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

Master Thesis

Kiriakos Gavouchidis

Supervisor: Dr. Dimitrios Efstathiou

Overview

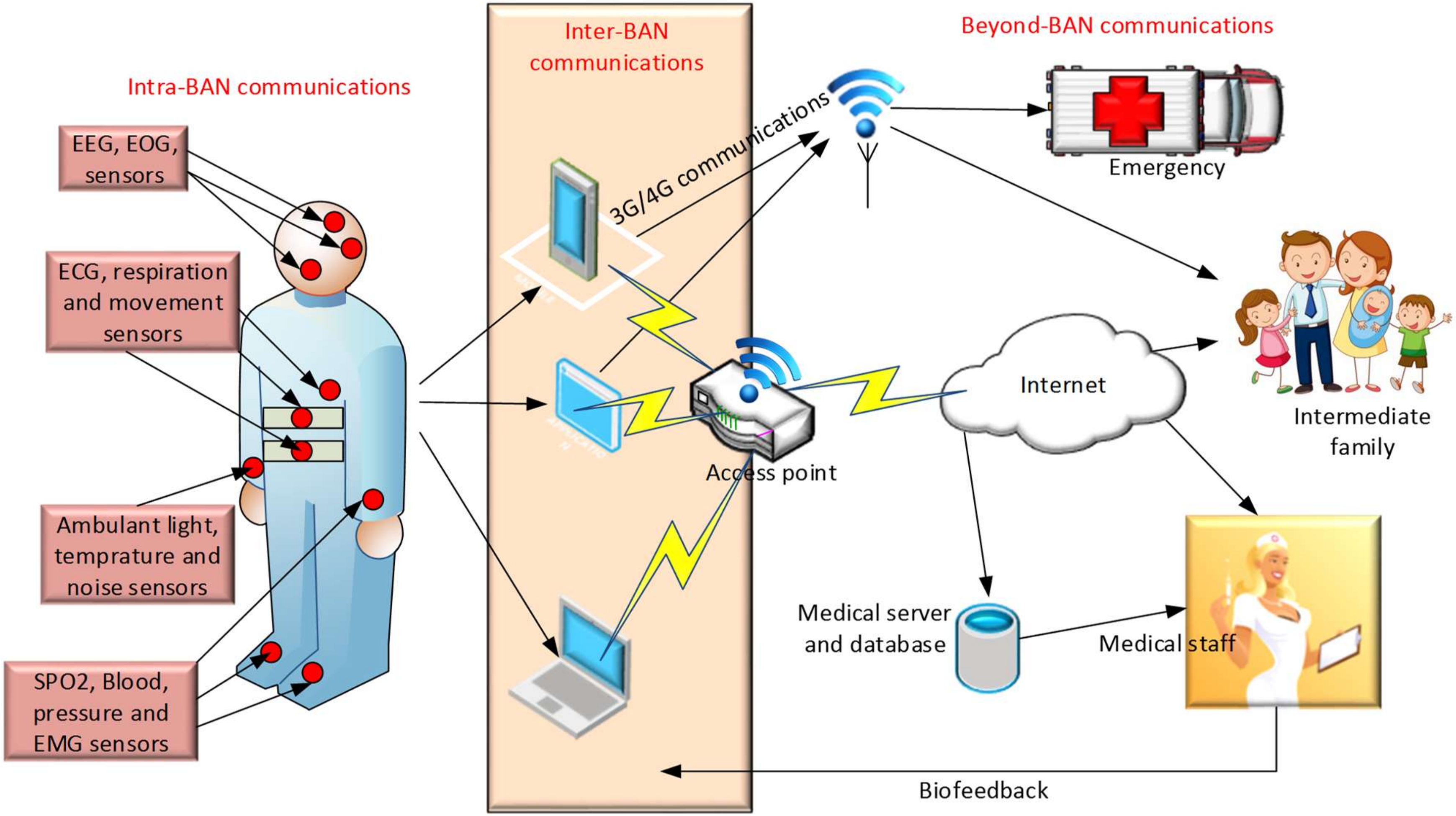
- Wireless Body Area Networks (WBANs)
- Medium Access Control (MAC) Standards for WBANs
  - MAC functionality in a WBAN
  - Multiple Access Techniques used in WBANs
  - The MAC protocol in IEEE 802.15.4, 4a, 4j, IEEE 802.15.6, and SmartBAN
  - Comparison of the standards
- WBAN Security

