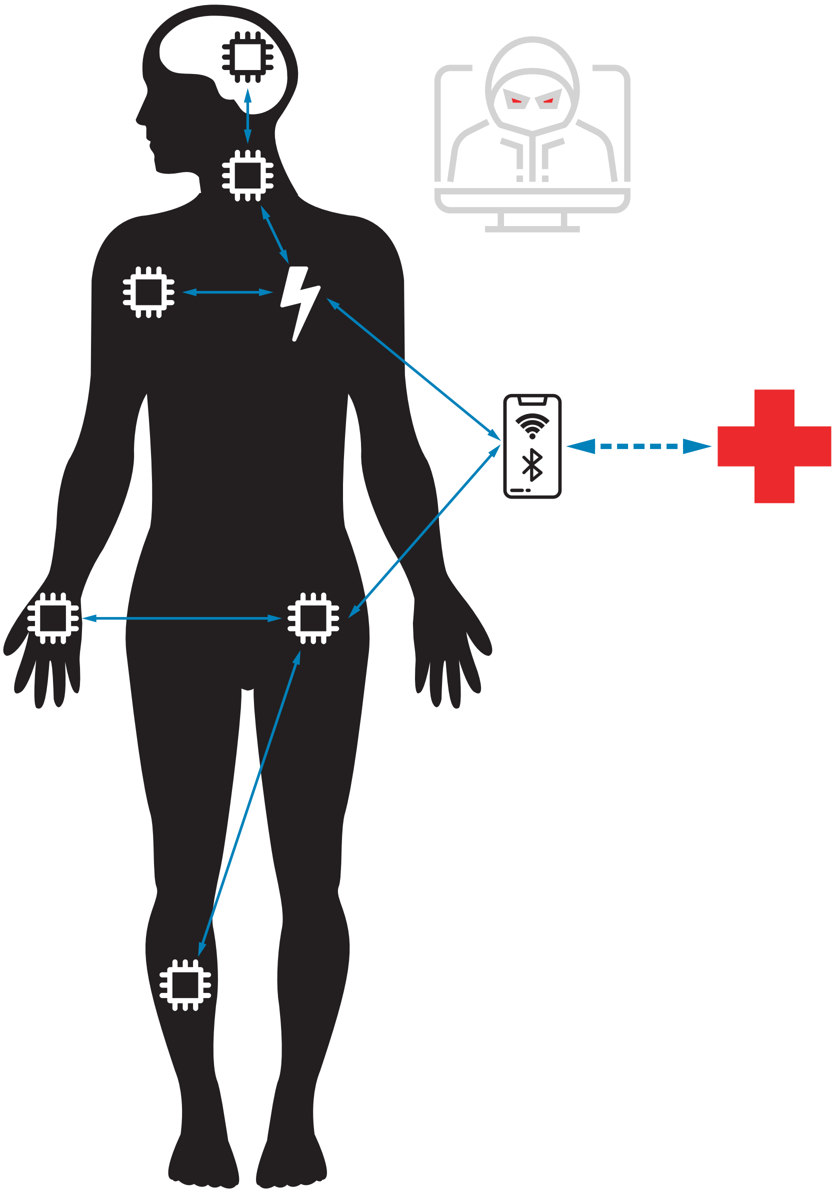
TU Delft

Erasmus MC
University Medical Center Rotterdam

Assessing the state of security of Medical BANs and the IEEE 802.15.6 standard



Georg Hahn

Assessing the state of security of Medical BANs and the IEEE 802.15.6 standard

by

Georg Hahn

to obtain the degree of Master of Science
at the Delft University of Technology.

Student Number:	5070848	
Project Duration:	January 1, 2021 - July 2 2021	
Graduation Committee:	Prof. Dr. Ir. Wouter A. Serdijn	TU Delft
	Assoc. Prof. Dr. Ir. Christos Strydis	Erasmus Medical Center
	Assoc. Prof. Dr. Ir. Zekeriya Erkin	TU Delft
	Muhammad Ali Siddiqi MSc (Supervisor)	Erasmus Medical Center

Contents

Abstract

Medical Body Area Networks (MBANs) are a cluster of possibly heterogeneous devices, communicating with each other in, on or around the human body. Through these devices, medical data is collected, processed in some way and transferred outside of the network. The IEEE 802.15.6 standard aims to govern communications between such devices. It includes a set of constraints for physical features and communication on the PHY and MAC level, as well as association/ disassociation protocols and security services that applications need to comply with. Given the high sensitivity of the medical data transmitted via MBANs, network security is crucial. This thesis consists of three main contributions: (a) a structured procedure to analyse the security features of the IEEE 802.15.6 standard by using realistic hypothetical scenarios is introduced (b) a thorough security analysis of the standard is conducted (c) recommendations on how to improve the security posture of the standard are given.

