.4 by adding as we see in the figure above (red section) a network layer, an application support layer and a security layer. ZigBee enables in this way the development of wireless sensor network systems. ZigBee consists of a feature set. The features set of ZigBee at a glance is given in Table 5.

Feature	ZigBee Feature Set	ZigBee PRO Feature Set
Network Scalability	Easily supports networks of hundreds of devices	Advanced support for networks of thousands of devices
Frequency Agility	O	X
Fragmentation	O	X
Channel selection	X	X
Automated Device Address Management	X	X+
Group Addressing	X	X+
Wireless Commissioning	X	X+
Centralized Data Collection	X	X+
Device Maintenance & Network Recovery	X	X
Group Broadcasts	X	X
Compatibility	Devices can participate in ZigBee and ZigBee PRO networks	Devices can participate in ZigBee and ZigBee PRO networks
AES128 Encryption/Authentication/Trust Centers	X	X
IEEE 802.15.4 Physical Radio	X	X
Global Operation in 2.4 GHz plus 915 MHz Americas/868 MHz Europe	X	X
Single-hop Extended Range – up to hundreds of meters	X	X
Reliable Self-Healing Mesh Network	X	X
Ultra-Low Power, Long Battery Life	X	X
Low Cost	X	X
Network Traffic Load	Average	Increased

Table 5 Features of ZigBee (x-standard, +-optimized, O-optional)

ZigBee incorporates a number of public application profiles that enable the deployment of networks and systems with interoperable multi-vendor devices. The ZigBee Alliance defines the public application profile as follows:

„A public application profile runs on ZigBee devices and contains specific details about what information a device can communicate and how this device should interact with other devices on the ZigBee network “.

Profiles can be public or private/manufacturer specific. The *manufacturer application profiles (MAP)* are interoperable with other ZigBee devices at the networking layer (e.g. routing, joining, etc.). Manufacturer specific devices build for manufacturer specific or proprietary applications. They developed outside the ZigBee Alliance, they must use a ZigBee allocated profile identifier and before go live they must be tested to ensure they work well in the ZigBee network environment.

Public applications profiles (PAP) guarantee interoperability at the network, the application layer and at the device level. PAPs allow the implementation of more generic applications than the MAPs. They develop publicly within the ZigBee Alliance. This ensures a significant peer-review. Meanwhile the development of public application profiles is an established process within the Alliance defined by a Profile Lifecycle. This established process has the advantage that end products undergo certification.

The current application profiles come from the follow industry divisions:

Smart Energy

The smart energy profile is used by applications of metering data and energy management providing in this way efficient and reliable energy usage.

Telecom

The telecom profile can be used in telecom value-added services and supplementary services to enhance and fulfill telecom network functions.

Home Automation

The home automation profile is used in the residential automation market. Original equipment manufacturer produces products for customers ranging from „do it yourself "homeowners to professional installers.

Personal Home & Hospital Care (PHHC) profile

The PHHC profile is used by all devices which jointly cooperate under the umbrella of a non-invasive health care application.

Commercial building automation profile

The commercial building automation profile is used by applications targeted at commercial building environment.

Wireless sensor applications profile

This profile enables wireless sensors networks (WSN) applications including environmental monitoring, asset tracking and machine monitoring.

For short range communications Bluetooth is a popular wireless protocol. However, in the case of WBANs the implemented protocol should support low energy consumption and should offer a self-organizing feature. These are the reasons why Bluetooth is not a feasible solution for WBANs and concurrently this is also the reason most of the WBAN applications in the IEEE 802.15.4/ZigBee era have implemented IEEE 802.15.4/ZigBee.

The advantages of ZigBee are:

- it supports mesh networks
- it supplies longer battery life due to its low duty cycle
- its communications characteristics enable low-latency communications
- low energy consumption between nodes due to the circumstance that the control of data transfer is on the node side and the node can sleep whenever possible, rather than keeping the hub continuously busy
- supports 128-bit security
- offers the complete basic functionality for the communication between wireless nodes
- is suitable for broadband deployment of the sensor/node network in a cost effective way

The disadvantages of ZigBee are:

- originally ZigBee came from the area of machine-to-machine monitoring control. This is the reason why most academia research projects employ IEEE 802.15.4-based hardware and software interfaces and do not take account of ZigBee
- it operates in the 2.4 GHz ISM band. This band is already overfilled with WLAN traffic

- studies [13] have shown that radio transmissions over 2.4 GHz around the human body suffer significantly from highly variable path loss causing ZigBee performance to fall or to be unsatisfactory
- data rate limitations. The maximum data rate supported by ZigBee is 250 kbps. This data rate is insufficient to support real-time and large-scale WBANs

These disadvantages prevent the widespread adoption of ZigBee and have led to the development of IEEE 802.15.6 standard.

2.4.6 IEEE 802.15.4j standard

A *medical body area network (MBAN)* is a wireless body area network (WBAN) used for the purpose of measuring or recording physiological parameters and other patient information and for performing diagnostic or therapeutic functions in health care facilities. An MBAN is like a cellular wireless system in miniature worn on a patient's body. The sensors are coordinated by a hub device to form a MBAN. The sensors round the body communicate their data to a central hub via MBAN short-range wireless-links to eliminate the necessity of cables. They are wearing by the patient or are located close to the patient. The hub transfers the data using the facility's network via a wired or wireless longer-range backhaul link (possibly Wi-Fi or Ethernet) to a central system. From the central system the data can be accessed and interpreted.

Mainly because of the second disadvantage in the above list (disadvantages of ZigBee), in 2012 the Federal Communications Commission (FCC) took regulatory action (MBAN Joint Proposal) and allocated the 2360-2400 MHz spectrum for medical body area networks (MBANs) use on a secondary basis in the United States making the U.S.A. the first country in the world to dedicate spectrum specifically for wireless health devices. An important benefit of the medical body area networks spectrum is the reuse of mature and low cost 2.4 MHz short-range radios for MBAN applications. In the same frequency band operates the Aeronautical Mobile Telemetry (AMT). To minimize the risk of interference FCC adopt rules that permit an MBAN device to operate only over relatively short distances and as a part of a low-power networked system.

This approach ensures that existing spectrum users can coexist with MBANs and results in greater spectral efficiency. The IEEE 802.15 Task Group 4j developed an amendment to the IEEE 802.15.4 standard extending its physical (PHY) layer and medium access control (MAC) sublayer solutions to the above-mentioned MBAN spectrum with just minimal changes. The 4j standard is backward compatible with IEEE 802.15.4 so that the current 802.15.4 implementations can be reused.

There are two main types of MBAN applications. The first type is the in-hospital patient monitoring and emergency ambulance applications which usually need 1-3 m communication range with duty cycle <= 20%. The second type is remote home monitoring applications which favor a longer communication range of about 10 m with duty cycle < 2%.

Due to the fact that the MBAN spectrum from 2360 to 2400 MHz is used for MBAN services on a secondary basis, the MBAN system must protect the primary users. In addition, interference from primary users must be acceptable. For the protection of the primary users, especially the aeronautical mobile telemetry sites, some rules have been established. FCC divide the MBAN spectrum in two sub-bands, the 2360-2390 MHz sub-band and the 2390-2400 MHz sub-band. In the first sub-band MBAN operations are allowed only in-door. MBAN applications used in mobile vehicles like ambulances are excluded from this rule. MBAN registration, coordination and control are required, so that the MBAN access only the assigned 2360-2390 MHz frequency band. Regarding the second sub-band MBAN operations are allowed anywhere. MBAN registration, coordination and control are not required.

Arrangements must be taken so that the used bandwidth should not be larger than 5 MHz. The value of transmission power in the 2360-2390 MHz band should not be larger that 1mW and 2390-2400 MHz band not larger than 20 mW.

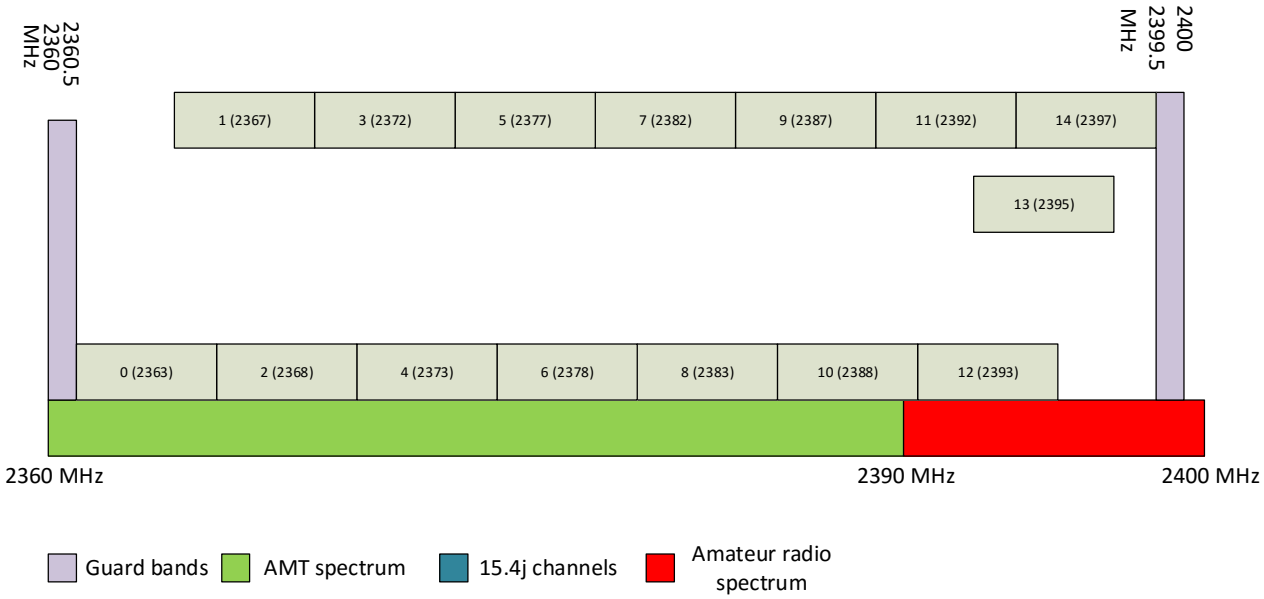


Figure 22 IEEE 802.15.4j Channelization

802.15.4j delivers a flexible channelization scheme allowing the coexistence of in-band primary and MBAN services. The channelization scheme consists of 15 overlapping channels with 0.5 MHz guard bands at the two band edges as can be seen in Figure 22.

2.4.6.1 IEEE 802.15.4j MAC sublayer standard

From the MAC point of view, the 802.15.4j standardization has the aim to provide MAC support making possible MBAN low-power implementation. For this reason, a new channel switch command defined to move out of a concrete MBAN spectrum when the MBAN coordinator must protect the primary services. A comparison with the coordinator realignment command from the IEEE 802.15.4 standard shows that the new channel switch command incorporates a time stamp which indicates the time at which the MBAN should switch to a new channel. In this way a re-channelization of different types of MBAN services can be achieved resulting in collisions avoidance and ensuring quality of service (QoS).

In the description of the IEEE 802.15.4 standard we referred to GTS, the guaranteed time slot. IEEE 802.15.4j proposes the multi-periodic GTS to better support low-duty cycle operations. In IEEE 802.15.4 the slots belong to a GTS allocation are available to the assigned device in every superframe. The difference here is that in the proposed multi-periodic GTS slots can be assigned from the coordinator to its device for operation every S slots, where $S = 2^K$ with K = 1 ... 8. K is the GTS period exponent. The selection of S as a power of 2 makes slot sharing less complicated and make the GTS slot allocation management easier. Multi-periodic GTS contributes to save power in the MBAN because it enables the MBAN devices to remain the most time in sleep mode.

Another MAC feature of IEEE 802.15.4j is the *coordinator switch*. The coordinator switch is a mechanism which if implemented allows the nodes to switch to another coordinator. This is necessary

for example in the follow case. If a patient with an array of nodes or sensors is in transportation from an operating room to a recovery room and monitored by a portable monitor to provide continuous care services. After that the patient is moved back to his patient room. In the patient room a bedside monitor is available. A switch of the nodes from the portable monitor to the bedside monitor would provide better data processing. Another advantage is the saving of power and thus longer battery life of the portable device. The clinician provides the identity information of the 'new' coordinator (e.g. bedside monitor coordinator) to the coordinator ('old') with which the nodes connected in the moment (portable monitor coordinator). After disassociation from the 'old' coordinator the nodes start a scanning process to find the 'new' coordinator whose identity is being broadcast within the beacon. The nodes need the channel number of the 'new' coordinator, its PAN ID and the MAC extended address. After that the nodes connect to the 'new' coordinator and communication can take place.

2.5 IEEE 802.15.4A

IEEE 802.15.4a is currently the most adopted standard for UWB-based MAC implementations used in low data rate and ranging applications. 802.15.4a defines a beacon-enabled superframe structure for UWB PHY layer communication (Figure 23).

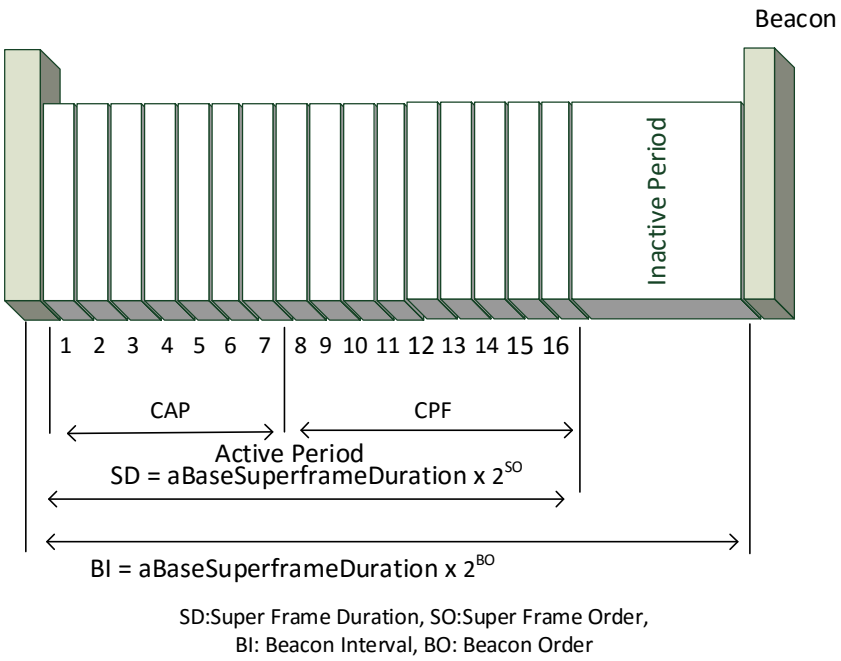


Figure 23 IEEE 802.15.4a superframe structure

802.15.4a allows at maximum 16 timeslots, the superframe is divided into a Contention Access Period (CAP) and a Contention Free Period (CFP). CAP supports random access using ALOHA and CFP consists of Guaranteed Time Slots (GTS) for high priority data traffic. IEEE 802.15.4a (formally called 802.15.4a-2007) specifies two additional physical layers (PHYs) for the original standard 802.15.4-2006, that was specified with four different PHYs. 802.15.4a merged into and it is part of 802.15.4-2011. One of the two new PHYs in 802.15.4a uses ultra-wideband (UWB).

The MAC sublayers for 802.15.4a and 802.15.4 are almost identical. The main difference is the mandatory use of ALOHA or slotted ALOHA in 802.15.4a rather than CSMA/CA due to the difficulty to perform *Clear Channel Assessment (CCA*) on the low-power UWB signal. CCA is a functionality in CSMA/CA to find out if the wireless medium is ready to receive data so that the transmitter may start sending it. ALOHA has better delay performance for routine signal monitoring (e.g. body temperature or blood pressure) and slotted ALOHA has better delay performance for continuous signal monitoring (e.g. Electrocardiography or Electroencephalography). A drawback of the IEEE 802.15.4a standard is that it does not support high data rate communication [14].

2.6 IEEE 802.15.6-2012 STANDARD

Due to growing importance of applications like health-monitoring WBANs has emerged to a key technology. WBANs operate in the vicinity of, or inside, a human body. IEEE 802 established a Task Group called IEEE 802.15.6 for the standardization of the WBANs and the goal to establish in this way a communication standard for low-power in-body/on-body nodes to serve a variety of applications. IEEE 802.15.6 is a standard for short-range (i.e. human body range), highly reliable wireless communications and it is not limited to humans. It allows a very low transmit power device operation. The main advantage of very low transmit power is not only reduction but also minimization of the specific absorption rate (SAR) into the body. A second advantage is the heightening of battery life. IEEE 802.15.6 also provides quality of service (QoS) and strong security [15].

IEEE 802.15.6 uses existing industrial scientific medical (ISM) bands or other frequency bands approved by regulatory and medical authorities. ISM bands as referred in the introduction are radio bands that are reserved internationally for purposes other than telecommunications, e.g. medical, scientific or industrial purposes. All approved standards of 802.15.x propose physical (PHY) and Medium Access Control (MAC) layers. In the next section we will describe the function and the services which MAC generally offers.

2.6.1 Function and Services of MAC in a WBAN

In this section we present the IEEE 802.15.6 reference model, and explain the time reference base for the case that the medium access of the nodes and the hubs is to be scheduled in time. After that we explain two basic terms for this standard, the *beacon* and the *beacon period*.

2.6.1.1 Reference model

In a WBAN all nodes and hubs internally partitioned into a PHY layer and into a MAC sublayer as Figure 24 shows.

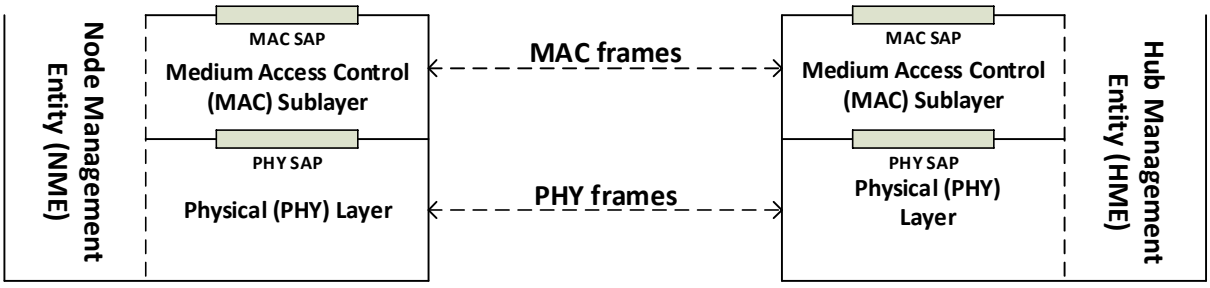


Figure 24 Reference model

In accordance with IEEE 802 reference model direct communications between a node and a hub take place at the PHY layer and at the MAC sublayer. At any given time both the PHY layer and the MAC sublayer in a node or in a hub use only one operating channel. Security key generations can happen inside or outside the MAC sublayer but message security services occur exclusively at the MAC sublayer.

Use case Transition/Reception

The MAC sublayer in nodes and hubs provides its service to the higher level, this is the MAC client. This happens through the *MAC service access point (MAC SA*P). SAP is located immediately above the MAC sublayer. The PHY layer provides its service to the MAC sublayer with the help of the PHY service access point (PHY SAP) which resides between the MAC sublayer and the PHY layer.

The transmission happens as follows:

The MAC Client passes via the MAC SAP its MAC service data units (MSDUs) to the MAC sublayer. The MAC sublayer passes MAC protocol data units (MPDUs, also known as *frames*) to the PHY layer via PHY SAP.

The reception happens as follows:

The PHY layer passes MPDUs (MAC frames) to the MAC sublayer via PHY SAP. The MAC sublayer passes MSDUs to the MAC client via the MAP SAP.

As we see in Figure 24 a *node management entity (NME)* and/or a *hub management entity (HME)* as a superset of NME can be used to exchange network management information with the MAC, the PHY and other layers.

2.6.1.2 Time reference base

If the medium access of the nodes and the hubs is to be scheduled in time, then a time reference base must be set up as shown in Figure 25.

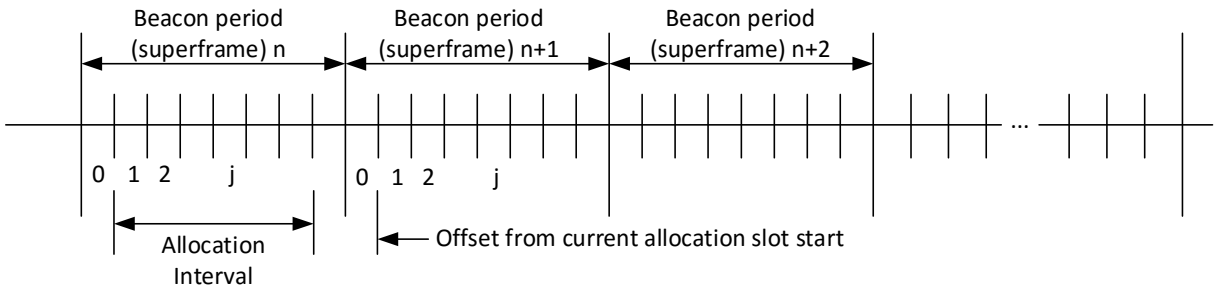


Figure 25 Time reference base

This time reference set up is explained in the next section.

2.6.1.3 Beacon and beacon period

A *beacon* is a frame transmitted by a hub to facilitate network management, such as the coordination of medium access and power management of the nodes in the body area network (BAN) of the hub,

and to facilitate clock synchronization therein. The IEEE 802.15.6 standard divides the time axis or channel into superframes of equal length or into beacon periods. The term *superframe* is used interchangeable with *beacon period* and used especially when no beacons are transmitted. The hub transmits beacons in each superframe except the idle superframes. A *beacon period* is a repetitive time interval to which medium access is referenced and in which a beacon is transmitted when appropriate, comprising the same number of time units, called allocation slots, of equal duration. Each superframe - beacon period - contains a number of slots. These slots which are used for the data transmission are numbered from 0 to s with s <= 255 and have equal duration. The definition of the superframe boundaries and the allocation of the slots happens through beacon transmission from the hub. The total time interval of the slots (or better say timeslots) is called *Contention Access Period (CAP)* during which nodes can attempt to communicate (Figure 26).

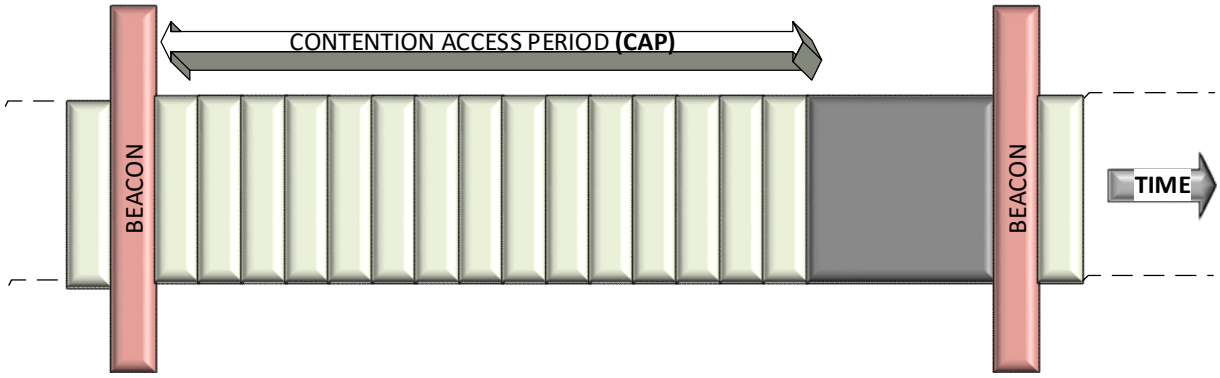


Figure 26 Two successive beacons and the CAP

An allocation interval consists of a number of allocation slots and also is referenced in terms of the allocation slot that includes it. A point of time can be referenced by the numbered allocation slot following it. A frame transition can include more than one allocation slots and must not necessarily starts or ends on an allocation slot boundary.

If time reference is needed for access scheduling in its BAN, the hub must choose boundaries of beacon periods and allocation slots therein. In the beacon mode operation which is described in 2.6.2.2.2 the hub communicates the boundaries by transmitting beacons at the start or other specified locations of beacon periods and optionally timed frames (T-Poll frames). These beacons or T-Poll frames contain a transmit time relative to the start time of the current beacon period. In the non-beacon operation mode (see 2.6.2.2.2) the hub communicate boundaries by transmitting timed frames (T-Poll frames) which in the same way as with the beacons they contain a transmit time relative to the start time of current superframe.

If a node requires a time reference in the BAN must derive the boundaries of beacon periods and allocation slots. The way to do that is to receive beacons or/and timed frames (T-Poll frames).

2.6.2 WBANs Characteristics

In this part of the we will study the characteristics of WBANs. The node type and the maximum allowable number in the WBAN, the network topology of the WBAN and the communication architecture are the items that we will focus on.

2.6.2.1 Types of nodes

There are three criteria by which the node type is distinguished; These criteria are their *functionality* in the WBAN, their *role* and finally their *implementation*.

2.6.2.1.1 Node type according to their functionality

Three node types exist from the view point of the node functionality. The sensor, the actuator, and the personal device. These node types are described in the following sections.

2.6.2.1.1.1 Sensor

A sensor is a system that converts a physical quantity and its amendment in appropriate electronic signals [16] [17]. Sensors are implantable or wearable. We distinguish also sensors in physiological sensors, biochemical sensors, biokinetics or ambient sensors.

2.6.2.1.1.2 Actuator

An actuator is an electrical, hydraulic, or pneumatic device (such as a relay) that controls the flow of material or power [18]. It provides feedback in the network by acting on sensor data.

2.6.2.1.1.3 Personal Device (PD)

Other names for PD are Body Control Unit, sink, PDA, body-gateway or personal server. The personal device is collecting the data received from actuators and/or sensors and interacts with the user or other users. Also the PD informs the user via PD-display/LEDs or via an external gateway.

2.6.2.1.2 Node type according to their role

There are three roles, also three node types we distinguish: the end node, the relay and the coordinator.

2.6.2.1.2.1 End node

An *end node* is an entity with a medium access control (MAC) sublayer, a physical (PHY) layer and optional it includes security services. The end node is limited to carry out the application for which it was installed. End nodes referred in this work as ***nodes***.

2.6.2.1.2.2 Relay

A Relay node performs two functions. It is an intermediate node receiving the data from the end node and sending it to the PD. Also it can serve itself as an end node sensing data. The intermediate function is very important in the case where the end nodes are at an extremity.

2.6.2.1.2.3 Coordinator

The coordinator or hub is the node (e.g. PDA) through which all other nodes communicate. It takes the role of a gateway to another coordinator, to a WBAN, to a trust center and generally to the outside world. A coordinator coordinates the medium access and power management of one or more nodes [15]. Coordinators are referred in this work as ***hubs***.

2.6.2.1.3 Node type according to their implementation

This section lists the node types are defined in the IEEE 802.15.6 standard.

2.6.2.1.3.1 Body surface node

As the name suggests a body surface node is placed on the surface of the skin. In a second constellation, the body surface node can be placed two centimeters away from the skin.

2.6.2.1.3.2 Implant node

Implant nodes are planted either inside the tissue or immediately underneath the skin.

2.6.2.1.3.3 External node

External nodes are not in contact with the human skin. They are installed from a few centimeters up to 5 meters away from the human body.

2.6.2.2 Number of nodes in a WBAN and Network topology

The IEEE 802.15.6 standard defines the maximum number of nodes (end nodes) in a WBAN as nMaxBANSize. According to the specification of the MAC sublayer parameters nMaxBANSize is set to 64. In general, the number of nodes in a WBAN is not limited. The organization of nodes and hubs in a body area network happens on the way that a concrete number of nodes (between 0 and nMaxBANSize) connected with exactly one hub, which coordinates as a gateway the communication. This logical set of one hub and n nodes is defined as *Body Area Network*. If we consider that per m^2 2-4 WBANs can coexist, a WBAN network will include maximal 4x64, these are 256 nodes. In practice, there are technical considerations that limit the possible maximum number of the nodes in a WBAN. Such technical considerations are the capability of the communication protocol, the network architecture or transmission techniques.

2.6.2.2.1 one-hop star BAN

A one-hop star BAN consists of a hub and some n nodes where n <= nMaxBANSize. Frame exchanges in this topology occur directly between the nodes and the hub. In the example we see in Figure 27 the node N1a exchanges frames directly with the hub H1. The same for the nodes N1b, N1c and N1d. In one-hop star BANs we have two types of transmission: The transmission from the node to the hub and the transmission from the hub to the node.

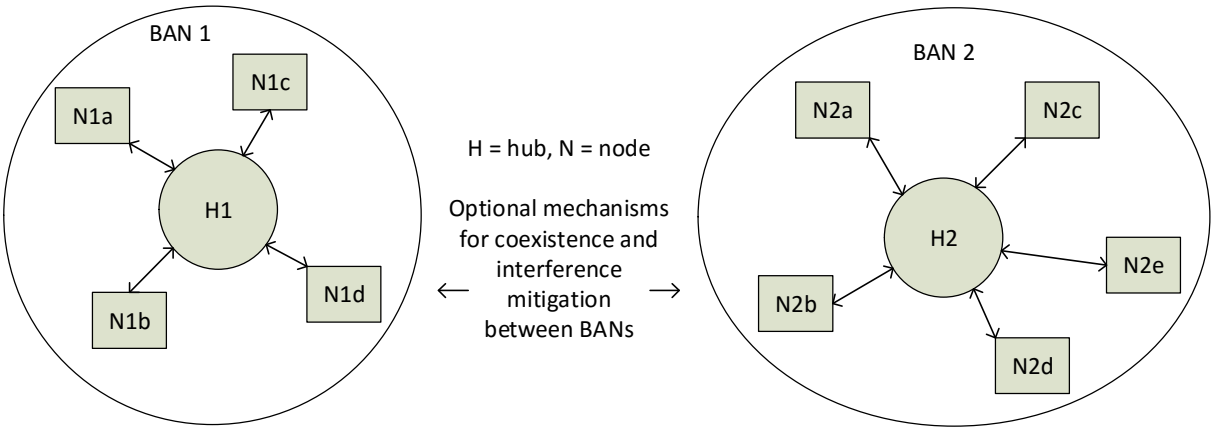


Figure 27 Network topology [15]

2.6.2.2.2 two-hop extended star BAN

In the two-hop extended star BAN the frame exchange can happen optionally through a relay node. As we see in Figure 28 N1c and N1f are relay nodes. The node N1d exchange frames with the hub H via the relay N1c and N1e exchange frames via the relay N1f.

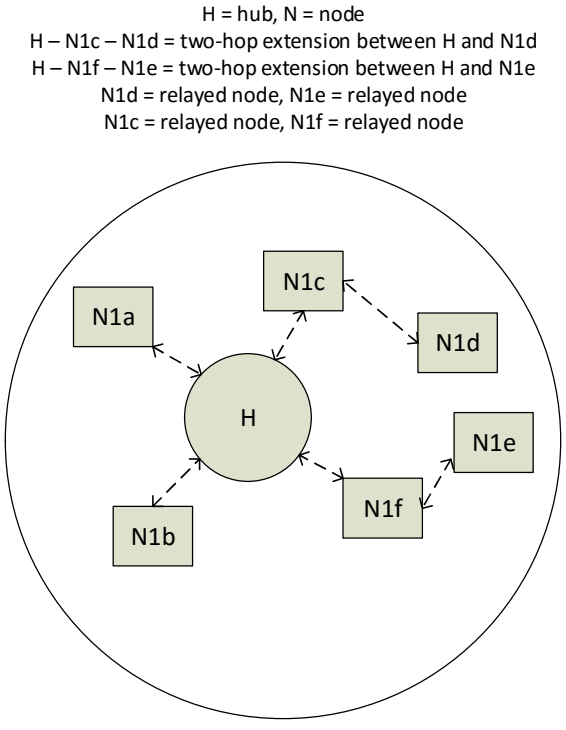


Figure 28 Two-hop extended star [15]

2.6.2.2.3 Communication methods in the star topology

There are two communication methods used in the star topology: the *beacon mode* and the *non-beacon mode*.

In the *beacon mode* the hub controls the communication. The hub transmits periodic beacons defining in this way the beginning and the end of a superframe, these two beacons are successive beacons. The length of the beacon period can be defined by the user. The availability of pending data for a node is indicated in the beacons.

In the case of a *non-beacon mode* no beacons transmitted regularly by the hub. Beacons can be requested to associate a device with the hub. The communication is asynchronous. A device communicates with the hub only when it needs to. A node in the network can send data to the hub using possibly CSMA/CA. Receiving data from the hub takes place by power up and poll the hub. If the hub cannot communicate the node must wait till it is invited to communicate. The non-beacon mode make sense in the use case of *light traffic* between nodes and hub. The hub is required to communicate boundaries by transmitting timed frames (T-Poll frames) with transmit time relative to the start time of the current superframe.

Some more detailed description of the communication or access methods are given in 2.6.4.2.2 (**Access classification and division**).

A comparison of both topologies one-hop star topology (star network) and two-hop star topology (multi-hop network) is given in Table 6:

Criteria	One-hop Networks	Multi-hop Networks
Node failure	In case of failure only the failed node will be affected	Overhead due to reconfiguration of the network part that includes the failed node
Transmission delay	Least possible delay from any sensor to PDA	Depends on the network configuration. Nodes closest to PDA which do not need a relay have less delay that the other nodes
Energy consumption	The further a hub from the PDA is, the more power is used to transmit the data	The nodes closest to the PDA need more power than the others because they forward also the data from the other nodes and not only the own data
Interference	Due to high-power demand for hubs which are far away from PDA interference increase	Low interference due to node transmission to neighbor nodes

Table 6 Comparison of one-hop and multi-hop networks

The latest version of the IEEE 802.15.6 standard only two hops are supported. This means that systems with more than two hops are not standard-compliant. Increasing the number of hops increases the WBAN complexity. Multihop transmission, as the table shows has more configuration overhead in case of failure, has higher transmission delay, needs lower transmission power and is characterized by low interference.

2.6.2.3 Communication architecture

Taking a look to the Figure 29 we see that there are three major parts or tiers the WBAN communication architecture consists of. These tiers are the intra-WBAN communication, the inter-WBAN communication and the Beyond-WBAN communication.

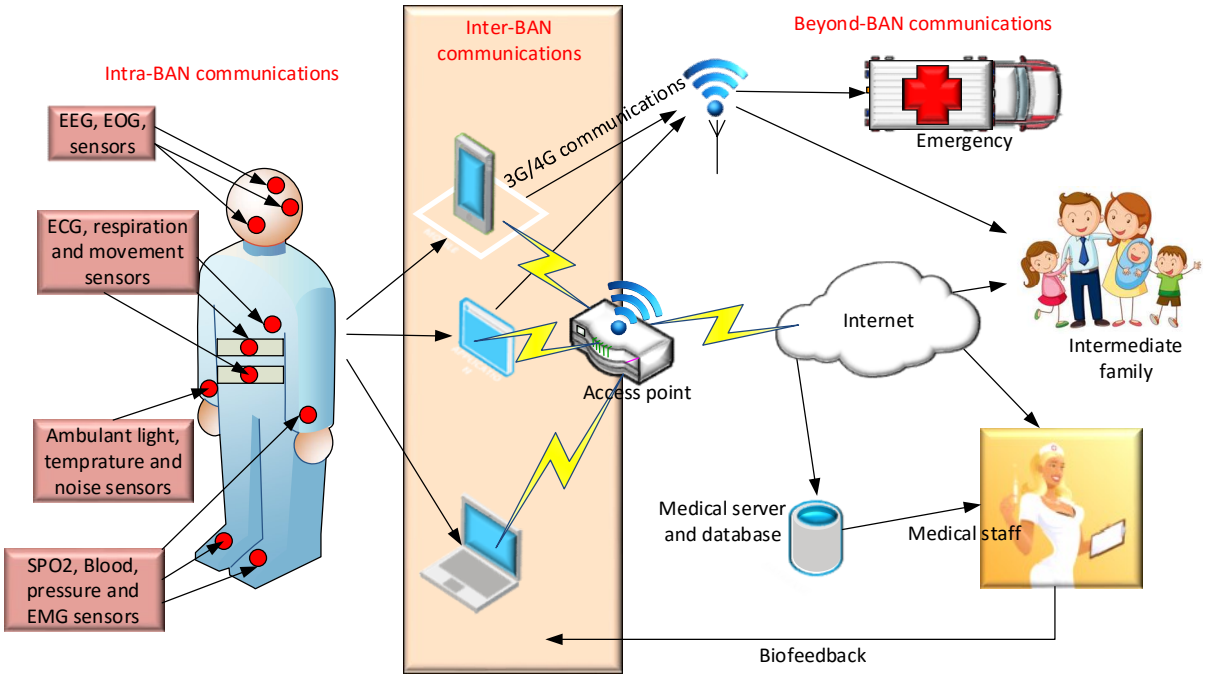


Figure 29 Communication architecture of WBANs

2.6.2.3.1 intra-WBAN communication

Intra-WBAN communication is referenced to radio communications of about 2m around the human body and sub-categorized as (1) point-to-point communication between nodes (body sensors) and (b) communications between nodes and the portable PD. This tier consists of all sensors and actuators, let's say nodes, which are in or on the human body and communicate to transmit the selected data. In case of running or walking the body is in action, so there is no a fixed position for the nodes. Also in any position assumed by the body the ideal position of the nodes is not always the same. The intra-WBAN communication environment is a dynamical one due to the fact that the position of every node depends on the application which is in use. The intra-WBAN communication in this tier depicts the interaction of the nodes taking in account the installed topology and the transmission ranges of the WBAN. Except the nodes, in the first tier consists also from the personal device. The potential different types of nodes send the data they collected to the PD within the intra-WBAN communications tier and the PD send the processed data to an access point in the next tier, the inter-WBAN communication tier.

2.6.2.3.2 inter-WBAN communication

In the second tier the PD communicates with one or more access points (APs). An access point can be a 3G/4G mobile phone, a pad, a laptop/PC in combination with a WLAN or a WLAN itself. WLAN is faster than cellular networks. Cellular networks have the advantage that the corresponding cellphones provide a user friendly interface. The access points are part of the whole infrastructure. The inter-WBAN communication offers the interconnection functionality between the first tier and the third tier, the beyond-BAN communications tier, connecting in this way the nodes with networks. Two different inter-WBAN communication architectures have been developed. The *Infrastructure based architecture* and the *Ad-hoc based architecture*.

2.6.2.3.2.1 Infrastructure based architecture

This type used in the most WBAN applications (Figure 30). It assumes limited space, let say a waiting room in a hospital, a home or an office. Its characteristics are:

- larger bandwidth
- centralized management and flexibility
- security control
- dynamic deployment in a limited space (e.g. hospital)
- the access point can take the function of a database server

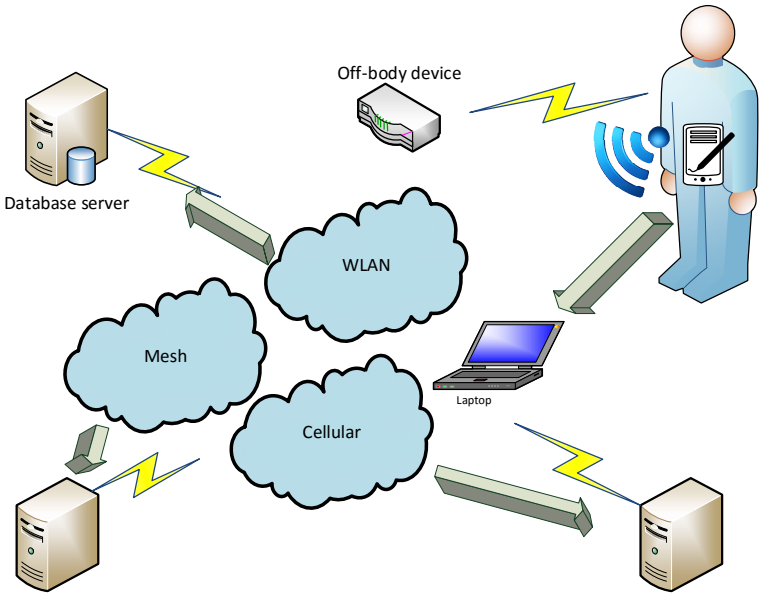


Figure 30 Infrastructure based architecture

2.6.2.3.2.2 Ad-hoc based architecture

Multiple access points are deployed building a mesh network to allow to the nodes to transmit information within medical centers, buildings or emergency rescue spots. This characteristic - the mesh network - leads to the possibility of fast and flexible deployment also when encountering a dynamic environment. Such environments are e.g. medical emergency care response or a disaster site. A difference to the infrastructure architecture is that ad-hoc based architecture (Figure 31) has a larger radio coverage. The result is higher patient mobility in a hospital for example where the ad-hoc architecture could be come in use. And this is the advantage compared to the infrastructure-based mode. The coverage area of the ad-hoc based architecture can be between 2m and 100m. The ad-hoc based architecture uses two categories of nodes. It uses nodes (sensors/actuators) in or around the human body and router nodes around a WBAN. Both categories use the same radio hardware to achieve multi-hop routing.