Goals of the Master Thesis

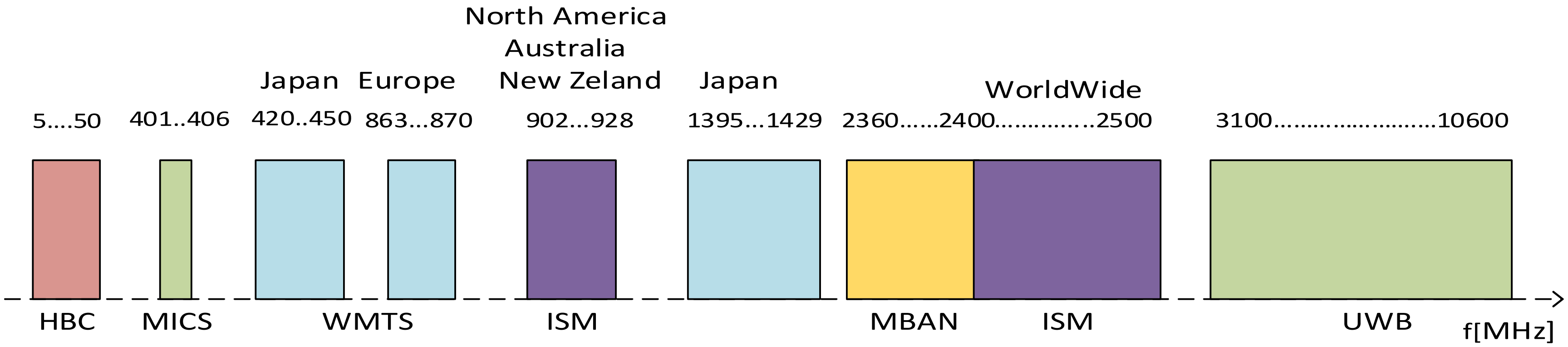
- Overview of the WBAN technology
- The main characteristics of MAC
- Evolution of the MAC standards
- Comparison
- Existing implementations
- Challenges in security of WBANs

Overview of the WBAN technology

- Wireless Body Area Network


Intra-BAN communications
Inter-BAN communications
Beyond-BAN communications
EEG, EOG, sensors
ECG, respiration and movement sensors
Ambulant light, temprature and noise sensors
SPO2, Blood, pressure and EMG sensors
3G/4G communications
Access point
Emergency
Intermediate family
Internet
Medical server and database
Medical staff
Biofeedback

Overview of the WBAN technology



- Radio frequency WBANs 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)

Overview of the WBAN technology

- WBAN applications
  - Healthcare
  - Sport and entertainment
  - Military and defense
- WBAN application requirements
  Power consumption, Coexistence, Antenna and radio channel, security and privacy, range and topology, bit rate, device form, safety, signal processing

MAC functionality

- MAC protocols classified in
  - *scheduled-* or *reservation-based MAC protocols*
  - *contention-based MAC protocols*
- Schedule based MAC protocols are divided into
  - *synchronous schedule based MAC protocols*
  - *asynchronous schedule based MAC protocols*
  - *hybrid schedule based MAC protocols*

Multiple Access Techniques

- Time Division Multiple Access (TDMA)
  - Each node transmits its data in its own time slot sharing the same frequency channel
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Transfer disabling for a node if other nodes are transmitting
- Frequency division multiple access (FDMA)
- Pure ALOHA (contention-based protocol)
  - Low energy efficiency, high rate of collisions
- Slotted ALOHA