Chapter 1

Introduction

1.1 Motivation and problem statement

The recent shift from stationary offline devices to interconnected, smart electronics and sensors created a massive range of novel technologies and applications. The so-called *Internet of Things* (IoT) has become one of the most disruptive technologies of our decade, enabling the creation of device networks, which try to create value in nearly every industry. Especially the healthcare sector experiences a massive technological change. So-called, *Medical Body Area Networks* (MBANs) are revolutionizing the way in which healthcare data is gathered and processed, by creating a network of interconnected nodes in, on or in the vicinity of the human body. *Nodes* can represent a variety of devices, e.g. medical implants, sensors and wearables, used to measure or send all kinds of biomedical signals, e.g. respiratory rate, mechanical motion, heart rate and many more. This facilitates multiple interesting applications in areas such as real time health monitoring, ambient assisted living (AAL) and pathology treatment.

Although MBANs show a very high potential for future applications, increased functionality is always accompanied by a proportional increase in potential risks. Given the sensitivity of the data processed by the nodes and the critical functionality of the network's actuators, a security-driven implementation is crucial. Cyber-attacks such as *Denial of Service* (DoS) can have life-threatening consequences for the patient and must be prevented. However, not only threats to the patient's life are an issue but the patient's privacy is also at stake. MBANs are handling massive amounts of highly sensitive *Personal Health Information* (PHI), for which confidentiality, integrity and availability needs to be ensured. Due to the limited resources in terms of electrical capacities (e.g. memory, battery life, . . .) offered by implanted or wearable nodes, this can often become a challenging task. Although some modern nodes manage to use state-of-the-art security implementations and protocols, there are still a number of attack vectors enabled through wireless connections and vulnerabilities.

To mitigate the threat landscape and implement security features across all MBAN applications, the IEEE created the 802 standardisation committee with the goal to create wireless communication standards for such networks. Since the meeting in 1980, the committee has proposed several standards in the IEEE 802.15 (IEEE 802 WG15) family, which specifies communication technologies for *Wireless Personal Area Networks* (WPANs)[1]. Some of the more popular standards released by WG15 include 802.15.1 (Bluetooth), 802.15.4 (ZigBee) and 802.15.4e (UWB). As WPANs and already existing communication technologies do not satisfy the requirements for medical communication, a new task group (TG6) was created. In 2010, the IEEE 802.15 TG6 or IEEE 802.15.6 published the first draft of a standard, optimised for low-power nodes for medical and non-medical applications, which was approved and ratified in 2012 [2].

IEEE 802.15.6 aims to govern MBAN communication on the PHY and MAC layer level. It also provides several security measures, as well as seven distinct association and disassociation protocols. However, like with any novel standard or technology, security issues have been found [3]. As finding the optimal security solution is an iterative task, the aim of this thesis is to improve the security of future MBAN applications, by improving the security posture of the IEEE 802.15.6 standard. Thus, answering the research question: **How can the IEEE 802.15.6 standard's security posture be improved in order to provide a secure framework for future MBAN applications?**

1.2 Thesis scope and contributions

In this section the initial scope of this thesis will be introduced by formulating a number of main objectives. Those objectives represent the key milestones of this research. Subsequently, the contributions made by this work will be listed.

Scope The main objectives of this thesis are the following:

i Give an overview of the basic principles and technologies of Medical Body Area Networks and the governing IEEE 802.15.6 standard.

ii Analyse the MBAN threat landscape and formulate extensive general security requirements that are applicable to every type of MBAN.

iii Introduce a structured analysis procedure to analyse the security posture of standards and apply it to IEEE 802.15.6.

iv Give recommendations on how to improve the IEEE 802.15.6 standard in terms of security.

Contributions The following contributions were made by this thesis:

- An overview of Medical Body Area Networks (MBANs), including all the most important building blocks was given.
- An overview of the current IEEE 802.15.6 standard with a focus on the security features and vulnerabilities was given.

- A structured procedure to exhaustively analyse the IEEE 802.15.6 standard in terms of security was introduced. Thereby, a set of security and physical requirements were introduced and, following the procedure, hypothetical scenarios were designed.
- The IEEE 802.15.6 standard's security posture was analysed and gaps between the standard and the defined requirements were found and summarised as findings.
- Specific recommendations on how to improve the security posture of the IEEE 802.15.6 standard were given and clustered into four distinct categories.