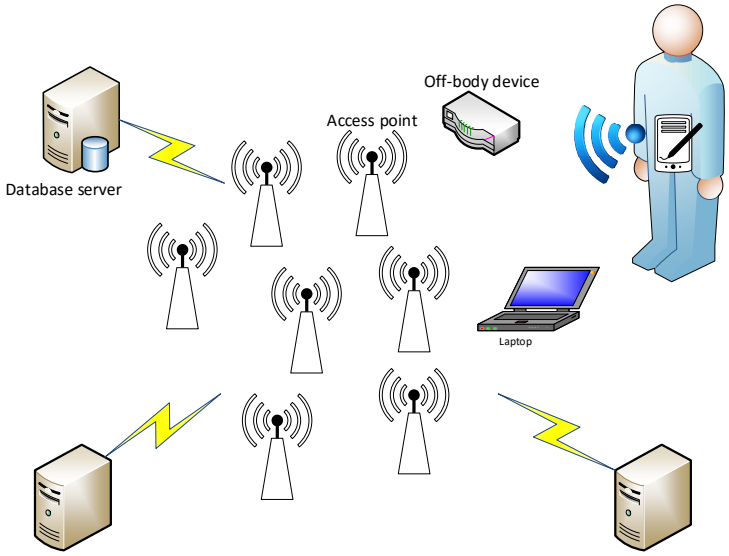


Figure 31 Ad-hoc based architecture

2.6.2.3.3 beyond-WBAN communication

The implementation of the beyond-WBAN communication is application specific. One of the most important components of this 3rd tier is a database with the user profile and the data history. Also a gateway (e.g. PDA) is in use to bridge the inter-BAN network with a metropolitan area network as can been seen in Figure 29. Through a SMS or through the internet doctors can been notified about the emergency status of the patient health.

2.6.3 Layers

As IEEE 802.15.1 and IEEE 802.15.4 the IEEE 802.15.6 protocol is offering a MAC and a PHY layer. In the next section both layers are described. Referring to the OSI model neither MAC nor PHY layers supply any application, presentation, session, transport or network layer. The IEEE 802.15.6 defines a new PHY layer and a MAC sublayer for WBANs providing in this way wireless technology for WBANs with following characteristics:

- Ultra-low-power
- low complexity
- high reliability
- low cost
- short range

IEEE 802.15.6 requires the development of a logical node management entity (NME) or a hub management entity (HME) to exchange network management information with PHY, MAC or other layers.

2.6.4 MAC Sublayer

In this section we describe the MAC frame formats, and the MAC functions of the IEEE 802.15.6 standard.

2.6.4.1 MAC frame formats

In this section we will discuss the general format of the MAC frame and after that we will consider the management type frames, the control type frames and the data type frames. Finally, I'll take a look to the MAC/PHY capability fields and the information elements.

2.6.4.1.1 General format

The PHY SAP delivers to the MAC sublayer and vice versa MAC frames. A MAC frame is an ordered sequence of mandatory and optional fields. An atomic field denotes a numerical value. A MAC frame field consists of octets. Let say that a MAC frame field has N octets, 0 till N-1. The octet 0 is containing the least significant bits (LSB) of that field and the octet N-1 is containing the most significant bits (MSB). The LSB are the first bits transmitted and the MSB are the last bits that are transmitted. The octet order is denoted as L-R, means from the left to the right of a multi-octet non-atomic field (Figure 32).

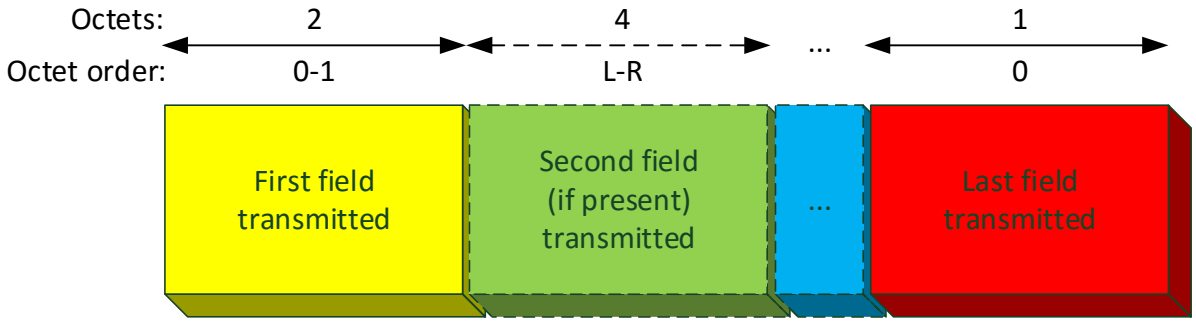


Figure 32 Octets and octets order

In the above Figure 32 the fields are aligned with octet boundaries. If fields are not aligned with octet boundaries, the number of bits and the corresponding bit order of encoding would be showed as can be seen in the next Figure 33.

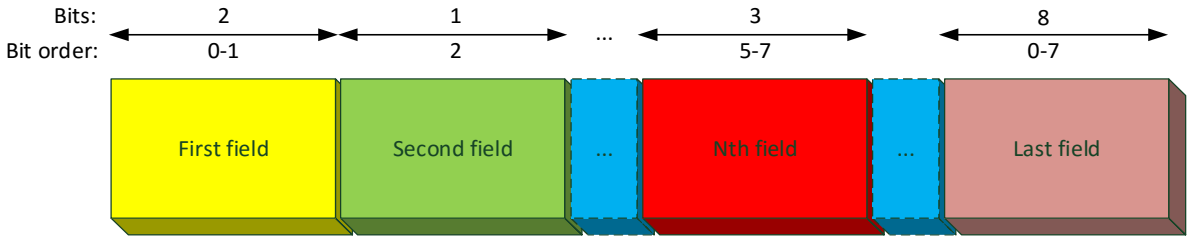


Figure 33 Fields are not aligned with the octet boundaries

If fields located on octet boundaries, then bit numbering restarts from zero. Depending on the perspective of the node or the hub, a field defined as a *sender*, if a node/hub is sending the frame containing the field and is defined as the *recipient* or *the intended recipient* if a node/hub is receiving or intended to receive the frame containing it. If a field is reserved in case of transmission is set to 0 and in case of reception is ignored. MAC includes special constants which are referenced as parameters. PHY dependent parameters denoted with a preceding „p “and PHY independent parameters denoted with a preceding „m “.

The MAC general format

Every MAC frame consists of a MAC header with fixed-length, a MAC frame body with variable length and a Frame Check Sequence (FCS) also with fixed-length as shown in Figure 34.

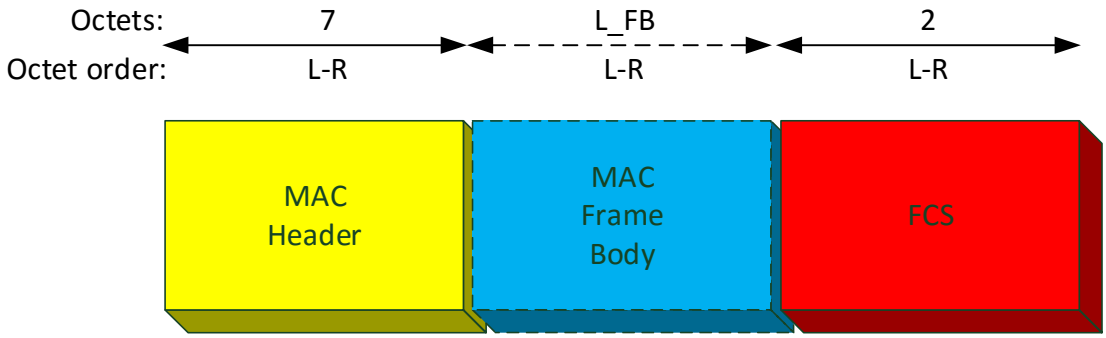


Figure 34 MAC frame format

The length of the MAC frame body is L_FB octets where 0 <= L_FB <= pMaxFrameBodyLength.

The MAC header

The MAC header (Figure 35) consists of the frame control (4 octets), the recipient id (one octet), the sender id (one octet) and the BAN id (one octet).

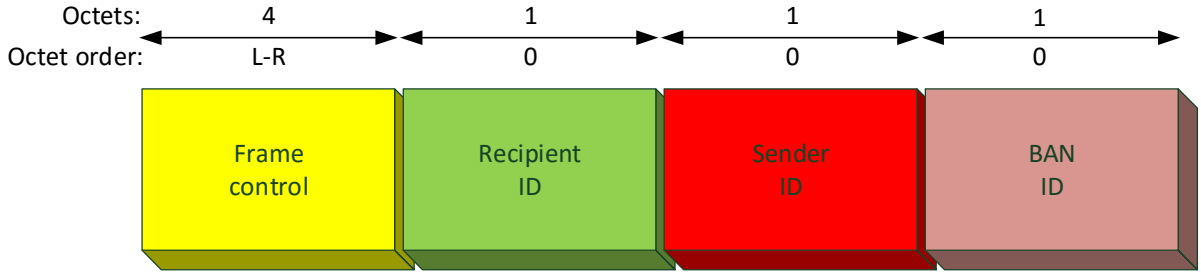


Figure 35 MAC header format

Recipient ID

The recipient ID is set to the NID or HID of the recipient of the current frame.

Sender ID

The sender ID is set to the NID or HID of the sender of the current frame.

BAN ID

The BAN ID field is set to the address of the BAN the current frame is delivered.

Frame control

The frame control is 4 octets long (Figure 36). It is formatted as follows:

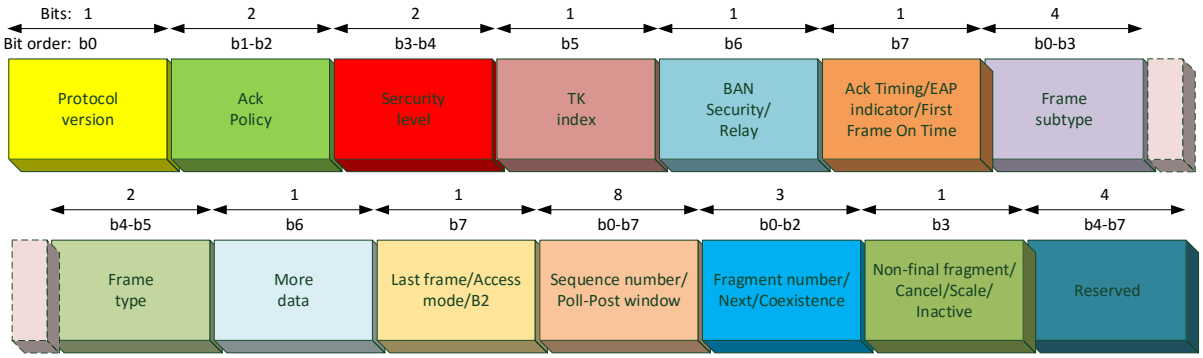


Figure 36 Frame control format

In the following, we will explain the parts of the frame control format that consists of:

Protocol version

Is set to zero and is invariant in size and place in IEEE 802.15.6. It has the length of one bit.

Ack Policy (Table 7)

The Ack policy represents the acknowledgement requirement of the current frame. The group acknowledgment (G-Ack) value is fitting to frames sent to hub having frame type set to data and frame subtype set to mG-AckDataSubType.

Field value	***Acknowledgment requirement***
00	No acknowledgment (N-Ack) or group acknowledgment (G-Ack)
01	Immediate acknowledgment (I-Ack)
11	Block acknowledgment later (L-Ack)
10	Block acknowledgment (B-Ack)

Table 7 Acknowledgement Policy field encoding

Security Level

Table 8 shows the security level of the current frame.

Field value b4 b3	Security level of current frame
00	Level 0 – frame not secured
01	Level 1 – frame authenticated but not encrypted
10	Level 2 – frame authenticated and encrypted
11	Reserved

Table 8 Security Level

Temporal key (TK) Index

A *pairwise temporal key* (PTK) is a secret bit string known both on the hub side and on the node side. PTK is used to secure frames send from the hub to the node and vice versa. GTK is the abbreviation for *group temporal key*. As we will see later the GTK is distributed via a GTK frame which is transmitted by a hub to a secure node securing multicast traffic. In frames secured by a PTK, the TK is set to the value of the PTK index field (please see PTK control) which is one-bit long. In frames secured by a GTK the TK is set to the value of the GTK index field (please see GTK control) which is also one-bit long. If the frame is unsecured the TK index is reserved.

BAN Security/Relay

This field is set to one in beacon, poll and T-Poll frames which is sent by a hub if the hub accepts only secured communication. The same field for the above kind of frames is set to zero if this hub accepts either secured or unsecured communication. In frames which are received from or sent to relaying nodes in a two-hop extended star network communication is set to one and it is used as a relay field. Otherwise the field is reserved.

Ack Timing/EAP Indicator/First Frame On Time

If the frame is a beacon frame this field is used as an exclusive access phase (EAP) indicator field. EAP is a time span set by a hub in a superframe for transfer of highest priority or traffic like emergency or medical implant event report. It is set to one the length of the exclusive access phase 1 (EAP1) in the current or next beacon period is nonzero. Otherwise is set to 1.

If the frame is a data type frame, a poll frame or a non-beacon management frame which is send by a hub to a node, this field is used as a First Frame On Time field. Is one in case the frame send is the first frame send by the hub to the node at the start of an allocation interval of a scheduled allocation assigned to the node. A detailed setting specification contained in the IEEE 802.15.5-2012 standard.

Frame Subtype

Indicate the frame subtype which is used as the name of the frame. A list of the frame subtypes listed in the next table.

Frame Type

Indicates the frame type. Frame types are management, control, data and reserved. The list of the frame types listed in Table 9.

Frame type value b5 b4	Frame type name	Frame subtype value b3 b2 b1 b0	Frame subtype name
00	Management	0000	Beacon
00	Management	0001	Reserved
00	Management	0010	Security association
00	Management	0011	Security disassociation
00	Management	0100	PTK
00	Management	0101	GTK
00	Management	0110-0111	Reserved
00	Management	1000	Connection request
00	Management	1001	Connection assignment
00	Management	1010	Disconnection
00	Management	1011-1110	Reserved
00	Management	1111	Command
01	Control	0000	I-Ack
01	Control	0001	B-Ack
01	Control	0010-0011	Reserved
01	Control	0100	I-Ack+Poll
01	Control	0101	B-Ack+Poll
01	Control	0110	Poll
01	Control	0111	T-Poll
01	Control	1000-1101	Reserved
01	Control	1110	Wakeup
01	Control	1111	B2
10	Data	0000	User priority 0 or allocation mapped data subtype
10	Data	0001	User priority 1 or allocation mapped data subtype
10	Data	0010	User priority 2 or allocation mapped data subtype
10	Data	0011	User priority 3 or allocation mapped data subtype
10	Data	0100	User priority 4 or allocation mapped data subtype
10	Data	0101	User priority 5 or allocation mapped data subtype
10	Data	0110	User priority 6 or allocation mapped data subtype
10	Data	0111	Emergency
10	Data	1000-1111	Allocation mapped data subtype
11	Reserved	0000-1111	Reserved

Table 9 Frame types

The different ACK methods, is one of the characteristics of IEEE 802.15.6 MAC. As we see in the above table this standard provides ACK methods like Immediate ACK (I-Ack), Group ACK (G-Ack), Block ACK (B-Ack), Late ACK (L-Ack), and No ACK (N-ACK).

More Data

The more data field has multiple use. We list the use cases:

a. Sender: node	Receiver: hub	frame: management or data type frame
b. Sender: node	Receiver: hub	frame: I-Ack and B-Ack frames
c. Sender: hub	Receiver: node	frame: non-beacon management or data type frame
d. Sender: hub	Receiver: node	frame: I-Ack and B-Ack frames
e. Sender: hub	Receiver: node	frame: poll, T-poll, I-Ack+poll, B-Ack+poll frames

Some of corresponding values will be discussed later.

Last Frame/Access Mode/B2

In beacon frames this field is set to one if a B2 frame should be transmitted in the current beacon period. Otherwise is set to zero. In non-beacon management it is used as a last frame field. It is set to one if the sender will not send another frame in the current allocation interval and it is set to zero otherwise.

Sequence Number/Poll-Post Window

The use of this field is wide. In beacon and non-beacon management type frames the field contains a sequence number. Also in data type frames it is used as a sequence number field. In poll, T-poll, I-Ack+poll, B-Ack+poll frames which sent by a hub to a node and in wakeup frames it is used as a poll-post window field. Also in B2 frames it is used as a poll-post window field.

Fragment Number/Next/Coexistence

Beacon and B2 frames use the field as a Coexistence field, non-beacon management type frames use it as a fragment number field, data type frames use it as a fragment number field, poll, T-poll, I-Ack+poll and B-Ack+poll frames sent by a hub to a node use it as a next field as well as in wakeup frames.

Non-final Fragment/Cancel/Scale/Inactive

Beacon and B2 frames use it as inactive field. Non-beacon management type frames and data type frames use it as a non-final fragment field. I-Ack, B-Ack, poll, t-Poll, I-Ack+poll and B-Ack+poll frames use it as a Cancel field and finally Wakeup frames use it as a Scale field.

MAC frame body

As we saw the length of the MAC frame body is 0 <= L_FB <= pMaxFrameBodyLength. If L_FB > 0 then is formatted as shown in the next Figure 37.

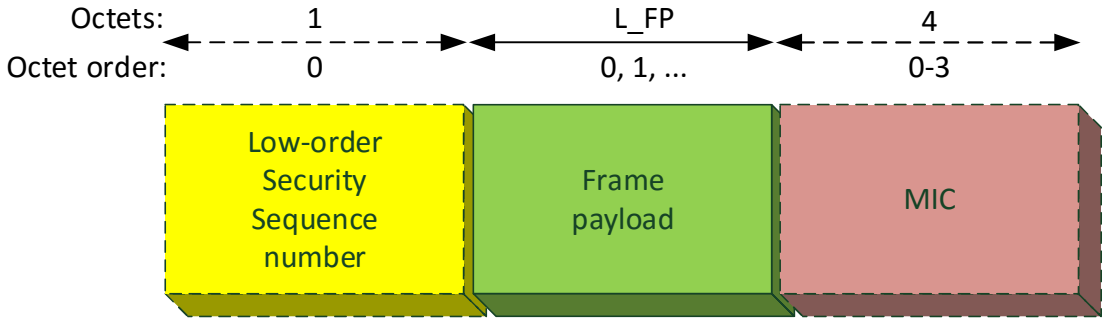


Figure 37 MAC frame body format

The Low-Order security sequence number field and the Message integrity code (MIC) field exist only in secured frames. The MIC field includes a message authentication code protecting in this way integrity and authenticity.

Frame payload

The frame payload consists of management type frames, control type frames and data type frames. The frame payload field is set to an unfragmented frame payload or is set to a fragment if the frame payload is carried in multiple frames. The length of the frame payload field is denoted as L_FP. For a frame payload with zero length the following applies: is the frame secured, then it still has a MAC frame body containing the Low-order security sequence number and MIC fields. Isn't the frame secured, then is has no mac frame body.

Frame Check Sequence (FCS)

The FCS is an error detecting code added to a frame. Error detection does not mean error correction. The frame check sequence consists of the 16 bits $a_{15}...a_0$ where a_{15} is the LSB and a_0 is the MSB. The 16 bits are the binary coefficients of a cyclic redundancy check (CRC) polynomial of degree 15.

2.6.4.1.2 Management type frames

A management type frame consists of mandatory fixed-length fields and also optional variable length components which called information elements (IEs). In this section I'll give a synopsis of the management type frames.

Beacon frame

The frame payload of the beacon frame has following structure (Figure 38):

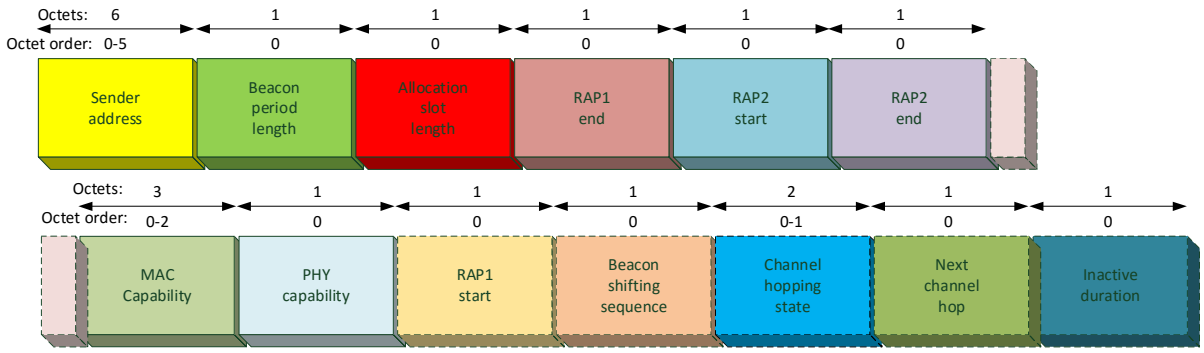


Figure 38 Frame payload format for beacon frames

Security association

The frame payload of the security association frame is formatted as follows (Figure 39):

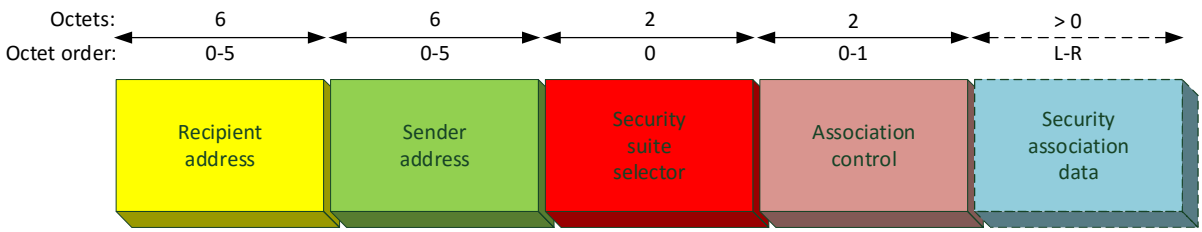


Figure 39 Frame payload format for security association frames

Security Disassociation

The frame payload of the security disassociation frame is formatted as follows (Figure 40):

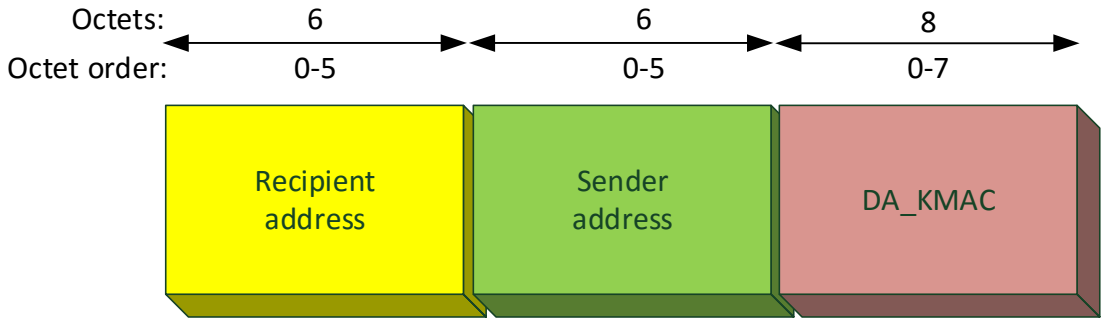


Figure 40 Frame payload format for security disassociation frames

Pairwise Temporal Key (PTK)

The frame payload of the PTK frame is formatted as follows (Figure 41)

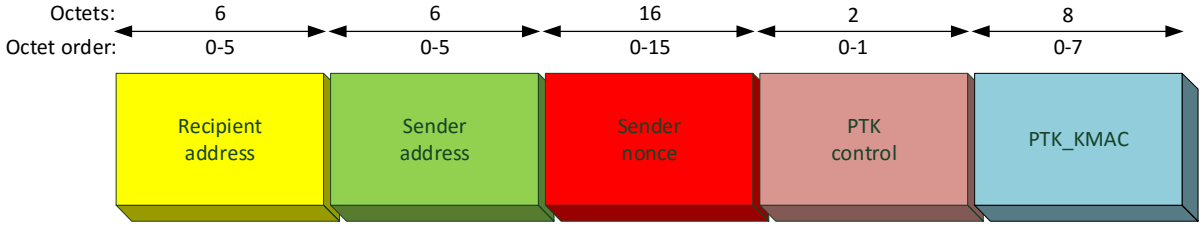


Figure 41 Frame Payload format for PTK frames

Group Temporal Key (GTK)

The frame payload of the GTK frame is formatted as follows (Figure 42):

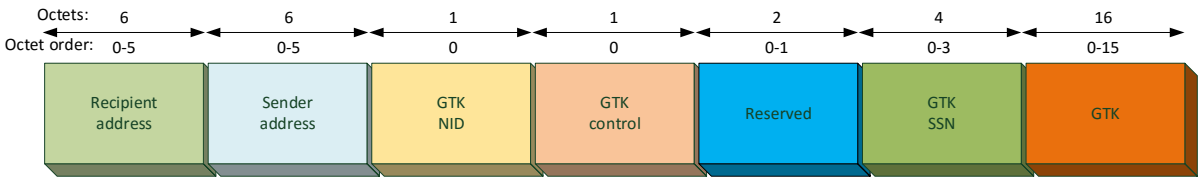


Figure 42 Frame Payload format for GTK frames

Connection Request

The frame payload of the connection request frame transmitted by a node to request creation or modification of a connection with a hub. It is formatted as follows (Figure 43):

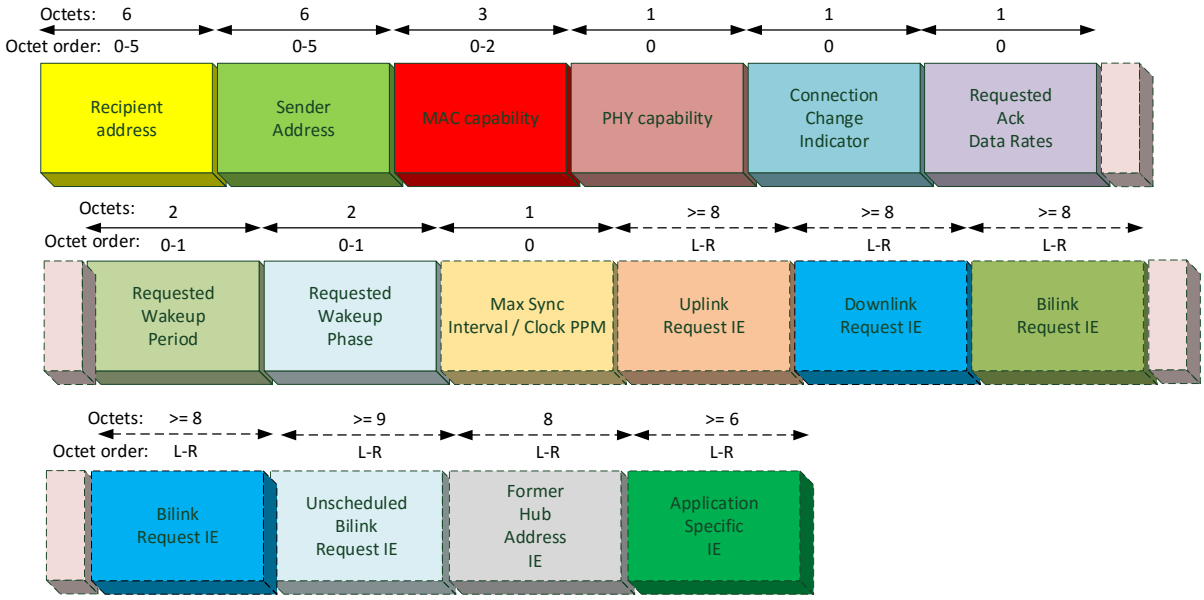


Figure 43 Frame payload format for connection request frames

Connection Assignment

The connection assignment frame transmitted by a hub to respond to a connection request. Also is used to change or initiate a connection assignment. It is formatted as follows (Figure 44):

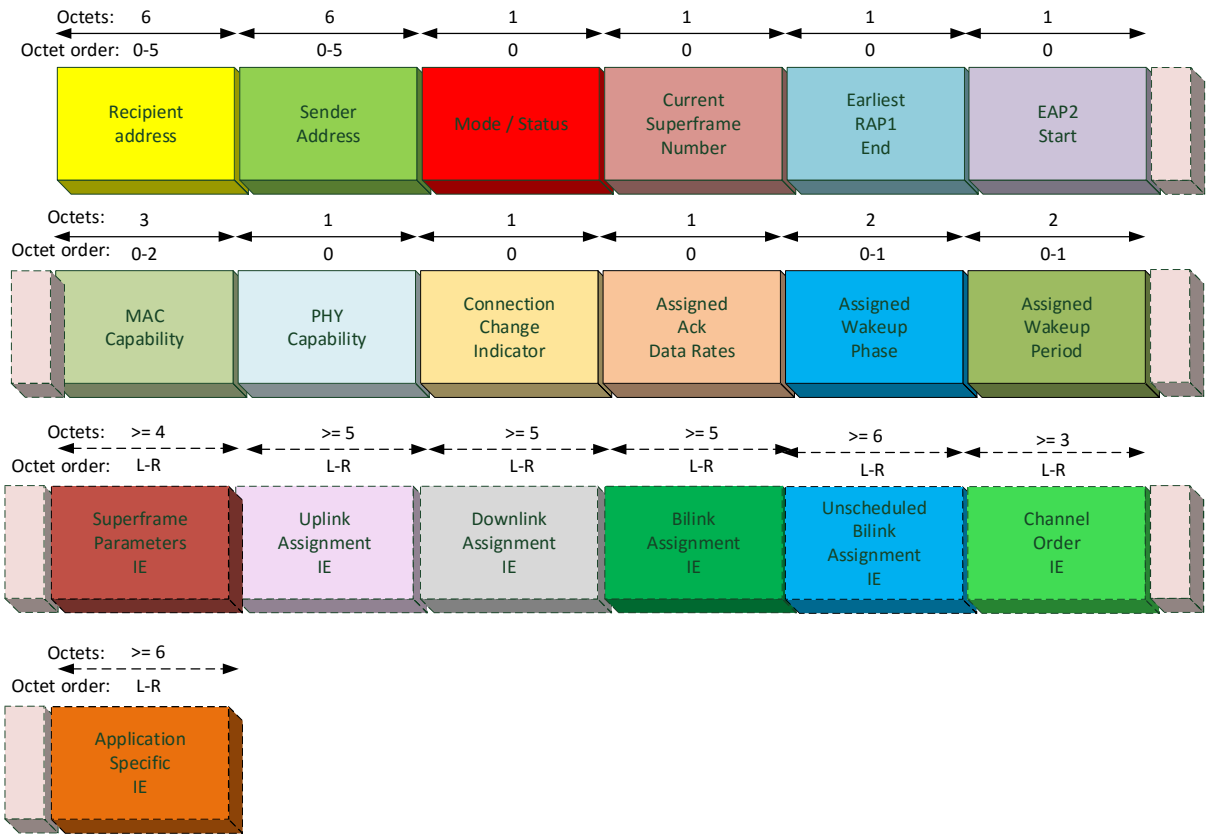


Figure 44 Frame payload format for connection assignment frames

Disconnection

This frame contains a frame payload which is transmitted by a hub to repeal the connection with a node or by a node to repeal the connection with a hub. Its format (Figure 45):

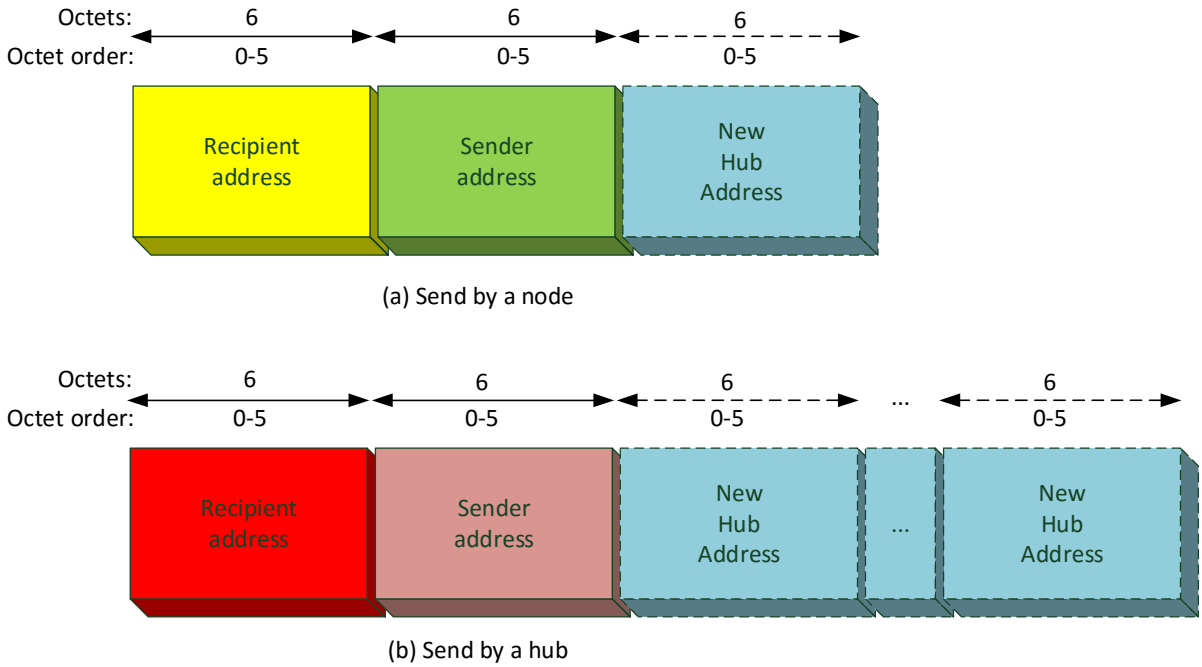
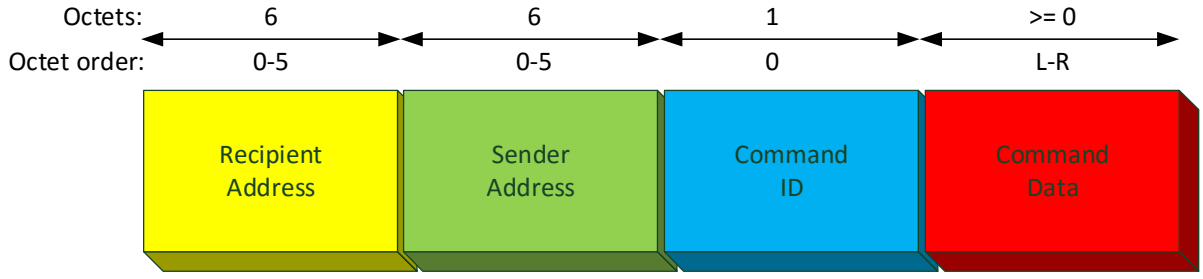


Figure 45 Frame payload format for disconnection frames

Command

The command frame contains a Frame payload which is optionally transmitted by a hub or a node. Its format (Figure 46):



1

Figure 46 Frame payload format for Command frames

2.6.4.1.3 Control type frames

The following control type frames are defined in IEEE 802.15.6-2012:

Immediate Acknowledgement (I-Ack)

The I-Ack frame can be transmitted from a node to a hub or vice versa. It acknowledges the receipt of the preceding frame and optionally provides a timestamp by a hub in terms of current allocation slot number and a current allocation slot offset in the frame payload for the node's clock synchronization. The I-Ack frame transmitted by a node to a hub does not contains frame payload. The I-Ack frame transmitted by a hub to a node selectively contains a frame payload as shown in Figure 47:

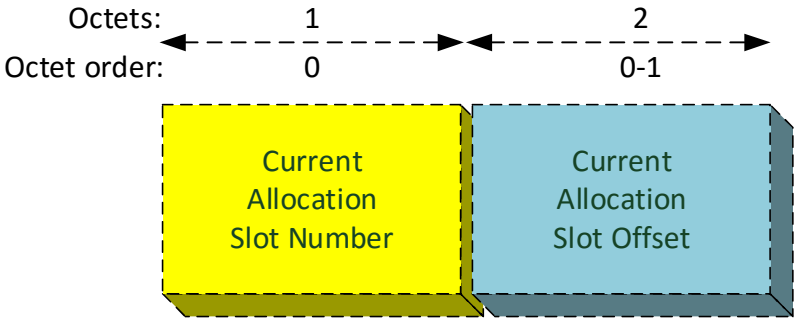


Figure 47 Frame payload format for I-Ack frames

Both fields presented are absent or both are present.

Block Acknowledgement (B-Ack)

The format of B-Ack can be seen in Figure 48.

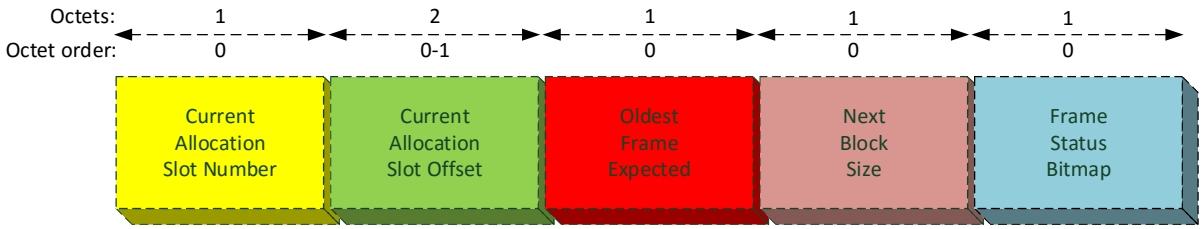


Figure 48 Frame payload format for B-Ack frames

Immediate Acknowledgement + Poll (I-Ack+Poll)

The I-Ack+poll frame is equivalent in function to an I-Ack frame followed by a T-Poll or a poll frame. It is transmitted by a hub to acknowledge the receipt of the preceding frame and also to send a poll to the addressed node.

Block Acknowledgement + Poll (B-Ack+Poll)

The B-Ack+poll frame is equivalent in function to an B-Ack frame followed by a T-Poll or a poll frame. It is send by a hub to acknowledge the receipt status of certain preceding data type frames and also to send a poll to the addressed node.

Poll

The poll frame contains no frame payload and is transmitted by a hub. Its function is to inform the node of a future poll or post or to give to the addressed node an immediate polled allocation.

Timed-Poll (T-Poll)

The format of the T-Poll frame is shown in Figure 49:

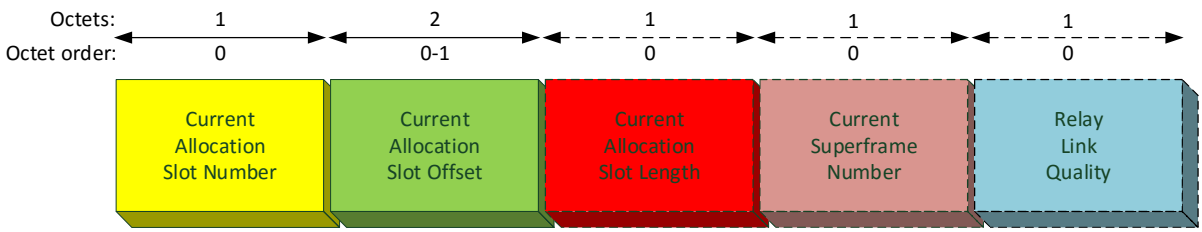


Figure 49 Frame Payload format for T-Poll frames

T-poll is send by a hub to grant to the addressed node(s) an immediate polled allocation that starts pSIFS after the end of the frame. T-poll is used also to inform the node of a future poll or post.

Wakeup

The wakeup format consists of two parts, the recipient address and the sender address (Figure 50).

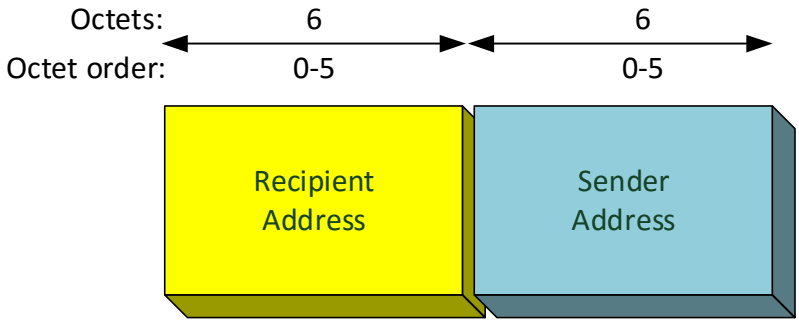


Figure 50 Frame payload format for wakeup frames

The wakeup frame is optionally transmitted by a hub to wake up a node which act in the medical implant communications service (MICS). MICS is the name of a specification for using a frequency band between 402 and 405 MHz in communication with medical implants. MICS allows bi-directional radio communication with a very low maximum transmit power of EIRP=25 microwatt.

B2 Frame

The b2 frame is optionally broadcast by a hub to announce b2-aided time-sharing information or to provide group acknowledgment. The parts of the b2 frame showed in Figure 51.