IEEE 802.15.4 MAC

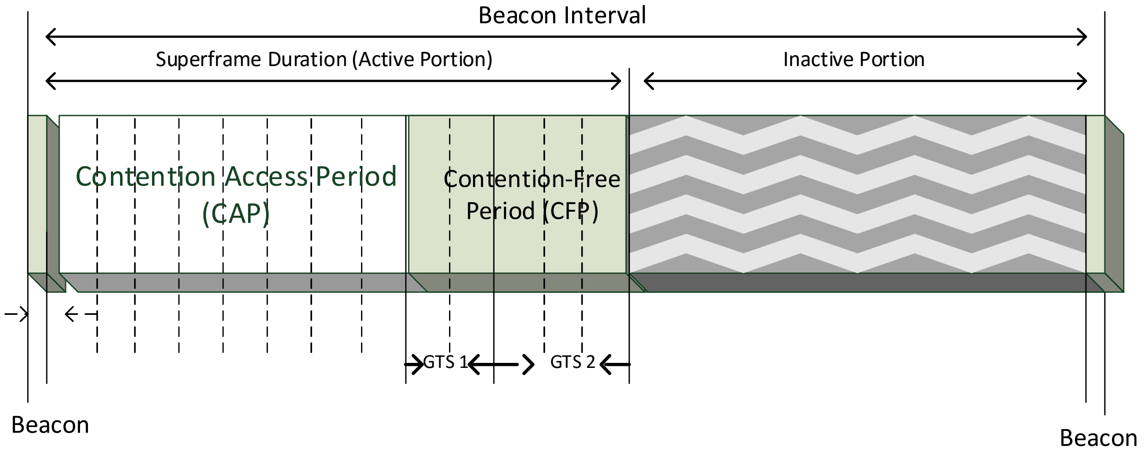
- Developed for the design and implementation of LR-WPANs
- Defines full-function (FFD) and reduced-function devices (RFD)
- The standard specifies a PAN coordinator (is a FFD) to manage the network
- Star topology, peer-to-peer topology, cluster tree network

IEEE 802.15.4 MAC

- Two modes of operation
  - Beacon-enabled mode
  - Nonbeacon-enabled mode
- Nonbeacon-enabled star topology: nodes communicate with the PAN coordinator in a contention-based way using CSMA/CA
- Advantage: nodes do not need to regularly power-up to receive a beacon
- Disadvantage: the coordinator cannot start communication. The nodes must poll the coordinator

IEEE 802.15.4 MAC

- The beacon-enabled mode provides a superframe structure
- The access to the channel is managed through the superframe
- IEEE 802.15.4 superframe structure

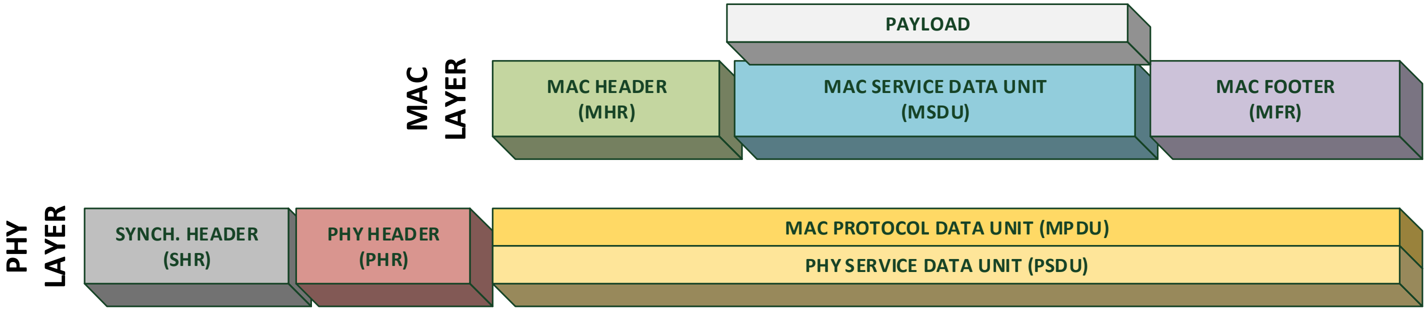

Beacon Interval
Superframe Duration (Active Portion)
Inactive Portion
Contention Access Period (CAP)
Contention-Free Period (CFP)
GTS 1
GTS 2
Beacon
Beacon