1.3 Thesis organisation

This work is structured in the following way: Chapter 2 introduces the concept of MBANs, to get a fundamental understanding on what they are, how they function and what the essential building blocks of the technology are. Chapter 3 discusses security requirements and the threat landscape MBANs are facing. The IEEE 802.15.6 standard is introduced in chapter 4. Here, a special focus lies on the security aspects and known vulnerabilities of the standard. In chapter 5, a structured process to analyse the security posture of the IEEE 802.15.6 standard is introduced and the standard is analysed. Furthermore, recommendations on how to improve the standard in terms of security are given. Chapter 6 concludes this work and proposes possible next steps to be taken.

Chapter 2

MBAN background

To give a basic understanding of the fundamental aspects of Medical Body Area Networks, this chapter will provide necessary background information.

MBANs, sometimes also referred to as the Internet of Medical Things (IoMT), are a subgroup of Wireless Body Area Networks (WBANs) which again are a subgroup of Wireless Sensor Networks (WSNs). Figure 1 illustrates the hierarchical dependence of WSNs, WBANs and MBANs.

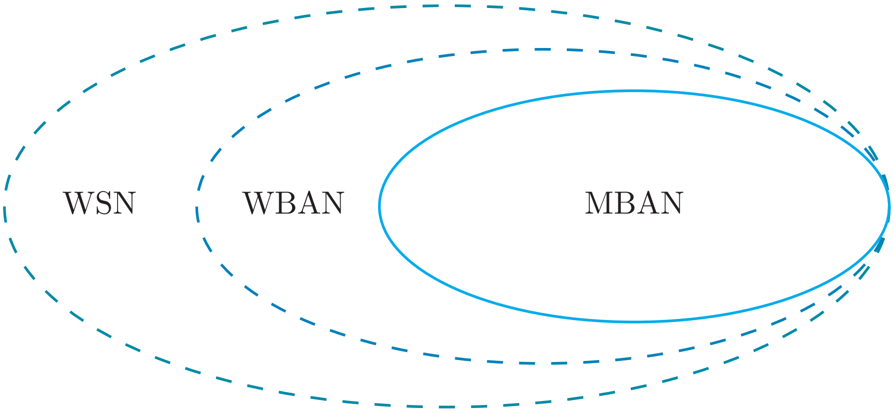


Figure 1: MBANs are a subset of WBANs, which are again a subset of WSNs.

WSNs are a set of sensors with high computational resources dispersed around the environment. Those sensors are often used to collect relevant data of current conditions in the environment they are in (e.g. traffic monitoring, industrial manufacturing, monitoring air toxicity in chemical plants, ...). While WBANs also consist of numerous wirelessly connected sensors, as well as actuators, they are specifically placed in, on or around the human body. Sensors and actuators in those networks very often do not have full computational capabilities, especially when implanted. The aim of those sensors is to gather biological data, which is then transmitted to a server, where more resource-intensive computations (e.g. data analysis, machine learning algorithms, predictive analytics, ...) are carried out. If needed, the server can also decide to initiate an action and send commands to the actuator nodes via a central coordinator. If the collected data is used for medical purposes, the network is called an MBAN. The exact differences between WSNs and WBANs are listed in table I.

Table I: Detailed comparison between WSN and WBAN [4].

Metric	**WSN**	**WBAN**
range	m/km	cm/m
number of nodes	hundreds	<10
node size	no special requirements	very small
node task	single or scheduled	multiple
network topology	fixed	variable
data loss	tolerable	intolerable
node placement	easily	difficult
bio-compatibility	-	critical
node life	months/years	the longer the better
safety	low	critical
security	lower	more critical
standard	IEEE 802.11.4	IEEE 802.15.6

To get an overview of the technology, the fundamental building blocks (i.e. node types, topologies, communication technologies and applications) of an MBAN will be introduced in the following section.

2.1 Node types

The wide variety of use cases for MBANs inherits a need for a multitude of different nodes with different requirements and challenges. Nodes mostly act as an autonomous device and need to be fully equipped with a communication system to relay data either to other nodes inside the network or to the outside world [1]. They can be classified by three main categories: (a) based on their functionality, (b) on the basis of the type of implementation and (c) on their specific role in the network. The three main categories are summarised in table II.

Table II: Classification of MBAN nodes based on three different criteria.