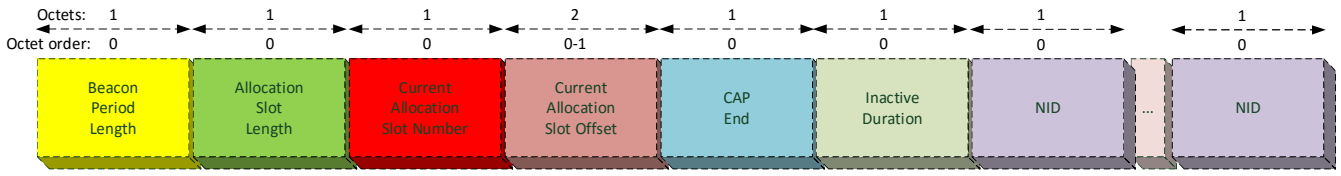


Figure 51 Frame payload format for b2 frames

2.6.4.1.4 Data type frames

A full or a fragmented Media access control service data unit (MSDU) is the content of a data type frame. A data type frame can also be MSDU-less.

An *emergency frame*, this is a data type frame of the subtype emergency, indicates through its transmission an emergency or medical implant event report.

Another kind of data type frame is the *user priority UP frame* with values UP=0...,6. This is transmitted to indicate that the frame payload is identified by the frame subtype and has a user priority UP. The transmission condition is that no information element (IE) of the connection request frame or the connection assignment frame transmitted in the past or received by the sender of the current frame contained an allocation ID comprising the frame subtype value and the user priority UP.

The *allocation mapped data subtype frame* is transmitted to indicate that the frame payload is identified by the frame subtype and has a user priority UP. The transmission condition is that an information element (IE) of the connection request frame or the connection assignment frame transmitted in the past or received by the sender of the current frame contained an allocation ID comprising the frame subtype value and the user priority UP.

2.6.4.1.5 MAC/PHY capability fields

There are part of beacons and other management type frames. They indicate the capabilities for nodes and hubs to support a given function. The format of mac capability is formatted as shown in Figure 52.

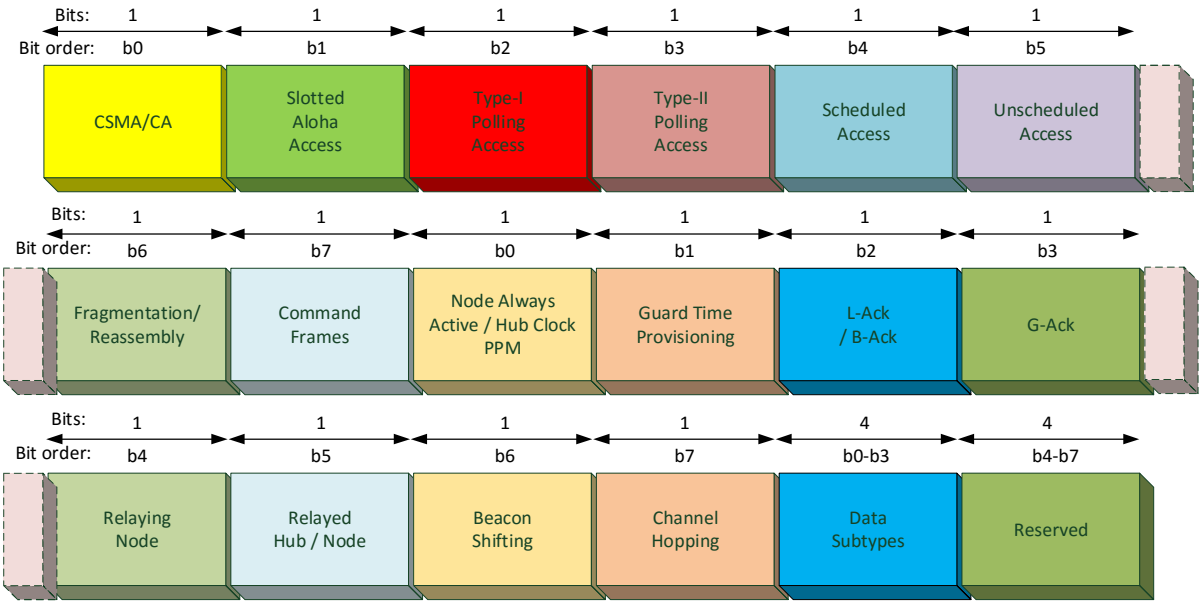


Figure 52 MAC Capability format

2.6.4.1.6 Information elements

The format of an information element (IE) is shown in the Figure 53.

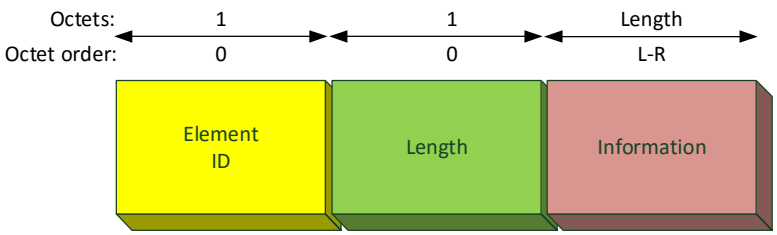


Figure 53 IE format – general

IE is optionally included in certain management type frames. The length field is the length of the information field in octets. The element id is a unique assignment id to information field according to the Table 10.

Element ID in decimal value	**IE name**	**Description**
0	Superframe parameters IE	Specifies superframe (beacon period) operation parameters
1	Uplink request IE	Specifies allocation slot-based requirements by a node for scheduled uplink allocation(s) in beacon or non-beacon mode with superframes
2	Downlink request IE	Specifies allocation slot-based requirements by a node for scheduled downlink allocation(s) in beacon or non-beacon mode with superframes
3	Bilink request IE	Specifies allocation slot-based requirements by a node for scheduled bilink allocation(s) in beacon or non-beacon mode with superframes
4	Type-I Unscheduled Bilink request IE	Specifies allocation slot-based requirements by a node for unscheduled bilink allocation(s) in beacon or non-beacon mode with superframes
5	Type-II unscheduled Bilink request IE	Specifies frame count-based requirements by a node for unscheduled bilink allocation(s) in non-beacon mode without superframes
6	Reserved	Reserved
7	Uplink assignment IE	Specifies allocation slot-based scheduled uplink allocation(s) assigned to a node in beacon or non-beacon mode with superframes
8	Downlink assignment IE	Specifies allocation slot-based scheduled downlink allocation(s) assigned to a node in beacon or non-beacon mode with superframes
9	Bilink assignment IE	Specifies allocation slot-based scheduled bilink allocation(s) assigned to a node in beacon or non-beacon mode with superframes
10	Type-I Unscheduled Bilink assignment IE	Specifies allocation slot-based unscheduled bilink allocation(s) assigned to a node in beacon or non-beacon mode with superframes
11	Type-II Unscheduled Bilink assignment IE	Specifies frame count-based unscheduled bilink allocation(s) assigned to a node in non-beacon mode without superframes

12	Reserved	Reserved
13	Nibble Encoded channel order IE	Specifies a list of 4-bit encoded channels in an operating band containing no more than 15 channels in the order of their selection by a hub as the operating channel
14	Channel hopping and ordering IE	Specifies a subset of channels included in channel hopping in the operating frequency band and/or a list of 8-bit encoded channels in the operating band in the order of their selection by a hub as the operating channel
15	Former hub address IE	Specifies the EUI-48 of the last hub with which the node was connected
16-244	Reserved	Reserved
255	Application specific IE	Provides user-defined application-specific information

Table 10 Assignment element id to information field

2.6.4.2 MAC functions

After some general thoughts an overview of the IEEE 802.15.6-2012 MAC sublayer functionality will be given. Especial the following issues will be considered: The frame processing, the abbreviated addressing, the full addressing, the priority mapping, the frame reception, the frame sequencing, the frame retries, the frame timeout, the frame separation, the frame acknowledgement, the duplicate detection, and the fragmentation and reassembly.

2.6.4.2.1 Frame processing

The frame processing provides the rules on preparing MAC frames for transmission and processing them on reception.

2.6.4.2.1.1 Abbreviated addressing

For every hub: A hub selects a one-octet BAN ID. This BAN ID should have a value between 0x00 and 0xFF. This address is an abbreviated address due to the fact that it is contained in the MAC header of all frames regardless the send direction (from or to the hub). The selected BAN ID is not in use from neighbor BANs. The hub selects also a one-octet hub id (HID) from an integer in the Connected_NID subset as given in the column NID notation in the Table 11. This abbreviated address contained in the MAC header of all frames sent from or to the hub. If a Connected_NID is already in use from a node connected to this hub the hub shall not reselect this Connected_NID as its HID. Also HIDs that are in use from neighbor hubs should not be selected.

For every node: a one-octet node id (NID) selected from an integer in the Connected_NID subset as given in the column NID notation. This NID is used as a *node's abbreviated address* contained in the MAC header of all frames send (unicast) to or from a node. The same NID shall also be used as an *abbreviated address of a group of nodes* contained in the MAC header of all frames sent (multicast or broadcast) to the nodes by a hub. The Broadcast_NID (in hex 0xFF) is the value of the Recipient ID field of the MAC header in beacon frames.

NID value in hex	NID subtotal	NID notation	NID usage
0x00	1	Unconnected_Broadcast_NID	For broadcast to unconnected nodes
0x01	1	Unconnected_NID	For unicast from/to unconnected nodes in a BAN
0x02-0xF5	244	Connected_NID	For unicast from/to connected nodes in a BAN
0xF6	1	Reserved	Reserved
0xF7-0xFD	7	Multicast_NID	For multicast to connected nodes in a BAN
0xFE	1	Local_Broadcast_NID	For broadcast to all nodes in a BAN
0xFF	1	Broadcast_NID	For broadcast to all hubs and nodes

Table 11 NID selection

These and other node NID transitions can be gathered from the diagram in the Figure 54.

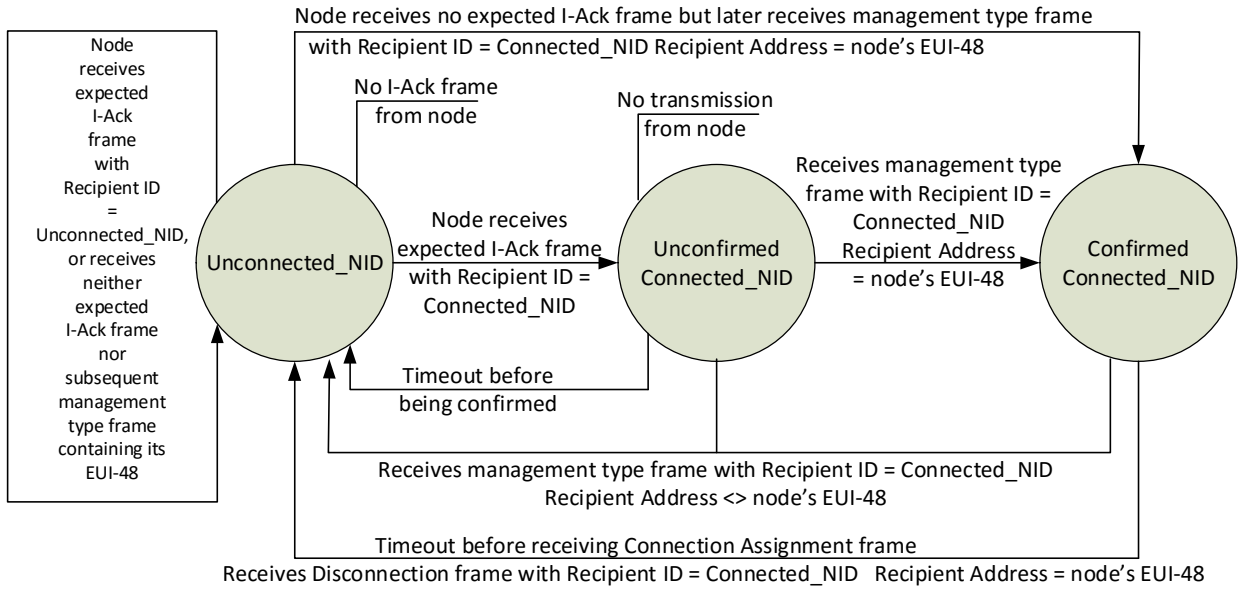


Figure 54 Node NID transition

2.6.4.2.1.2 Full addressing

Sometimes instead of abbreviated addressing full addressing is desired. EUI-48, the IEEE defined 48-bit global identifier is used for that, namely to uniquely identify a sender or a recipient. If a hub sends a beacon the EUI-48 of the hub is included in the frame payload of the beacon. The same is for the EUI-

48 values of sender or recipient regarding other management type frames. IEEE defines EUI-48 as follows: EUI-48 is an identifier whose limited uses include: (a) a 48-bit identifier used to address hardware interfaces within existing IEEE 802 or IEEE 802-like networking applications or (b) a 48-bit identifier of a specific hardware instance that is not necessarily a network address [19].

2.6.4.2.1.3 Priority mapping

There are exist user priority values as can be seen in Table 12. These values have to do with prioritization of medium access of data and management type frames. E.g. the frame payload „emergency or medical implant event report “of frame type data has the highest user priority 7.

Priority	**User priority**	**Traffic designation**	**Frame type**
Lowest	0	Background (BK)	Data
	1	Best effort (BE)	Data
	2	Excellent effort (EE)	Data
	3	Video (VI)	Data
	4	Voice (VO)	Data
	5	Medical data or network control	Data or management
	6	High-priority medical data or network control	Data or management
Highest	7	Emergency or medical implant event report	Data

Table 12 User priority mapping

2.6.4.2.1.4 Frame reception

We distinguish here between node reception and hub reception. The reception conditions for both cases listed below.

Node reception

A node receives a frame if

1. The recipient id field of the MAC header of the frame is set to its own NID (any applicable Unconnected_Broadcast_NID, multicast_NID, Local_Broadcast_NID, or Broadcast_NID).
2. The sender id field of the MAC header of the frame is set to the HID of the desired hub with which the exchange frames takes place.
3. The BAN ID field of the MAC header of the frame is set to an expected value.
4. The protocol version of the MAC header of the frame is set to a supported value.
5. The frame checks sequence (FCS) of the frame is valid, i.e., equal to the FCS value it calculates over the applicable fields received.

Hub reception

A hub receives a frame if

1. The recipient id field of the MAC header of the frame is set to its own HID.
2. The sender id field of the MAC header of the frame is set to the NID of an expected sender or the Unconnected_NID.

3. The BAN ID field of the MAC header of the frame is set to an expected value.
4. The Protocol Version of the MAC header of the frame is set to a value it supports.
5. The frame checks sequence (FCS) of the frame is valid.

Received frames are ignored from a hub or a node if they are duplicate or if the sender in the sender address field of the frame payload is not set to the EUI-48 of the expected sender or the receiver in the recipient address field is not set to the own EUI-48.

2.6.4.2.1.5 Frame sequencing

Two different cases regarding frame sequencing will be analyzed. The frame sequencing for management type frames and the frame sequencing for data type frames.

2.6.4.2.1.5.1 Management type frames

If a sender exchanges non-beacon management type frames with a recipient the frame sequence sends for secured (a) and unsecured communication (b) is presented in Figure 55.

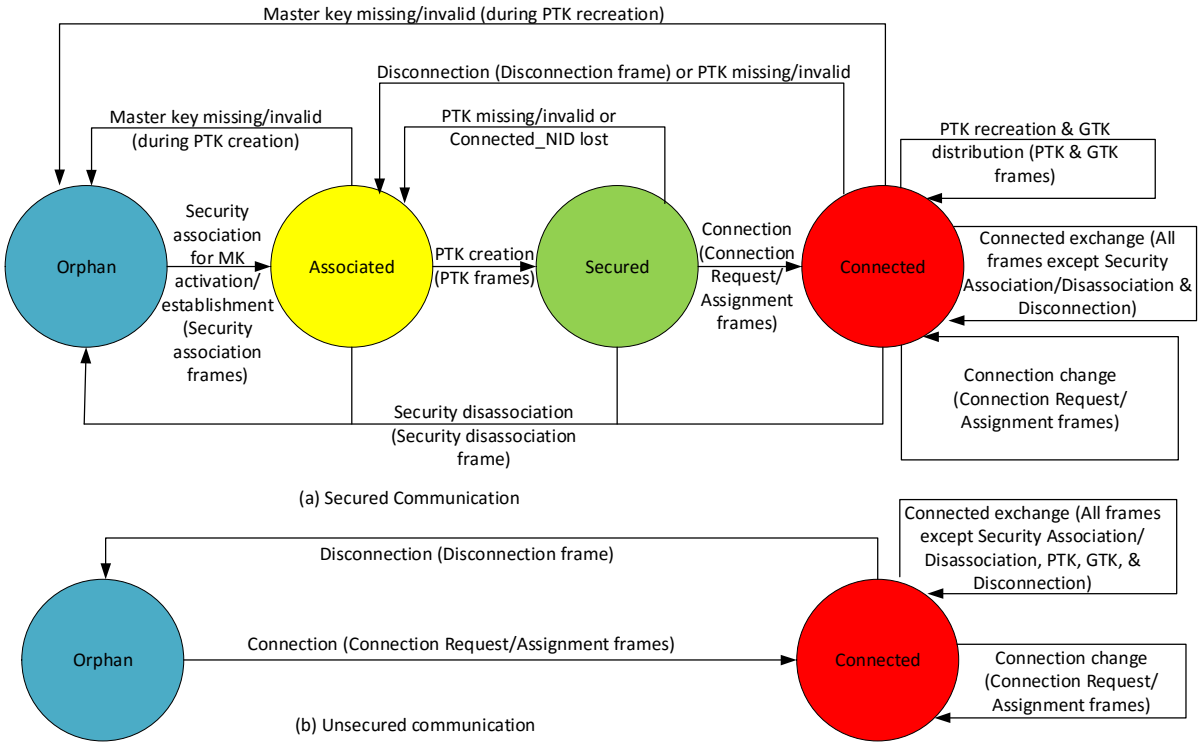


Figure 55 MAC state diagram

If a sender sends a management type frame f to the receiver and expect an I-ACK frame and a management type frame f+1 in this order but the I-Ack frame does not received and only the f+1 frame received, then the sender should consider that frame f has been received. It follows that the sender should now process the frame f+1.

It may be the case that the sender fragments a frame payload that could otherwise be part in a management type frame without length limitation. The sender shall extract the fragments in sequential octet order and transmit them in the same way beginning with the first which was extracted.

2.6.4.2.1.5.2 Data type frames

Here are some rules regarding frame sequencing in the case of data type frames.

a. If there is no payload in the data type frame sending by a sender, the MAC header field sequence number is set as if the frame contained a new MAC service data unit (MSDU).

b. Regarding the sender, the MSDUs sent arrive in the MAC SAP in a specific order (octet order). In this same order the sender shall transmit the MSDUs to the recipient. The MSDUs contained in data type frames which all of them have the same frame subtype and addressed to the same recipient(s). The same is for the recipient. MSDUs which transmitted to the recipient by the same sender and contained in data type frames of the same frame subtype are released from the same recipient to the MAC Client in the octet order in which they were received.

c. When the sender fragments an MSDU the fragmenting process consists of the extraction of the fragments in sequential octet order. In the same order the fragments extracted they are also sent by the sender.

d. Two MSDUs which are contained in data type frames which do not have the same frame subtype or they are not addressed to the same recipient, these both MSDUs can be transmitted by the sender independently.

2.6.4.2.1.6 Frame retry

The IEEE 802.15.6-2012 standard allows for nodes and hubs the retransmission of frames that they did not necessarily receive from the same recipient. It must be taken into account to take care about factors like channel conditions, medium availability, delay requirements and fairness policies.

2.6.4.2.1.7 Frame timeout

A node or a hub shall handle an expected frame, such as I-Ack or B-Ack frame, as not arriving after waiting for the physical layer preamble of the frame for a given amount of time (mTimeOut). To determine that an expected I-Ack, B-Ack, I-Ack+Poll or B-Ack+Poll frame did not arrive, the end of this frame should be estimated by assuming the expected length and the data rate currently applicable to that frame. For all other expected frames, the end frame estimation happens using the expected length of the frame and the highest mandatory data rate of the operating frequency band as specified in the corresponding PHY clause.

2.6.4.2.1.8 Frame separation

Short interframe space (SIFS), is the amount of time in msec required for a wireless interface to process a received frame and to respond with a response frame (ACK). It is the difference in the time between the first symbol of the response frame in the air and the last symbol of the received frame in the air [20]. Two successive frames are separated by a minimum interframe space (MIFS). pSIFS is the receive-to-transmit or transmit-to-receive turnaround time and pExtraIFS is the synchronization error tolerance.

In the case of a sender: if the sender is to send a frame pSIFS or pMIFS after the previous frame, the frame shall occur between pSIFS and pSIFS+pExtraIFS or between pMIFS and pMIFS+pExtraIFS, respectively, after the end of the previous frame.

In the case of a recipient: if a recipient is to receive a frame pSIFS or pMIFS after the end of the previous frame, it shall be ready to receive a frame no later than pSIFS or pMIFS, respectively, after the end of the previous frame. Also the recipient shall not exit receive state earlier than mTimeOut after the end of the PHY preamble of the expected frame.

2.6.4.2.1.9 Frame acknowledgement

The field ack policy in the MAC header of a frame to be transmitted is set from a node or hub as given in Table 13. A received frame should be acknowledged from the recipient by sending an immediate ACK (I-Ack) or block acknowledgment (B-Ack). This should be done

- if the criteria described in the above section *frame reception* which qualifies a frame as received are met and
- if required by the acknowledgment policy set in the frame (see below).

The recipient may send an I-Ack+Poll or B-Ack+Poll frame not only to acknowledge the received frame but also granting an immediate polled allocation or announcing a future poll or post.

Frame type name	Frame subtype name	Ack Policy field
Management	Beacon	N-Ack
Management	Security Association	I-Ack
Management	Security Disassociation	I-Ack
Management	PTK	I-Ack
Management	GTK	I-Ack
Management	Connection Request	I-Ack
Management	Connection Assignment	I-Ack
Management	Disconnection	I-Ack
Management	Command	I-Ack
Control	I-Ack	N-Ack
Control	B-Ack	N-Ack
Control	i-Ack+Poll	N-Ack
Control	B-Ack+Poll	N-Ack
Control	Poll	N-Ack
Control	T-Poll	N-Ack
Control	Wakeup	N-Ack
Control	B2	N-Ack
Data	Data subtype set to mG-AckDataSubtype	G-Ack
Data	User-defined data subtype other than mG-AckDataSubtype	N-Ack, I-Ack, L-Ack, or B-Ack

Table 13 Acknowledgement (ACK) policy field setting

If sender and recipient are not at *connected state,* the hub or the node send an I-Ack or B-Ack using the lowest mandatory data rate of the operating frequency band. If sender and recipient are at *connected state,* the hub or the node send an I-Ack or B-Ack using the data rate indicated in the Assigned Ack Data Rates field of the last connection assignment frame exchanged with the recipient.

2.6.4.2.1.9.1 No acknowledgment (N-ACK)

If a node or hub sends a frame with the Ack policy field set to N-Ack, then it requires no acknowledgment at all. If the recipient received a frame containing an Ack policy field set to N-Ack, no acknowledgment will be sent.

2.6.4.2.1.9.2 Group acknowledgment (G-ACK)

A group acknowledgment is sent only from a node to a hub. To set the Ack policy field to G-Ack two conditions must fulfill. The transmitted frame is a data type frame and has the frame subtype set to mG-AckDataSubtype. The second one is that G-Ack is supported from the hub as indicated in its last transmitted MAC Capability field.

The hub acknowledges these data type frames (having Ack Policy field set to G-Ack and the frame subtype field set to mG-AckDataSubtype) by including the NIDs of the nodes (which send the G-Ack) in the frame payload of the next B2 frame. The specification here specifies that the hub should send the B2 frame as soon as permitted. If the node does not get the expected B2 frame it may retry the frame. An example for a group acknowledgment is shown in the Figure 56.

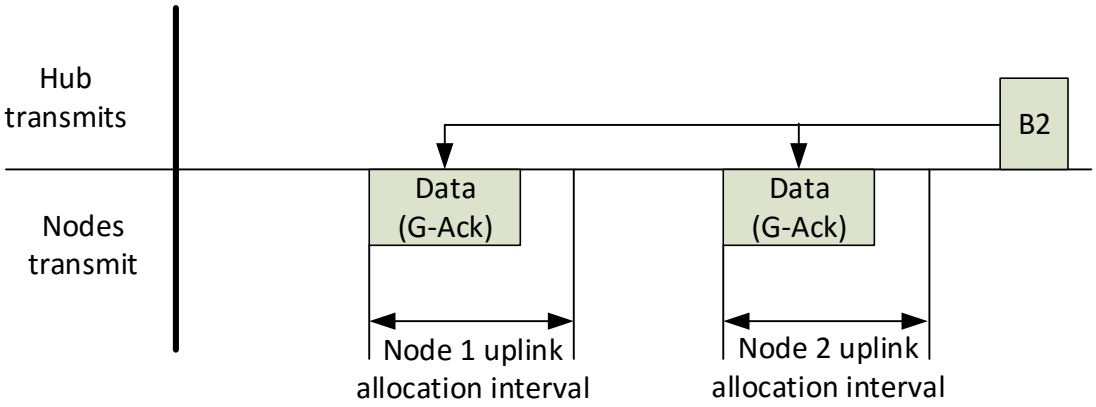


Figure 56 Group acknowledgment (G-Ack)

2.6.4.2.1.9.3 Immediate acknowledgment (I-Ack)

A node or a hub that requires an immediate acknowledgment, fills the Ack policy field of the transmitted frame with the value I-Ack. The recipient acknowledges this received frame by sending back an I-Ack frame pSIFS msec after the end of the received frame. Some examples are shown in Figure 57.

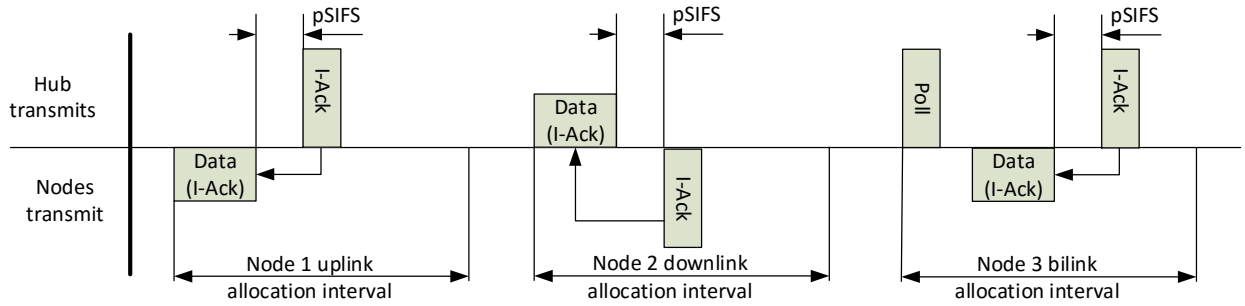


Figure 57 Immediate acknowledgement (I-Ack)

2.6.4.2.1.9.4 Block acknowledgment later (L-Ack) and block acknowledgment (B-Ack)

A block transmission is a transmission of data type frames whose reception status will be provided in the next B-Ack frame and whose frame subtype is the same as that of the data type frame preceding this B-Ack frame. A block transmission starts from the first frame sent after the last B-Ack frame received and ends with the next earliest frame with the Ack policy field set to B-Ack (Figure 58).

A node or a hub send a data type frame with B-Ack if:

- the frame contains a whole MSDU
- the recipient supports L-Ack/B-Ack

The recipient send back a B-Ack frame pSIFS msec after the end of the received frame.

A node or a hub (here called the source) send a frame with L-Ack if:

- the frame contains a whole MSDU
- the source has sent a frame of the same frame subtype with B-Ack and received a B-Ack frame acknowledging that frame and containing a frame payload
- that B-Ack frame was the last B-Ack frame received from the recipient

Regarding the number of transmitted frames in a block transmission is to say that the source shall not transmit more frames than allowed as specified in the last B-Ack frame received. The source ends a block transmission with a frame having the Ack policy field set to B-Ack.

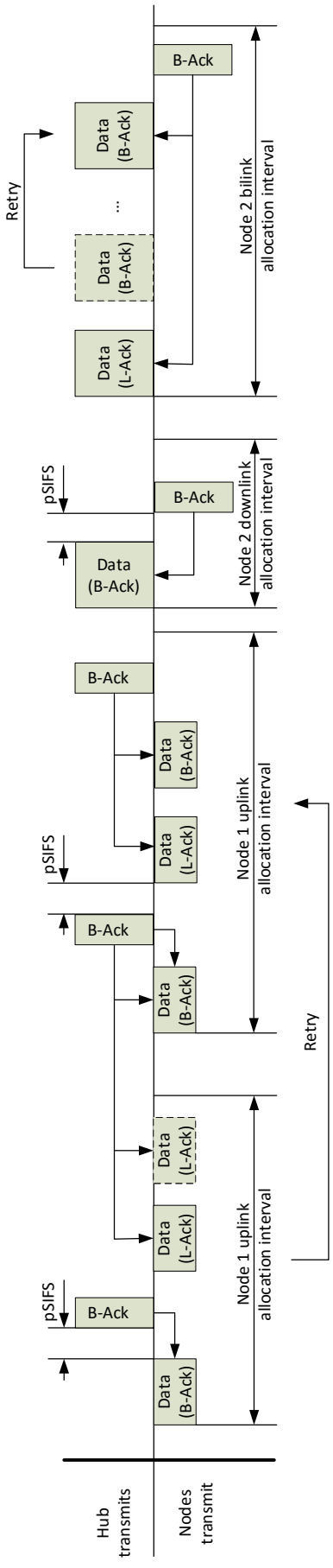


Figure 58 L-ACK and B-ACK

2.6.4.2.1.10 Duplicate detection

The recording of the sequence number and the fragment number of the MAC header of the last non-beacon management type frame received from each sender is a requirement for the recipient. In this way the recipient can recognize the next management type frame received from the same sender with the same sequence number and fragment number of the MAC header as a duplicate frame. The frame will be discarded. The same procedure is defined also for data type frames.

2.6.4.2.1.11 Fragmentation and reassembly

If the recipient supports fragmentation the sender may fragment a frame payload that could otherwise be included in a management type frame without length limitation.

If the received MSDU has missing fragments, then the recipient will discard it. Before the recipient delivers the MSDU to the MAC client the recipient shall completely reassemble the MSDU in the correct order.

2.6.4.2.2 Access classification and division

The establishment of a time base is a requirement for a hub if this hub should provide time referenced allocations. This happens regardless of whether the hub is to transmit beacons. The hub transmits a beacon in each beacon period (unless it is an inactive superframe) or does not transmit a beacon in any superframe (beacon period). To prevent transmission collisions with neighbor BANs the hub shift (rotate) its beacon transmission time for all scheduled allocations according specific rules (beacon shifting) from one offset from the start of current beacon period to another offset from the start of next beacon period. If a hub should not support time referenced allocations in its BAN, it operates without a time base and inferentially do not need to transmit beacons at all.

We will present three access modes for hub operation:

- Beacon mode with beacon periods (superframes)
- Non-beacon mode with superframes
- Non-beacon mode without superframes

2.6.4.2.2.1 Beacon mode with beacon periods (superframes)

This mode is characterized by existing access phases in each active beacon period. The hub transmits a beacon and provides access. On the contrary in an inactive superframe a hub does not transmit any beacon and does not provide any access phases.

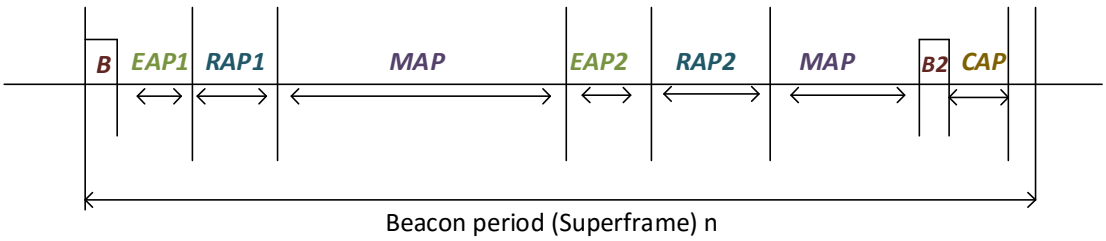


Figure 59 Layout of access phases in a beacon period for beacon mode

The hub places the access phases ordered as following (Figure 59):

- Exclusive access phase 1 (EAP1)
- Random access phase 1 (RAP1)
- Managed access phase
- Exclusive access phase 2 (EAP2)
- Random access phase 2 (RAP2)
- Managed access phase
- Contention access phase (CAP)

In EAPs, RAPs and CAPs the node look for resource allocation via either the Aloha access procedure or CSMA/CA. CAP, RAP1 and RAP2 are used for regular traffic. EAP1 and EAP2 are used for high priority traffic such as reporting emergency events. MAP phases are utilized for bilink-, downlink-, uplink- and delay bilink allocation intervals. Polling is used in MAP phases for resource allocation. Depending on the application any of these periods can be disabled by setting the duration length to zero. The beacon frame B2 is send if the length of the following CAP is non-zero.

2.6.4.2.2.2 Non-beacon mode with superframes

In the non-beacon mode with superframes a hub has only a managed access phase (MAP) in any superframe (beacon period) as shown in Figure 60.

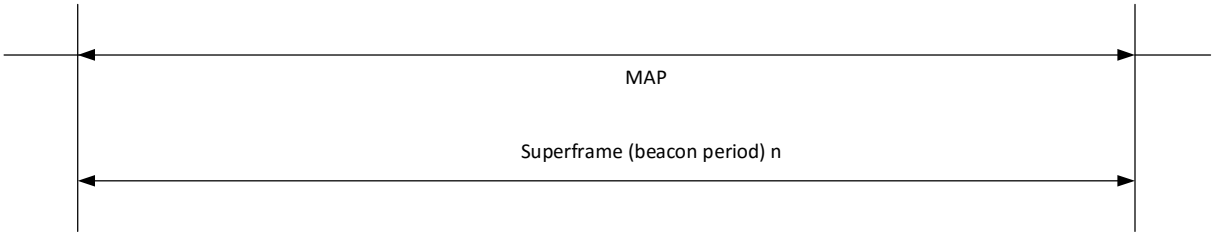


Figure 60 Non-beacon mode with superframes

2.6.4.2.2.3 Non-beacon mode without superframes

A hub provides unscheduled bilink allocation intervals which comprise type-II polled allocations and/or posted allocations. A node after determining that the hub is operating in this mode may treat any time interval as a portion of EAP1 or RAP1 and uses CSMA/CA based random access to obtain a contended allocation (Figure 61).

In summary we determine three types of access mechanisms exists in each period of the superframe:

(a) *Scheduled access and its variants (connection-oriented contention-free access)* – This access mechanism schedules slot allocation in one or multiple upcoming superframes.
(b) *Unscheduled and improvised access (connectionless contention-free access)* – This access mechanism utilizes posting or polling for resource allocation.
(c) *Random access mechanism* – In this access mechanism either the slotted CSMA/CA or Aloha procedure are used for resource allocation.

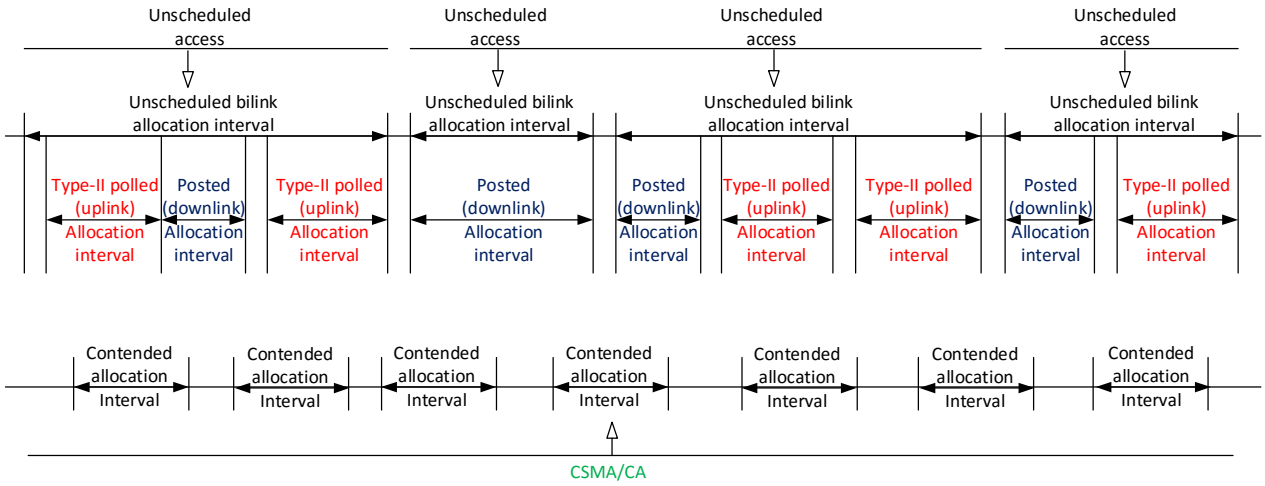


Figure 61 Allocation intervals and access methods for non-beacon mode without superframes

2.6.4.2.3 BAN creation/operation and node connection/disconnection

In this section we describe the BAN creation/operation and the node connection/disconnection.

2.6.4.2.3.1 BAN creation/operation

Based on policy regulations, channel conditions, application requirements and coexistence considerations a hub choose an operating channel to start a BAN. A new channel can be chosen if regulations require it or/and a hub may hop to new channels periodically achieving interference mitigation and frequency diversity. Before sending a frame to the hub, a node shall find the operating channel of the hub. The hub selects an applicable access mode as described above in the chapter 2.6.4.2.2 (**Access classification and division**). We refer to one use case, the use case the hub selected beacon mode with superframes. In this case the hub transmits T-Poll frames each addressed to Unconnected_Broadcast_NID and provides a Type-I polled allocation to facilitate unconnected nodes connection or reconnection with the it.

2.6.4.2.3.2 Node connection

The connection procedure is described in the Figure 62. The node transfers a connection request frame to the hub and the hub answers with an I-Ack and a connection assignment frame. The node responds with an I-Ack frame.

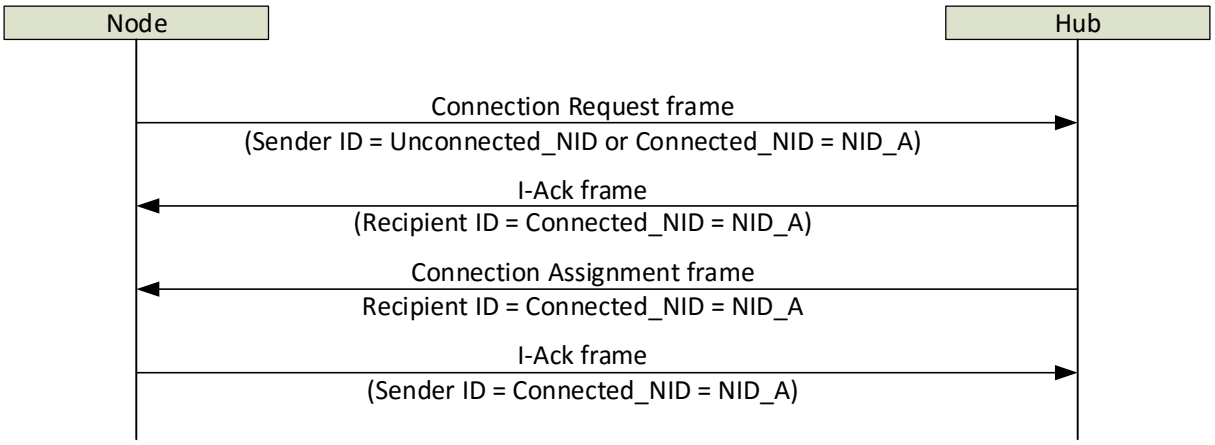


Figure 62 Connection procedure

2.6.4.2.3.3 Node disconnection

The node disconnection can be initiated by node or by hub. Both cases showed in Figure 63. Figure 63 (a) shows the node disconnection initiated by node and (b) shows the node disconnection initiated by hub.

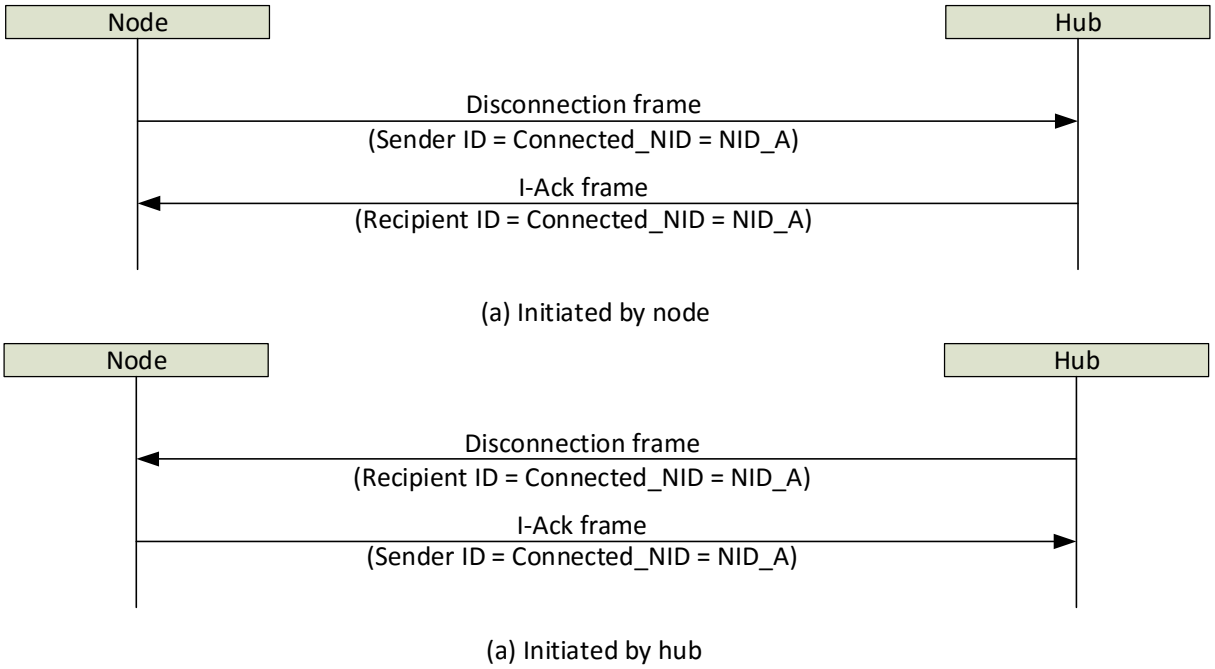


Figure 63 Disconnection procedure

2.6.5 Physical Layer

The IEEE 802.15.6 standard defines a Medium Access Control (MAC) Layer supporting three physical layers (PHY): The Narrowband (NB), the ultra-wideband (UWB) and the Human Body Communications (HBC) frequency.