IEEE 802.15.4 MAC

- Contention-based transactions take place in the CAP
- CFP is reserved for high priority data
- If a node wants to communicate with the coordinator it requests a guaranteed time slot (GTS)
- In the inactive part of the SF nodes go into the sleep state
- The CAP slots are accessed using CSMA/CA

IEEE 802.15.4 MAC

- The MAC sublayer handles the access to the physical radio channel (with CSMA/CA)
- Four type of MAC frames defined in this standard: Data frame, Beacon frame, Ack frame, MAC command frame
- The frame structure:



IEEE 802.15.4 MAC

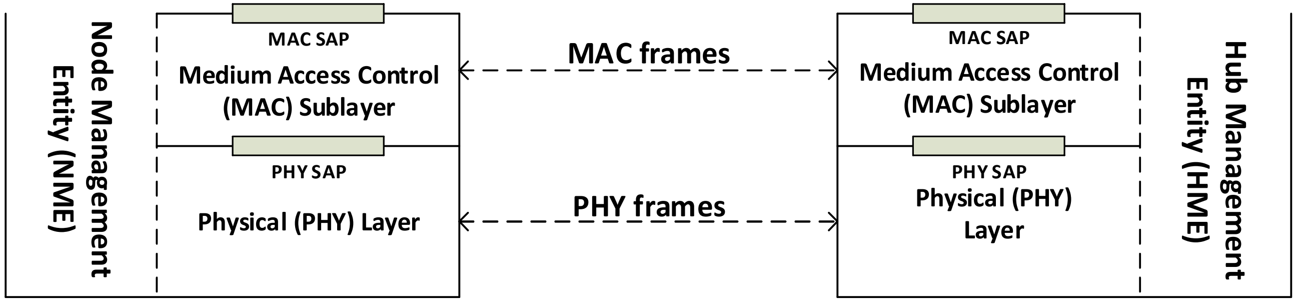
- Responsibilities of the IEEE 802.15.4 MAC
  - beacon generation through the coordinator
  - node synchronization to the network beacons
  - supporting PAN association and disassociation
  - supporting coordinator and node security
  - handling and managing GTS

IEEE 802.15.6 MAC

- A standard for short-range (human body), highly reliable wireless communications
- It allows a very low transmit power device operation

IEEE 802.15.6 MAC - Function

- Reference model


Node Management Entity (NME)
MAC SAP
Medium Access Control (MAC) Sublayer
PHY SAP
Physical (PHY) Layer
MAC frames
PHY frames
MAC SAP
Medium Access Control (MAC) Sublayer
PHY SAP
Physical (PHY) Layer
Hub Management Entity (HME)