Functionality	Implementation	Role
Sensor	Invasive	End node
Actuator	Semi-Invasive	Relay node
Hybrid	Wearable	Coordinator node
Central Control Unit (CCU)	Ambient	

Categorisation based on Functionality

This type of categorisation of MBAN nodes looks at the functionality the node has in the network. Additionally, each node needs to show certain characteristics in order to be successfully implemented. The different node types based on functionalities are described as follows:

- **Sensor:** The main task of a sensor node is to gather relevant data and transmit it, either to another node or to a coordinator. Depending on the application and use-case, different types of, either medical or non-medical signals can be collected. Some of the main domains the signals can be in are: mechanical, optical, temperature and bio-electrical. Sensor nodes need to be able to efficiently handle variations in signal characteristics (e.g. frequency, noise, data rate, . . .). Due to the very limited memory space, they need to transmit data in a specified time interval in order to mitigate the risk of overflowing the buffer, thereby losing data [5]. Not only the memory space, but also power storage capacities are scarce, making it crucially important to design effective protocols and processes.

- **Actuator:** An actuator node's main task is to perform an action on the human body based on the information it receives from other nodes. This action can entail initiating action potentials on axons or stimulating certain areas of the brain. As it is sometimes challenging to recharge actuator nodes, the action performed needs to be carried out in an energy-efficient manner.

- **Hybrid:** A node is classified in the hybrid category when it has both, sensing and actuating features. The most prominent representative of this category are implantable medical devices (IMDs). For example, an implantable cardiac defibrillator (ICD) can both sense cardiac arrhythmia and deliver shocks to treat the condition. Although IMDs are not yet ready to be implemented in MBANs commercially, manufacturers like Zarlink and Medtronic are already equipping their IMDs with communication modules. As hybrid nodes are inherently more complex than sensor and actuator nodes, since they are a combination of the two, a new set of challenges arises. Hybrid nodes typically offer more processing power, memory space and battery capacity. However, the implementation of secure, reliable communications is still challenging. Hybrid nodes also come in bigger form factors, which can have an impact on the usability and patients' comfort.

- **Central Control Unit (CCU):** The central control unit, sometimes also called central coordinator, personal control unit or base station, is the main point of coordination. It collects the data sent by sensor nodes, transmits signals to actuator nodes and is responsible for relaying the gathered information to beyond-MBAN communication channels. Given the energy consuming and CPU intensive tasks this node has to accomplish, the CCU usually possesses considerably more battery power and memory space than other nodes, as well as greater processing power.

Another challenge that is true for every node in an MBAN is, that it is difficult to create networks with nodes from different vendors, as they are often not interoperable. MBAN nodes also need to guarantee a high *Quality of Service* (QoS) and high reliability.

Categorisation based on Implementation

Here, the type of implementation based on proximity to the human body is the key classifier. WBAN nodes can be split into four categories:

- **Invasive:** Nodes in this category are implanted under the skin or in the human body.
- **Semi-Invasive:** Here, a part of the node is implanted, and another part is outside the human body.
- **Wearable:** These nodes are located on the human body and most often need to have direct contact with the skin in order to function properly.
- **Ambient:** Nodes that are in close proximity, surrounding the body, are part of this category.

Categorisation based on Role

Based on the function or role in the network, nodes can be classified into three distinct categories:

- **End node:** As the name already suggests, end nodes are at the end of a communication line. they either collect data and send it to another node or receive data from another node and perform an action.
- **Relay node:** Relay nodes receive data from a node in the network and relay it to another node. In this way the communication distance can be enhanced, while simultaneously reducing the energy of the signal.
- **Coordinator node:** Those nodes act as a coordinator in the network, orchestrating the routing procedure and processes.

Some example nodes classified by the introduced classifiers can be seen in table III.

2.2 MBAN architecture

The MBAN technology consists of different communication layers that can be split up into three tiers [6]:

- Tier 1: Intra-MBAN communication
- Tier 2: Inter-MBAN communication

Table III: Classification of several example nodes found in a WBAN.