Which of the three physical layers should be chose depends on the application of the WBAN, if it is a medical or a non-medical application and if the nodes are in, on or off-body nodes.

We consider here the narrowband (NB) as example. The NB PHY has the following duties:

- Activation/deactivation of the radio transceiver
- Clear Channel Assessment (CCA) within the current channel
- Data transmission/reception

2.6.5.1 Protocol Data Unit (PDU)

Outgoing from OSI model protocols describe rules that control horizontal communication, that is, conversations between processes that run at corresponding layers. This communication take place at every layer except the first layer using a kind of message that is send between corresponding software elements on two or more devices. Since these messages are the mechanism for communicating information between protocols, they called protocol data units (PDU). The implementation of each PDU depends on the features and requirements of the corresponding protocol.

2.6.5.2 Service Data Unit (SDU)

The communication higher than layer one is a logical communication. The only hardware connection is at the physical layer. Lower layers provide services to the layers above them: they handle and manage data received from the layer above. Each protocol creates a PDU for transmission that includes headers required by that protocol and data to be transmitted. In order for a protocol to communicate, it must pass down its PDU to the next lower layer for transmission. When a protocol, let say protocol N, pass down its PDU to the next lower layer N-1, this PDU becomes the data that the layer N-1 protocol going to service. For this reason, the layer N PDU called the layer N-1 Service Data Unit (SDU). The layer N-1 builds its own PDU using the SDU (PDU from layer above) and the rules for its own PDU format (header/footer). The layer two PDU is converted to bits and sent at layer one. The mechanism described here called *data encapsulation* due to the fact that the entire contents of the higher-layer message are encapsulated as the data payload of the message at the lower layer.

2.6.5.3 Physical Protocol Data Unit (PPDU)

The PPDU is the PDU of the physical layer. The PPDU frame in the IEEE 802.15.6 specification consists of three parts (Figure 64): The *Physical Layer Convergence Procedure (PLCP) preamble*, a *PLCP header* and a *PHY Service Data Unit (PSDU)*.

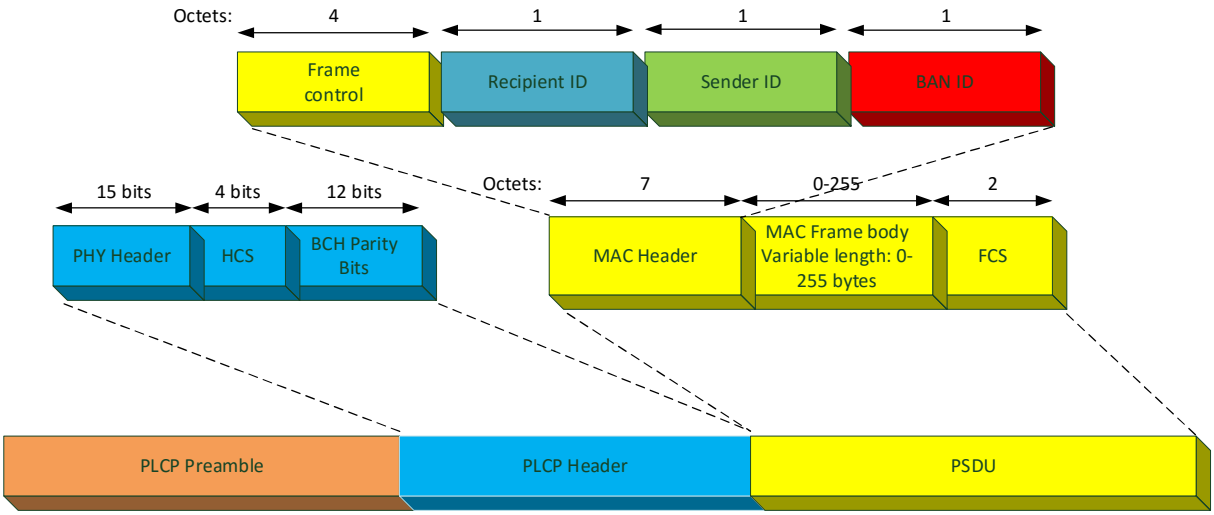


Figure 64 Structure of NB PPDU based on IEEE 802.15.6

2.6.6 WBANs-Requirements in IEEE 802.15.6

The goals of the IEEE 802.15.6 standard defined in purpose. These goals are translated in the same standard document in several requirements. A list of these requirements is following here.

WBAN requirements

- A WBAN must allow priority services
- A WBAN must implement selfheal mechanisms
- A WBAN must be secure
- Regarding Receiver sensitivity

Given additive white Gaussian noise (AWGN) for a PER <= 10% with a PSDU of 255 octets, a compliant device should achieve sensitivities listed in the table below (Table 14):

Frequency band (MHz)	Information data rate (kbps)	Maximum input level at sensitivity (dBm)
402 to 405	75.9	-95
	151.8	-92
	303.6	-89
	455.4	-83
420 to 450	75.9	-90
	151.8	-87
	187.5	-84
863 to 870 902 to 928 950 to 958	101.2	-94
	202.4	-91
	404.8	-87
	607.1	-82
2360 to 2400 2400 to 2483.5	121.4	-92
	242.9	-90
	485.7	-87
	971.4	-83

Table 14 Receiver Sensitivity Numbers

- In a $6m^3$ cube the physical layer must support up to 10 co-located and randomly distributed WBANs
- Support of bit rates from 10 Kb/s to 10 Mb/s
- Operation of WBANs in a heterogeneous environment
- To achieve operation in power constrained environments IEEE 802.15.6 requires from WBANs to implement power saving mechanisms
- Within range coexistence of In-body and On-body WBANs
- A Narrowband WBAN should be able to support high data rates and to cover different environments. Therefor NB WBANs can incorporate UWB technology
- Each WBAN can support 256 nodes
- Transmission at 0.1 mW (-10 dBm) should be possible by any participating device
- Maximum radiated transmission power less than 1 mW (due to specific absorption rate (SAR) of the Federal Communication Commission which is 1.6 W/Kg in 1g of body tissue)
- *Jitter* less than 50 ms. Jitter is defined as the deviation from true periodicity of a presumed periodic signal, often in relation to a reference clock source [21]
- Latency for medical applications less than 125 ms and for non-medical applications less than 250 ms. *Latency* is defined as a time interval between the stimulation and response, or, from a more general point of view, as a time delay between the cause and the effect of some physical change in the system being observed [22]

Node requirements

- It should be possible to add or remove nodes in the WBAN network in less than three seconds
- Use case "the person wearing the WBAN(s) is on move". Reliability of data if the person wearing the WBAN(s) is on move. No loss of data due to unstable channel conditions which could enter because of running, walking, sitting or other "moving" activities. Such activities could cause fading [23]

2.7 MAC PROTOCOLS FOR COGNITIVE RADIO BODY AREA NETWORKS

Cognitive radio (CR) is a form of wireless communication in which a transceiver can intelligently detect which communication channels are in use and which are not, and instantly move into vacant channels while avoiding occupied ones. This optimizes the use of available radio-frequency (RF) spectrum while minimizing interference to other users [24].

Determination of the CR geographic location, user identification and authorization, signal encryption and decryption, sense neighboring wireless devices in operation, regulation of output power and modulation characteristics, are some of the possible functions of CR.

A *cognitive radio body area network (CRBAN)* is a CR-enabled WBAN.

The difference between CRBANs and other wireless networks is the fulfillment of specific requirements for the medium access control (MAC) sublayer through CRBAN MAC protocols. MAC plays a key role in CR functions like

- Resource allocation
- Channel sensing
- Spectrum sharing
- Spectrum mobility

In this section we will examine some of the current MAC protocols for CRBANs. CRBANs evolve to a key technology in wireless networks including fifth-generation mobile networks. The main reason for that is the spectrum scarcity problem. The benefit of CR is that unlicensed users through CR can access underutilized licensed or white space spectra. The term white space usually refers to unoccupied portions of spectrum in the VHF/UHF terrestrial television broadcasting frequency bands. Some countries test to improve the utilization of the highly valued spectrum resource by implementing sharing of the spectrum between the primary television service and other services. Broadband wireless applications belong to the main focus of sharing trials, but also other applications like machine-to-machine communications (e.g. WBANs or CRBANs) [25] may have an advantage in that they use white spaces. The common pattern involved with all these alternative wireless applications is their low-power nature, which makes them well-suited for operation under a license-exempt regulatory framework. CR technology enables unlicensed users or secondary users (SUs) to access underutilized licensed spectrum in the case the primary users (PUs) are idle. In general, PUs are noninterfering among themselves, i.e., they can transmit at the same time. SUs operate within the interference range and on the same channels as PUs. A PU accesses its channel without sensing. The access of the SUs is called *opportunistically access*. We explain here the meaning of the four CR functions which mentioned above.

Resource allocation is the assignment of not occupied channels to SUs according to some QoS requirements.

Channel sensing is the estimation of the channel state information and the analysis of the radio environment.

Spectrum sharing is the function of avoidance of harmful interference between PUs and SUs.

Spectrum mobility describes the handover of the channel from the SU to the PU if a PU user detected and in the same step the assignment of a vacant channel to SU for re-establishing communication. Spectrum mobility is a main novel concept introduced by CR.

CR technology can help reducing electromagnetic interference in WBANs which otherwise may cause malfunction. Through CR technology also QoS can be achieved in wireless communication between medical devices. This happens by defining priority levels for the different devices. The MAC sublayer controls the most of radio modules which perform the above mentioned-tasks. There are only few existing MAC protocols for CRBANs in contrast to the number of WBAN MAC protocols. In the next section we will examine some MAC design issues.

2.7.1 MAC design issues

There are some differences between the CR MAC and the traditional MAC protocols. One of the differences is the number of available channels. In CRBANs this number varies both in time and spatial dimensions. In traditional WBAN networks it is fixed for every user. Another difference is that MAC protocols in CR networks take care to protect PUs from interference. The follow issues must be considered in case of a CR MAC protocol design: Self-coexistence, energy efficiency, cross-layer design, opportunistic sensing, and optimized spectrum decision which are described next.

2.7.1.1 Self-coexistence

Prevention of a possible collision and interference with PUs and provoked by the SU is one of the most important subject for the MAC protocol in CRBANs.

The term *co-existence* is the ability of radio to coexist with other radios in the same spectrum bands but using different protocols. There are two different types of co-existence; incumbent co-existence, between licensed and unlicensed users and self-coexistence, between secondary users. CR can be thought as the next development step after self-coexistence, i.e., automated coexistence based on dynamic frequency selection, dynamic channel selection and transmit power. Self-coexistence is not easy to achieve in a CR scenario, because

- of the non-deterministic activities of PUs
- no existence of frequency allocations
- neighboring SUs compete for the same white spaces

Effective spectrum access can be achieved using one of two possible approaches. The underlay and overlay approach.

In the underlay approach a wide frequency band (e.g. UWB) must be applied to enable the SUs not to exceed the interference limit PUs can tolerate. Use of let say UWB means that the SUs use lower energy levels and wider frequency bandwidth (bandwidths higher than 500 MHz) to enable a short range high data rate and to generate a signal that PUs interpret as noise. Because of the interpretation of the signal as noise, it is not needed to issue the spectrum handover. The underlay approach enables the SU to use the spectrum even in the presence of PU activity.

In the overlay approach the transmission power is higher and the frequency bandwidth is limited in range. When a PU appears, the licensed channel must immediately be vacated (service interruption loss) and the SU must find also immediately another channel. The overlay approach requires appropriate and accurate sensing and signaling mechanisms to deal with PU activity.

2.7.1.2 Energy efficiency

The minimization of energy waste in CRBANs is important due to the small batteries used by the CRBAN sensors. The waste of energy depends on factors such data collisions, packet overhead, idle listening, traffic fluctuation and overhearing.

Overhearing is the reception of a packet or part of a packet destined to another node.

All these factors must be taken into account to provide energy efficiency.

2.7.1.3 Cross-Layer design

Cross-Layer design is necessary because the function of spectrum management is performed from all network layers and not only from the PHY layer and the MAC sublayer as spectrum sensing does. A coordination of all the layers of the protocol stack is a must in the implementation to achieve reliability and network performance.

2.7.1.4 Opportunistic sensing

From the perspective of PUs, s*pectrum sensing* helps to determine, if a channel is busy (it has primary user activity) or it is idle. Sensing times are decided by CR MAC protocols.

If a SU get or has the opportunity, it senses a channel and maintain a list of empty channels. These channels are independent of other nodes. Opportunistic sensing is the process where the CR node transmits its data packet without sensing but using a channel from the empty channel list. This bring with it the advantage of a short transmission delay. For sensing the complete channel, a node must cooperate with the other nodes to adjust the sensing priorities.

2.7.1.5 Optimized spectrum decision

CR-aware MAC protocols choose the best spectrum using minimum time and energy. Different methods are in use to learn and decide which is the best spectrum like fuzzy logic or the Markov decision process.

2.7.2 MAC protocols for CRBANs

The main intention to use cognitive radio (CR) is to maintain the signal-to-noise ratio (SNR) for data exchange and to manage the disadvantages of high coexisting interference in WBANs. Using dynamically scanning and switching channels, WBANs can save energy, reduce packet delays and drops and avoid coexisting interference. In this part of the work we will give an overview of five different MAC protocols for CRBANs where these practices are in use. These are:

- the CR-Based MAC protocol for cognitive wireless sensor body area networking
- the dynamic channel adjustable asynchronous cognitive radio MAC protocol
- the asynchronous MAC protocol for spectrum agility
- the cognitive radio for medical body area networks using ultra-wideband

2.7.2.1 CR-Based MAC protocol for cognitive wireless sensor body area networking (CR-MAC)

This protocol is characterized by the capability of the nodes to dynamically adjust their transmission power according to the level of traffic urgency. Separate types of sensors are used for critical and non-critical health information. Critical and non-critical nodes are implemented as reduced function devices (RFD) and hubs are implemented as full function devices (FFD). The receiver circuit on the hub side enables the reception of critical and non-critical packets simultaneously [26].

2.7.2.2 Dynamic channel adjustable asynchronous cognitive radio MAC protocol

The *dynamic channel adjustable asynchronous cognitive radio MAC* (DCAAC-MAC) protocol provides low latency, configurability, energy efficiency and no need for synchronization in wireless MBANs due to its fast channel switching capability. At the initialization phase every node selects after a scanning process the channel with the best conditions, e.g. low signal-to-noise ratio (SNR). Node and hub communication takes place as follows. Each CR-BAN node sleep and wake up periodically and independent from other nodes or hubs. If the node has packets to send, it sends at first a preamble. The hub receives the preamble, sends an ACK to the node to acknowledge the received preamble and it stays awake to receive the data packet. The node sends the data packet to the hub. After that node and hub go to sleep mode. During the communication process if the node detects interference on its channel, e.g. noise or PUs, it switches to another channel.

One substantial requirement of cognitive radio is spectrum sensing. There exist two techniques for spectrum sensing in a CR environment. There are the *energy detection* and the *feature detection*. The feature detection method detects PUs by extracting specific features. On the one hand feature detection is the most effective spectrum sensing method for CR networks. On the other hand, it is computationally complex and requires significantly long sensing times. DCAA-MAC uses the energy detection method for spectrum sensing because it is the optimal method to sense the presence or absence of PUs.

In DCAA-MAC the node switches to another channel if the address of the destination is not decoded. Not decoded destination address means that PUs have appeared or interference occurred. Through

the use of energy detection for channel switching DCAA-MAC provides QoS. The protocol has low energy consumption, low latency and can coexist with simultaneously operating networks.

2.7.2.3 C-RICER, an asynchronous MAC protocol for spectrum agility

The *cognitive-receiver initiated cycled receiver (C-RICER)* MAC protocol is an energy-efficient MAC protocol, which was designed for operating in high interference WBASN environments. A *wireless body area sensor network (WBASN)* is used in the literature the same as a WBAN. C-RICER reduces interference and energy consumption through adjustment of channel frequency and transmission power through early detection of interference in its working channel.

A well-known contention-based receiver-initiated MAC protocol is the RICER protocol with one of its variants, the RICER3b protocol. In the RICER3b protocol the destination node wakes up periodically and transmits a short wakeup beacon to indicate that is not sleep. After that it monitors the channel waiting for a response. In the case of no response it goes back to the sleep mode. If a node has data to send, it remains awake, monitors the channel waiting for a wakeup beacon from the destination nodes. After receiving the wakeup beacon, the transmitter node sends back a buzz signal to the destination node signaling the data transfer and then starts transmitting data. The receiver receives the buzz signal, stays awake and waits for the data of the sender node. Figure 65 shows the conceptual operation in a C-RICER. The data communication in C-RICER is based on RICER3b. The hub (coordinator) of the WBASN performs periodically channel sensing. It depends on the detected level of interference, if the WBASN would switch to the lowest interference channel, preventing in this way coexisting interference. The processes of sensing and channel switching are continuously processes during the WBASN operation. Due to the unpredictability of the appearance of channel interferences frequent channel switching demands a considerable amount of energy. C-RICER resolves that using power adaption prior the channel switching.

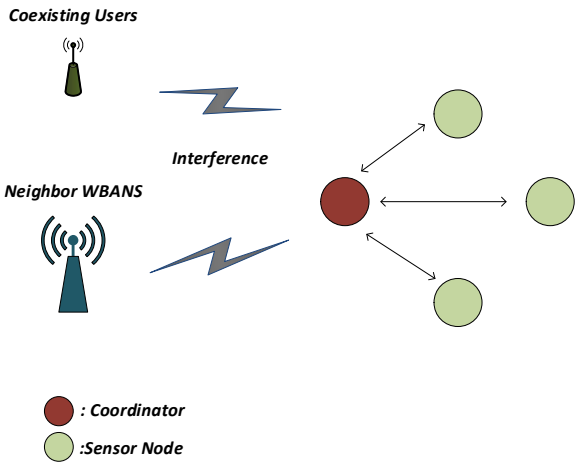


Figure 65 C-RICER in WBASN

The main working mechanism of C-RICER consists of the follow two tasks:

- data exchange
- a cognitive task

The data exchange task selects the data. The cognitive task in C-RICER handles channel sensing, transmission power adaption and channel switching according to the interference level. We will comment briefly on the three steps.

2.7.2.3.1 Channel sensing

This is the initial step in detecting interference. The *received signal strength indicator (RSSI)* has been established for the measurement of the interference level in different channels. *Signal strength* is based on the output power of the transmitter (the original strength of the signal), the sensitivity of the receiver (how well the receiving device can hear weak signals), the gain of the antenna at both ends of the path, and the path loss, or attenuation of the signal as it travels through the air from the transmitter to the receiver. Signal strength is expressed in units of decibels (dB). Due to the low-power levels and the attenuation of free space, an RSSI value is expressed as a negative number. The more negative the number, the weaker the signal strength; conversely the closer the number is to zero, the stronger the signal. An example for the relation between RSSI range and signal quality is given in the

Table 15.

RSSI Range	Signal Quality
Better than -40 dB	Exceptional
-40 dB to -55 dB	Very Good
-55 dB to -70 dB	Good
-70 dB to -80 dB	Marginal
-80 dB and beyond	Intermittent to No Operation

Table 15 Relation between RSSI range and signal quality

In WBANs the hub is the device most suited for channel sensing. As a consequence of that, exploiting the energy at the hub leads to prolong the network's lifetime. The hub of C-RICER periodically scans the interference level of its current channel. If the measured value is greater than a threshold value, the hub scans for the interference level of the remaining channels.

2.7.2.3.2 Transmission power adaption

The algorithm of the power adaption strategy is given in the Figure 66.

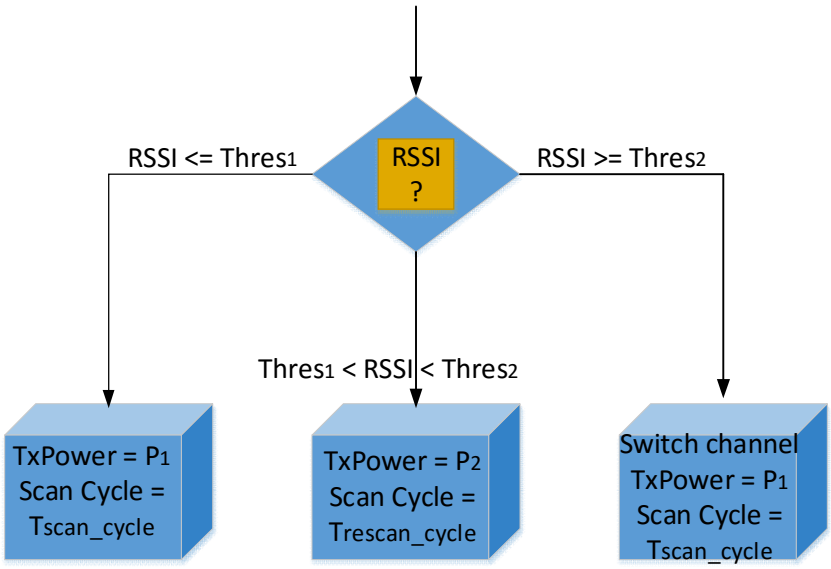


Figure 66 Power adaption strategy in C-RICER

The transceiver at each node is proposed to have two specific transmission powers (TxPowers), P_1 and P_2, where $P_1 < P_2$. Two interference threshold values $Thres_1$ and $Thres_2$ are introduced with $Thres_1 < Thres_2$. $Thres_1$ and $Thres_2$ are also defined for the transceiver at each node. SNR is the signal-to-noise radio and RSSI is the received signal strength indicator. The packet error rate will increase proportional to the interference levels $Thres_1$ and $Thres_2$. $Thres_2$ should be selected in such a way that the interference starting to affect the packet error rate, by use of P_2, is still acceptable for the sending of control packets. The power adaption strategy algorithm is as follows.

If the RSSI of the current working channel is less or equal than $Thres_1$ (RSSI <= $Thres_1$):

The transceiver of each sensor node will operate with the default transmission power of P_1.

If the coordinator identify that the RSSI value of current channel is between $Thres_1$ and $Thres_2$ ($Thres_1$ < RSSI < $Thres_2$):

The transceiver of each sensor node will increase the TxPower and operate with the transmission power of P_2. Once the nodes operate with transmission power P_2, the hub will adaptively change its scanning cycle by quickly coming back in T_{rescan_cycle} seconds to rescan the channel. After scanning, if the RSSI value of the current channel becomes less than $Thres_1$, the WBASN will return back to use P_1. On the other hand, if the RSSI value is still greater than $Thres_1$, the hub scans the remaining channels to build the channel interference map, and the WBASN will switch to a new channel with the lowest interference level among the map. The transmission power is changed to the default value P_1. The change of the transmission power to P_1 reduces the use of a high TxPower P_2 for long time which costs energy.

If the value of RSSI is greater or equal than $Thres_2$ (RSSI >= $Thres_2$):

The hub scans the remaining channels to build the channel interference map and the whole network will switch to the channel with the lowest interference level in the interference map without changing transmission power.

The hub utilizes the wake up beacon message to broadcast its TxPower information to the nodes. The wake up beacon message is added one dedicated bit which contains the information of TxPower level. The nodes will extract this bit from the wake up beacon message. If this bit is zero, P_1 is used. If not, P_2 is used.

2.7.2.3.3 Channel switching

When the interference level of the current working channel is greater than $Thres_2$ or it is still high after rescanning, based on the information in the interference map the WBASN will decide to switch to a new channel. Here we will describe the algorithm used by the C-RICER hub to notify the channel switching information to the nodes. This algorithm is shown graphically in the Figure 67. Slave is the node and coordinator is the hub.

Traditional cognitive radio networks use at each node two transceivers, one for sharing channel information and one for data exchange. In WBASNs every node or hub consists only of one transceiver making the channel switching process more complicated. Another issue here is the fact that nodes wake up only if they want to send data. This means that nodes with different sensing functions wake up randomly and do not receive the channel switching information which is send by the hub. Under

these circumstances the hub maintains a checklist for nodes that received the channel switching information.

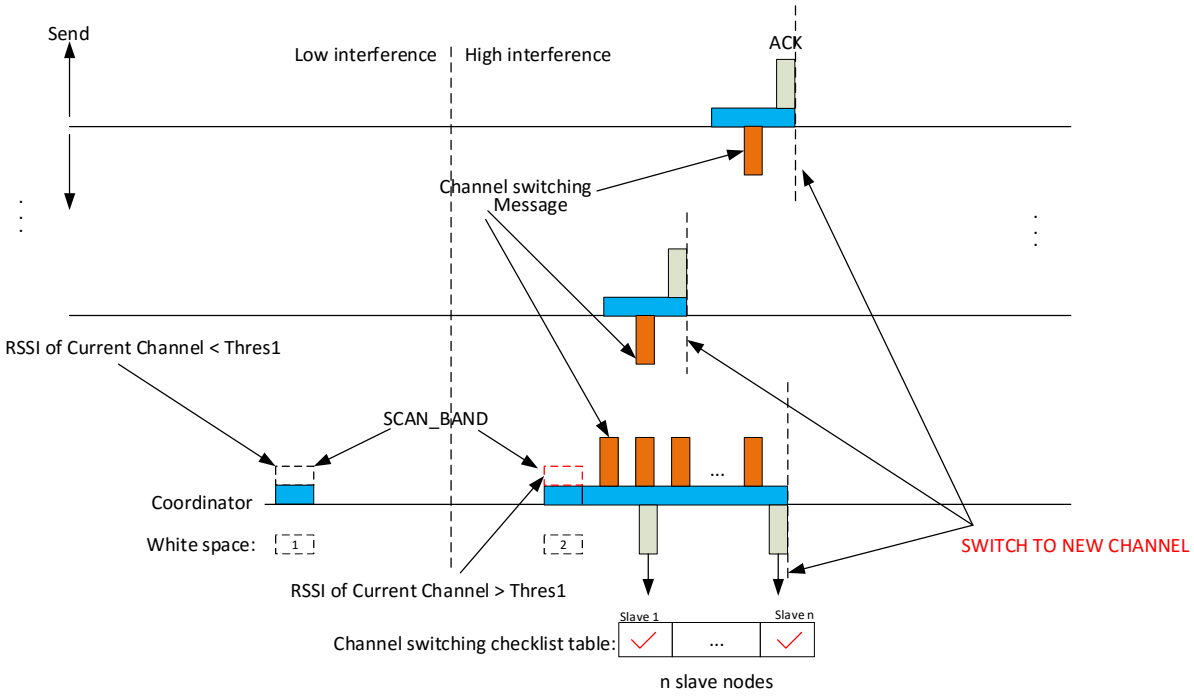


Figure 67 Channel switching algorithm of the C-RICER protocol

In the interference map every listed channel has a unique index. After a channel switching decision, the hub prepares a *channel switching message* attaching to it the index of the channel with the lowest RSSI among the channels in the interference map. After preparing the channel switching message the hub broadcasts it periodically to the complete set of nodes and waits to receive the ACK message from every node separately. The node sends an ACK message to the hub after the successful receiving of the channel switching message. The hub receives the ACK message from the node and inserts this node in the checklist. When the checklist is complete, that means that every node has got the channel switching message and send successful its ACK to the hub, the hub switches to the new channel.

In the case, that the node must send data packets to the hub it wakes up and wait for a wake up beacon message from the hub. If during the period of waiting for the hub beacon message, the node receives a channel switching message it will respond as described above.

If after the period $T_{waite\ checklist}$ the hub does not receive an ACK of a node which has already switched to the new channel, the hub will switch to the new channel even if its checklist is not complete. For nodes that lost the channel information a backup channel is proposed in order to update the working channel of the WBASN.

2.7.2.4 Cognitive radio for medical body area networks using ultra-wideband

As underlined during the description of IEEE 802.15.4j, MBANs have been introduced to unlicensed frequency bands and because of the mutual interference primary users must be protected. Cognitive Radio technology based on ultra-wideband technology can be employed to cope with the typical challenges in MBANs and help to increase the efficiency of spectrum usage. [27] describes a MBAN

architecture where CR based on UWB plays the lead role. We will describe it having my focus on the MAC sublayer aspects.

In the proposal the cognitive capabilities of CR are implemented within the first-tier intra-WBAN and especially in the body network controller (BNC) or hub as can be seen in the Figure 68. The main goals are frequency agility and frequency-domain spectrum shaping capabilities that result to interference avoidance.

The basis for the CR-based solution is

- the UWB technology defined in IEEE 802.15.6 which includes the use of impulse radio (IR)
- use of the ECMA-368 interface multiband orthogonal frequency-division multiplexing (MB-OFDM) [28]

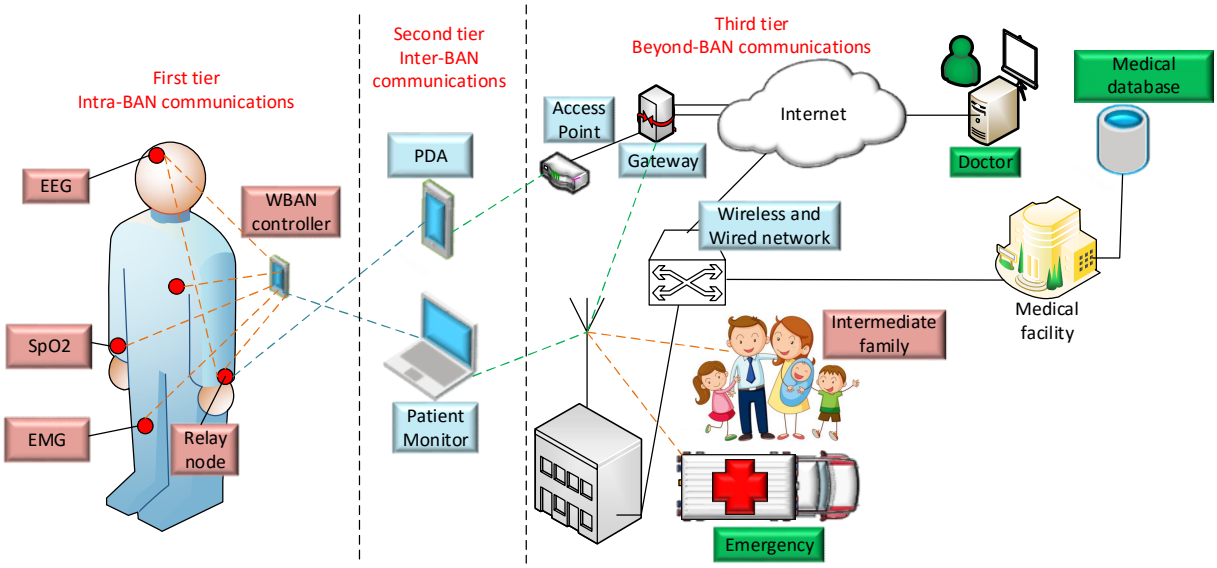


Figure 68 Three-tier architecture for MBANs using CR

Before get deeper into the matter we will explain some terms:

Impulse radio (IR) is a form of ultra-wide bandwidth (UWB) spread-spectrum signaling with properties that make it a viable candidate for short range communications in dense multipath environments [29]. As we saw, the major goal of the IEEE 802.15.6 standard is the definition of a MAC sublayer supporting different PHY layers, including UWB.

UWB is used and proposed in two variants: (a) *Impulse Radio UWB (IR-UWB)*, which is based on the transmission of a single and relative long pulse per symbol or a concatenation of short pulses per symbol. IR-UWB technology is proposed as a solution with objectives including low-cost, low-power, and low complexity body area wireless devices with high reliable wireless communications. (b) *Frequency modulated UWB (FM-UWB)* which is proposed for low-power consumption and characterized by reliability especially in medical applications.

ECMA International is an industry association founded in 1961 and dedicated to the standardization of Information and Communication Technology (ICT) and Consumer Electronics (CE) [30]. The ECMA standard ECMA-368 is the *High Rate ultra-wideband PHY and MAC standard* for mixed populations of portable and fixed electronic devices.

The ECMA-368 MAC provides:

- a contention-based and distributed reservation-based channel access mechanism
- mobility handling
- interference handling
- a synchronization facility for coordinated applications
- device power management
- secure communication
- mechanism for measuring the distance between two devices

The ECMA-368 MAC specification proposes that no device acts as a central coordinator but rather all devices are equipped with all required MAC functionality. Also here we have superframes which divide the channel time. Every superframe consists of a beacon period (BP) and a data period. The main goals of the BPs are: network synchronization, exchange reservation and scheduling information. BPs consists of time slots. To achieve network synchronization every device is required to listen for beacons for a minimum number of superframes (time) before starting its transmission. If a device discovers a beacon, it synchronizes to that beacon. In the data period *prioritized contention access (PCA)* is used for sending and receiving data by the devices. PCA permits multiple devices to contend for medium access, based on traffic priority. Just as well, during the data period devices send and receive data using the *distributed reservation protocol (DRP)* which allows the device to access the medium within a negotiated reservation.

ECMA-368 uses *Multiband orthogonal frequency-division multiplexing (MB-OFDM)* and divides the frequency spectrum in 14 bands with a bandwidth of 528 MHz each of them. MB-OFDM is a form of ultra-wideband technology that differs in approach to the impulse, or direct sequence form of ultra-wideband. MB-OFDM transmits modulated data simultaneously over multiple carriers, called subcarriers, spaced apart at precise frequencies. The subcarriers are precisely spaced at exactly the reciprocal of the symbol interval, ensuring that they are orthogonal to each other. The generation of the OFDM signal happens in the frequency domain using an IFFT, an inverse Fast Fourier transform to create a time-domain multiplexed signal. The demultiplexing of the subcarriers take place at receiver using a FFT, a fast Fourier transform. The implemented Fast Fourier Transform algorithms offer nearly 100 percent efficiency in capturing energy in a multi-path environment with slightly increasing transmitter complexity. Beneficial attributes of MB-OFDM include high spectrum flexibility and resiliency to interference and multi-path effects [31].

MB-OFDM can achieve a higher data throughput as the single band OFDM and it can reach rates from 53.3 to 480 Mb/s up to 10m. Another advantage is that UWB signals are not a risk to patient's safety and also they are not a significant source of interference. The structure of the impulse radio transceivers is simple and additional they have very low-power consumption. For these reasons impulse radio transceivers are good candidates for wearable biomedical sensors.

Making use of UWB technology in a WBAN, a hub (or BNC as referred above) can be turn into a *cognitive radio controller (CRC)*. The hub here as CRC is defined as a central unit which controls the transmission parameters of the nodes for wireless access. The nodes are the cognitive radio (CR) clients. The requirements for nodes, e.g. low cost, small in size and low-power dissipation, can be satisfied using IR-UWB radio interface in the first tier in Figure 68. The use of IR-UWB for the

communication between nodes and hub is an implementation of the IEEE 802.15.6 standard specification. The connection of the hub with the second tier is implemented using the ECMA-368 standard. Apart from high data rates the use of MB-OFDM leads to the implementation of *Detect and avoid (DAA)* (a set of technologies in UWB designed to avoid interference), and the implementation of cognitive radio (CR). The hub consists of two transceivers, an IR-UWB transceiver and an MB-OFDM UWB transceiver. The MAC sublayer performs the coordination of the access time periods so collisions and interference can be avoided.

The MAC sublayer specification from the IEEE 802.15.6 standard is used for the intra-WBAN tier and the MAC sublayer specification from the ECMA-368 standard is used for the inter-WBAN tier.

2.7.2.5 Challenges and open research issues for CRBANs

In this section we describe some challenges and open research issues for CRBANs.

Every CRBAN device should be CR-able, also the nodes.

The first challenge is the issue of the implementation of CR attributes to sensors. The execution of cognitive actions such as learning and sensing through radio-equipped sensors leads to high energy consumption. In a CR environment the implementation of the complete CR functionality in every network device, (e.g. hubs and nodes for example) increases the design complexity of the network devices. In some of the presented CRBAN architectures the cognitive attributes have been applied to the hub rather than the nodes. To improve QoS it is significant to introduce the CR attributes to all devices, hubs and nodes. Making also nodes CR-able will allow them to make independent decisions. This will make CRBANs fully cognitive improving additionally interference reduction.

Focus on the MAC

Current research in CRBANs takes care about issues like energy efficiency, collision avoidance and mitigation of interference. The handling of these issues takes place on the MAC sublayer, what means that current research is focused on the MAC sublayer.

Using physical location information to mitigate interference

Physical location information of devices can be a parameter that can be used to reduce mutual interference. Radio-frequency identification (RFID)-based transceivers can be used for the detection of the location of devices. RFID transceivers are suitable for CRBANs due to their low-power transmission but on the other hand they can generate interference.

QoS challenges

To provide QoS in CRBANs is a challenge due to the existing resource constraints, such as processing power, limited power, bandwidth and so on. Primary users (PU) communication must be protected from secondary user activity which can cause interference. Challenges in this area in CRBANs are the accurate predicting of a primary user arrival at the channel, false alarms and missed detections of primary users.

Energy harvesting

CR sensors have many functions which demand enough energy for their operation. Some of them are route discovery, transmission and reception of data, data processing, spectrum sensing, channel negotiation, and frequent spectrum handoffs. This is the reason why CR sensors are power-constrained devices. An additional fact is that in CRBANs the replacement of batteries is unpractical. Energy harvesting is a challenge and will have an impact on the lifetime of CRBANs. Different energy sources

contribute to energy harvesting. These are sources as energy from the human body, natural energy, thermal, electromagnetic, and mechanical energy. An energy-efficient protocol contributes also to an extension of the network life.

2.8 SMART BODY AREA NETWORK (SMARTBAN) MAC

The smart body area network has been defined from the European Telecommunications Standards Institute (ETSI) in 2015. The scope of ETSI was to define a low complexity medium access protocol (MAC) for SmartBAN. The ETSI specification used for this work describes the channel structure, the MAC frame formats and the MAC functions [32].

The key features of the SmartBAN MAC are

1. the use of separate channels for data and control traffic
2. a guarantee for very low latency emergency messaging, if needed from a time-critical application
3. increase of channel utilization and retransmission through the use of scheduled but unused time slots by secondary users

Target applications for the SmartBAN MAC protocol are medical, health, sport and leisure applications like stress monitoring, apnea monitoring, fall monitoring, safety monitoring or blood pressure fluctuation monitoring.

The SmartBAN MAC protocol performs channel access using two logical channels, the data channel (DCH) and the control channel (CCH). The devices operate in the ISM band within 2401 - 2481 MHz. Using a bandwidth of 2 MHz 37 DCHs and three CCHs are available.

The node connection process to the network starts with monitoring the CCH. The hub selects one control channel (CCH) from a list of control channels and sends one *Control Beacon Frame (C-beacon)* to the CCH every T_c seconds. Only hubs are allowed to send to the control channels (CCH). After receiving the C-beacon a node knows the hub and initialize a connection to it. A hub can be implemented with two transceiver chains. In this case, the hub communicates simultaneously on DCH and CCH. If only one transceiver chain is in use, the hub must allocate slots to itself in the DCH for transmitting the C-beacons and for hub-to-hub communication. Figure 69 shows the CCH.

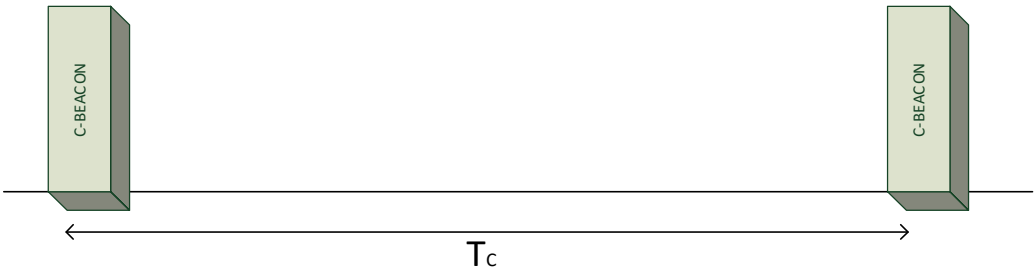


Figure 69 Control Channel (CCH)

Figure 70 shows the access periods in a data channel (DCH). Between two data beacon frames (D-beacons), that send by the hub, there exist three different periods. The scheduled access period, the control and management (C/M) period and an inactive period.