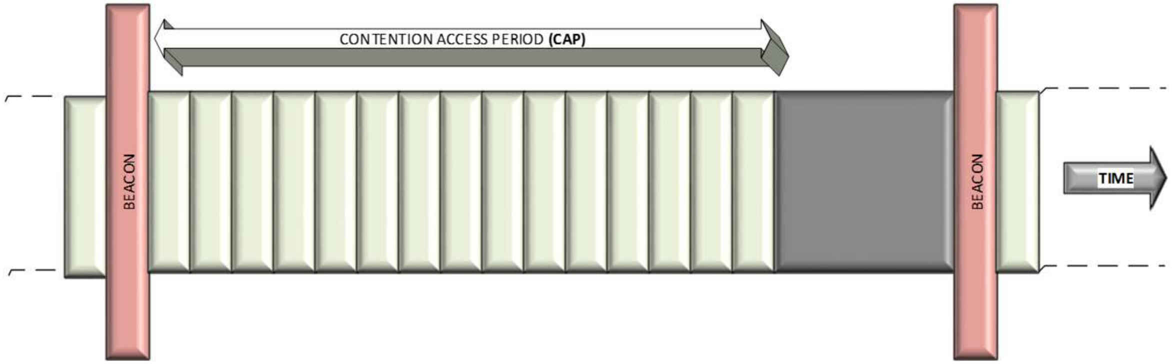
- Transmission: The MAC client passes via the MAC service access point (SAP) its MAC service data units (MSDUs) to the MAC sublayer
- The MAC sublayer passes frames (MAC protocol data units) to the PHY layer via the PHY SAP

IEEE 802.15.6 MAC - Function

- 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
- IEEE 802.15.6 divides the time axis or channel into superframes of equal length or into beacon periods
- Each superframe contains a number of timeslots used for the data transmission

IEEE 802.15.6 MAC - Function

- The total time interval of the timeslots is called Contention Access Period (CAP)



- A frame transition can include more than one allocation slots and must not necessarily starts or ends on an allocation slot boundary

IEEE 802.15.6 MAC - Characteristics

- Node types according to their functionality
  - Sensor (converts a physical quantity in electronic signals)
  - Actuator (controls the flow of material or power)
  - Personal device (collects the data and interacts with users)
- Node types according to their role
  - **End node** (includes MAC, PHY and optional security services)
  - Relay (receives data from end node and send it to the PD)
  - Coordinator (hub, all other nodes communicate through it)
- Node types according to their implementation
  - Body surface node
  - Implant node
  - External node

IEEE 802.15.6 MAC - Characteristics

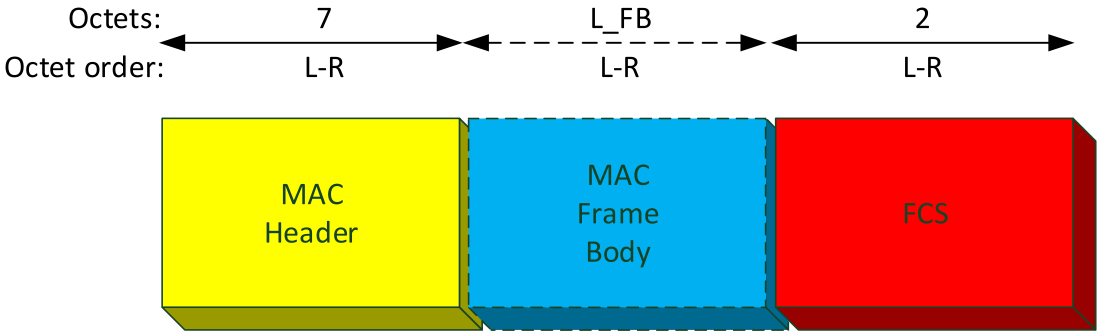
- The logical set of one hub and n nodes (max 64) is defined as Body Area Network
- One-hop star BAN
- Two-hop extended star BAN (relay nodes)
- Communication methods
  - Beacon mode
  - Nonbeacon mode

IEEE 802.15.6 MAC - Characteristics

- In the beacon mode the hub controls the communication
- In the non-beacon mode:
  - the communication is asynchronous
  - A node communicates with the hub only when it needs to
  - Nodes use CSMA/CA
  - Receiving data from the hub takes place by power up and poll the hub

IEEE 802.15.6 MAC – Frame formats

- A MAC frame is an ordered sequence of mandatory and optional fields
- The MAC general format:



- The MAC header and the Frame Check Sequence (FCS) have fixed-length, and the MAC frame body has variable length