Nodes	Functionality	Implementation	Role
Heart rate sensor	Sensor	Wearable	End node / Relay node
Insulin pump	Actuator	Semi-invasive	End node
Cochlear Implant	Hybrid	Semi-Invasive	End node
Mobile phone	CCU	Ambient	Coordinator node
ECG / EMG / EEG	Sensor	Wearable / Invasive	End node / Relay node
Endoscope capsule	Sensor	Invasive	End node
Gyroscope	Sensor	Wearable	End node / Relay node
Pacemaker	Hybrid	Invasive	End node / Relay node
Smart watch	CCU	Wearable	Coordinator node
Stimulation electrode	Actuator	Semi-invasive	End node
Vagus nerve stimulation	Hybrid	Invasive	End node / Relay node

- Tier 3: Beyond-MBAN communication

As seen in figure 2, in tier-1 the different sensors and actuators gather biological data, e.g. blood pressure, ECG, EEG and transmit it, depending on the network topology to a collector node where the data is classified. In tier-2, the collected data gets transmitted to a coordinator acting as a sink. This coordinator can be a smart phone, computer or other personal communication device and it is used to classify the data and subsequently transfer it via WLAN, GPRS or similar technologies to remote servers in tier-3 (e.g. cloud infrastructure).

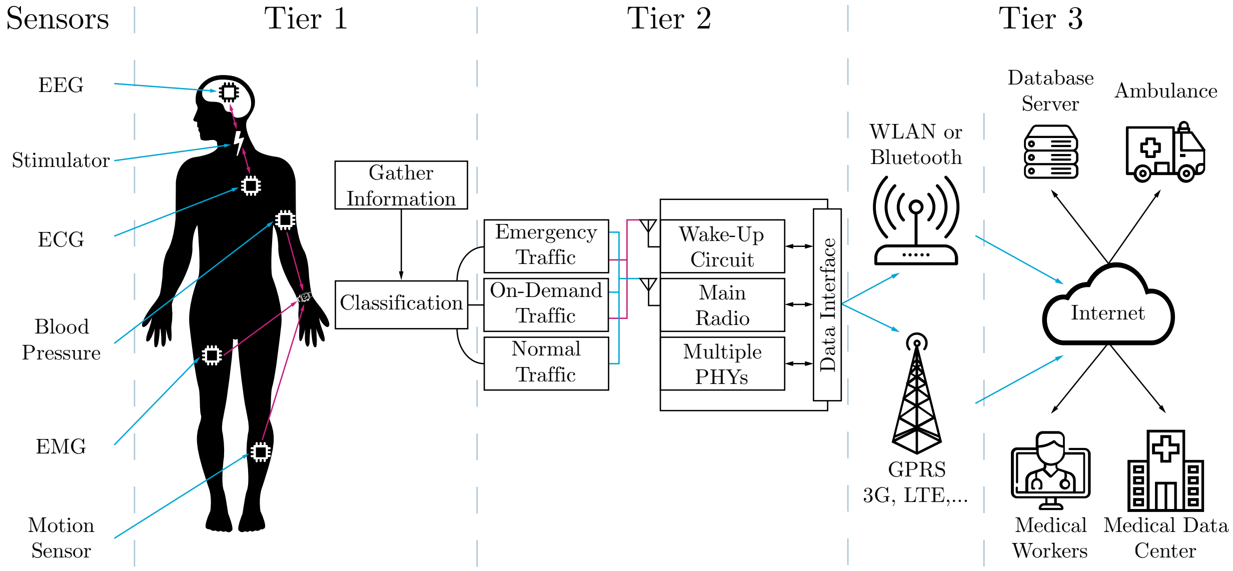


Figure 2: A detailed overview of a WBAN architecture for medical and non-medical applications, based on [7].

These servers collect and analyze the data and either provide it to a medical professional which in turn performs medical diagnostics or the server directly calculates the next action using technologies like machine learning. In the case of receiving abnormal data, tier-3 endpoints will carry out emergency responses and alarms to speed up the process [4]. Additionally, if implemented nodes have enough processing capabilities, data could be processed in a closed loop in tier-1 and tier-2. This could be useful for highly time critical calculations or if the network is not connected to a tier-3 cloud server.

2.3 Topologies

Depending on the application, the sensor and actuator nodes in tier-1 can be connected in different topologies, such as *star, tree or peer to peer.*

Star topology

Amongst these, the most popular is the star, as this arrangement does not need a routing protocol, making the delay between data packets minimal. Here, a data collector acts as base station to which all sensor and actuator nodes are connected. This central coordinator often has superior energy and computational capacities when compared to other nodes, as managing the entire network is a resource-intensive task. While the simplicity of this topology yields great advantages, the central coordinator represents a *single point of failure* (SPOF), which is sub-optimal for high availability systems like MBANs. A use case of this approach is given in [8], where a wireless, WBAN-based 3-lead ECG is realised. The usually wired ECG leads have been replaced by sensor nodes, which gather the ECG data and subsequently send it to a central base station for post-processing.