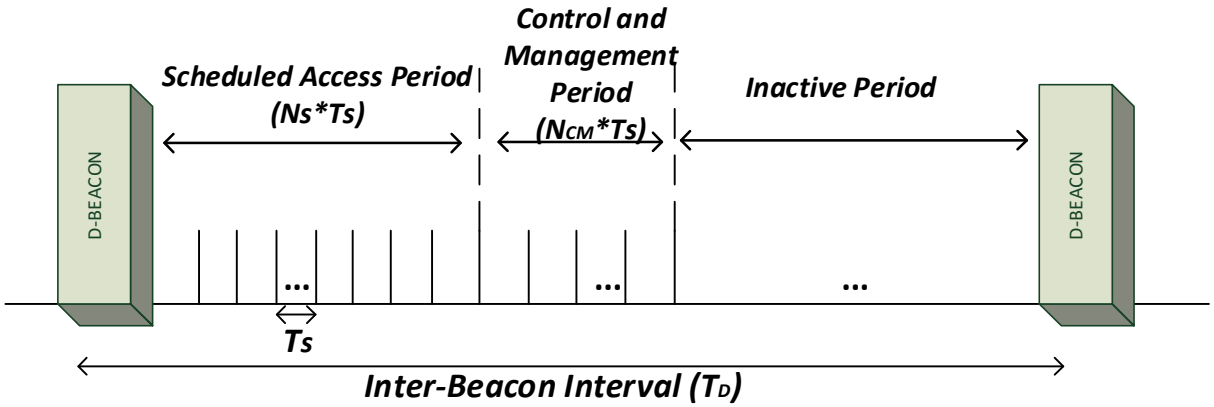


Figure 70 Access periods in the data channel DCH

Every one of these periods are divided into time slots with equal length T_s (in seconds). All three periods together build the *Inter-Beacon Interval* T_D (in seconds). Any device transmitting in a time slot should take care that its transmission happens within the duration of that time slot.

SmartBAN can coexist with other WBAN technologies, and it has a configurable QoS control in the form of four User Priority (*UP*) levels (Table 16):

User Priority (UP)	Data type	Contention Probability	
		CP_{max}	CP_{min}
0	Low priority	1/8	1/16
1	Mid priority	1/4	1/16
2	High priority	1/2	1/8
3	Very high (emergency)	1	½

Table 16 SmartBAN user priorities

In the current MAC sublayer specification, due to the limited range of 1.5 m and due to the properties and functions of SmartBAN, only a single-hop star topology is considered.

A MAC frame which also called *MAC protocol data unit (MPDU)* is constructed by a MAC header, a MAC frame body and a frame parity. There are three different types of frames with separate MAC frame bodies: management, control and data.

The management frames are divided into seven different subtypes: *data Beacon (D-Beacon), connection request (C-Req), connection assignment (C-Ass), slot reassignment (S-Ras), disconnection request (D-Req), disconnection response (D-Res),* and *Inter HUB*. Subtypes of the frame type control are acknowledgement (ACK) and negative acknowledgement (NACK). Data frames are divided into different subtypes based on the user priority.

The different access periods use various channel access mechanisms:

- scheduled channel access
- slotted aloha channel access
- multi-use channel access

The scheduled access period uses the scheduled channel access or the multi-use channel access. The control and management period uses the slotted aloha channel access or the multi-use channel access. A hub shall support scheduled, multi-use and slotted aloha channel access. Nodes shall always support scheduled and slotted aloha channel access.

The structure of scheduled access slot is shown in the Figure 71. It consists of two transmission periods, the data frame transmission time and the ACK frame transmission time. IFS is the inter-frame spacing that complete the scheduled access slot structure. During the data frame transmission time, the device allocated the time slot shall transmit. The transmission is carried out as in TDMA, e.g. without contention. During the ACK frame transmission time the receiver transmits an ACK frame, if transmission was successful. Otherwise, the receiver shall transmit a negative acknowledgement frame (NACK).

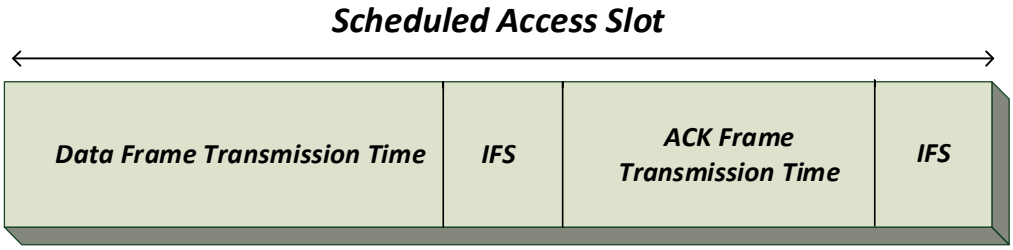


Figure 71 Scheduled access slot structure

To obtain one or more new scheduled allocations, a node shall send a C-req frame in the C/M period to the hub. The hub grants the scheduled allocation request sending a C-Ass frame to the node in the C/M period. The C-Ass frame indicates the scheduled access interval(s) and their direction (downlink/uplink).

The structure of the control and management slot is shown in the Figure 72. We have here also two transmission periods. In the data/management frame transmission time any device wishing to transmit either data or management frames may transmit. An ACK or NACK frame is send by receiver depending on successful or not successful receipt.

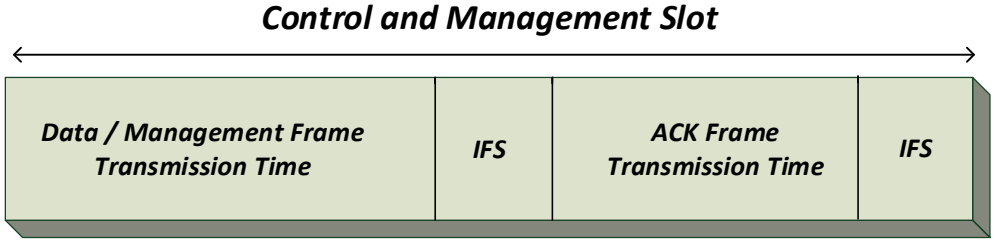


Figure 72 Control and management slot structure

The structure of the multi-use access slot is shown in the Figure 73. It consists of a sensing period and at most of two transmission periods. Depending on the traffic type (emergency traffic or any traffic), on the user-type (slot owner, non-slot owner, any user) and the access period, any device wishing to transmit shall sense the channel for a specified period T_{MUA}. In the case that channel is busy, the device waits for the next multi-use access time. Otherwise (channel is idle) the device transmits the data during the data frame transmission time. In case of successful receipt an ACK is transmitted by the receiver.

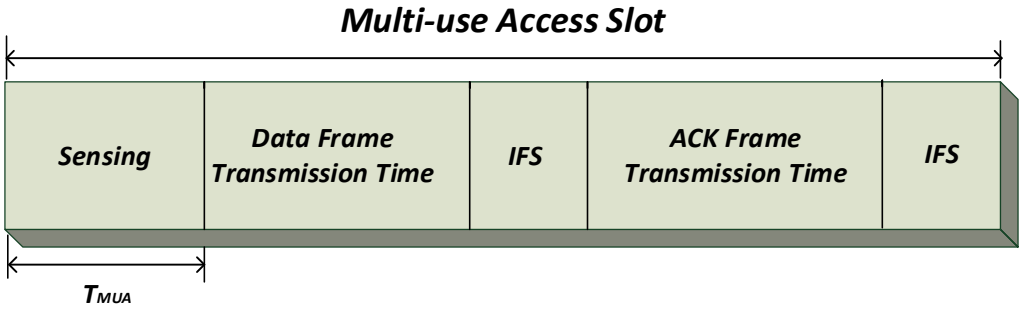


Figure 73 Multi-use access slot structure

Management frames are transmitted by nodes or hubs using the *slotted aloha channel access (SACA)*. A SACA session is started by transmitting in a time slot in the C/M period with a probability of *CP* (*contention probability*). The value of CP is chosen based on the user priority of the traffic and on number of transmission attempts. SACA utilizes the control and management slot structure.

The Multi-use channel access is divided into two access methods, the *priority channel access (PCA)* and the *Re-use channel access (RCA)* which can be used together or independently, depending on implementation.

PCA is used to transmit emergency traffic. If a node receives from a higher layer a packet with the highest user priority, it will initiate PCA. PCA guarantees very low latency for time critical applications. Radio energy expenditure and radio on time increases only 1-2%, if PCA is enabled.

RCA allows the use of an allocated slot in the scheduled access period by other users when the allocated user is not using the slot. The advantage of RCA is the capability to utilize the scheduled, but unused slots, during the scheduled access period by random access users. This results to increased opportunities regarding the channel utilization of the WBAN as well as retransmission. The drawback of RCA is slightly increase of protocol complexity and protocol overhead.

2.9 Some MAC protocols

In this section we will describe some well-known existing MAC sublayer protocols proposed for WBANs. Pros and cons of the proposed protocols will also be disclosed.

2.9.1 Heartbeat Driven protocol (H-MAC)

The *heartbeat driven MAC protocol (H-MAC)*, also known as *hybrid MAC* [33], improves energy efficiency by the exploitation of the heartbeat rhythm information in order to synchronize the nodes.

Heartbeat rhythm is in every human body. H-MAC is TDMA-based and originally implemented for a star topology WBAN. No beacons are transferred for node synchronization. A hub is responsible for network coordination. The biosensors of the nodes select sensory data. The heartbeat rhythm is extracted from this sensory data through ECG wave-peak detection and it is naturally synchronized. In other words, the heartbeat rhythms are represented by peak sequences. Dedicated time slots are assigned from the H-MAC protocol to each node guaranteeing collision-free transmission. The peak intervals are used from H-MAC for data communication. The hub assigns the time slots and calculates the frame cycles for synchronization. Advantages of H-MAC are the reduction of the energy cost required for synchronization due to the natural synchronization, the prolongation of the network life and the avoidance of collisions. A disadvantage is that it does not support sporadic events, the used slots are dedicated and they are not traffic adaptive. This means low spectral efficiency, if the traffic is low. Another disadvantage is that heartbeat rhythm is not accessible by all kind of sensors. In that case synchronization is not possible [34] [35].

2.9.2 *Reservation-based dynamic TDMA (DTDMA) protocol*

The DTDMA protocol is used for periodic WBAN traffic. Slots are assigned to nodes that have data to send. After sending and successful receiving of the data the same slots are released to other nodes. As in IEEE 802.15.4 the access to the channel is managed through superframes. Each superframe consists of:

1. a beacon, which carries control information like slot allocation
2. a CFP period used for data transmission
3. a CAP period for short command packets using slotted-ALOHA
4. a configurable inactive period for energy saving purposes

The order of CAP and CFP period in DTDMA is in opposite order as in IEEE 802.15.4. First the CFP period and second the CAP period. This order allows nodes to send CFP traffic earlier as CAP traffic. Another difference is that the length of the inactive period is configurable and not fix. The inactive period is increased if there is no CFP traffic. The superframe structure of DTDMA is given in the next Figure 74.

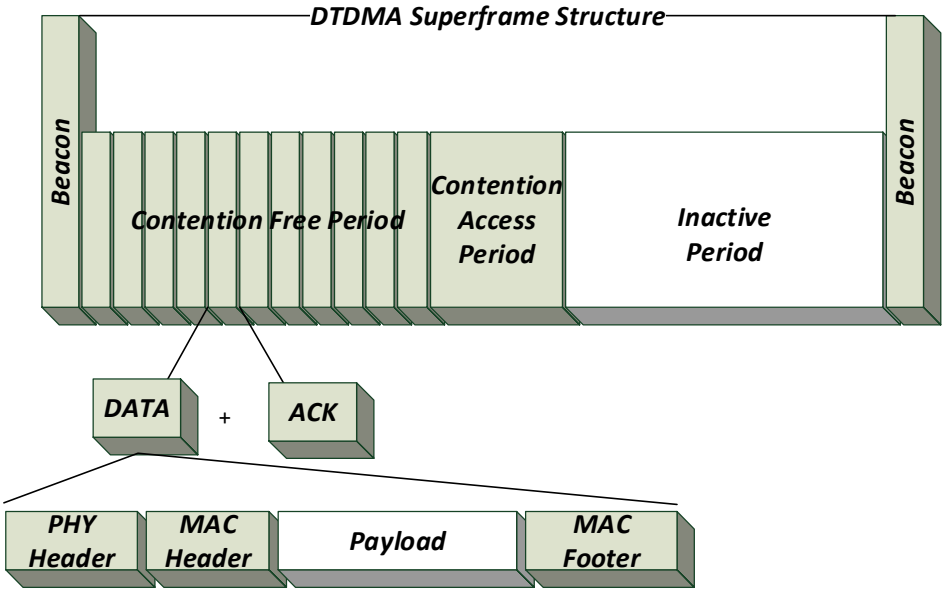


Figure 74 DTDMA superframe structure

Compared with the IEEE 802.15.4 DTDMA is more dependable regarding low packet dropping rate and low energy consumption. Its disadvantage is that it does not support on-demand and emergency traffic. Considered for the MICS band it has some limitations, e.g. it can operate only on one sub-channel and not simultaneously on the entirety of the ten sub-channels of the MICS band [35].

2.9.3 *PB-TDMA protocol*

The PB-TDMA protocol is based on the TDMA protocol. PB-TDMA is avoiding collisions through the assignment of every node to specified slots. These slots are repeated in a fixed cycle. A complete slot cycle is called frame. As Figure 75 shows in PB-TDMA each TDMA frame incorporates a preamble and a data transmission slot.

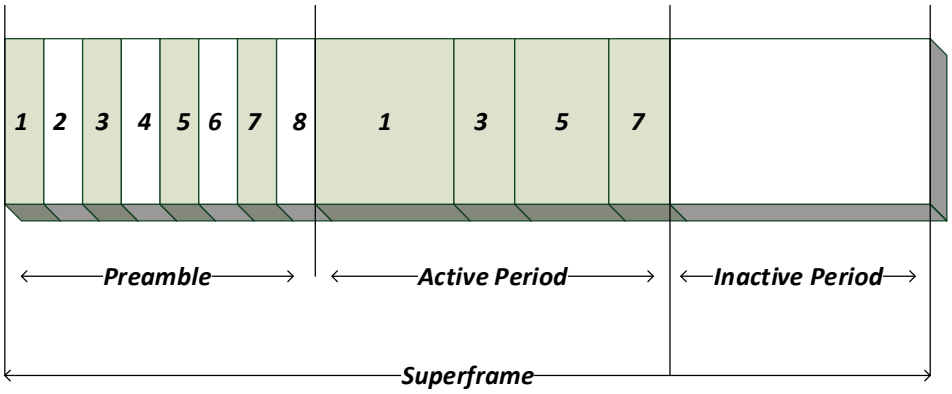


Figure 75 PB-TDMA superframe structure

During the preamble a node listens to the channel and transmits its data in a data transmission slot. The preamble contains for every node a dedicated subslot. The subslot is used to activate the hub through hub-ID broadcasting before the transmission. The hub receives the preamble and identify the sending node. The nodes turn off their radio if they do not have any data to transmit for saving power consumption of the nodes. When the node must transmit data or the node discovers its own ID in the preamble it turns on the radio.

The PB-TDMA protocol outperforms the IEEE 802.15.4 and S-MAC protocols in terms of energy efficiency [35]. The disadvantages of PB-TDMA are preamble overhearing and the limitation of handling sporadic events.

2.9.4 BodyMAC protocol

The BodyMAC protocol is based on TDMA. The channel is bounded by TDMA superframe structures with beacons, and downlink and uplink subframes as shown in Figure 76. Synchronization is achieved by beacon.

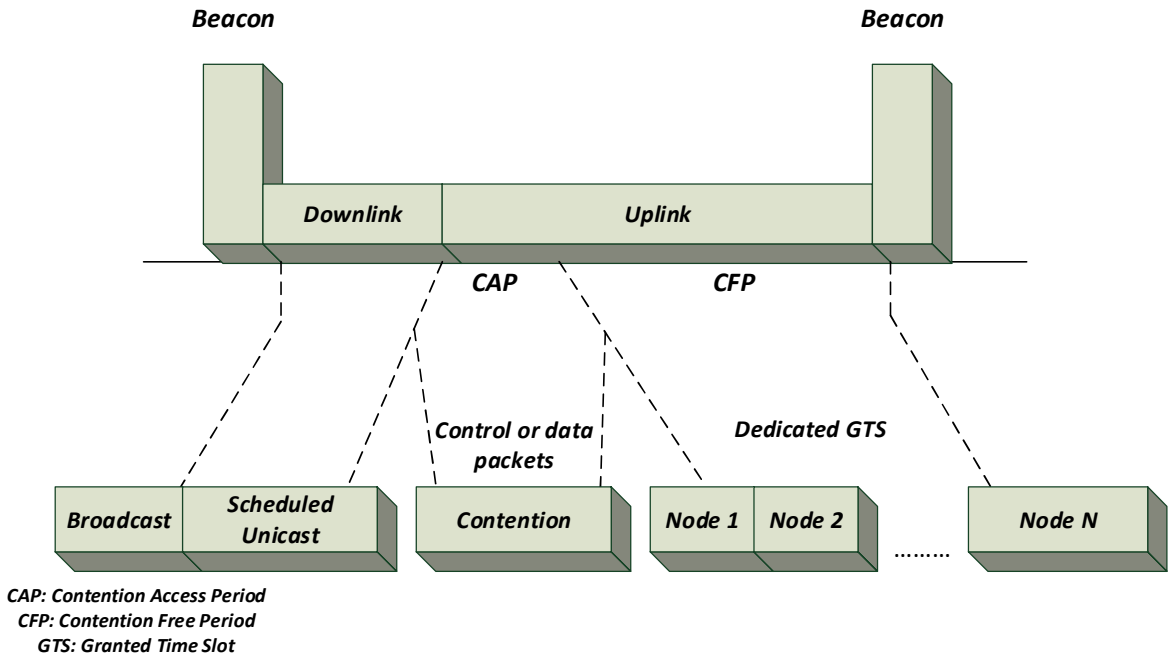


Figure 76 BodyMAC superframe structure

The uplink frame is scheduled for normal traffic and the downlink frame is scheduled for on-demand traffic from the hub to the nodes. Emergency traffic is not supported. The uplink frame consists of a CAP period for the transport of small size MAC packets and the CFP period which is used for the transmission of normal data in a TDMA slot. The hub assigns GTS to nodes in CFP to avoid collision and defines the duration of the downlink and uplink superframes. In the CAP period BodyMAC uses the CSMA/CA protocol.

An advantage of BodyMAC is the handling of on-demand traffic. BodyMAC protocol facilitates sleep mode and emphasizing energy minimization. If there is no data to send the nodes remain in the sleep mode. The use of a flexible bandwidth management - BodyMAC use three bandwidth management procedures, adjust bandwidth, Periodic bandwidth and Burst bandwidth - improves network stability. A disadvantage is that for low-power implants (nodes) the wake up procedure is not defined. For low-power implants the hub first must wake up the implant and after that the hub send synchronization packets. In a third step the hub requests or send data in the downlink subframe. For this problem exist workarounds like the use of wakeup radio to wake up the implants before using the downlink subframe [35]. For the uplink frame in CAP the used CSMA/CA results to high energy consumption due to collision issues and Clear Channel Assessment (CCA).

FLAMA, LEACH and Heed use TDMA as power-efficiency mechanism. At first we will mention TRAMA on which FLAMA is based.

2.9.5 TRaffic-Adaptive Medium Access (TRAMA)

TRAMA uses a TDMA scheme which based on a distributed slot selection algorithm. This algorithm exploits the information about traffic at each node to determine which node can transmit at a particular time slot. Node traffic information is used for avoiding the assignment of slots to nodes with no traffic to send. The same node traffic information allows nodes to determine when they should switch off (idle mode) and stop listening the channel, reducing in this way energy consumption. The TRAMA-algorithm requires nodes to exchange two hop information, but only every 100 frames to

amortize the overhead. Nodes also, synchronize their transmission schedules. The result of the synchronization is reduction of energy consumption by ensuring that unicast and broadcast transmissions incur no collisions [33].

2.9.6 Flow-Aware Medium Access (FLAMA)

FLAMA is another TDMA-based protocol. It uses frames and it adapts medium access schedules to the traffic flows exhibited by the application. FLAMA improves on TRAMA with the difference that it removes the periodic traffic information exchange between two-hop neighbors. This information is now transmitted upon request only. This makes FLAMA more efficient as TRAMA resulting in energy saving, high reliability and smaller delays. Low-power and/or high traffic applications can use FLAMA. It is simple enough and it can be run by nodes with limited memory, limited processing communication and power capabilities [33].

2.9.7 Low-Energy Adaptive Clustering Hierarchy (LEACH)

The LEACH MAC protocol is a TDMA-based protocol that integrates clustering and simple routing. The network nodes are partitioned from LEACH into clusters. In each cluster there exists a *clusterhead*. This is a dedicated node that is responsible for creating and maintaining a TDMA schedule. The other nodes in a cluster except the clusterhead are the *member nodes*. LEACH assigns to the member nodes TDMA slots. The TDMA slots are used to exchange data with the clusterhead. If a member node does not use its time slot, it is in the sleep state. The clusterhead node aggregates the data of the cluster members and transmits it to the sink node or to other nodes which take the role of a relay. If relay nodes are used, the clusterhead must spend significant energy for the transmission. The clusterhead is always switched on and it is responsible for long-range transmissions. The role of the clusterhead is taken from every node in rotation. This prevents that a node, the clusterhead, spends its complete energy and dies. The dead of the clusterhead would mean that all nodes in this cluster become useless. Every node decides independent when it serves as a clusterhead taking into account when it served last time as clusterhead. The optimal number of clusterheads in a network is 5% of the number of nodes in it. LEACH can achieve about eight times lower overall energy dissipation if we compare it with the case where the nodes send their data directly to the sink [33] [36].

2.9.8 Hybrid Energy-Efficient Distributed clustering (Heed)

Heed selects periodically clusterheads according to the node residual energy and a secondary parameter, such as node proximity to its neighbors. Heed terminates in O(1) iterations. It incurs low message overhead, and also achieves uniform cluster head distribution in the network. With appropriate bounds on node density and cluster transmission ranges, Heed can almost guarantee connectivity of clustered networks. The use of Heed is effective in prolonging the network lifetime and supporting scalable data aggregation [33] [37].

The next three protocols B-MAC, wiseMAC and STEM are use the LPL as mechanism to achieve power efficiency.

2.9.9 Berkeley MAC (B-MAC)

LPL, the *low-power listening,* is a power-efficient mechanism that plays an important role in the performance of a MAC protocol. In LPL nodes wake up for short time and only check the channel activity. If channel is idle the nodes sleep again. If not, they stay at the channel until they receive the data or the medium becomes idle. This called also *channel polling*. LPL is performed regular regardless of any synchronization activities between nodes. A long preamble is send from the sender before

sending the data in order to detect the polling on the other end (receiver) [33]. The periodic sampling of LPL is efficient in high-traffic node environments. Periodic sampling is also efficient under variable traffic conditions.

B-MAC is organized in slots and its operation is based on schedules. It employs long preambles. The goal of the long preambles is to keep the receiver awake to catch the actual packets. B-MAC also employs LPL to reduce the power consumption in the preamble sampling period. LPL is used with application-level control over check time, back-off window size, and power-down policy (e.g., no sleeping at the sink). Advanced Clear Channel Assignment (CCA) is used to handle random noise [38].

2.9.10 Wireless Sensor MAC (wiseMAC)

The wiseMAC protocol is based on CSMA with preamble sampling. It uses long preambles and employ low-power listening (LPL) having the same goals as the B-MAC protocol, to minimize energy waste coming from idle listening and overhearing. Idle listening is reduced using a preamble to signal the destination node, here called hub, of a packet arrival. In infrastructures which apply wiseMAC, the hub(s) are energy unconstrained. They can listen continuously, they can send any amount of signaling traffic and they are exploited by wiseMAC protocol. Hubs during downlink (communication from hub to node) transmit without requiring from nodes continuously listening. In the other communication direction, the uplink, the hub can listen continuously with unlimited power. The nodes sample regularly the medium through listening to the radio channel for a short duration. If the medium is busy the node listens until the medium is idle again or a frame is received [33].

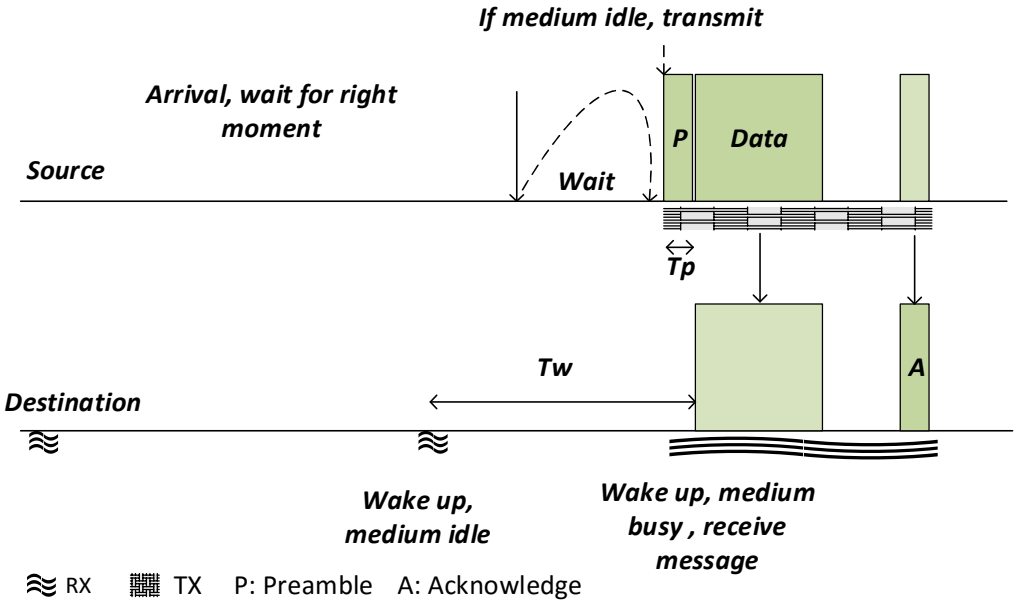


Figure 77 wiseMAC

Figure 77 shows the wise MAC concept. The same as in B-MAC, periodic sampling of LPL in wiseMAC is efficient in high-traffic node environments and under variable traffic conditions.

2.9.11 Sparse Topology and Energy Management (STEM)

STEM aims at providing reduction of energy consumption of the nodes. It organized randomly using two radios, a very low-power radio (signaling radio) to wake up a target node and a second radio for data communication. The STEM operation is based on schedules. To be efficient STEM uses LPL on the signaling radio. To reduce the associated latency target nodes explicitly acknowledge the wakeup on the signaling radio. STEM is suitable for events based applications and low traffic applications [39].

S-MAC, T-MAC, P-MAC and D-MAC use scheduled-contention to achieve power efficiency.

2.9.12 Sensor MAC (S-MAC)

S-MAC is a synchronous contention-based MAC protocol with the low duty cycle mode as default node operation mode. It synchronizes its transmission schedule and listening periods maximizing throughput. This happens through organization of the nodes into clusters by local time synchronization. All nodes of the same cluster are managed through an independent schedule which consists of the three periods SYNC, DATA and SLEEP. As the SYNC period starts with operation all nodes of the same cluster wake up and synchronize clocks with each other. The size of the SYNC packet is very short. The SYNC packet includes the information about the next SLEEP period. In the DATA period nodes send their data. For unicast frame transmissions the Request To Send (RTS)/Clear To Send (CTS) mechanism is applied. Broadcast frames are sent without RTS/CTS. If the SLEEP period starts all nodes that are not involved in the communication process return to sleep. Nodes that are involved in the communication process they return to sleep after they have finished the transmission of data and acknowledgements (ACK). S-MAC introduces the concept of coordinated sleeping for the nodes of the same cluster. S-MAC also reduces energy consumption by complete turn off the radio during sleeping periods [33].

A scheduled-contention mechanism like this of the S-MAC protocol uses sleep schedules and reduces idle listening. A disadvantage of S-MAC is that for specific WBANs their nodes, e.g. defibrillator nodes, are not required to wake up periodically for schedule exchange with their cluster nodes. S-MAC implementations perform well for on-body applications but they are not sufficient to handle sporadic events like emergency or on-demand events.

2.9.13 Timeout MAC (T-MAC)

The T-MAC protocol is a contention-based protocol which can handle varying load with low-power consumption. T-MAC applies a synchronized duty cycle schedule amongst the nodes. The node is awakening for a time period which is called active time. The length of the duty cycle duration depends on the information traffic load of the network. If the network traffic load is high, the duty cycle becomes large and the nodes can handle the high traffic load. If the network traffic load is low, then the duty cycle takes a small value and the nodes save power, making the problem of idle listening less present. The node stays awake till no activation event appears in a certain period of time. This can lead to overhearing because the node is awake although it is not involved in data transmission [33].

A special characteristic of T-MAC is the *Future Request-to-Send (FRTS)* packet. With this packet the node notifies the target receiver that it still has a message for it, but it prohibited to access the medium in the moment. The FRTS packet includes the length of time for which communication is blocked. The receiver of the FRTS packet knows that it will be the future target of an RTS packet and must be awake by that time. The next Figure 78 shows the case where node C loses contention and overhears a CTS packet. In this case node C sends FRTS packet to its target receiver D. The FRTS packet includes the length of the data transmission from node A to node B. For this time length the communication is

blocked. D knows in this way that it will be a future target of an RTS packet from C and it will be awake for this time period.

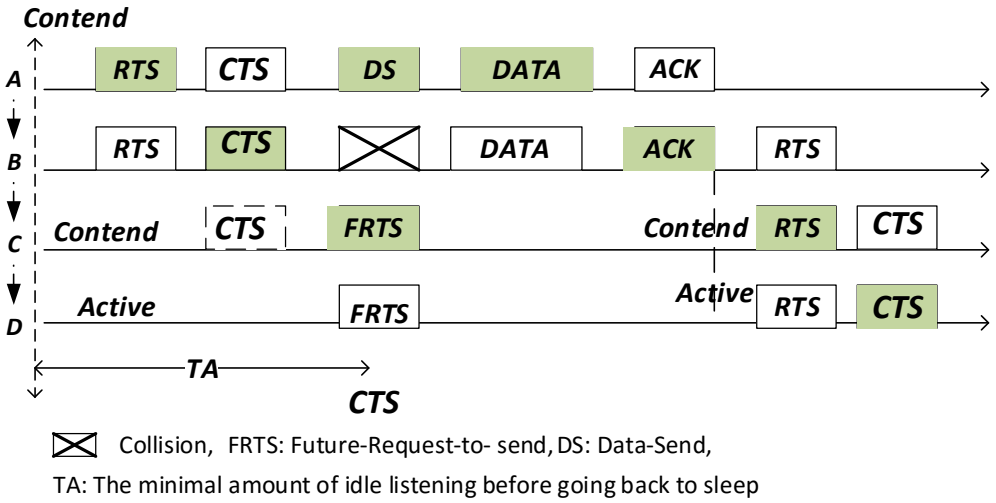


Figure 78 FRTS in T-MAC

2.9.14 Pattern-MAC (P-MAC)

P-MAC is organized in hybrid mode and the operation is based on listening. It uses a distributed, adaptive TDMA-like scheme in which nodes exchange traffic patterns to establish in which slots they should be awake to accommodate the load. Within a slot nodes use CSMA/CA to verify who will actually be sending and receiving [40].

2.9.15 Data gathering MAC (D-MAC)

The so-called *data forwarding interruption problem* is a problem of MAC protocols for multi-hop wireless sensor networks, that utilize listen/sleep duty cycles. The problem here is that not all the nodes on a multi-hop path to the destination node are aware of the forthcoming arrival of on-going data. Because some of the nodes go to sleep, a latency arises as a result of sleep delay. D-MAC is an energy-efficient low-latency protocol designed for priority-based applications to solve the data forwarding interruption problem in *convergecast wireless sensor networks*. Across many wireless sensor networks *convergecast* and *broadcast* are the fundamental communication patterns. The goal of broadcast is to transmit a message from a source node to all other nodes in the network. The goal of convergecast for a destination node is to collect messages from all other nodes in the network during a very short time window. Convergecast in wireless ad hoc network requires proper coordination among the nodes to avoid high packet collision rates near the destination node. Tree-based convergecast schemes are often used to improve energy efficiency by reducing duplicate transmissions, which in turn reduce collisions and interference. For convergecast the *convergecast tree* is constructed. This is a directed spanning tree having as root the destination node and with edges directed towards the destination node. During the actual convergecast round, a message is propagated from the source (leaves of the tree) along the pre-computed directed tree [41].

D-MAC is organized in slots and the operation is based on schedules. It addresses the latency overhead of S-MAC for the convergecast communication pattern, by staggering the wake-up scheme giving the sleep schedule of a node an offset, which is a function of its level on the data-gathering tree. D-MAC achieves low latency by assigning subsequent slots to the nodes that are consecutive in the data transmission path. The duty cycle is adjusted according to the network workload [42].

Standards such as IEEE 802.15.1, Bluetooth Low Energy, IEEE 802.15.4/ZigBee, IEEE 802.15.4a, SmartBAN, and IEEE 802.15.6 are open-standard technologies supported by the scientific communities or alliances.

The following MAC protocols, such as ANT, ANT+, RuBee, Sensium, Zarlink, Insteon and Z-Wave belong to the group of proprietary wireless technologies.

2.9.16 Advanced and adaptive Network Technology (ANT)

ANT is a dedicated MAC protocol developed by ANT Wireless for use in ultra-low-power wireless personal area networks (LR-WPANs) and wireless sensor network applications. It is targeted at applications, (e.g. heart rate monitors, temperature sensors, and bike power sensors) with a periodic transfer of small amounts of sensor information between several interconnected devices.

ANT defines a wireless communications protocol stack and establish standard rules for co-existence, data representation, error detection, authentication, and signaling. It is similar to Bluetooth low energy protocol, operates in the world-wide license-free 2.4 GHz ISM frequency band and is suitable for any kind low data rate sensor.

The medium is accessed with TDMA. Each channel has a single master device and slave devices. The channel can be unidirectional from a master to a slave or from a slave to a master, or bidirectional. ANT supports the channel configuration as a broadcast channel, and optional as an acknowledged channel or a burst messaging channel. As every ANT-powered node can act as transmitter (master), a receiver (slave) or a transceiver in different channels (Figure 79), ANT allows forming very complex network topologies from simple point-to-point, to complex mesh networks.

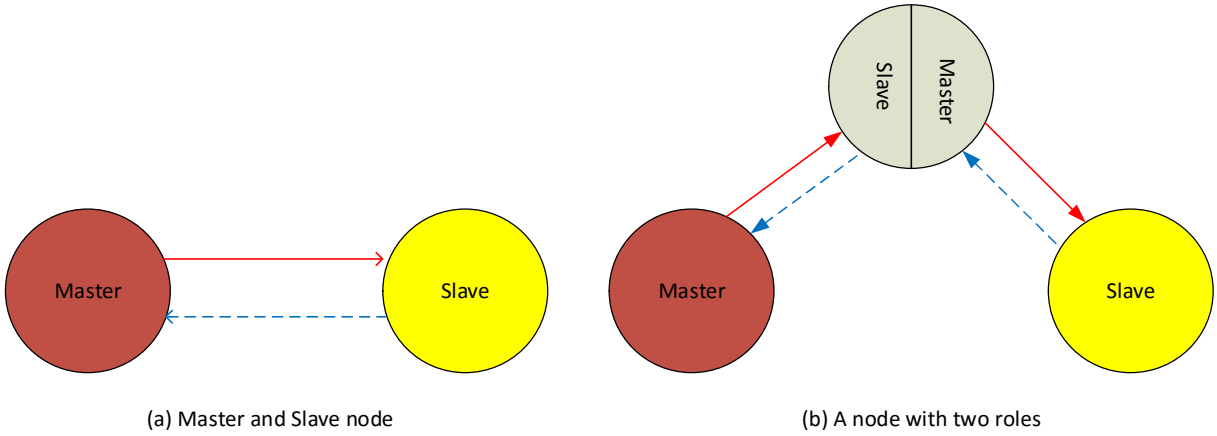


Figure 79 The different roles of a node in the ANT technology

Taking into account that to build optimal TDMA schedules, traffic characteristics should be known a priori and consequently ANT is best suited for relatively small networks. ANT powered nodes can

operate for years compared to days or months for other technologies [33] [43]. The next Figure 80 shows the ANT model and its correspondence to the OSI model.

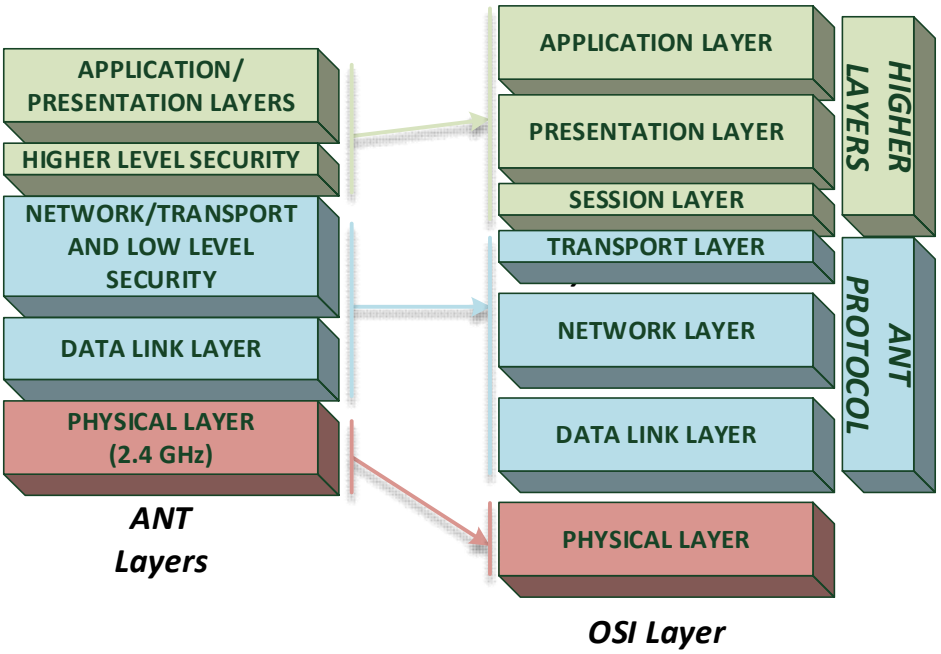


Figure 80 ANT model and its correspondence to the OSI protocol

Other advantages of ANT are:

- The ANT interoperable ecosystem
- Low development and system cost
- Stack size orders of magnitude smaller than Bluetooth low energy, that results in lower ANT chip size and cost
- 64-bit network key with additional application layer security
- Up to 2^32 addressable devices
- Low latency
- Flexibility to trade-off data rate against power consumption
- Support for various transmission modes up to a net data rate of 20 kbit/s
- An over the air data rate of 1 Mbit/s for low duty cycle operation

2.9.17 ANT+

ANT+ is an extension to the ANT protocol that uses the same communication method but includes profiles defining data formats and channel parameters enabling products from different manufacturers to communicate seamlessly. Device profiles are managed by the ANT+ Alliance and defined for different classes of products (e.g. heart monitors, weight scales) [33] [43].

2.9.18 IEEE 1902.1 (RuBee)

RuBee is a wireless data communication protocol that operates within the low frequency radio wave range of 30-300 kHz. Unlike other technologies, its signal does not include an electric field component but uses long wave magnetic signals to send and receive short data packets (128 byte) in short range

networks (0.5 to 30 meters). RuBee nodes referred to as *tags*. Tags have a crystal and can keep track of time, and also have a battery and a static memory. A tag can be a controller, a responder or both of them, so peer-to-peer communications is possible. A controller initiates communications and a responder replies with a data packet that is emitted at a fixed interval after controller packet ends. RuBee specifies a single fixed frequency of 131.072 KHz.

The disadvantage of RuBee is that it is very slow (1200 baud). Its advantages:

- RuBee tags have ultra-low-power consumption in terms of battery life (longer than 10 years)
- Stable operation (very resistant to interference) on or in steel structures, underwater, and obstacles due to the absence of the electric field
- The Food and Drug Administration (FDA) classified 1902.1 as a Non-Significant Risk (NSR) Class 1 device in medical visibility applications
- RuBee has no effect on pacemakers or ICDs
- RuBee has no electromagnetic interference (EMI) or electromagnetic compatibility (EMC) in the operating room
- The U.S. Navy granted RuBee HERO ordnance (Hazards of Electromagnetic Radiation to Ordnance and classified the 1902.1 Auto-ID wireless tags, handhelds and base stations with a zero safe separation distance (SSD). SSD is the minimum distance between the delivery system and the weapon beyond which the hazards associated with functioning (denotation) are acceptable [44]. The U.S. Navy's HERO certification is recognized as one of the most demanding and critical RF safety programs in the world
- It provides asset security and visibility in harsh environments, where electric-field-based technologies like RFID, ZigBee, and Wi-Fi are unable to operate
- RuBee is the only wireless technology approved by the US Department of Energy (DoE) for use in high security, top secret areas. It was approved with an intrinsic safety zero SSD.

RuBee is applied in industrial (asset management and tracking) and military environments and is an alternative to other low-power wireless networks of nodes based on the IEEE 802.15.4 standard, such as ZigBee [43] [45] [46] [47].