IEEE 802.15.6 MAC – Frame formats and functions

- The frame payload consists of management type frames, control type frames, and data type frames (e.g. emergency frame)
- The Frame Check Sequence (FCS) is an error detecting code added to a frame
- MAC function overview:
  - Frame processing
  - Addressing
  - Priority mapping

IEEE 802.15.6 MAC – Frame functions

- MAC frame processing overview:
  - Frame reception (rules on preparing frames for transmission and processing on reception)
  - Frame sequencing
  - Frame retries
  - Frame timeout
  - Frame separation
  - Frame acknowledgement
  - Duplicate detection
  - Fragmentation and Reassembly

Standards Comparison

- IEEE 802.15.1 (Bluetooth)
  - Limited scalability due to limited nr of nodes
  - High-power consumption (40 mW)
- BT Low-Energy
  - Latency less than this of standard BT
  - It reduces power consumption
- IEEE 802.15.4
  - First protocol enabling nodes/hubs to share the wireless platform
  - Designed for WPANs with the features low-cost, low power consumption (0.5mW-1mW), and operation in short range (10-100m)

Standards Comparison

- IEEE 802.15.4
  - o Cannot support efficient high data rate applications (<= 250 kbps)
  - o Scores over BT: lower cost, lower power consumption, longer battery life, scalability features, smaller latency, supports standard-based security
- IEEE 802.15.6
  - – Its target: wearable devices
  - – The first international standard for WBANs

Standards Comparison

- IEEE 802.15.6
  - Operates in low-power and short range (<3m)
  - The MAC supports multicast, unicast, and broadcast communication
  - Shorter header -> higher data rates
  - The frame control field format combines frame type and subtype to classify different frames
  - Collisions are combated using the User Priority. UP prioritizes the medium access of some frame types (e.g. frame type emergency)
  - Complex and unsuitable for ultra-low-power devices

Standards comparison

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

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: Yes
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	Yes
SmartBAN	TBD	TBD	Yes

MAC sublayer challenges

- IEEE 802.15.6 defines message exchange protocols and packet formats. This help to achieve simple tasks.
- In what order do we schedule allocation intervals?
- When should relays be used?
- When should we cope with failed packet reception?
- WBAN topology and density changes need to be addressed in the MAC protocol design
- Limited sensitivity in WBANs (the min signal power for reliable communication)
- Managing interference if multiple people wearing WBANs

WBAN Privacy and Security

- Privacy is the right of every individual to control its own data
- Data security is the protection of data sored inside the WBAN or data being transferred outside of the WBAN from unauthorized users
- WBAN security requirements
  - Data storage requirements (e.g. dependability)
  - Data access requirements (e.g. revocability)
  - Other requirements (e.g. authentication)

MAC security specifications

- IEEE 802.15.4 MAC
  - Data confidentiality
  - Data authenticity
  - Replay protection
- The beacon, data, and control packet types can include security information. Only the ACK packet type cannot
- Eight different security levels, each of them is controlled by a specific security suite with different properties

MAC security specifications

- IEEE 802.15.6
  - Three security levels
    - Level 0 - Unsecured communication
    - Level 1 - Authentication but not encryption
    - Level 2 - Authentication and encryption
  - In level 0 the transmission of messages happens in unsecured frames
  - Level 1 provides authenticity, replay defense, and integrity validation but not confidentiality, and privacy protection
  - The selection of the security level happens when the node is joining the WBAN

Security challenges in WBANs

- Balance of security and efficiency due to limited computation and storage capabilities of WBANs (lightweight cryptographic characteristics)
- Balance of security and safety (secure access control, patient safety = WBAN data can be accessed whenever needed)
- Balance of security and usability (human interactions to setup data security mechanisms, WBAN devices easy to use)
- Device interoperability

Conclusions of the Master Thesis

- There are many exciting perspectives for the further development of the WBAN technology in the MAC sublayer
- In our days security is a fundamental feature
- 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