Tree topology

The tree topology is, similar to the star, governed by a single root node at the top of the structure. It can also be seen as a multi-hop star topology, where the root node on top acts as the coordinator and the branching sensor and actuator nodes collect the data. Although this topology offers great flexibility and, due to the subordinate relay nodes, higher reliability, the root node is also a SPOF. Kim et al. [9] proposed such a WBAN configuration, using a multi-hop tree topology.

Peer-to-peer topology

An arrangement where sensor nodes in a radio range are either directly communicating to each other or communicating through multi-hops is called a peer-to-peer network. This type of topology does not rely on an upstream data-transfer, but much rather transfers collected data from node to node without paying attention to the network's hierarchical structure. This topology trades energy efficiency and battery lifetime for increased reliability, since in case of node failure the network can be routed and managed from different nodes in the networks. Although this is a great advantage, routing protocols become increasingly more complex and are often difficult to realise. Given the inherent complexity, this topology is not as commonly used as previous configurations.

Due to the restricted area of the human body, the maximum amount of sensor and actuator nodes in a network are also limited. As seen in table I the number of nodes on the average WBAN is usually less than 10 (although there are exceptions in some more futuristic hypothetical applications). But not only the number of nodes is limited, also the number of coexisting MBANs within a certain perimeter is limited. This coexistence of inter-MBAN communication alongside other types of beyond-MBAN communication technologies can lead to interference which may disturb traffic within the network. Interference may lead to packet collisions, making signal coordination infeasible [10]. Mahapatro et al. [11] proposed an interference mitigation strategy for WBANs, where they enable two or more WBANs to negotiate a common schedule, rather than working independently.

2.4 Communication technologies

MBAN applications lack off-the-shelf components and libraries, and most communication layers have to be defined by the developer, current MBANs show a very high degree of heterogeneity. Over the many years of research in this field, MBAN applications started to employ a plethora of wireless communication technologies on an as-needed basis.

Although MBAN gateways communicate with tier-3 servers via long distance communication technologies (e.g. LTE, GPRS, WiMax, ...), in this section only short-range technologies will be discussed. These short-range technologies are commercially available and find their primary applications in WSNs and WBANs. They are not specifically crafted for the medical sector, but nevertheless find a broad application in MBANs, due to the widely available, standardised parts and protocols.

Bluetooth

The IEEE 802.15.1 standard, also called *Bluetooth* has been widely adopted and implemented in a variety of e-health and telemedicine applications [12]. Especially its high dormancy and data rate of up to 3 Mbps makes it a popular choice in the medical sector. It operates in a star topology, where a master and up to seven slaves build a network within a scope of 10m. The master node (CCU) dictates the function of the network. Although those specifications are useful for some applications, certain limitations of this technology, like high bandwidth requirements, small size networks, not supporting multi-hop communication, and long start-up time for devices makes it unfeasible for MBANs [12]. Especially the high power requirements turned out to be problematic, which is why the existing standard was optimised.

Bluetooth Low Energy

Bluetooth low energy (BLE) [13], also known as Bluetooth 4.0 is a derivative of the Bluetooth standard, with the aim of reducing energy consumption by using low duty cycle operations. In addition to that, latency, pairing duration and start-up time are strongly reduced in comparison to Bluetooth, which makes it suitable for low-latency applications. Also, the time needed to establish a connection is vastly decreased, with BLE taking less than 3ms to connect a new device, which is a major improvement when compared to Bluetooth's 100 ms. The data rate is lower with up to 2 Mbps and continuous data reporting operations consume similar amounts of energy to Bluetooth, which makes BLE unsuitable for health monitoring applications.

ZigBee

ZigBee is a short-range communication protocol, building upon the IEEE 802.15.4 standard, which offers a framework for PHY and MAC layers for Personal Area Networks (PANs). ZigBee defines specifications for the network layer, like the network topology and provides a framework for programming applications in the application layer [14]. The communication within this protocol relies on small, low-energy radios and allows interoperability between different applications. Some of the more prominent advantages of this technology are [1]:

- Robust and reliable data transfer
- Scalable
- Low-cost
- Easy to implement
- Short-range operation

Those advantages make this technology, besides Bluetooth, the most prominent in MBAN applications. When compared to the Bluetooth standard, ZigBee uses only one third to half the energy, but data rates of up to 250 Kbps are considered low and higher latency might not be compatible with real-time monitoring applications or may restrain upscaling of MBAN networks. Due to longer channel fades, emergency data transmissions can experience higher delays, which is why ZigBee cannot guarantee high QoS for MBAN applications [12]. Furthermore, ZigBee operates in the non-licensed ISM band and can suffer from severe interference problems in the presence of WiFi networks [15].