2.9.19 Sensium

Sensium is an ultra-low-power platform with embedded local intelligence for use in the medical and healthcare area. The so called "digital plasters", a multiple embedded-Sensium platform, can continuously monitor key physiological parameters on the body. The selected raw data or processed information can be wirelessly transmitted to a Sensium server installed into a PDA or a smartphone.

Figure 81 shows the Sensium platform.

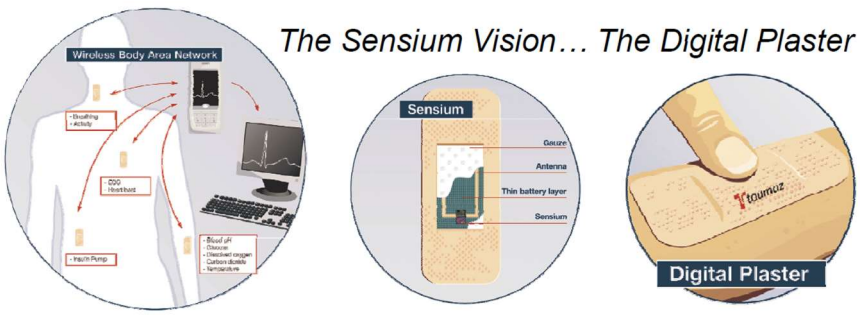


Figure 81 The digital plaster

The Sensium platform implements a network star topology. The body-worn slave nodes send periodically multiple vital signs (sensor readings) via single-hop communication in real-time to a central master node. The nodes are in a centrally controlled standby or sleep mode until it is time to send data during the assigned time slots. In this way energy consumption is reduced. Sensium operates in the 862 – 870 / 902 - 940 MHz ISM bands and is capable of 50 kbps data transmission rate over a maximum distance of 10 m. Sensium lacks basic security features [33].

Sensium is implemented as a system-on-chip (SoC) and integrates a wireless transceiver, a full-custom-hardware MAC, a digital microprocessor core, IO peripherals, on-chip memory, micropower analog-to-digital converter (ADC) and custom sensor interfaces. Up to three independent sensors can be connected to a single SoC. The sensor sample interval and number of samples per sample time can be independently set for each sensor enabling sensors to be optimally sampled.

A node consists of the sensors, the SoC, the battery and the antenna, they build together a thin and flexible patch, that is attached to the patient for a period of four to seven days. After this period the patch is thrown away and a new one is attached, if necessary.

The hardware MAC protocol is a custom design with the follow characteristics:

- It ensures ultra-low-power operation
- It guarantees robust performance
- Control of the RF channel selection
- Listen-before-transmit (LBT) compliance
- Link establishment
- Data transfer
- Sleep management

2.9.20 Zarlink

Zarlink (now Microsemi) produces radio transceiver chips that can be used for implantable medical devices (IMDs). The main aspects of the designed chips are reliability and low-power wireless communications. The Zarlink transceiver supports a deep-sleep mode of operation and it is usually in this mode, so the current consumption is very low. The transceiver wakes up by a specially coded 2.45 GHz wakeup message using an ultra-low-power sniffing method, or with the help of the emergency message of an IMD processor. The high performance MAC delivers data rates up to 800 kbps (also possible are 400 and 200 kbps) and operates in MICS 402-405 MHz band (10 MICS channels) and 433-434 MHz (two ISM channels). One of the chips that implements this technology is the ZL70101 Medical Implantable RF Transceiver. ZL70101 includes a MAC that implements a communication protocol specifically designed for the requirements of high-reliability IMDs. The MAC protocol includes Reed-Solomon forward error correction together with CRC (cyclical redundancy check) error detection and retransmission. This leads to an extremely reliable data link. The chip requires only three external components. Device manufacturers are able to use board space savings to increase battery size, to support advanced functionality, and to reduce overall system bill of material cost.

A simplified block diagram of the ZL70101 shows Figure 82:

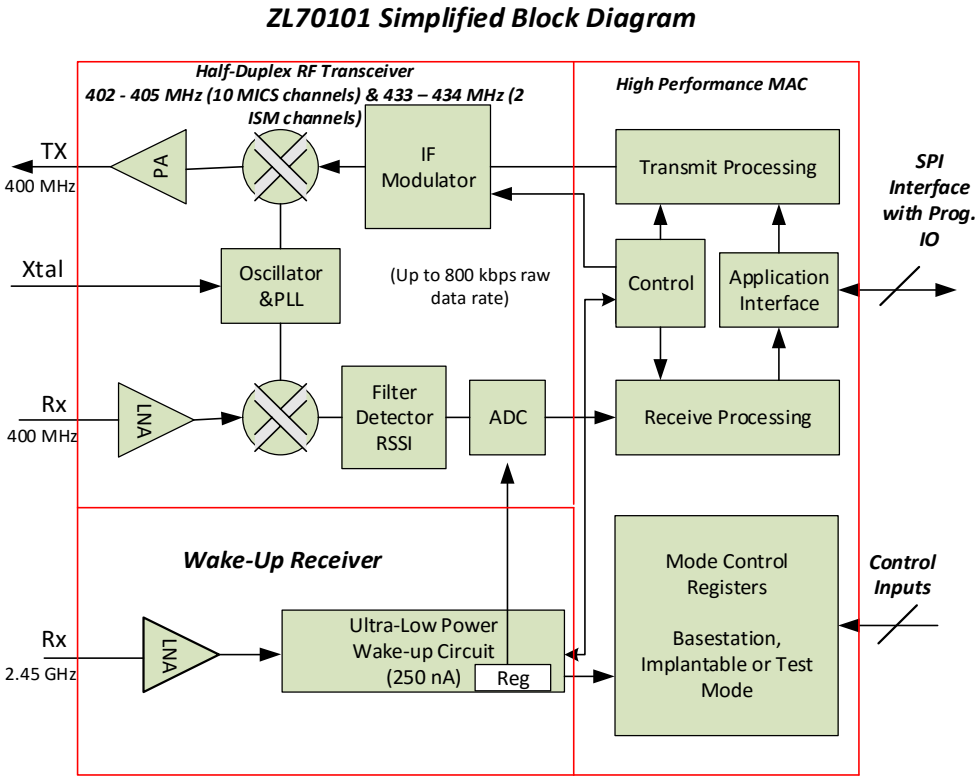


Figure 82 ZL70101 Simplified Block Diagram

The high performance MAC consists of a control unit, a transmit processing unit, a receive processing unit, an application interface and a base station [33] [43].

2.9.21 Insteon

Insteon is a dual-mesh network technology (two uncorrelated media) optimized for home management and control. It enables simple, low-cost devices to be networked together using powerlines, the 900 MHz ISM band, or both. All Insteon devices are peers. Any device can transmit, receive or repeat without a master controller or complex routing software. Adding more nodes makes an Insteon network more robust, due to the fact that Insteon nodes repeat each other's messages by *simulcasting* them at precisely the same time. Simulcasting is the method Insteon propagates messages. This means that with more nodes in the network the Insteon signal gets stronger [43].

2.9.22 Z-Wave

Z-Wave protocol developed by Sigma Designs, Inc. and it is targeted at building automation, entertainment electronics and wireless sensors networks. It works in the 2.4 GHz ISM band and enables networking consumer electronics either internally, or with the user via remote control. Z-Wave uses simple and reliable, low-power radio waves that easily travel through floors, cabinets and walls. A Z-Wave network comprises controlling devices (controllers) and AC powered slave nodes that can act as routers. Slave nodes continuously listen to the wireless medium for incoming transmission. Controllers are active on demand and can be battery powered. For the operation of the Z-Wave wireless system a controller hosts a routing table to the entire network. If a packet needs to be routed over multiple hops, the controller embeds the route to the forwarded packet. Z-Wave has at maximum 232 nodes. Z-Wave networks can inter-connect via gateways. The Z-Wave MAC sublayer is shown in Figure 83 [43].

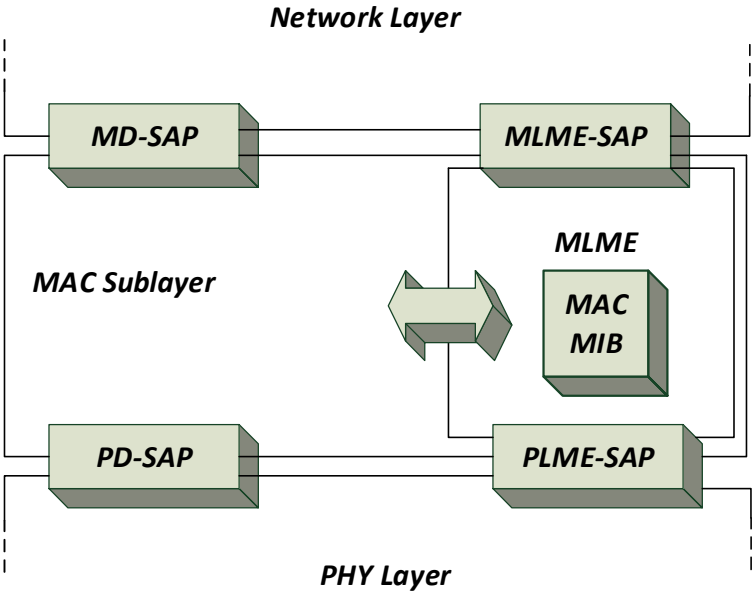


Figure 83 Z-Wave MAC sublayer

The MAC sublayer of Z-Wave handles the access to the physical layer and it performs following tasks:

- Frame acknowledgment
- Retransmission
- Providing a reliable link between two peer MAC entities

The MAC sublayer provides two services to the network layer, the MAC data service, accessed through the MD-SAP, and the MAC management service, accessed through the MLME-SAP. The MD-SAP supports the transport of network layer protocol data units (NPDU) between peer network layer entities. The MLME-SAP allows the transport of management commands between the next higher layer and the MLME [48].

Each MAC frame (MPDU) consists of (Figure 84):

- An MHR, which comprises address, frame control and length information
- A MAC data payload of variable length. Acknowledgment frames do not contain a payload
- A MAC Footer (MFR), which contains a frame check sequence (FCS)

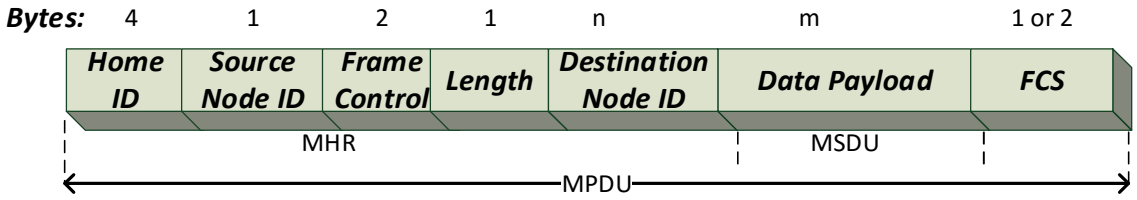


Figure 84 Z-Wave MAC frame format

2.9.23 PSMA-based MAC

PSMA-based MAC protocols is a small family of MAC protocols. The WBAN sensor nodes of the PSMA-based MAC protocols sense a preamble in order to detect if the channel is busy or idle. The MAC is based on the *Preamble Sense Multiple Access (PSMA)*. At the beginning of every data packet every node attaches a preamble sequence. The existence of the preamble in the channel indicates that the channel is busy. This helps to minimize false alarms. PSMA-based MAC protocols use a beacon enabled superframe structure like the superframe structure of IEEE 802.15.4a standard. Figure 85 shows the superframe structure by data transmission.

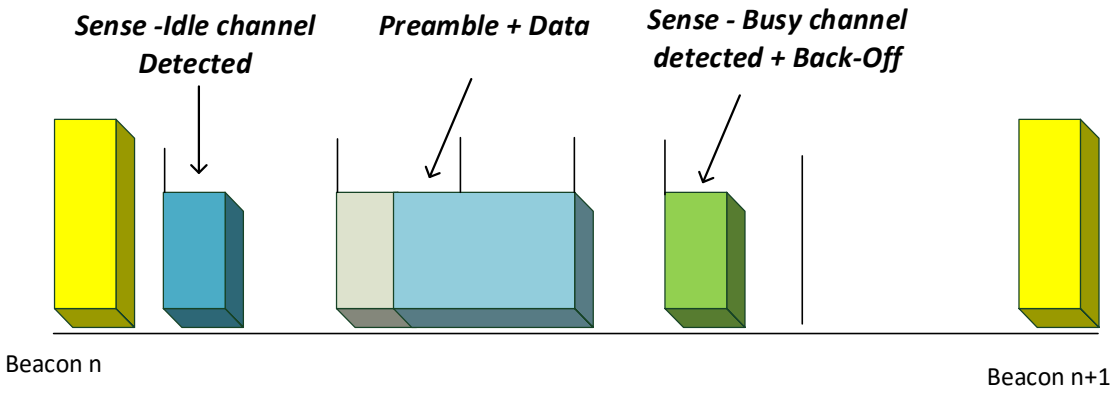


Figure 85 Data transmission using a superframe structure with PSMA-based medium access

Figure 86 shows a PSMA-based channel access mechanism.

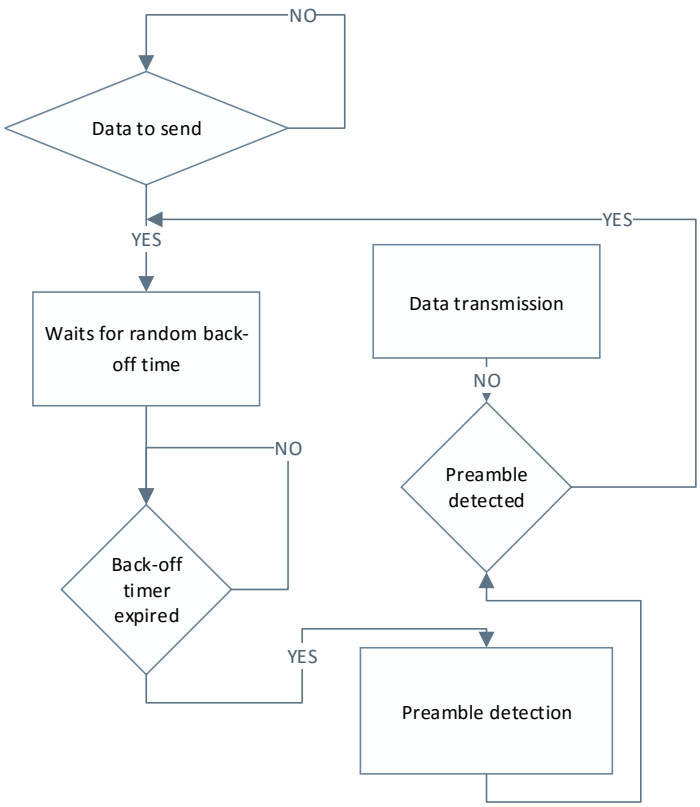


Figure 86 PSMA based channel access mechanism

A drawback of PSMA-based MAC is that it requires an IR-UWB based receiver at the node end in order to sense the channel using PSMA. All existing complexities that involved using IR-UWB receivers in nodes are ignored. Another drawback is collisions, due to the missing solution for the case where two or more nodes perform preamble sense simultaneously.

2.9.24 MAC protocol based on Exclusion Regions (ER)

An exclusion region is an area surrounding a receiver, such that the transmitter nodes within an ER cause interference to each other. The MAC protocol proposed in [49] is based in transmit and receive antenna patterns and the directionality of the antenna. The transmitter nodes that are not located inside an ER of a targeted receiver do not cause interference to it (Figure 87).

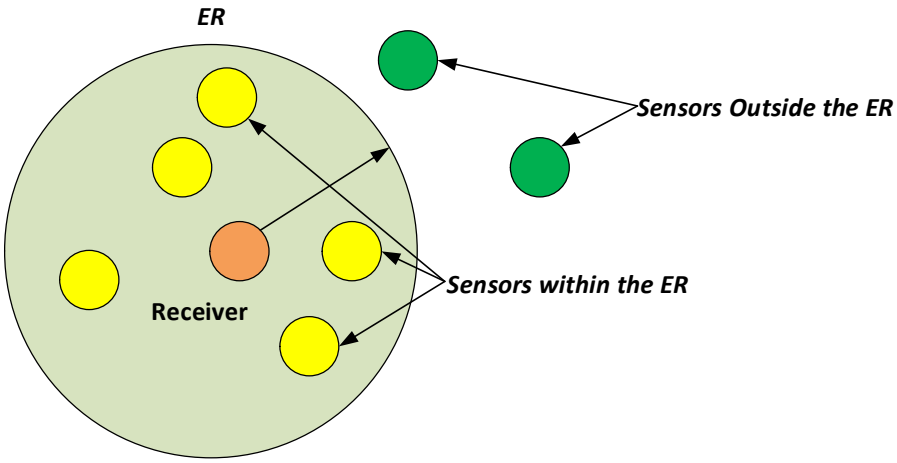


Figure 87 ER based UWB communication

Nodes within the same ER communicate using *Time Hopping codes (TH-codes)*, while the nodes outside the ER communicate concurrently. TH-codes are used in order to communicate control messages and sensor initialization. The communication of all nodes is asynchronously. The advantages of this MAC protocol are:

- Minimization of interference that can occur in a multiple UWB transmission environment
- Throughput optimization using concurrent transmissions in mutually exclusive ERs

The drawbacks of the ER-based MAC protocol are

- Multiple access for nodes within the same ER is not an important task
- The issue pulse synchronization is not prioritized
- Assumes that a node can determine whether is within the range of an ER

2.9.25 Uncoordinated Wireless Baseborn Access for UWB networks (UWB²)

UWB² use orthogonal time hopping codes for multiple access in a shared medium. Each node is identified through a unique TH-code that is used in the same way as in section before in order to communicate control messages and sensor initialization.

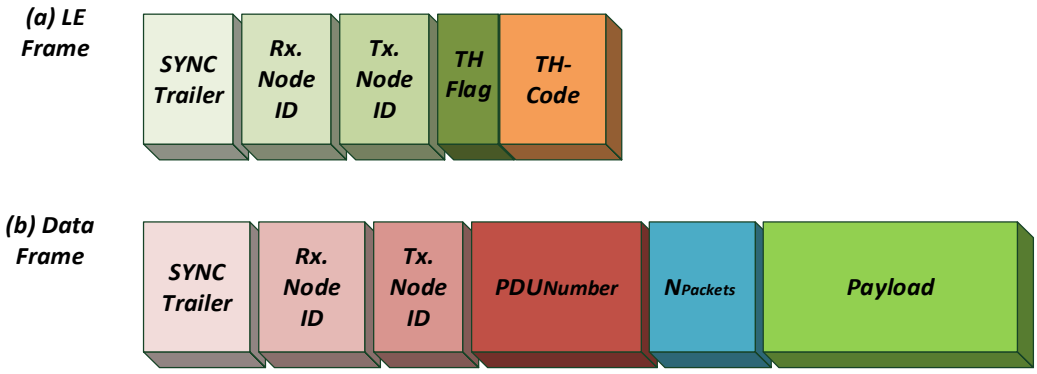


Figure 88 (a) LE frame format used for sensor initialization, (b) Data frame format

We will describe in this point the sensor initialization and the data communication. A sensor node sends a Link Establishment (LE) frame using the common TH-code. This TH-code will be used in the communication between the sensor node and the hub (coordinator node). The hub then replies with a Link Control (LC) message and listens to the TH-code allocated for the sensor node. After sensor initialization data communication starts using the suggested TH-code and the data frame format as shown in Figure 88.b. Acknowledged and un-acknowledged data communication is supported by UWB^2.

The advantages of UWB^2 MAC are

- The use of orthogonal TH-codes makes unnecessary the CCA
- Avoiding the CCA we save energy

The disadvantages of UWB^2 MAC are

- The protocol assumes the use of a UWB receiver at the sensor node end
- If LC frame is lost, the MAC protocol does not provide a method for re-initialization of the data transmission. In this case the data communication can be inhibited permanently
- There is no method to avoid or minimize collisions that happen during the use of the common TH-code for control messages

2.9.26 Ultra-wide band MAC (U-MAC)

U-MAC is an adaptive medium access control (MAC) protocol. Its nodes periodically advertise their current state, so that neighbor nodes can proactively assign transmit power and data rate values for new links. The main goal of the design of U-MAC was the optimization of the global network performance [50].

The network topology U-MAC supports, is a hybrid multi-hop topology. This kind topology provides to the nodes the flexibility to switch their operation mode. If an access point is available the node switches to the *centralized mode* otherwise to the *ad hoc mode*, also called *distributed mode*. For the decision in which mode to operate a node monitors a dedicated hello message channel. If the node detects in the hello message channel any access point hello messages, it switches to centralized mode. The node stays in the centralized mode if it hears access point hello messages periodically. Otherwise, it switches to the distributed mode.

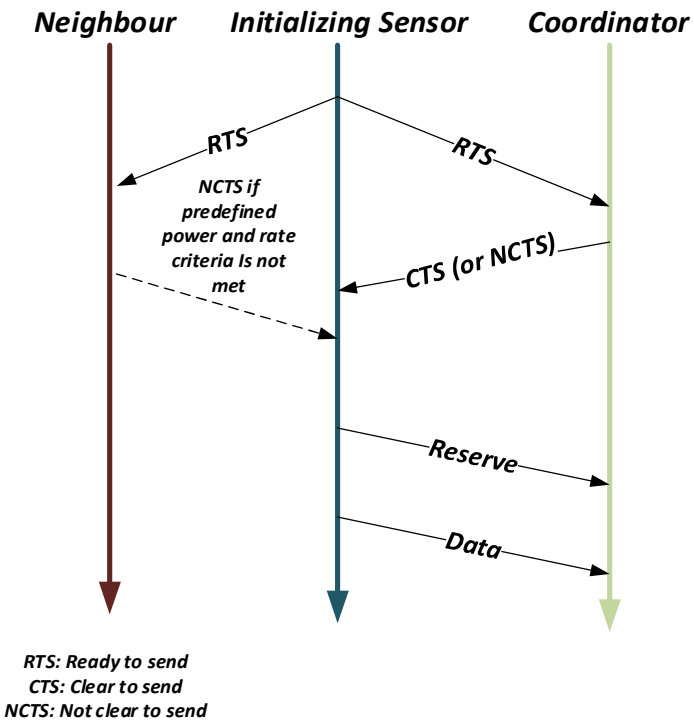


Figure 89 Node initialization in U-MAC

After the reception of a hello message a node can determine the ranging information of its neighbors and adjust dynamically its transmit power and data rate values. The U-MAC approach is more node centric compared with other MAC approaches which are hub (coordinator) centric. U-MAC supports also a prioritized delivery mechanism and uses similar to UWB^2 MAC unique TH-codes to provide multiple access to the shared medium and common TH-codes for control messages.

Figure 89 shows the mechanism of node initialization in U-MAC. If a node wants to send data (Initializing node) to a coordinator or a neighbor node, it sends a Ready to Send (RTS) message. The coordinator or the neighbor node determine if the transmission criteria for data rate (admissible data rate) and transmit power are satisfied. The transmission criteria are determined using the Signal to Noise Ratio (SNR) and the interference level. If the criteria are not satisfied, the coordinator or the neighbor node send a Not Clear to Send (NCTS) message. Otherwise, a Clear to Send (CTS) message is transmitted to the initializing node. In case of NCTS the Initializing node must reduce its transmit power and its data rate. In case of CTS the initialization process is done and the data can be transmitted. During the data transmission, the link parameters can be dynamically adjusted using the hello message channel as described before.

The proactively approach of U-MAC has the follow advantages:

- Lower link setup latency (compared with reactive approaches)
- Lower control overhead (compared with reactive approaches)
- Double throughput
- Better adaptation to high network loads

The disadvantages of U-MAC are:

- It allocates significant processing load to the sensor nodes. This is a conflict to the principles of WBAN design, which demand minimization of sensor node processing load due to reduction of power consumption
- The use of a UWB receiver at the sensor node end in order to receive hello messages leads to increased power consumption and requires complex hardware

2.9.27 Dynamic Channel Coding MAC (DCC-MAC)

DCC-MAC is a joint PHY/MAC architecture for 802.15.4a-like networks based on pulse position modulation UWB (PPM-UWB). Unlike traditional approaches, it fully utilizes the specific nature of UWB to obtain high rates at low protocol complexity. It is the first MAC protocol that adapts the channel code (and thus the bit rate) to interference from concurrent transmissions instead of implement exclusion. In order to avoid a complex mutual exclusion protocol at the MAC sublayer, DCC-MAC proposes an interference mitigation scheme. This scheme is based on a modification of PHY that cancels much of the interfering energy, in particular from nearby interferers. A dynamic channel coding is used to cope with the remaining interference. Sources constantly adjust their channel codes to the level of interference and send incremental redundancy as required. Contention between sources sending to the same destination is solved by a "private MAC" protocol that involves only the nodes that want to talk to the same destination. The "private MAC" does not use any common channel; this avoids the issues of hidden and exposed terminals. Rate Compatible Punctured Convolution (RCPC) codes are in use to perform dynamic channel coding. TH-codes as in U-MAC and UWB^2 are used to achieve multiple access to the shared medium.

The advantages of DCC-MAC are:

- It fully satisfies the application requirements of 802.15.4a in terms of link lengths, rates and mobility
- It achieves a significant increase in network throughput, compared to traditional MAC protocols like 802.15.4, that are separated from the physical layer

The drawbacks of DCC-MAC are as follows:

- If an UWB receiver is used at the sensor node end, then DCC-MAC has the same drawbacks as U-MAC and UWB^2
- Mitigation of interference at the expense of physical layer complexity
- A great amount of processing takes place at the sensor nodes causing an increased power consumption. DCC-MAC assumes that the sensor nodes always transmit at the maximum allowable transmit power. A power controlling approach for power stringent WBAN applications of UWB might be more suited
- Resynchronization is permitted with each data packet. WBAN applications recommend synchronization per session

2.9.28 Multiband MAC for IR-UWB

Multiband MAC for IR-UWB proposes multiple access through allocation of a unique frequency band per coordinator data communication link. Sensor initialization and control message transfer occur using a common control channel, which is assigned with a unique frequency band. Data communication and control use a 500 MHz bandwidth. The common control channel is shared with multiple users by the use of TH-codes.

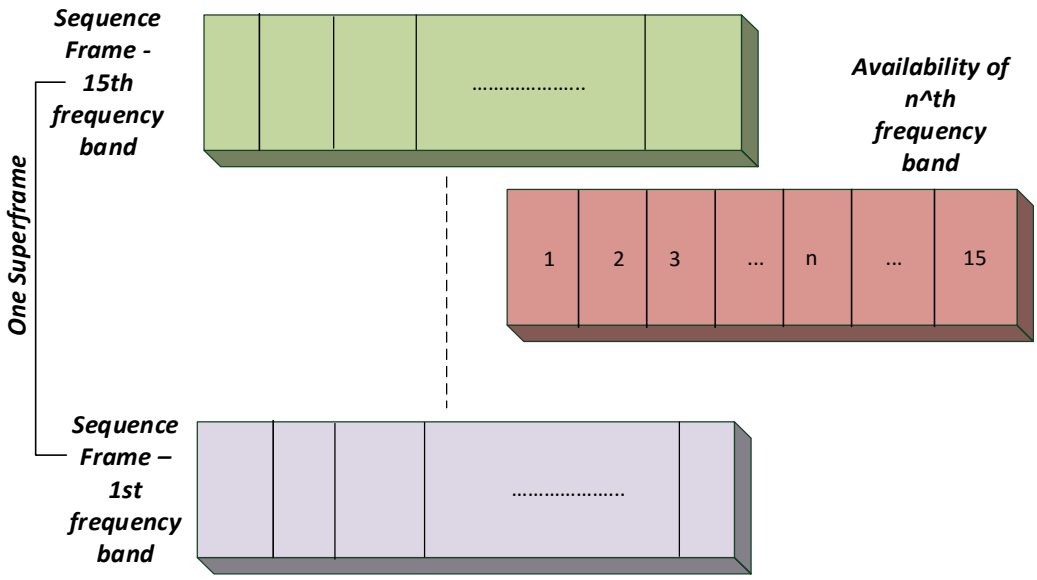


Figure 90 The superframe structure of multiband MAC

As shown in Figure 90 a superframe structure defined for data and control message transmission. A superframe consists of 15 sequence frames and each of them is used for data transmission in each band. The availability of a specific frequency band for data transmissions is indicated by the use of an *availability frame* between two superframes. If a node wants to continue its data transmission in a particular band, must send consecutive UWB pulses in the specified time slot allocated to point out that this frequency band is occupied. Other nodes sense these UWB pulses within the corresponding time slots of the availability frame and determine in this way if a particular band is available for data transmission or not.

The advantages of Multiband MAC for IR-UWB are:

- It can be used for concurrent data transmissions from multiple numbers of sensor nodes due to the use of different frequency bands
- Reduction of the collision probability (due to the first advantage)
- Increase of throughput
- Low latencies
- Implementation of high data rate applications

The drawbacks of Multiband MAC for IR-UWB are:

- Increased hardware complexity due to operation of the nodes in multiple frequency bands in order to send data in different frequency bands. WBANs dislike hardware complexity
- To access the common control channel more complexity added due to the fact that data signals must be modulated into TH-codes
- The nodes sense the UWB pulses during the availability frame. To achieve this, the use of a UWB receiver at the node is necessary and also the implementation of energy consuming pulse sensing mechanisms

2.9.29 Pulsers

Pulsers uses an update of the IEEE 802.15.4a superframe structure to provide a guaranteed delivery for nodes with high QoS requirements. It uses an extended Contention Free Period (CFP). The

Contention Access Period (CAP) consists of two time slots for the exchange of initialization messages and control messages. A node that wants to send data, it requests the allocation of a guaranteed time slot (GTS) in the CFP in the next superframe using one of the both CAP time slots.

Advantages of Pulsers are:

- Is well suited for WBAN applications with high data rate requirements
- Reduction of power consumption. Between the data transmission slots, nodes can be inactive (inactive mode)
- Latency reduction through network control decentralization (that achieved using a peer-to-peer relay mechanism)

Disadvantages of Pulsers are:

- All disadvantages of IEEE 802.15.4a if applied in WBAN applications
- These is no synchronization mechanism proposed for Pulsers. A precise timing synchronization for the TDMA-based multiple access mechanism is an important issue

2.9.30 Transmit-only MAC

Implantable or wearable WBAN nodes are battery powered, therefore power consumption is a critical factor. The efficiency of a MAC-protocol is a synonym for low-power consumption. The lower the power consumption, the higher the efficiency. Some of the MAC protocols presented in this work have limitations when used in UWB based WBAN applications. Due to the low-power operation of IR-UWB transmitters, IR-UWB receivers must detect pulses with low-power level. To reach this goal a complex and high-power consuming receiver architecture is inevitable. The asynchronous MAC protocol described here, the Transmit-only MAC protocol, enables the use of a transmit-only hardware design at the node end. Its characteristics are:

- Transmission of data packets with a much higher data rate than the required data rate. The sensor nodes can then sleep longer before sending the next data set
- In order to reduce the number of collisions each node transmits at a preallocated and unique transmission slot
- Every WBAN in the same region has a unique pulse rate
- The state of the channel is unknown by the node during the node transmission
- No network feedback exists

Figure 91 shows the frame structure for the Transmit-only MAC protocol.

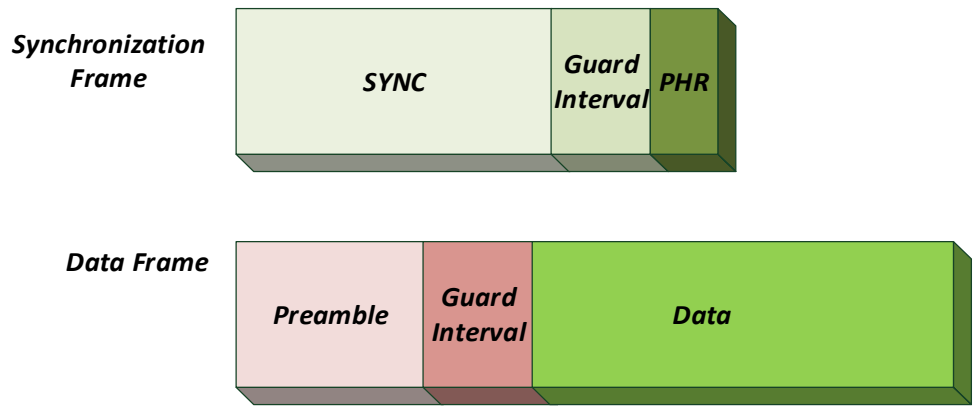


Figure 91 Frame structure for Transmit-only MAC protocol for WBAN

A sensor node is first connected to the network through self-synchronization at the gateway node. After the synchronization with the gateway a guard interval follows. This guard interval allows the receiver to prepare for the receipt of information in the physical header (PHR). The PHR includes information symbol rate, chirp rate and the timing for the next transmission window. After the establishment of the initial communication with the gateway node the data frame will be used in the successive transmissions. It consists of a preamble, a guard interval and the data itself. The preamble supports the receiver to achieve fine synchronization. The guard interval prepares the receiver for data reception. Transmit-only MAC keeps the data frame overhead to a minimum to reduce the chances of collision (due to the short transmission period).

The drawbacks of the transmit-only MAC protocol are:

- The increase of the network traffic leads to reduction of the data delivery capacity in the network due to collisions that come from the asynchronous transmission of pulses
- Changing of channel conditions does not lead to dynamically adjust of the transmit power
- Network rescheduling requires manual intervention

2.9.31 Battery-aware TDMA protocol

The cross-layer-design target for the battery-aware TDMA protocol is to prolong the battery lifespan of the nodes while guaranteeing reliable and timely message transmission. The following parameters play together (joint effect) an important role in this MAC protocol:

- Electrochemical properties of the battery
- Time-varying wireless fading channels
- Packet queuing characteristics

The operation of the battery-aware TDMA is similar to IEEE 802.15.4 beacon enabled mode. As described in this work, in this mode the nodes listen periodically to beacons from coordinator. The battery-aware TDMA frame structure consists of the beacon slot, active time slots and inactive period (Figure 92).

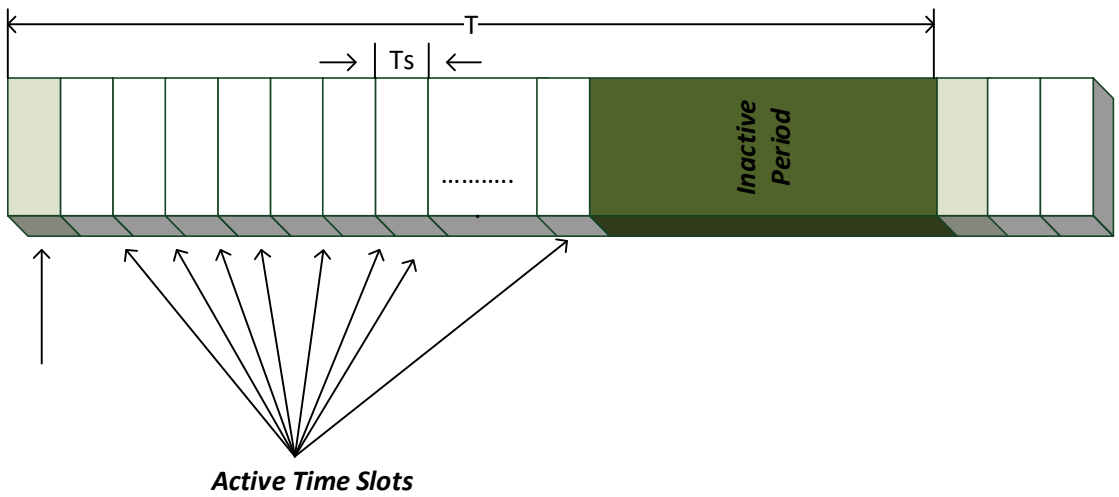


Figure 92 Battery-aware TDMA frame structure

The application requirements can set the frame length due to its adaptability. The nodes wake up if the beacon periods begin. The data transmission of every node takes place at its own distinct time slot T_s. To save energy each sensor node is active during the beacon slot and its own time slot only when it has packets to transmit, otherwise, it sleeps. Through the use of guaranteed time slots (GTSs) reliable and timely delivery of packets is achieved.

The drawbacks are:

- There is no mechanism for emergency data
- High average delay and packet drop rate due to similarly holding of packets in buffer for a long time

2.9.32 Priority guaranteed MAC protocol

The priority guaranteed MAC uses a new superframe structure (Figure 93).

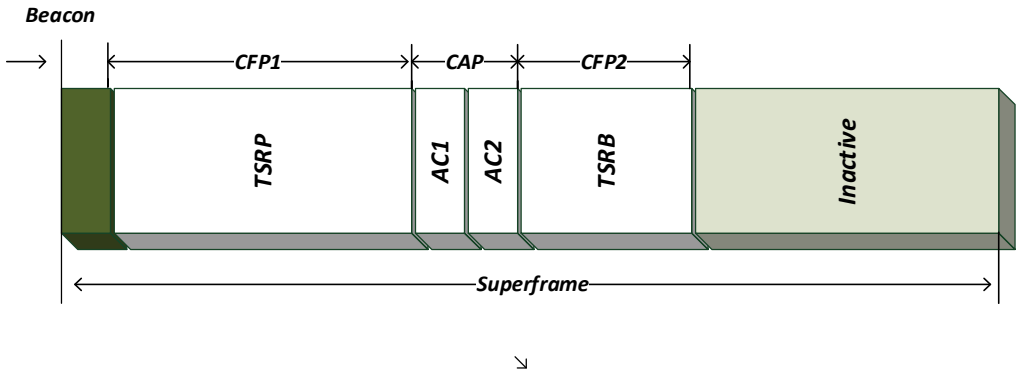


Figure 93 Priority guaranteed MAC superframe structure

The active period consists of the following parts:

- A beacon
- Time slot reserved for period traffic (TSRP)
- Control channel AC1
- Control channel AC2
- Time slot reserved for bursty traffic (TSRB)

AC1 is used for uplink control of life-critical medical applications. AC2 is used for uplink control of consumer electronics (CE) applications. The access to the control channels AC1 and AC2 is implemented using randomized ALOHA. Priority guaranteed MAC uses TDMA to assign GTS within two data channels TSRP and TSRB.

The advantage of priority guaranteed MAC is that it out performs IEEE 802.15.4 consuming less energy. The disadvantages of priority guaranteed MAC are:

- Its complex superframe structure
- Its lack of variability to support emergency traffic

2.9.33 Energy-Efficient Low Duty Cycle MAC protocol (E2ldcMAC)

WBANs have a fixed network topology. Energy-Efficient Low Duty Cycle MAC is based on this fact. It uses TDMA for the medium access. The topology for which this MAC protocol is designed consists of a master node (MN), on body nodes and a monitoring station (MS). The MN collects data from the nodes and communicates with the MS (Figure 94).

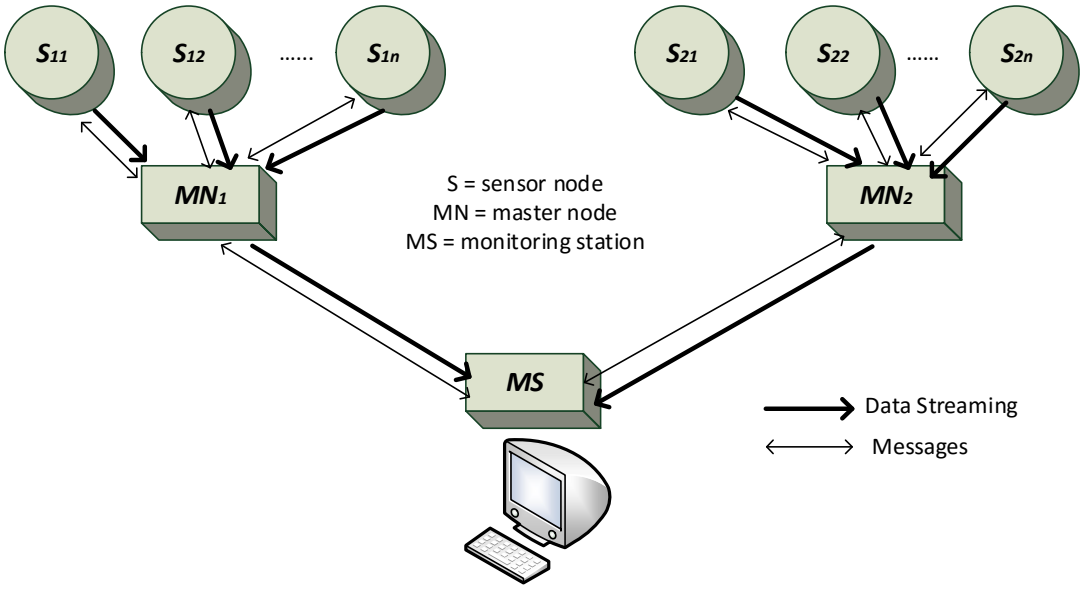


Figure 94 Network topology energy-efficient low duty cycle MAC

MS analyzes the received data. MN performs the network connection and synchronization. Figure 95 shows the TDMA frame structure that consists of multiple time slots. Time slots S_1 to S_n are allocated to nodes. Time slots RS_1 to RS_k are in use only by request. K, the number of the RS slots depends upon targeted packet drop, number of nodes and packet error rate.