Ultra Wide Band

According to the FCC, which is the entity that first approved this technology, UWB (IEEE 802.15.3) are signals with a bandwidth of at least 500 MHz. This expanded bandwidth leads to an increased throughput, which is essential for MBANs with a high number of nodes and real-time monitoring applications. The UWB technology not only offers increased data rate, but it does that at an exceptional power efficiency. A major drawback of this technology, however, is that at high data frequencies the power consumption increases drastically, often making design of such a network challenging.

Table IV shows a comparison of the discussed and some additional wireless communication technologies used in MBANs.

Table IV: Comparison of wireless communication technologies used in MBANs

Technology	Spectrum	Data rate	Range	Current consumption	Access Method
Bluetooth	2,4 GHz	1-3 Mbps	10-100 m	30 mA	CSMA
BLE	2,4 GHz	1 Mbps	10 m	15 mA	FH + TDMA
ZigBee	868 MHz, 915 MHz 2,4 GHz	3-24Mbps	10 m	15 mA	CSMA
UWB	3,1-10,6 GHz	480 Mbps	<10 m	1 mA	CSMA, TDMA
RFID	850-960 MHz	10-100 Kbps	30 m		Slotted Aloha
ANT	2,4 GHz	1 Mbps	30 m	Ultra low	TDMA
Sensium	900 MHz	160 Kbps	5 m	Low	TDMA, FDMA

2.5 Possible applications

Now, after discussing all the necessary details to understand the concept of MBANs, some potential applications will be presented. According to IEEE 802.15 TG6 applications can be classified into medical (MBAN) and non-medical (WBAN) applications. Medical applications can be further split into four categories, namely implantable, semi-invasive, wearable and remote control of medical devices. The applications discussed in this section, however, are not yet commercially available, but should much rather be seen as potential ways this technology can be implemented in the future.

2.5.1 Medical applications

Medical applications are certainly an important implementation of the WBAN technology. With the potential to revolutionise current medical procedures, they facilitate a tremendous improvement of the effectivity of doctor-patient interactions and offering enhanced independence to the patient, as remote solutions decrease the time needed to be spent at a medical facility.

a) **Implantable:** In this category, sensor and actuator nodes are usually implanted inside the body, beneath the skin or in the blood stream. Here are some of the example applications:

   - **Cardiac diseases:** A common procedure to prevent arrhythmia in high-risk patients, is to implant a cardiac pacemaker which will autonomously deliver shocks whenever needed. However, traditional pacemakers are rather chunky and invasive, and implanting the leads can be challenging. Therefore, next generation leadless cardiac pacemakers (LCPs) use MBAN technology to miniaturise the form factor (up to 80% smaller) and reduce invasiveness of the application. The self-contained electrode system of the LCP gets implanted directly into the right ventricle, eliminating several complications occurring with traditional pacemakers, like lead fracture and pocket infections [16]. With the use of MBANs, biological signals can also be gathered and analysed to prevent myocardial infarction. Thereby multiple sensor nodes monitor the patients' vital signs which get sent to a remote monitoring centre, where it is decided if therapy needs to be delivered [17], [18].
   - **Cancer detection:** A network of sensor nodes can be implemented to detect cancer, for instance by measuring the amount of nitric oxide included in cancerous cells. By monitoring related data, doctors can potentially diagnose tumours without the need of biopsy, providing more rapid analysis and treatment [19].

b) **Semi-invasive:** Applications in this category can have a mixture of implanted and wearable sensor and actuator nodes. A possible application in this domain is:

   - **Diabetes control:** The golden standard for glucose monitoring is to self-monitor blood glucose levels through taking a small blood sample by pricking the finger. This method is rather invasive and inconvenient for the patient [20]. Therefore, *continuous glucose monitoring systems* (CGMS) have been realised. Here, an FDA-approved glucose sensor node is implanted into the body. The monitored blood glucose levels are then sent to an insulin pump, which decides if actions need to be taken. There are already a variety of commercial solutions available, like the DexCom G5 and the MiniMed 670G from DexCom Inc. and Medtronic Inc., respectively. These commercial applications have the potential to be expanded into a whole infrastructure of glucose monitoring sensors and connecting them to a cloud processing infrastructure for extensive data processing.

c) **Wearable:** Here, sensor nodes are usually attached to the skin using straps or worn by the patient in the form of a fabric, wristband, headgear and many more. Some applications of this approach are:

   - **Epileptic seizure detection:** Traditional, wired methods of epilepsy detection are not adequate for long-time monitoring without restricting patient mobility. With the use of MBAN technology a real-time monitoring system to prevent and predict incoming seizures can be realised. Escobar Cruz et al. [21] proposed a system to detect tonic-clonic seizures. A wearable glove with sensor nodes collects ECG signals and sends them to the patient's phone, which in turn communicates with a cloud computing server. With the help of a support vector machine, a form of machine learning algorithm, abnormal signals are recognised and detected. If a seizure is imminent an automatic SMS message gets sent to a medical professional or a relative.