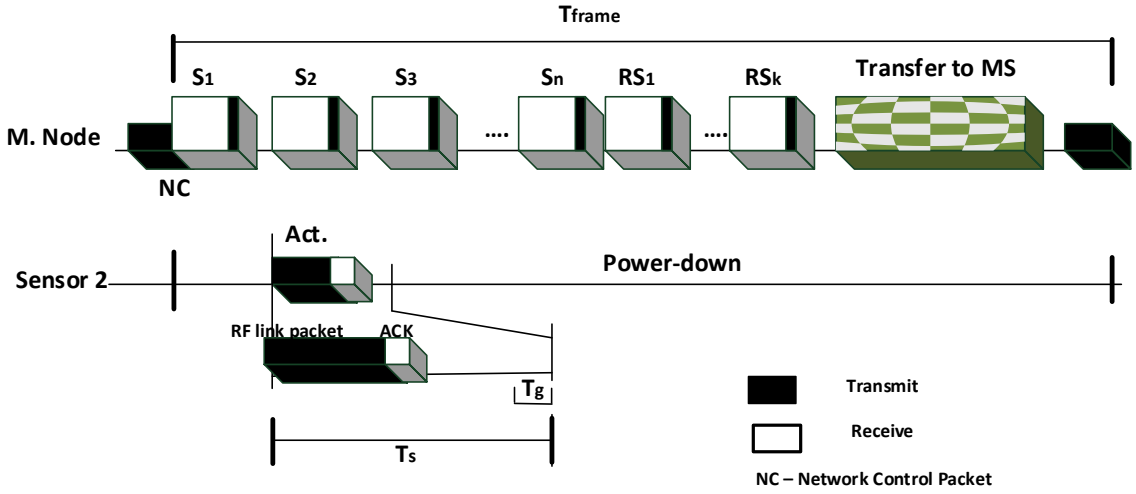


Figure 95 TDMA frame structure

Between two consecutive time slots guard band time is inserted to avoid collision and overlapping of packet transmission due to clock drifts. Two use cases for communication can be applied. The first one is the use case with one transceiver in the MN and the second is the case with two transceivers. The second use case allows the simultaneous communication of MN with the nodes and the MS.

Advantages:

- The protocol outperforms in term of energy for high communication data rates
- It also outperforms in term of short burst of data

Disadvantages:

- The use of a network control packets for periodic synchronization after N time frames results to additional energy consumption
- There is no CAP to accommodate small burst of data
- There is no mechanism for on-demand traffic

2.9.34 A power-efficient MAC protocol for WBANs

The MAC protocol proposed here deals with on-demand, emergency and normal traffic. It maintains two wakeup mechanisms for reliable transmission:

- wakeup radio for emergency or on-demand data transmission
- traffic based wakeup for transmission of normal traffic

Nodes that monitor routine physiological parameters like temperature generate periodically normal traffic. In the case of emergency traffic that also generated from sensor nodes it is important to response in less than one second and have access to the channel. On-demand traffic is initiated by the hub or a human (e.g. physician) to gather diagnostic or prescription data from sensor nodes. Figure 96 illustrates the MAC mapping of the WBAN traffic.

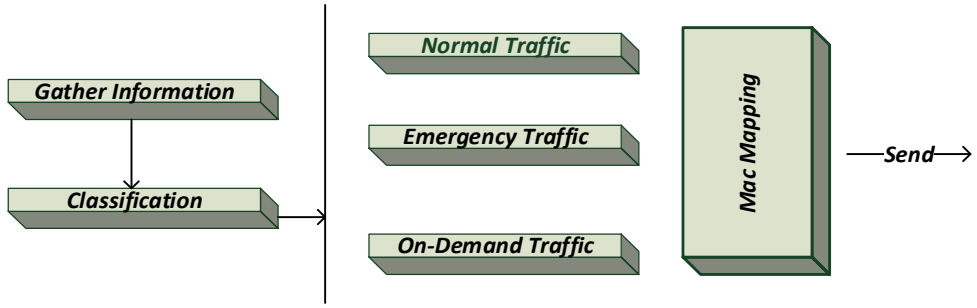


Figure 96 WBAN traffic classification

This MAC protocol defines a new superframe structure. The time axis of the superframe has the following parts:

- A beacon message
- A configurable contention access period (CCAP) for a short burst of data
- A contention free period (CFP) where GTS are assigned to end nodes to avoid collisions

The complete superframe can be seen in the Figure 97.

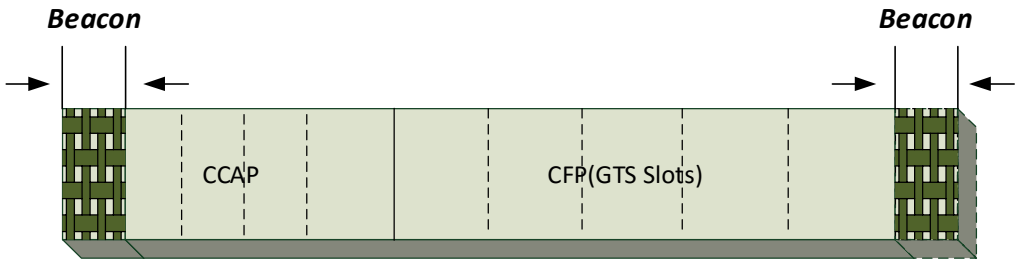


Figure 97 Frame structure

In the CCAP period slotted ALOHA is in use. The hub (coordinator) organizes a traffic-based wakeup table taking into account the applications requirements. Energy waste due to overhearing and idle listening can be avoided by the use of a periodic sleep and wakeup mode.

The data transfer models for normal traffic, updating traffic-based wakeup table, emergency traffic and on-demand traffic are shown in the Figure 98.

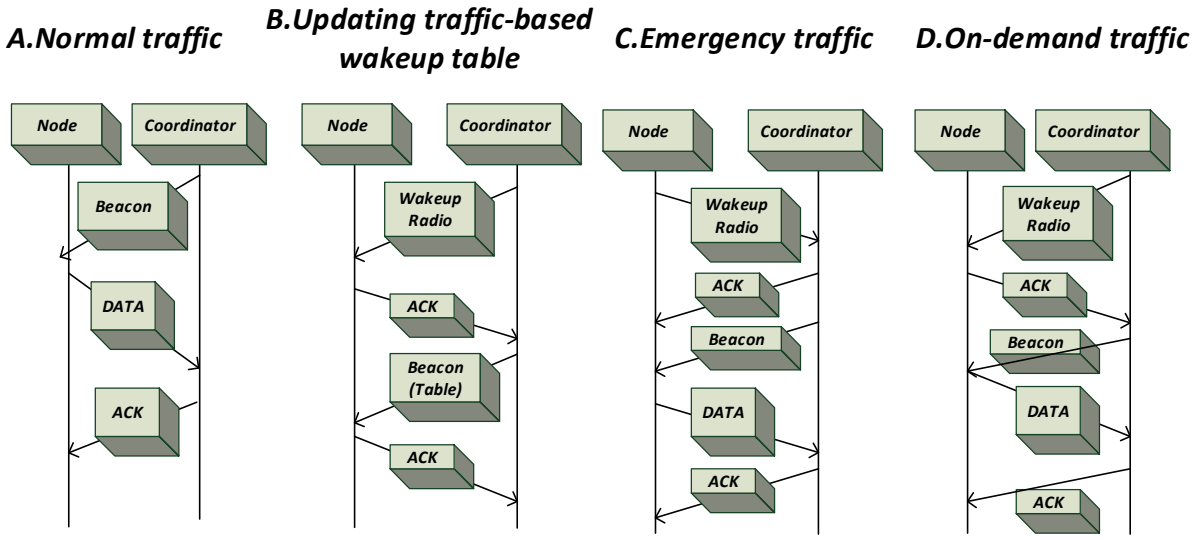


Figure 98 Data transfer models for normal, emergency and on-demand traffic

(a) shows the case of normal traffic. The hub transmits a beacon to the node, after that the node sends the data and the hub acknowledges the receipt. (b) shows the updating process of the traffic-based wakeup table. (c) is the case of emergency traffic. A wakeup radio mechanism is used. To access the channel, the node sends a wakeup radio signal to the hub. Unlike normal traffic it is not necessary for the node to wait for the beacon since this may exceed the delay requirement. (d) shows the on-demand traffic case where channel access achieved by the transmission of a wakeup radio through the hub.

2.9.35 Energy Efficient Medium Access protocol

The Energy Efficient Medium Access protocol is proposed in [51]. It based upon centrally controlled wakeup and sleep mechanisms to maximize energy efficiency. The use of a star topology, a hub (master node) that coordinates sensor nodes (slave nodes) are its basic architecture characteristics. At maximum eight nodes belongs to a hub. The hub has high computational capabilities.

Three processes build the basic operation of this protocol:

- Link establishment
- Wakeup service process
- Alarm process for emergency data

By the link establishment the slave node joins a cluster. After the link establishment get assigned a unique sleep time. The reason for this assignment of a unique sleep time is to avoid overhearing and idle listening. The wakeup service process allows communication between master and slave nodes. If the node (slave) has emergency data to send it initiates the *Alarm process* for communication with the hub. The *wakeup fallback time (WFT)* is a mechanism to calculate a specific time interval in case of communication failure for a node during its assigned wakeup process. For this time interval the slave node passes into the sleep mode. Meanwhile the collected data packets are buffered by the node for future transmission. If the hub fails to communicate with the node it passes also in the sleep mode for a time calculated by WFT. WFT is responsible for the avoidance of time slots overlapping.

Drawbacks:

- Complex implementation
- No mechanism to handle with on-demand traffic
- One cluster has a limited number of nodes
- Communication initialization occurs only by the master node (hub)
- The Link establishment process handles only one node at a time

2.9.36 MedMAC

As many other MAC protocols for WBANs the MedMAC protocol improves channel access and intends to reduce energy dissipation. It uses TDMA. The length of the assigned time slots is varying according to node requirements. The multi-superframe structure for MedMAC is shown in Figure 99.

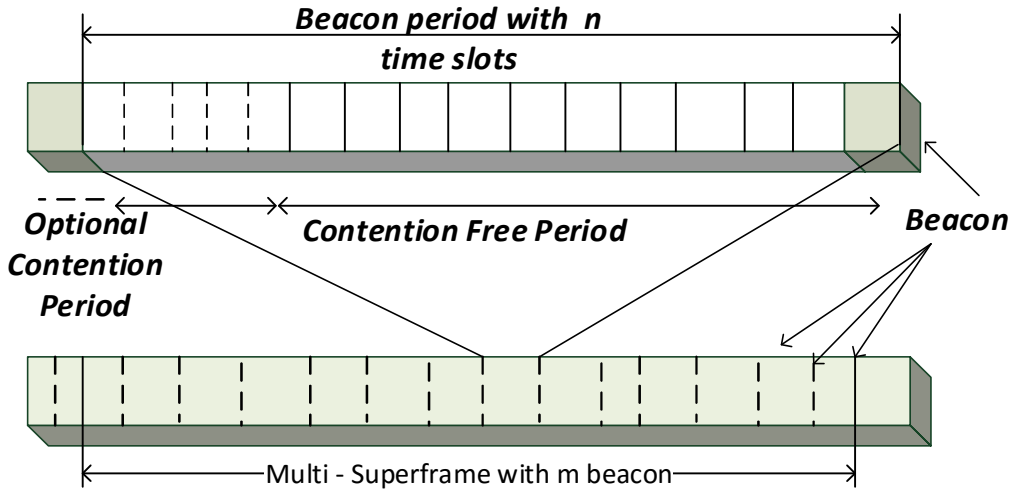


Figure 99 Multi-frame structure for the MedMAC protocol

An optimal contention period is used for low data communication, network initialization and emergency traffic. MedMAC uses the *Adaptive Guard Band Algorithm (AGBA)* and timestamp scavenging for hub and node clock synchronization. AGBA faces the clock drift problem and maintains the device synchronization to prevent collisions. GTS is also used to avoid collisions of data packets. Between two consecutive time slots AGBA embeds adjustable guard band time that depends on clock drift of devices. The *Drift Adjustment Factor (DAF)* has the task to monitor the guard band and to prevent the bandwidth waste using additional guard bands.

Advantages for apps with low data rates (e.g. temperature):

- MedMAC outperforms IEEE 802.15.4 with respect to energy consumption
- Collisions avoided using GTS

Drawbacks:

- MedMAC does not consider high data rates. High data rates in WBANs with wearable and implanted nodes is a main use case

2.10 Hardware and Devices

The choice of the hardware platform is one of the most important aspects during the design process of a WBAN. The application requirements dictate WBAN design issues like physical shape, packaging, processing capabilities, and battery consumption at the core of a WBAN's architecture design.

A body sensor consists of (Figure 100)

- a radio module (RF module)
- the signal sensor module
- a memory module and
- the microcontroller unit

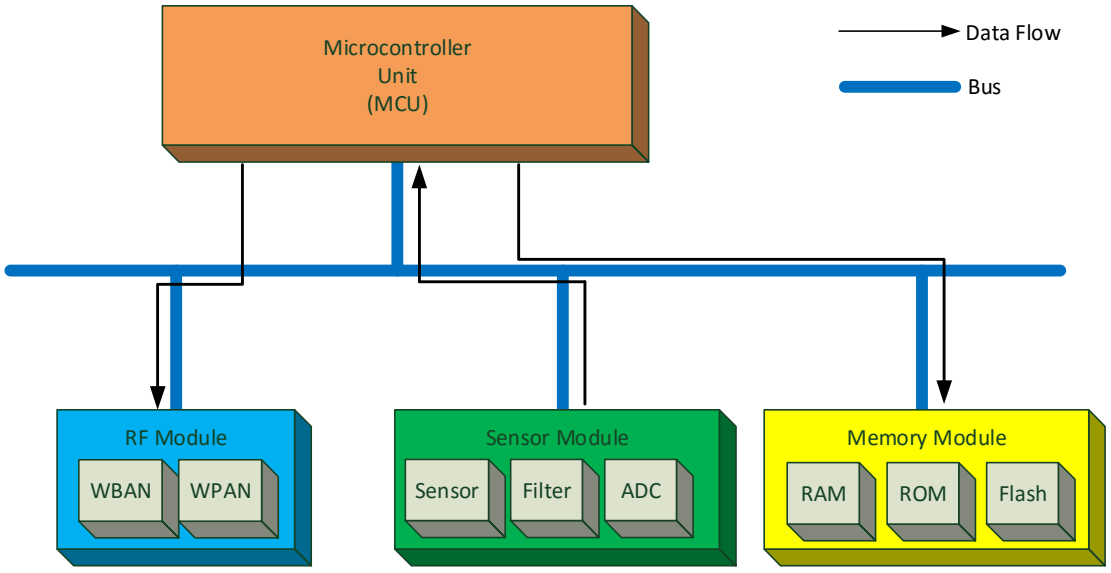


Figure 100 Modules of a sensor node

Body sensors gather vital signals. These collected signals have their origin and correspond either to different physiological user conditions or physical activities. After the signal is gathered it is digitized and finally transmitted by the radio transmitter of the sensor. Sensors in WBANs are in direct contact with the human body or are implanted in the body. Physical compatibility to human tissues and the size of the sensors are immense important. The continuous advances in *Micro Electro-Mechanical Systems (MEMS)* lead to the development of smaller and wearable sensor devices, devices in the range of 1 to 100 micrometers. The sensor sends the selected data (analog or digitized signals) to its *Microcontroller unit (MCU)* for immediate processing. Specialized pre-processing or filtering of the selected data can be used before the transmission through the sensor. The pre-processing or filtering can be implemented as

- an intermediate hardware component or
- as software running in the MCU

The radio transceiver of the sensor eliminates the need to communicate with a coordinator node via wires for the transmit of the selected data. Next we describe three types of devices used in WBANs:

- wearable node devices
- implantable node devices
- in vivo node devices.

2.10.1 Wearable node devices

The realization of small wearable node devices that are amenable to every day monitoring was an elusive goal through the years. The latest MEMS-based node and hub devices targeted at bio-monitoring applications. The effectiveness and reliability of these devices led to use them not only for different types of motion sensing applications but also for automated drug delivery systems. There are many types and shapes of wearable node devices. ECG monitoring nodes employ electrodes which are made of *silver chloride (AgCl)* adhered to the different regions of the torso. Disadvantages due to the long-term usage of the electrodes are skin contact problems and failure of electrical contacts. To solve these problems a new type of wearable nodes has been implemented. Electrodes embedded into textile fabrics that can be worn as regular clothing garments. This alternative is better suited to human motion because it is free from skin problems and it is more flexible if they compared to AgCl-based electrodes since their shape is adaptable if the body moves. Some types of commercial available node devices are listed below:

Accelerometer/Gyroscope is used to recognize and monitor body posture. The *glucometer* analyzes the blood sample giving then a glucose reading. Recently, non-invasive glucose monitoring is possible through optical sensing and infrared technology. The *blood pressure sensor* measures systolic and diastolic human blood pressure. The *CO_2 gas sensor* measures changes in CO_2 levels and monitors oxygen concentration during the respiration process. The *ECG sensor* records the electrical activity of the heart. The *EEG sensor* measures the electrical activity within the brain. The *EMG sensor* measures electrical signals generated by muscles during contraction or rest phases. The *pulse oximetry sensor* measures oxygen saturation. *Humidity and temperature sensors* measure the humidity of the immediate environment around a person and the temperature of the human body.

2.10.2 Implantable node devices

Sophisticated implanted (medical) nodes with integrated wireless technology support an increasing range of diagnostic, therapeutic and other applications. A network of on-body and implanted nodes can stimulate muscles to restore lost limb function. A radio-controlled valve implanted in the urinary

tract and operated by the patient on-demand helps to restore bladder control. An implanted pacemaker communicates the patient data to base station or hub. These are examples of implanted node devices which require a reliable wireless communication link. The wireless communication link interrogates in regular or irregular intervals the implant. One-way wireless links obtain patient health data or node performance data. Two-way wireless links enable external reprogramming of the implanted node. We discuss here two types of communication links:

- The inductive loop communication
- The Radio Frequency communication

2.10.2.1 Inductive coupling

There are many applications which still use electromagnetic coupling to implement a communication link to implanted devices. These applications use an external coil held near or very close to the patient. This external coil couples to a coil implanted just below the skin surface. The implant does not need a battery. It is powered by the coupled magnetic field. This alternating field is used also to transfer data into the implant. Regarding the data transfer from implant to a coordinator node data is transferred by altering the impedance of the implanted loop that is detected by the external coil and electronics. With the use of the inductive loop small data packets can be transferred from an implanted node (due to absence of a battery). This kind communication link is used if continuous, long-term communication is required. An application example is the cochlear implant used to restore hearing. Another inductive coupling application is the *Abdominal Aortic Aneurysm (AAA)*. A shaped tube is inserted into the sufferer through a keyhole in the groin. The tube is placed in the affected area. An included pressure sensor that evaluates the patient's health can provide data at any time and for many years. This procedure results to an avoidance of an abdominal surgery and the patient can be easily monitored. Inductive coupling operates with a base band of 13.56 MHz or 28 MHz. Other frequencies can also be used. The use of inductive coupling is not practical if space is limited or the nodes are to be implanted deep within the patient. The node achieves the best power transfer when using large transmit and receive coils. Another disadvantage is that inductive coupling does not support very high data rates and a communication session can not be initiated from inside of the body.

2.10.2.2 RF communication in the body

The difference between RF communication and inductive coupling is that RF communication increases bandwidth and makes possible the operation of a two-way data link. A two-way data link enables the implant to initiate a communication session. To achieve this RF communication requires a suitable antenna, electronics, and an implanted battery. The radio frequency (RF) communication allows the transfer of larger data packets.

Wireless communication through air is a very well documented and researched area. Wireless communication through the human body is a new study area. For a wireless signal the human body is often an unfriendly and uninviting environment. A main aspect here is the physical size of the node. A small antenna on the one side and an effectively coupling to the transceiver on the other side, taking into account the low power constraints imposed by implantable devices, are requirements to in-body communication system design. The human body is composed of varied components. These components are not predictable and change with patient age, with weight lost, or changes in posture. It is very difficult to calculate the in-body communication system performance due to the fact that each individual is different. A surgeon does not care about wireless performance but implants the implant into the best position to perform its main function. The operation in different environments and positions is an important requirement of implanted RF communication systems. Understanding of the

mechanism of wave propagation and attenuation inside human body is crucial in order to design power efficient in-body communication schemes. Radio frequency simulation is an important instrument to achieve this.

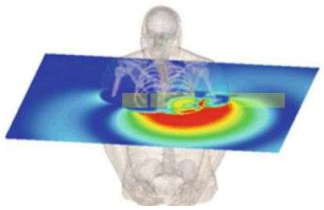


Figure 101 The field radiated from the loop antenna of an implanted pacemaker at 400 MHz

Figure 101 makes visible the field radiated from a loop antenna of an implanted pacemaker at 400 MHz. Radio frequency simulation uses here visible human (Visible Human Project http://www.nlm.nih.gov/research/visible/visible_human.html) and whole body statistical shape models. The fields showed in Figure 101 were simulated using the time domain solver of CST MICROWAVE STUDIO (www.csr.com). The human phantom consists of 32 different tissues at a 1 mm resolution.

2.10.3 In vivo node devices

Recent improvements in multimedia technology and image sensing make possible to encapsulate video cameras into pills which can be swallowed in order to inspect inside the body areas which were difficult to reach with traditional medical devices. High definition video recorded and transmitted to an on-body receiver for live monitoring.

Some small set of commercial sensor nodes with their operating system and the supported standard are listed below (Table 17):

Name	OS support	Wireless standard
BAN node	TinyOS	IEEE 802.15.4
BTNode	TinyOS	Bluetooth (BT)
eyesIFX	TinyOS	TDA5250
iMote	TinyOS	BT
iMote2	TinyOS or .NET	IEEE 802.15.4
IRIS	TinyOS	IEEE 802.15.4
Micaz	TinyOS	IEEE 802.15.4
Mica2	TinyOS	IEEE 802.15.4
Mulle	TinyOS or TCP/IP	IEEE 802.15.4 or BT
TelOS	TinyOS	IEEE 802.15.4
ZigBit	ZDK	IEEE 802.15.4

Table 17 A small list with commercial sensor nodes.

More information can be found in [52].

2.11 STANDARDS COMPARISON

The definition of the different standards is a process of evolution. Table 18 summarizes the main differences between the primary requirements for MAC protocols. These are the features power consumption, battery life, and scalability. Table 19 compares some other characteristics of the mentioned WBAN MAC sublayer standards. These are frequency band, the data rate, the medium access, the network topology, the node operating space, the maximum application throughput, the maximum number of nodes, the maximum number of channels, the security, and the maximum transmission latency. All these features depend on the MAC sublayer protocol defined in the respective standard. The access mechanism and the MAC frame format are two important MAC sublayer characteristics. The frame format builds a specification of the MAC frame types and the resulted MAC sublayer functionality.

IEEE 802.15.1 operates in the 2.4 GHz ISM band with a peak power of 45 mA at 3.3 V. Bluetooth uses 3 Mbps as data rate and it designed for a 100 m wireless communication range. These characteristics make IEEE 802.15.1 adequate for medium-rate WBANs. Bluetooth is an extremely ubiquitous standard. It can easily be adapted to several other networks and its latency is less than 10 sec. One disadvantage regarding its use for WBANs is its limited scalability due to the limited number of auxiliary nodes. Another disadvantage is its high-power consumption (40 mW). Bluetooth LE is an extension of Bluetooth 4.0 and operates in the 2.4 GHz ISM band with a peak power of 28 mA at 3.3 V. The coverage area of BLE is 1 – 10 m in contrast to standard Bluetooth (1 – 100 m), it reduces power consumption but has a limited scalability with latency less than this of standard Bluetooth.

IEEE 802.15.4 was pioneer in the issue of enabling nodes and hubs to share the wireless platform. It was designed for WPANs, with the features low-cost, low-power-consumption (0.5 mW – 1 mW), and operation in a short range (10-100m). IEEE 802.15.4 is used in the IoT (Internet of Things) but it cannot support efficient high data rate applications due to the fact that its maximum data rate is up to 250 kbps. IEEE 802.15.4 operates with a peak current of 20 mA. The advantage of the its non-beacon mode is that the nodes do not need to regularly power-up to receive a beacon. The circumstance that the hub cannot start communication with the nodes and the nodes must poll the hub is a disadvantage. In the nonbeacon-enabled peer-to-peer topology the communication devices must keep permanently their radio on. Otherwise some communication mechanisms must be applied. IEEE 802.15.4 scores over IEEE 802.15.1 because of its lower cost, the lower power consumption, longer battery life, scalability features, a smaller latency value 20 – 30 ms and last but not least because it supports standard-based security.

IEEE 802.15.4a is an enhancement of IEEE 802.15.4 standard offering an alternative PHY. Its goal is to provide high-precision ranging (1 m and better) and reliable communications taking into account low-cost and low-power devices. CSS, a spread spectrum technique, added to IEEE 802.15.4a to compete with ultra-wideband (in the 2.45 GHz band). It is applicable for apps with low-power consumption and low data rates (<= 1 mbps). If we increase the number of packets, communication in IEEE 802.15.4a becomes unstable. Therefore, it is only suitable for low data rate communication and for applications with relaxed throughput requirements (drawback). The IEEE 802.15.4a MAC sublayer supports all topologies and device types supported by IEEE 802.15.4. The main difference regarding the MAC sublayer between IEEE 802.15.4 and IEEE 802.15.4a is its channel access strategy. IEEE 802.15.4a uses random ALOHA. Due to the multi-user interference robustness of UWB, random ALOHA provides passable throughput for light and medium traffic loads. CSMA/CA access is for IEEE 802.15.4a only an option in case of high traffic loads and also to enable CSS. IEEE 802.15.4a differs from its predecessor having power consumption less or equal 0.1 mW.

The IEEE 802.15.4j standard is a ZigBee PHY and MAC modification and provides the same low-power mesh-networking and robust protocol with a slightly different frequency spread avoiding the crowded unlicensed spectrum, and improving reliability and robustness. IEEE 802.15.4j includes a new channel switch command to move out of a concrete MBAN spectrum to the secondary one if the MBAN hub must take care about the primary services and protect them. In case of communication loss with the hub a node in IEEE 802.15.4 sends a notification command and hopes that the hub will discover it and respond with a hub realignment command. A comparison with the IEEE 802.15.4 hub realignment command shows that the new channel switch command of IEEE 802.15.4j incorporates a time stamp which indicates the time where the MBAN should switch to a new channel. With this method a re-channelization of different types of MBAN services can be reached resulting in collisions avoidance and ensuring also QoS. IEEE 802.15.4j supports better than IEEE 802.15.4 low duty cycle operations using the multi-periodic guaranteed time slot (GTS). This enables that the MBAN devices sleep most of the time and reduce power consumption. In IEEE 802.15.4 the slots belong to a GTS allocation are available to the assigned device in every superframe. The difference with 4j here is that in the multi-periodic GTS, slots can be assigned from the hub to its device for operation every S slots, where $S = 2^K$ and K = 1 .. 8 where K is the GTS period exponent. The selection of S as a power of 2 makes slot sharing less complicated. The GTS slot allocation management becomes easier. The proposed MAC features coordinator switch and association proxy build also a difference to IEEE 802.15.4. These features simplify MBAN device pairing and contribute to less power consumption.

The target applications of IEEE 802.15.6 are wearable devices. This standard supports a variety of applications ranging from healthcare to consumer entertainment. IEEE 802.15.6 is the first international standard for WBANs. Its aim is to integrate all possible features in a unique standard. IEEE 802.15.6 operates in low-power and short range (< 3m). The MAC of IEEE 802.15.6 supports multicast, unicast, and broadcast communication. The MAC header is made up of 7 octets. The shorter MAC header of 802.15.6 (compared with the IEEE 802.15.4 MAC header) enables it to offer higher data rates as shown in Table 19. In narrowband IEEE 802.15.6 offers a data rate up to 971.4 Kbps. The same issue effects also transmission power, IEEE 802.15.6 operates with a peak current of 3 mA (NB). This means lower burden for the transceivers which operate with 802.15.6. The frame control field format of IEEE 802.15.6 combines the frame type and frame subtype fields to classify different frames. This is a more efficient method than the method IEEE 802.15.4 applies. IEEE 804.15.4 uses only the frame type. Collisions in IEEE 802.15.6 are combated using the User Priority (UP). UP prioritizes the medium access of some type frames. E.g. the frame payload ‘emergency or medical implant event report’ (frame type data) has the highest User Priority 7. The application classes given in Table 18 (battery life and latency) are specified in the ISO/IEEE 11073 Draft for Point-of-Care (PoC) medical devices. These application classes are supported from IEEE 802.15.6. It supports three connectivity levels, unsecured communication, authentication only and authentication and encryption. Although the IEEE 802.15.6 standard was created to cover the complete spectrum of WBAN functionality in practice it is a complex and therefore unsuitable for ultra-low-power devices.

SmartBAN designed for ultra-low-power devices offering an efficient and simple MAC/PHY System. Ultra-low-power consumption and low latency for emergency systems are characteristics of SmartBAN. The SmartBAN standard specifies the smallest coverage area (<= 1.5 m) than all other standards and a latency of up to 125 ms which is lower than the lowest IEEE 802.15.6 App class F latency (up to 300 ms). [53]

WBAN MAC standards	Power Consumption	Battery life	Scalability
IEEE 802.15.1	40 mW	1-7 days	Limited
Bluetooth LE	0.147 mW	4 years (~100 µAh per day coin cell)	Limited
IEEE 802.15.4	0.5 mW – 1 mW	4-6 months	beacon-enabled mode: Limited nonbeacon-enabled mode: ✓
IEEE 802.15.4a	0.1 mW		Limited
IEEE 802.15.4j	50 mW		Limited
IEEE 802.15.6	~ 10 mW	(*) App class A: 0.13095-0.19156 years, app class B: 0.20489 years, app class D: 0.68493 years, app class E: 1.47530-1.92350 years, app class C: 21.3336 years, app class F: 0.04839-0.20581 years	✓
SmartBAN	TBD	TBD	✓

Table 18 BAN standards comparison: Power Consumption, Battery Life, and Scalability

WBAN MAC standards	Frequency band	Data Rate	Medium access	Network topology	Coverage area	Max app throughput	# nodes	# channels	Security	Latency
IEEE 802.15.1	2.4 GHz ISM	1, 1.2, 3, 24 mbps	TDMA	star scatternet	1-100 m	2.1 mbps (2.0)	7 active 255 total	79	shared key AES-CCM	< 10 sec
Bluetooth LE	2.4 GHz ISM	1 mbps	FH + TDMA	piconet star	1-10 m (1)	236 kbps	App limited	3	128 bit AES-CCM	3 - 6 ms
IEEE 802.15.4	868.3 MHz 902-928 MHz 2405-2480 MHz	868/915 MHz: 20/40 kbps 2.4 GHz: 250 kbps	CSMA/CA, GTS	star clustertree mesh	10-100 m	151 kbps	Up to 65536 devices per network	868.3 MHz: 1 902-928 MHz: 10 2405-2480 MHz: 16	128 bit AES-CCM	20-30 ms
IEEE 802.15.4a	UWB: 250-750 MHz 3244-4742 MHz 5944-10234 MHz CSS: 2400-2483.5 MHz	UWB:110 kbps, 851 kbps(nominal), 6.81 mbps, 27.24 mbps CSS: 1 mbps (nominal) 250 kbps	Random ALOHA CSMA/CA	star clustertree mesh	10-100 m		Up to 65536 devices per network	UWB: 16 CSS: 14	128 bit AES-CCM	
IEEE 802.15.4j	healthcare-MBAN: 2360-2390 MHz MBAN anywhere: 2390-2400 MHz	250 kbps		star clustertree mesh	~ 10-30 m		65535	2360-2390 MHz: 7 2390-2400 MHz: 3	128 bit AES-CCM	
IEEE 802.15.6	402-958 MHz 2360-2483 MHz 3.1 GHz - 10.6 GHz	Narrowband (NB): 402-405 MHz: 75.9-455.4 kbps 420-450 MHz: 75.9-187.5 kbps 863-870 MHz: 101.2-607.1 kbps 902-928 MHz: 101.2-607.1 kbps 950-958 MHz: 101.2-607.1 kbps 2360-2400 MHz: 121.4-971.4 kbps 2400-2483.5 MHz: 121.4-971.4 kbps UWB: 3,000-5,000: 394.8-12,636 kbps 6,000-10,000: 487-15,600 kbps HBC: 21 MHz: 164.1-1,312.5 kbps	CSMA/CA slotted ALOHA EAP	star multihop star	< 3 m out-body	674.7 kbps (NB)	64 nMaxBANSize	Narrowband (NB): 402-405 MHz: 10 420-450 MHz: 12 863-870 MHz: 14 902-928 MHz: 60 950-958 MHz: 16 2360-2400 MHz: 39 2400-2483.5 MHz: 79 UWB: 3,000-5,000: 3 6,000-10,000: 8 HBC: 21 MHz: 1	128 bit AES-CCM	(*) App class A<3 s (*) App class B<3 s (*) App class D<3 s (*) App class E<3 s (*) App class C<60 s (*) App class F<300 ms
SmartBAN	2401-2481 MHz ISM	Nominally < 100 kbps	(a) Scheduled Channel Access (as TDMA) (b) Slotted ALOHA (c) Multi-use channel access	single-hop star	<= 1.5 m			37 data channels and 3 control channels	TBD	< 125 ms

Table 19 WBAN standards comparison

2.12 MAC SUBLAYER CHALLENGES

Due to the evolution of WBAN MAC sublayer protocol design we consider in this section the challenges from the IEEE 802.15.6 point of view and the achievements that have been reached so far. Reliability for WBANs is vitally important. The reason for that is the kind of applications WBANs used for, the healthcare applications.

IEEE 802.15.6 does not specify the complete MAC protocol. Only basic requirements which ensure interoperability amongst devices are treated. Message exchange protocols and packet formats build the main aspect of this standard which used to achieve simple tasks e.g. acknowledge the reception of a packet or assign an allocation interval. Further research questions have not been resolved. Some of these are described here.

In what order do we schedule allocation intervals? When should relays be used? Which is the decision process regarding the question which type access to use: Improvised, scheduled or contention-based? When should we cope with failed packet reception using retransmission of the packets?

It is important to understand the problems and the issues behind these questions. The Knowledge of the channel characteristics will lead us in smart decisions. For example, in case of transmission failure it does not make sense to try an immediate retransmission of the failed packet because the channel is likely to still be in an outage.

WBAN topology and density changes relative to body movements resulting in nodes moving into or out of coverage. The orientation of the nodes in relation to each other as well as the human body can 'shadow' the signal. This use case (e.g. topology changes) need to be addressed in the MAC protocol design. Robustness in supporting multiple WBANs in parallel applications is another field needs to be addressed. Severe attenuation of the wireless signal between node and hub (attenuation of over 100 dB has been observed) may push the received signal power below of the sensitivity of the receiver. Receiver's sensitivity is the minimum signal power level which guarantees reliable communication. Sensitivity is limited in WBAN nodes due to their relatively small antennas and simple energy-efficient designs. These facts show us that the *behavior of the wireless channel around the human body* or in other words ***the unique characteristics of the wireless channel*** represents a unique set of challenges to reliable communication.

Another use case, the use case 'people move' generates the next challenge regarding reliable communication. Due to the fact that the nodes in a WBAN are coordinated by a hub, a large number of devices can coexist in a single network without having them interfere each other. If multiple people wearing WBANs node coordination is impossible. ***Minimizing or managing the interference*** is also an important challenge.

The proposed MAC protocol do not provide efficient delay performance and network throughput at varying traffic. Also the synchronization of duty cycles (see definitions) of the hubs and nodes taking into account variant traffic characteristics and power requirements build a challenge. In order to be able to serve higher throughput applications such as video WBANs need to support a wide range of throughput rates (1 kb/s to 10 Mb/s). ***Application requirements*** build another challenge for reliable communication.

Some issues MAC protocols should support are: prolong sensor lifetime, support of the energy efficiency requirement of WBAN applications, energy saving by periodically switching the radio on/off

and flexible duty cycling. Instead of idle listening channel polling should be used to find out if the nodes are awake to transmit or to receive. If nodes have low duty cycle they shouldn't receive frequent control packets and synchronization in the case that they do not intent to receive or to send data. We recognize here a major challenge for WBANs: ***extreme energy efficiency***.

Additionally, specific QoS requirements need to be met by the MAC protocol proposal. The high sampling rate from sensors in a WBAN should be managed by transmit data packets with the earliest deadline or permit data to be send out as soon as possible. A reason for this requirement and challenge is for the example the case of emergency applications. The MAC protocol must allow quick access of the nodes to the channel due to the fact that life critical data must reach 'the fastest way' the coordinator in the WBAN.

As we presented in a previous section there are two kinds of MAC proposals, the contention-based such as Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) and the scheduled- or reservation-based such as TDMA. One property of the contention-based proposal is that they do not need to apply strict time synchronization. However, they suffer from heavy collision in case of high traffic nodes. Scheduled-based proposals like TDMA MAC on the other hand are energy efficient, do not suffer from contention, idle listening or overhearing and reduce the duty cycle. However, they must face a different challenge. Their periodic time synchronization requires extra energy.

3 WBAN PRIVACY AND SECURITY

Privacy and security of WBANs are two independent from each other issues. Privacy is the right of every individual to control its own data (personal information about them). To control its own data means to control the selection and use of personal information. Security here has the meaning of data security. Data security is the protection of data stored inside the WBAN or data being transferred outside of the WBAN from unauthorized users.

3.1 WBAN PRIVACY

Strict data access limitation only to authorized users is a main privacy aspect. HIPAA, the Health Insurance Portability and Accountability Act, is a US government initiative (1996) that specified mandatory privacy rules for the protection of personal health information. Data encryption and access control based on cryptography are required in order to ensure patient data privacy in WBANs.

3.2 WBAN SECURITY

Due to the critical role of patient-related data stored in a WBAN, data security becomes an important factor. WBANs incorporate and implement open and dynamic structures where patient data prone to be lost and prone to malicious modification. WBAN data security is characterized by the main aspects

- Secure data storage
- Fine grained distributed data access control

Each of these aspects carry on its own requirements which are listed and described below in Table 20. The data storage requirements are dependability, confidentiality, and dynamic integrity assurance. The data access requirements are access control, revocability, accountability, and non-repudiation. Some other WBAN security requirements are availability, and authentication.

Data storage Requirements	
Dependability	Data should be retrievable without difficulty even if node failure or data deletion happens.
Confidentiality	Confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes. During storage periods patient data should be kept confidential at a node or local server. Data confidentiality should be resilient to device compromise attacks.
Dynamic integrity assurance	It shouldn't be possible to modify patient data during storage periods by an illegal way. Data check and detection should perform by nodes dynamically.
Data access Requirements	
Access control	Unauthorized access to WBAN generated patient data should be prevented by the enforcement of a fine-grained data access policy.
Revocability	Compromised nodes or nodes with malicious behavior should lose their privileges in the WBAN.

Accountability	A user who abuses privileges should be identified and held accountable.
Non-repudiation	Original patient data cannot be denied by the source that generated it.
Some other requirements	
Availability	Patient data should be always available, even under denial-of-service (DoS) attacks.
Authentication	Authentication of the sender of the patient data and prevention of injection from outside the WBAN.

Table 20 Major security requirements for data security and privacy in WBANs

3.3 Differences between WBAN and WSN security requirements

Between the security requirements for WBANs and WSNs are a few differences. Compromised nodes in WBANs can be removed and replaced through human intervention, so it is not necessary to remove them through software as in WSNs. There is also a difference regarding the types of attack that can take place through a compromised node in WBANs and WSNs. Generally speaking, network routers trust their neighbors. But, if its neighbors lie, a router could be deceived about the proper route, and this can happen in WSNs. In WBANs it is not necessary to handle with strategies for routing attacks prevention due to the fact that the nodes have the hub in their communication range and their communication range is generally very limited. We also do not need strategies for prevention of attack propagation, because WBANs are small scale networks with nodes that are in communication range with each other. Common security requirements for WBANs and WSNs are confidentiality, message integrity, and node authentication [54].

3.4 Vulnerability of WBANs

In the area of computer security *vulnerability* is a weakness which allows the attacker to reduce a system's *information assurance*. Information assurance is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. As almost any network as well as the WBANs are vulnerable. Attacks against WBANs can be classified in three main categories [55]:

a. Attacks on network availability, so called Denial-of-Service (DoS) attacks
b. Attacks on secrecy and authentication
c. Attacks on service integrity

The next section analyzes the first attack category, the DoS attacks and countermeasures against them. Section 3.4.2 takes care about the second attack category, the attacks on secrecy and authentication.

3.4.1 Attacks on network availability (DoS attacks) and countermeasures

Table 21 shows different kinds of DoS attacks and their defense in the OSI layers physical, link, network, and transport layer.

OSI Layer	**DoS attack**	**Defense**
Transport layer	Flooding	Client Puzzles
	De-synchronization	Authentication
Network layer	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Authorization monitoring
	Black holes	Authorization, monitoring, redundancy
	Spoofed, Altered, or Replayed information attack	Link layer encryption, authentication, new path if retransmission
	Acknowledgment Spoofing attack	Use reliability mechanisms to choose the next hop
	Selecting Forwarding	Difficult to detect
	Sinkhole attack	Network monitoring, physical device monitoring
	Wormhole attack	Tight time synchronization, network monitoring, physical device monitoring
	Hello Flood attack	
	Sybil attack	Node identity verification, device resetting, regular changing of keys
Data Link layer	Collision	Error correcting code
	Unfairness	Small frames
	Exhaustion	Rate limitation
Physical layer	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proof, hiding

Table 21 DoS attacks in the OSI-layers transport, network, link, and physical

3.4.1.1 Transport layer attacks

The transport layer in a WBAN can be attacked through *Flooding* and *De-synchronization*.

3.4.1.1.1 Flooding

In *Flooding* an attacker or group of *zombies* (zombie is a compromised computer) attempts to exhaust server resources by setting up and tearing down TCP connections. The attacker initiates a request on every connection. The flooding attacks flood devices (e.g. inter- or Beyond-BAN communication servers) with a high rate of connections from a valid source. A type of flooding is SYN flooding. SYN flooding takes advantage of a flaw in how most hosts implement the *TCP three-way handshake*, this is the TCP connection establishment process. When host B receives the SYN request from A, it must keep track of the partially-opened connection in a “listen queue” for at least 75 seconds. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never

replying to the SYN/ACK responses of host B. The reply of host A is required for connection establishment. The victim's listen queue is quickly filled up. This ability of removing a host from the network for at least 75 seconds can be used as a denial-of-service attack. In a WBAN the personal device (PD) is a very attractive target for flooding. Making the PD unavailable in the network the attacker put the system out of action. A high-power resources PD with sufficient memory, and implemented security mechanisms is a good countermeasure against flooding.

3.4.1.1.2 De-synchronization

In *De-synchronization* the attacker fakes the *sequence number* in data packets between nodes and force the nodes to request the transmission of missing frames. The sequence number is set by the sender and it is used from the receiver to know if the sender is resending the previously transmitted data packet or if the message is a new data packet. The attacker forges some messages with wrong sequence numbers and causes infinite retransmissions, which result to needless energy consumption and bandwidth waste. The countermeasure regarding De-synchronization is authentication.

3.4.1.2 Network layer attacks

Inside a WBAN node does not route their packets. Routing is an issue if multiple WBANs communicate with each other through their coordinators and this is the reason why it is important to take care about network layer attacks countermeasures. We describe the most usual of them: The Spoofed, Altered, or Replayed information attack, the *Spoofing attack,* the *Selective Forwarding,* the *Sybil attack,* the H*ello Flood attack,* the S*inkhole attack,* and the *Wormhole attack.*

3.4.1.2.1 Spoofed, Altered or Replayed information attack

The S*poofed, Altered or Replayed information attack* is the most direct attack where the intruder alters the routing information and disrupt the network. The consequences of this attack is e.g. the creation of routing loops, extend or shorten source routes, repel or attract network traffic, false error message generation, network partition, replay attacks, and increased end-to-end latency. A countermeasure against spoofed, altered or replayed information attacks is the combination of link layer encryption and authentication. Another countermeasure is to use a new path if the failed message has to be retransmitted.

3.4.1.2.2 Acknowledgement Spoofing attack

In the *acknowledgement spoofing* attack (Figure 102) the attacker makes use of an acknowledgment packet and sending it to a node (A) to convince this node that another dead node (red node) is alive or a weak link is strong. All packets sent to a dead node or sent via a weak link are lost. The countermeasure is to use reliability mechanisms to choose the next hop.

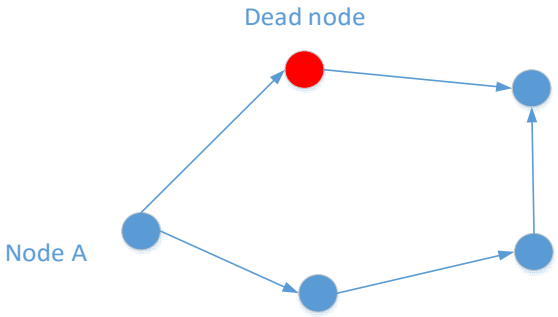


Figure 102 Acknowledgment spoofing attack

3.4.1.2.3 Selective Forwarding

In *Selective Forwarding* (Figure 103) the attacker node(s) choose a data flow path of interest and become part of the WBAN. The attacker nodes make a selection of the received packets, they drop some of them (e.g. packets of a specific source) and some other are forwarded reliable. This kind of attack is difficult to detect.

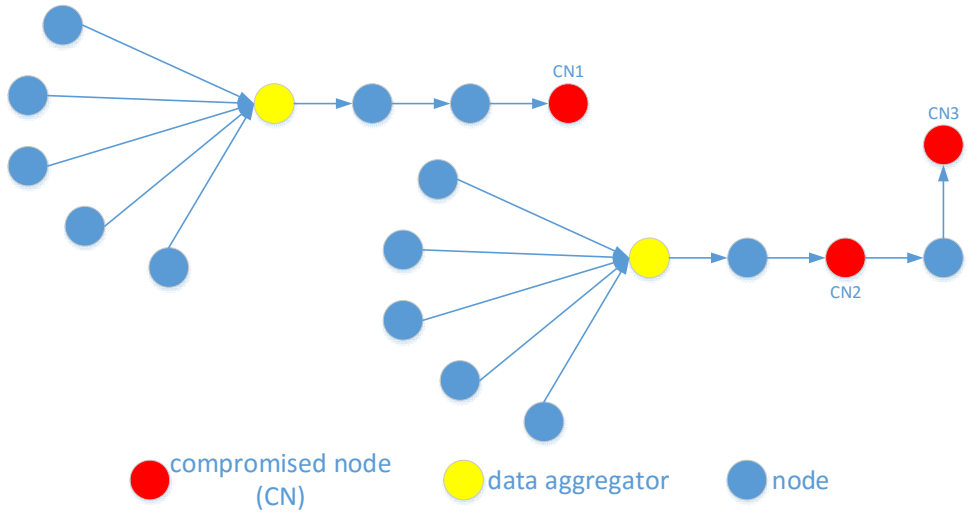


Figure 103 Selective Forwarding attack

3.4.1.2.4 Sinkhole attack

In a *Sinkhole attack* the attacker attracts traffic to a malicious part of the WBAN. After a node is compromised, it advertises low latency routes and it gives to its neighbor nodes the impression of packet routing. The neighbor nodes forward their packets to the compromised node, thus creating a sinkhole in the network. Since the routes advertised by the sinkhole attack are hard to detect, it is difficult to protect the WBAN against them. Network monitoring and physical device monitoring is a way to detect the Sinkhole attack.

3.4.1.2.5 Wormhole attack

In a *Wormhole attack* the attacker receives packets in a network point, forwards them with the help of a wireless or wired link that has less latency than the network links, and transmit the packets to another network point. Wormhole attacks use invisible channels and therefore it is difficult to defend against them. Tight time synchronization could be a defend strategy or network and physical device monitoring.

3.4.1.2.6 Sybil attack

The *Sybil attack* uses a compromised node to present multiple identities to the network and targets to confuse *geographic routing protocols*, since the intruder appears to be in more than one locations at once. A *geographic routing protocol* is mainly proposed for wireless networks, it relies on geographic position information, and based on the idea that the source sends a message to the geographic location of the destination instead of using the network address. Node identity verification is the countermeasure against the Sybil attack. Prevention can also be done by regular changing of keys, and device resetting.

3.4.1.2.7 Homing attack

Nodes with special responsibilities like the hub attract intruders interest because they provide critical services to the WBAN. Location based protocols that rely on geographic routing expose the network to the *homing attack.* A passive traffic observer (intruder) learns location and presence of critical resources. Once found, the nodes can be attacked. A countermeasure against the Homing attack is confidentiality for message headers and message content. Sharing cryptographic keys between all neighbors enables the network to encrypt the headers at each hop and prevents traffic observation.

3.4.1.2.8 Black holes

In a *Black hole attack* a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination. After receiving the packets, the malicious node drops them without transmit them to their destination. The countermeasure against the Black hole attack uses geographic routing, and takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect the attacks.

3.4.1.2.9 Misdirection

This DoS attack targets the sender. In *Misdirection* messages are forwarded along wrong paths. The network traffic is diverting away from its intended destination.

3.4.1.2.10 Neglect and greed

A *neglectful node* (malicious node) is a node that may even acknowledge data receipt to the sender, but it drops messages on an arbitrary basis. If the node also gives unnecessary priority to its own packets, it is also *greedy*. Use of multiple routing paths and the transfer of redundant messages are countermeasures against this attack.

3.4.1.2.11 Hello Flood attack

The “hello-packet” broadcasting is a requirement for many protocols to nodes. Nodes announce in this way themselves to their neighbors. After getting the hello-packet the receiver node assumes that the

transmitter node is its neighbor. There cases where this assumption is wrong. This happens in the case of the *hello flood attacks*. The attacker uses a high-powered antenna to gain the confidence of the WBAN nodes that it is member of their neighborhood. The attacker then can establish a high quality route. This is a method to create a wormhole (4.4.2.5). The wormhole has not any implications to the intra-BAN communications of the WBAN. But the Hello Flood attack in intra-BAN communications provoke body nodes to reply to the hello packets, this is needless power consumption.

3.4.1.3 Data Link layer attacks

Data Link layer security countermeasures protect the WBAN against the outsider attacks. The most usual outsider attacks against WBANs are the *collision attack*, the *unfairness attack*, and the *exhaustion attack*.

3.4.1.3.1 Collision attack

By the *Collision* attack the attacker listens to the channel. After the detection of the start of a message, the attacker sends out its own message interfering in this way the original message. This can lead to a corruption of the frame header and to the rejection of the transmitted data packet. A collision attack is difficult to detect due to the fact that the only thing we know is the receipt of wrong messages. The likelihood of a successful collision attack in a WBAN is high and error correction is an important countermeasure.

3.4.1.3.2 Unfairness attack

The *Unfairness attack* degrades the service (network performance) through interruption of the MAC priority schemes. Normally in a WBAN every node has the same priority to get the common channel. The rule here is that the first node that tries, gets hold of the channel. All other nodes have then to wait for a random length of time and after this random time period they try again to transmit their packets. This rule guarantees the fairly channel access of the nodes. Unfairness attackers could utilize these network characteristic to attack the WBAN. They transmit their packets without waiting or just waiting for a very short time and prevent normal nodes to transmit their data packets. A countermeasure is to prevent the channel from being captured for long time periods using small time frames, so the channel is captured for a small amount of time. The attacker however can swindle through quick responds when needing access.

3.4.1.3.3 Exhaustion attack

By the *Exhaustion attack* a self-sacrificing node keeps always the channel busy, exhausting in this way the battery resources. In the normal case a sender node transmits first a control packet to start its transmission. The receiver has to acknowledge this invitation sending also a control packet if it is available. The receiver cannot distinguish if the sender node is a normal node or an attacker node. So if the attacker node transmits control packets repeatedly, they force the receiver to acknowledge them without a break. Rate limitation is used as defense against this attack.

3.4.1.4 Physical layer attacks

Essentially, there are two types of physical layer attacks, Jamming and Tampering.

3.4.1.4.1 Jamming attack

Jamming is a well-known attack on wireless communications. Jamming interferes with the radio frequencies used by the nodes. It works by denying service to the nodes as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. An attacker with the right tools can easily jam the 2.4 GHz frequency. The signal is dropped to a level where the WBAN can no longer function. A WBAN consisting of *N* nodes can be put out of service with *k* randomly distributed jamming nodes, where $k << N$. The attack is simple and effective especially by single-frequency networks. Even sporadic jamming can provoke interference. Countermeasures against jamming include switching to a lower duty cycle and conserving as much power as possible. The nodes should wake up periodically to check up whether the jamming is over. Conserving the energy resources, the nodes may be able to outlive an intruder, who consumes a high amount of energy due to jamming at greater expense.

3.4.1.4.2 Tampering attack

In the *tampering attack* the nodes are physically tampered. The attacker replaces the node or a part of its hardware, or may damage one or more nodes. Tampering is also if the attacker accesses patient's information through electronic interrogation or if the attacker shares cryptographic keys. Nodes prone to physical tampering due to their limited external security features. The advantage of WBANs regarding tampering attacks is that the nodes are under surveillance of the patient or the WBAN-user. It is not easy for an attacker in any manner to damage or access the nodes without being detected. Patient or WBAN-user awareness is the best countermeasure against this attack. WBAN users should be advised that only authorized people should be allowed to have access to the WBAN.

3.4.2 Attacks on secrecy and authentication and countermeasures

The same as in traditional networks WBANs and WBAN applications need protection against *injection*, modification of packets and *eavesdropping*.

Electronic Eavesdropping, is the act of electronically intercepting conversations without the knowledge of at least one of the participants. WBANs use the open features of the wireless channel. An attacker can intercept in an easy way the radio communications between the wireless nodes and steal the health data. Attackers can also find the location of the patients using eavesdropping, a quiet life threatening situation.

In this section we describe some usual solutions against attacks on secrecy and authentication: *TinySec*, *Hardware encryption*, *Elliptic Curve Cryptography*, *Identity-based encryption*, and *Biometrics*.

3.4.2.1 TinySec

TinySec is a security architecture for wireless sensor networks and was developed as a first try to add security to the TinyOS suite, an open source software component-based operating system for wireless sensor networks. TinySec implements encryption and authentication and applies to the link layer of wireless sensor networks. It makes use of RC5 and Skipjack block ciphers in cipher block chaining (CBC) operation mode and has low overhead. Using Tinysec we have for the authentication process an increase of 3% of the packet power consumption. We have also an increase of only 10% of packet power consumption for the encryption process. TinySec uses a group key (software-based symmetric keying) shared among nodes network-wide, cluster-wide and pair-wise for the encryption of data packets. The generated packets are secure. TinySec calculates a *Message Authentication Code* (MAC) for the complete packet (incl. the MAC header). A message authentication code can be considered as a cryptographically secure checksum of a message and builds a common solution to achieve message

authenticity and integrity [56]. TinySec relies on a single key that provides only a baseline security level. TinySec cannot be used to protect against node capture attacks. If an intruder learns the key or compromises a node, he can have access on the complete network information. In the same case the intruder can inject his own packets, a really weak issue in TinySec, may be the weakest.

3.4.2.2 Hardware encryption

In contrast to TinySec which implements a software encryption, ZigBee established a successful hardware-based symmetric keying. The hardware encryption achieved through the use of the ChipCon 2420 ZigBee compliant RF transceiver. The CC2420 is a true single-chip 2.4 GHz (unlicensed ISM band) RF transceiver designed for low-power low-cost robust wireless applications. CC2420 provides inter alia data encryption and data authentication. It executes IEEE 802.15.4 security operations with AES encryption utilizing 128-bit keys. The disadvantage of the hardware encryption is the dependence on the specific sensor node platform because there are sensor nodes that they do not offer hardware encryption support.

3.4.2.3 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a practicable alternative for the public key cryptography in wireless sensor networks. The advantages of elliptic curve cryptography that they make it an alternative for public key cryptography are small key size, compact signatures, and comparatively fast computation. There are several different implementations of ECC, but ECC is not the top choice for WBANs. ECC implementations consume more energy than symmetric systems. A proposed solution for this problem is to use both ECC and symmetric systems. A possibility can be to use ECC only for infrequent and security-sensitive operations. Such operations are for example code updates or key establishment by the initial network setup.

3.4.2.4 Identity-Based Encryption

Identity-based encryption (IBE) is a type of public-key encryption where the user public key is a unique information about the identity of the user (e.g. the email address of the user). The sender can encrypt a message using for example the email address as a key. The receiver gets its decryption key from a trusted central authority. IDKEYMAN [57], an Identity-based key management scheme is one of the Identity-based encryption proposals for WBANs. IDKEYMAN uses IBE to set up pair-wise symmetric keys achieving data confidentiality and integrity. IDKEYMAN is designed for a publisher-subscriber architecture and it is only used to exchange pairwise symmetric keys between publisher and subscriber. Computational overhead on the publisher side can be reduced through the use of symmetric keys in all communications after the setup. The benefits using IDKEYMAN that uses IBE in the bootstrapping phase are

- Minimization of energy consumption
- The advantages of the security strength of public key

3.4.2.5 Biometrics

Biometrics is a mechanism in the key establishment and the authentication of body sensor nodes. It uses the measurement of physiological body characteristics as an important parameter in a symmetric key management system. The most appropriate physiological signals can be used for biometrics are the ECG (electrocardiogram), and the interpulse interval (timing information of heart beats). These

signals offer proper time variance and randomness. A biometric physiological value should have the following characteristics to be useful:

- It should be universal, available by most patients
- It should be easily measured and collected
- It should be distinctive, different in any two patients
- It should be effective, implementing a secure biometric system
- It should be difficult to compromise and difficult to guess
- It should be acceptable by the public

Actually there exist low cost sensor devices implemented for medical applications which can trace biometric physiological signals. This means that in future WBANs the implementation of a biometric based system wouldn't be an additional system requirement.

3.4.3 Attacks on service integrity

In the attacks against the service integrity the intruder changes the WBAN data before the data reaches the PS. The intruder forces the network to accept the false data value. The PS receives manipulated data and this leads usual to a disaster.

3.5 MAC Sublayer Security specifications in WBANs

In this section we will give an overview of the existing MAC Sublayer security specifications for IEEE 802.15.1, Bluetooth LE, IEEE 802.15.4, ZigBee, IEEE 802.15.4a, and IEEE 802.15.6. The ETSI SmartBAN MAC Sublayer security specification is not finished yet.

3.5.1 IEEE 802.15.1

For the protection of the nodes from attacks Bluetooth uses authentication, built-in encryption, and frequency hopping. The Bluetooth frequency hopping schemes operate with 1600 hops/sec and implement an automatic output power adaption bringing the range to the minimum necessary. A disadvantage of the Bluetooth security is that the *E0* 128-bit key length stream cipher can be attacked through a divide-and-conquer type attack. *E0* is a stream cipher that combines the data with a generated sequence of pseudorandom numbers using XOR. The key length is normally 128 bit but it may vary. Some problems cause also the use of Personal Identification Number codes during the generation encryption keys and link keys due to the fact that the keys can be guessed (four digits long keys). Bluetooth hasn't a key management protocol. This results to problems with the generation and distribution of the PINs and eventually to network security problems.

3.5.2 Bluetooth LE

Devices for BT LE are low-power devices and they have low computation capabilities. This circumstance undermine the privacy of the data transmitted using BT LE. According to the Bluetooth developer portal [58] BL LE is always secure and protected due to the Bluetooth Core Specification that provides features for encryption, data integrity, and privacy of the user's data. [59] demonstrates how somebody can perform eavesdropping on a BT LE device, intercept and reassemble packets on a BT LE wireless network, and breaking the encryption of BL LE. [59] also provides a sniffer to follow connections. This reduces significantly the confidence to BT LE protocol, especially for WBANs where the protection of patient data is a major issue.

3.5.3 IEEE 802.15.4

In IEEE 802.15.4 the MAC sublayer is responsible for the security (macSecurityEnabled attribute is set to TRUE). It provides security services on specified incoming and outgoing frames when higher layers request to do so. IEEE 802.15.4 supports:

- Data confidentiality
- Data authenticity
- Replay protection

The implementation of security through a device is optional. Devices that implement security support a mechanism for the MAC sublayer to provide cryptographic transformations on incoming and outcoming frames.

Regarding the four packet types acknowledgement, beacon, data, and control only the first one cannot include security information. For the other three packet types security information like integrity protection or confidentiality protection can be integrated whenever required. There exist different security levels which can be implemented. Every security level is controlled by a specific security suite. IEEE 802.15.4 specifies eight different security suites with different security properties, protection levels, and frame formats. An application has a choice of security suites and selects through the selected security suite the type of security protection.

Table 22 lists the different security suites defined.

Name	Description	Access control	Confiden-tiality	Frame integrity	Sequential Freshness
Null	No security				
AES-CTR	Encryption only, CTR mode	X	X		X
AES-CBC-MAC-128	128-bit MAC	X		X	
AES-CBC-MAC-64	64-bit MAC	X		X	
AES-CBC-MAC-32	32-bit MAC	X		X	
AES-CCM-128	Encryption & 128-bit MAC	X	X	X	X
AES-CCM-64	Encryption & 64-bit MAC	X	X	X	X
AES-CCM-32	Encryption & 32-bit MAC	X	X	X	X

Table 22 Security modes in IEEE 802.15.4

This classification includes the mode null (no encryption), the mode encryption only (AES-CTR), the mode authentication only (AES-CBC-MAC), and the mode encryption together with authentication (AES-CCM). In AES-CTR, confidentiality protection is implemented using Advance Encryption Standard (AES) block cypher with counter mode. The MAC can be 16, 8, or 4 bytes long. The longer the MAC the lower the possibility for a possible intruder to guess the MAC. Each suite that includes encryption, allows to the recipient to optionally enable replay protection. The standard requires that radio chips implement the Null suite and the AES-CCM-64 suite. The IEEE 802.15.4 security architecture is sound.

It consists of many well designed security features. Despite some included pitfalls a proper use of the security API leads to secure applications [60].

3.5.4 ZigBee Security Services

In addition to the specified security functionality and services of IEEE 802.15.4 ZigBee which is built upon IEEE 802.15.4 defines additional security services. The additional services offered by ZigBee include processes for key exchange and authentication. The ZigBee standard specifies a trust-center. The ZigBee hub carries the trust-center functionality. The following roles are taking over:

- Trust manager: The trust manager controls the authentication process if nodes request to join the WBAN
- Network manager: The network manager maintains and distributes the key
- Configuration manager: The configuration manager ensures end-to-end security

3.5.5 IEEE 802.15.4a

IEEE 802.15.4a is the first international standard that specifies a PHY for precision ranging. The precision ranging is specified for the IR-UWB option of IEEE 802.15.4a. Ranging capable devices (RDEVs) in IEEE 802.15.4a are responsible for the optional ranging support. A RFRAME is the ranging frame and it can be set using a ranging bit in the PHY header of the packet. A range between two RDEVs is calculated via two-way RFRAME exchange and tracking its arrival time which is $2T_2 + T_1$ (Figure 104).

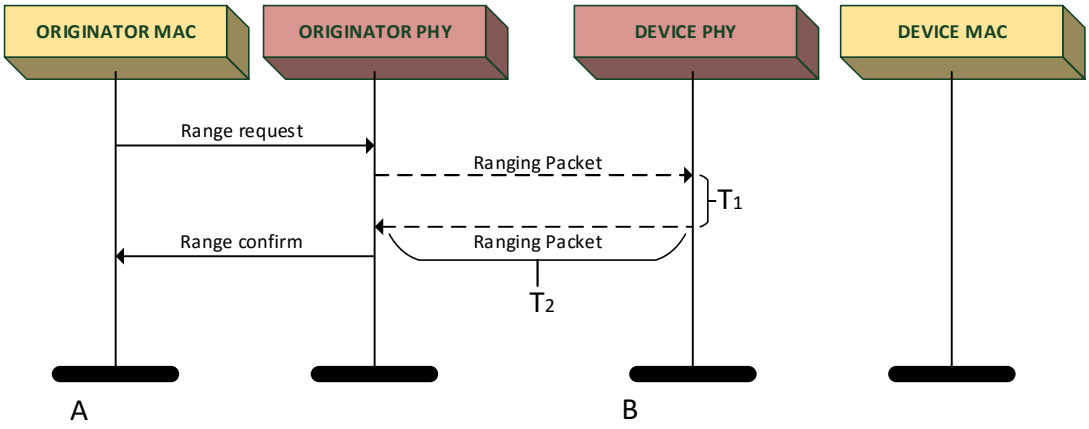


Figure 104 Message exchanges in two-way time of arrival based ranging

The range information is in security-related sensor applications a critical parameter. Unfortunately, the range information provided by the standard IEEE 802.15.4a can be subject of attacks. Different attacks are possible, such as *Snooper attacks*, *Impostor attacks*, and *Jamming attacks*.

- In a *Snooper attack* an antagonistic device listens to ranging exchanges, and attempts to find out positions of the RDEVs
- In an *Impostor attack* an antagonistic device send a RFRAME for originating, and target the RDEVs in such a way to confuse their acquisition timing
- *Jamming attack:* During the transmission of RFRAMEs an antagonistic device jams to entirely injure acquisition and ranging

In order to guarantee the integrity of the range information and ranging traffic, and in order to countermeasure such attacks, the IEEE 802.15.4a standard defines a *private ranging* mode. The private

ranging mode uses dedicated longer preambles that guarantee higher security. The nodes use a secure protocol to exchange the sequences that they are going to be used in the next ranging cycle. Impostor attacks can be prevented in this way and snooper attacks become more difficult because a snooper now must hark to eight different waveforms. The private ranging is implemented through two operation phases, authentication and ranging [61].

3.5.6 IEEE 802.15.6

IEEE 802.15.6 offers three security levels for nodes and hubs. Each of these levels has its own frame format, protection level, and properties. The IEEE 802.15.6 security model is derived from the IEEE 802.15.4 security model.

The three security levels are

- Level 0 – Unsecured communication
- Level 1 - Authentication but not encryption
- Level 2 - Authentication and encryption

Level 0

The transmission of messages happens in unsecured frames. Unsecured frames do not provide message authenticity, replay defense, integrity validation, confidentiality, and privacy protection.

Level 1

The transmitted frames in Level 1 are secured authenticated but not encrypted. Level 1 security provides message authenticity, replay defense, and integrity validation but not confidentiality, and privacy protection.

Level 2

The transmitted frames are secured authenticated and encrypted. Level 2 security provides message authenticity, replay defense, integrity validation, confidentiality, and privacy protection. The data is transmitted in secured authentication and encryption frames. The selection of the security level takes place when a node is joining the WBAN. A pre-shared Master Key (MK) is activated in the case of unicast communication and a Pairwise Temporal Key (PTK) is used once per session. In the case of multicast communication an established Group Temporal Key (GTK) is shared with the group of receivers (multicast group). The security structure of IEEE 802.15.6 is given in Figure 105.

The Authentication relies on:

- Diffie-Helman key exchange procedures
- Techniques:
    - no pre-shared secret
    - pre-shared secret (password or master key)
    - built secret (public key hidden or display)

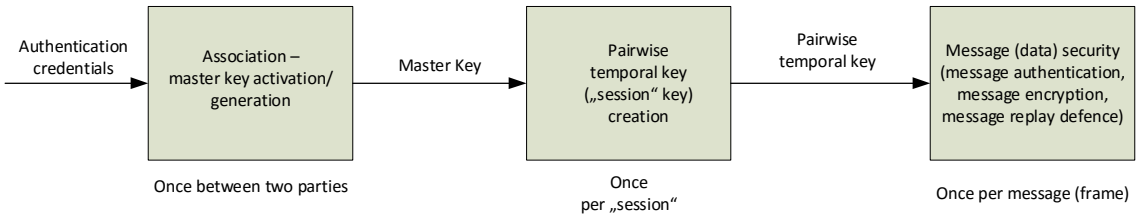


Figure 105 Security structure of IEEE 802.15.6

3.5.7 Cognitive radio for an ultra-wideband MBAN

One attractive characteristic of UWB technology for MBANs is the inherent noise-like behavior due to their extremely low maximum *effective isotropically radiated power (EIRP)* spectral density of -41.3 dBm/MHz. E*ffective isotropically radiated power (EIRP)* is the amount of power that a theoretical isotropic antenna (which evenly distributes power in all directions) would emit to produce the peak power density observed in the direction of maximum antenna gain. EIRP take into account the losses in transmission line and connectors and includes the gain of the antenna. The EIRP is often stated in terms of decibels over a reference power emitted by an isotropic radiator with an equivalent signal strength. The EIRP allows comparisons between different emitters regardless of type, size or form. From the EIRP, and with knowledge of a real antenna's gain, it is possible to calculate real power and field strength values.

$$EIRP\ |_{log} = P_T - L_C + G_a$$

where EIRP and P_T (output power of transmitter) are in dBm, cable losses (L_C) is in dB, and antenna gain (G_a) is expressed in dBi, relative to a (theoretical) isotropic reference antenna [62].

The inherent noise-like behavior of UWB makes it difficult to detect. Robustness against jamming, and no need for complex encryption algorithms in low-cost transceivers are two benefits resulting from this behavior. On the other side nodes in CR networks carry out cognitive actions like sensing, adapting, and learning. These cognitive actions may be subject to attacks. Typical characteristics of CRBANs, e.g. severe resource constraints, represent additional challenges for security and privacy.

3.6 Security Challenges and Future Research Topics

Security, efficiency, and practicality are important elements in WBANs, well we consider them as a unit.

A challenge in the area of WBAN security is the balance between *security and efficiency*. High efficiency in WBANs is necessary to achieve security, both for the WBAN applications as well as for the hardware resources due to their constraints. The computation and storage capabilities of WBANs are limited because of the small size of the nodes and their restricted power supply. For these reasons the cryptographic characteristics of WBANs should be as lightweight as possible regarding computation and storage overhead.

The patient safety makes necessary that the WBAN data can be accessed whenever needed. Inflexible data access could be dangerous for a patient, especially if the patient is unable to respond or in emergency scenarios. On the other side a laxly access control scheme is an opportunity for intruders,

security suffers. It is really a challenge to achieve strong data security and at the same time to allow flexible access, it is difficult to balance *security and safety*.

The WBAN devices should be easy to use (usability) and foolproof because the users are not experts but rather patients. As the setup of the data security mechanisms is patient-related, the human interactions with the whole WBAN, should be only a few and intuitive, balancing in this way *security and usability*.

Device interoperability is also a challenge for WBANs. If nodes from different manufacturers are in use it is difficult to introduce data security mechanisms with common settings and operation with all WBAN devices.

The increased use of WBANs in the health sector and in the industry results to more attacks from criminals and this can be a driver for the development of the WBAN security technology. Future research topics in the area of WBAN security are:

1. The use of private key operations. Recent public key cryptography studies have shown that public key operations may be practical in sensor nodes. However, the realization of private key operations in sensor nodes is very expensive and the issue here is to improve efficiency.
2. QoS and security. The addition of security services in a WBAN degrades its performance, and finally its QoS. Current studies regarding WBAN security focus on specific topics such intrusion detection, key management, or secure routing and ignore QoS. QoS and security services need to be handled together in WBANs.
3. Cloud computing integration. The use of WBAN technology for ubiquitous healthcare can change our everyday life. Humongous data need to be efficient processed and stored. The coming of cloud computing technology integration in WBANs is also a security challenge.

4 SUMMARY

A WBAN is expected to be a very important technology, a technology that can save lives through continuous monitoring and early detection of problems.

In the first part of this work we introduced the WBAN technology, we list the WBAN applications and their requirements. After that we introduced the MAC functionality and services, the multiple access techniques are in use, and we presented the existing standards for the MAC sublayer protocol for WBANs in a detailed and appropriate way for a Master Thesis. MAC sublayer standards as IEEE 802.15.4, IEEE 802.15.6, and SmartBAN were described in detail. Afterwards we considered more than thirty implementations of the standards including implementations that belong to the group of proprietary wireless technologies (e.g. RuBee). And last but not least we compared the existing MAC sublayer standards focusing on their main characteristics. The first part ends with a presentation of the MAC sublayer challenges.

There are many exciting perspectives for the further development of the WBAN technology in the MAC sublayer to profit from the potential of ubiquitous healthcare, and other application areas like military, defense, sport, entertainment, biofeedback, and parameter monitoring.

In the second part of the Master thesis we introduced WBAN privacy and security and we presented eighteen different vulnerabilities, the most usual for WBANs. For the standards presented in the first part of my work, we described the corresponding MAC sublayer security specifications. Also the second part of the work ends with a section mentioned on the WBAN security challenges.

In our days where network attacks are every day phenomenon, security is a fundamental feature for their deployment. In every deployed WBAN security and privacy requirements must be satisfied. Security approaches coming from other network types are not applicable to WBANs. Security solutions in WBANs should be lightweight and inexpensive in term of resource consumption. The research in this very interesting area is in its infancy and there is a lot of work to be done.

5 BIBLIOGRAPHY

1. [Online] https://en.wikipedia.org/wiki/Octet_(computing).

2. [Online] https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Gesundheit/Gesundheitsausgaben/Gesundheitsausgaben.html.

3. *IEEE Standard for Local and metropolitan area networks — Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).* 2011.

4. **Riccardo Cavallari, Flavia Martelli, Ramona Rosini, Chiara Buratti, Roberto Verdone.** A Survey on Wireless Body Area Networks: Technologies and Design Challenges. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS.* 2014, Vol. 16, NO. 3.

5. [Online] http://www.maximintegrated.com/en/app-notes/index.mvp/id/5259.

6. [Online] https://en.wikipedia.org/wiki/Specific_absorption_rate.

7. [Online] https://en.wikipedia.org/wiki/Nyquist_rate.

8. [Online] https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439.

9. [Online] https://en.wikipedia.org/wiki/IEEE_802.15.4.

10. **Pei Huang, Li Xiao, Soroor Soltani, Matt W. Mutka, Ning Xi.** The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey. 2013, Vol. 15, NO. 1.

11. **Jamil. Y. Khan, Mehmet R. Yuce.** *New Developments in Biomedical Engineering.* s.l. : InTech, 2010. pp. 612-614. ISBN 978-953-7619-57-2.

12. [Online] https://en.wikipedia.org/wiki/Contention_(telecommunications).

13. [Online] www.zigbee.org.

14. **Thotahewa, Kasun Maduranga Silva, Redouté, Jean-Michel, Yuce, Mehmet Rasit.** *Ultra Wideband Wireless Body Area Networks.* Switzerland : Springer International Publishing, 2014. 978-3-319-05287-8_2.

15. *IEEE Std 802.15.6-2012, IEEE Standard for Local and metropolitan area networks—Part 15.6: Wireless Body Area Networks.* 2012.

16. [Online] http://wwwiaim.ira.uka.de/Teaching/VorlesungRobotikIII/Pdf-Files/2SW_InterneSensoren.pdf.

17. **Yang, Guang-Zhong.** *Body Sensor Networks.* s.l. : Springer, 2014. ISBN 978-1-4471-6373-2.

18. [Online] http://www.businessdictionary.com/definition/actuator.html#ixzz3ejWibXo0.

19. [Online] https://standards.ieee.org/develop/regauth/tut/eui48.pdf.

20. [Online] https://en.wikipedia.org/wiki/Short_Interframe_Space.

21. [Online] https://en.wikipedia.org/wiki/Jitter.

22. [Online] https://en.wikipedia.org/wiki/Latency_(engineering).

23. *Lecture in Wireless and Satellite Networks.* **Efstathiou, Dimitrios.** Informatics Department, TEI of Central Macedonia, Serres, Greece : s.n., 2015.

24. [Online] http://searchnetworking.techtarget.com/definition/cognitive-radio.

25. **Carles Anton-Haro, Mischa Dohler.** *Machine-to-Machine (M2M) Communications Architecture, Performance and Applications.* s.l. : Woodhead Publishing, 2015. 978-1782421023.

26. **Sabin Bhandari, Sangman Moh.** A Survey of MAC Protocols for Cognitive Radio Body Area Networks. *Sensors.* 2015, Vol. 15, pp. 9189-9209.

27. **RAÚL CHÁVEZ-SANTIAGO, KEITH E. NOLAN, OLIVER HOLLAND, LUCA DE NARDIS, JOÃO M. FERRO, NORBERTO BARROCA, LUÍS M. BORGES, FERNANDO J. VELEZ, VÂNIA GONÇALVES AND ILANGKO BALASINGHAM.** COGNITIVE RADIO FOR MEDICAL BODY AREA NETWORKS USING ULTRA WIDEBAND. *IEEE Wireless Communications.* August 2012, 2012, Vols. 1536-1284/12.

28. *High Rate Ultra Wideband PHY and MAC Standard.* s.l. : ecma International, 2008. 3rd Edition.

29. **Moe Z. Win, Robert A. Scholtz.** Impulse Radio: How it works. *IEEE COMMUNICATIONS LETTERS.* 1998, Vols. Vol. 2, No. 1, January 1998.

30. [Online] http://www.ecma-international.org/memento/index.html.

31. [Online] http://www.radio-electronics.com/info/wireless/uwb/mb-ofdm-uwb.php.

32. **European Telecommunications Standards Institute.** ETSI TS 103 325 V1.1.1 (2015-04) Technical Specification Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN. 2015.

33. **Sergio Gonza´lez-Valenzuela, Xuedong Liang, Huasong Cao, Min Chen, Victor C.M. Leung.** Body Area Networks. *Autonomous Sensor Networks: Collective Sensing Strategies for Analytical Purposes.* s.l. : Springer-Verlag Berlin Heidelberg, 2013.

34. *A Comprehensive Survey of MAC Protocols for Wireless Body Area Networks.* **A. Rahim, N. Javaid, M. Aslam, Z. Rahman, U. Qasim, Z. A. Khan.** s.l. : Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, 2012.

35. **Sana Ullah, Bin Shen, S.M.Riazul Islam, Pervez Khan, Shahnaz Saleem, Kyung Sup Kwak.** A Study of Medium Access Control Protocols for Wireless Body Area Networks. *Sensors.* 2010, Vol. 10, No. 1, pp. 128-145.

36. **Holger Karl, Andreas Willig.** *Protocols and Architectures for Wireless Sensor Networks.* s.l. : WILEY, 2007.

37. **Younis, O., Fahmy, Sonia.** HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on Mobile Computing.* 2004, Vol. 3, 4.

38. **Joseph Polastre, Jason Hill, David Culler.** Versatile Low Power Media Access for Wireless Sensor Networks. *ACM SenSys.* November 3-5, 2004.

39. **C. Schurgers, V. Tsiatsis, S. Ganeriwal, M. Srivastava.** Optimizing Sensor Networks in the Energy-Latency-Density Design Space. *IEEE Transactions on Mobile Computing.* 2002.

40. *PMAC: an adaptive energy-efficient MAC protocol for wireless sensor networks.* **T. Zheng, S. Radhakrishnan, V. Sarangan.** Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International : s.n.

41. **Zhang, Y., Huang Q.** *Coordinated convergecast in wireless sensor networks.* Atlantic City, NJ, USA : IEEE Military Communications Conference, 2005.

42. *An Adaptive Energy-Efficient and Low-Latency MAC for Data Gathering in Sensor Networks.* **G. Lu, B. Krishnamachari, C. Raghavendra.** Int. Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN) : s.n., 2004. 0-7695-2132-0.

43. **Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, Victor C. M. Leung.** Body Area Networks: A Survey. *Mobile Networks & Applications.* Springer, 2011, Vol. 16, 2.

44. [Online] http://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4676.

45. [Online] http://www.lockheedmartin.com/us/news/press-releases/2014/february/isgs-asset-tracker-0219.html.

46. [Online] http://www.designfax.net/cms/dfx/opens/article-view-dfx.php?nid=4&bid=499&et=news&pn=01.

47. [Online] http://www.ru-bee.com/page13/page24/.

48. **ITU-T.** *G.9959 (02/2012).* 2012.

49. **Thotahewa, Kasun Maduranga Silva, Redouté, Jean-Michel, Yuce, Mehmet Rasit.** *Ultra Wideband Wireless Body Area Networks.* Switzerland : Springer International Publishing, 2014. pp. 25-26. 978-3-319-05287-8_2.

50. **Raja Jurdak, Pierre Baldi, Cristina Videira Lopes.** U-MAC: a proactive and adaptive UWB medium access control protocol. *WIRELESS COMMUNICATIONS AND MOBILE COMPUTING.* 2005, Vol. 5, pp. 551-566.

51. **O. Omeni, A. C. W. Wong, A. J. Burdett, and C. Toumazou.** Energy efficient medium access protocol for wireless medical body area sensor networks. *IEEE Transactions on Biomedical Circuits and Systems.* 2008, Vol. 2, 4, pp. 251-259.

52. [Online] https://en.wikipedia.org/wiki/List_of_wireless_sensor_nodes.

53. **Kiriakos Gavouchidis, Dimitrios Efstathiou.** OVERVIEW OF MEDIUM ACCESS CONTROL (MAC) LAYER STANDARDS FOR WIRELESS BODY AREA NETWORKS (WBANS). *To be published.* 2016.

54. **Sungyoung Lee et. al.** [Online] http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3274185/.

55. **Elaine Shi, Adrian Perrig.** Designing secure sensor networks. *IEEE Wireless Communications.* 2004, Vol. 11, pp. 38-43.

56. **Chris Karlof, Naveen Sastry, David Wagner.** TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. [ed.] ACM. *SenSys.* Second ACM Conference on Embedded Networked Sensor Systems, November 2004, pp. 162-175.

57. **S. Sankaran, et al.** IDKEYMAN:An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Networks. [ed.] Albany. *The 5th Annual Symposium on Information Assurance (ASIA'09).* 2009.

58. [Online] https://developer.bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx.

59. **Ryan, Mike.** *Bluetooth: With Low Energy comes Low Security.* s.l. : iSEC Partners, 2013.

60. *Security Considerations for IEEE 802.15.4 Networks.* **Naveen Sastry, David Wagner.** Philadelphia, Pennsylvania, USA : ACM, October 1, 2004. 158113925X/04/0010.

61. *Ranging in the IEEE 802.15.4a Standard.* **Zafer Sahinoglu, Sinan Gezici.** 2006. IEEE Wireless and Microwave Technology Conference (WAMICON).

62. [Online] https://en.wikipedia.org/wiki/Equivalent_isotropically_radiated_power.