- **Mental status monitoring:** The wide variety of physiological signals collected by modern wearable sensor enable a multitude of different diagnostic possibilities. One of them is to use those signals to detect the mental health status of patients, of which stress monitoring is the most common [22]. Collected audio and heart rate signals fed into machine learning algorithms can potentially detect mental stress levels in children, creating the possibility to remotely monitor child safety [23]. Other ways to use the collected data are to implement suicide risk monitoring [24] or monitor the state of mental health in chronically depressed patients [25].
- **Sleep analysis:** Healthy sleep is one of the most essential needs in order to maintain mental, as well as physical health. Conditions like sleep apnoea and insomnia can cause severe damage to an individual's well-being, if left untreated. To monitor the sleep cycle a technique called *polysomnography* (PSG) is used. Here, data of brain waves, blood oxygen level, heart rate, breathing and eye movement is collected, traditionally through a wired system, and used to analyse the sleep stages. Proposed MBAN architectures for monitoring sleep disorders can reduce the complexity of wired monitoring [26]. Haoyu et al. [27] have proposed an automatic sleep apnoea diagnostic system, based on pulse oximetry and heart rate.
- **Assessing fatigue and athletic readiness:** Whether it be soldiers, firemen, policemen or professional athletes, stressful situations and the rush of adrenaline might masque the exhaustion and fatigue of the body. Failure of muscles can have serious consequences in some situations, which is where the MBAN technology comes in. A combination of lactic acid and motion sensors can be used to assess physical readiness and bodily fatigue [26]. Such a system can also be useful in the training phase of athletes, where the collected data can be used to optimize workout intervals and rehabilitation times.

d) **Remote control:** MBANs offer a wide variety of remote monitoring and telemedicine applications. Those remote capabilities allow for exciting concepts, such as: *Ambient Assisted Living* (AAL), where the monitored data is stored on back-end medical network [19] and care decisions are made based on that data. This helps elderly and people in need of care to prolong the home-care period, delaying the need for treatments in medical facilities. The real time monitoring feature of MBANs can also be used to track recovery processes and remotely administer medication if needed.

2.5.2 Non-medical applications

The WBAN technology is not only of use in the medical sector but it can also improve the quality and effectiveness of many non-medical tasks. The interconnection of WBAN and IoT networks can create a completely connected environment, which opens the gates for a multitude of possibilities. To illustrate the vastness of possibilities, also beyond the MBAN realm, some WBAN applications will be introduced in the following.

- **Non-medical emergencies:** In case of a fire, normally fire alarms produce a loud sound to warn people in the area. Deaf people however can often not recognise those alarms. Here, an interconnected WBAN can help to alert people who may not be able to recognise existing alarm sounds. Also, workers in industries where there might be danger of a poisonous gas leak could potentially be alerted by such a system [28].

- **Biometric authentication:** This topic is a highly discussed one in the realm of WBANs. Recorded biometric signals, like ECG, EMG and electrodermal activity (EDA) in connection with biometric features (e.g. iris scan, fingerprint, ...) can be used for user authentication or to generate keys. This technique, called *cognitive biometrics* is implemented in *Future Attribute Screening Technology* (FAST), developed by the United States Department of Defence [29]. It offers many advantages over traditional authentication methods (something you have vs. something you know), as this technique is especially hard to forge, steal or lose [28].

- **Lifestyle and fitness:** IoMT devices have had an enormous impact on the commercial market in the past years. Smart-watches and fitness trackers can help professionals, as well as ordinary people keep an eye on basic physiological functions. However, those devices are not considered as WBANs in our context, as the current applications merely consist of a BLE link between two devices. In future applications a number of interconnected sensor nodes, integrated in a WBAN infrastructure, can monitor exhaustive health metrics far beyond the capabilities of today's smart-watches. Although those applications might not replace thorough medical checks, they spread health awareness and support people in living a healthier life. A more futuristic application of this idea is to monitor the mood of an individual and, based on that data, adapting the environment.

Chapter 3

MBAN security requirements and threat landscape

Now, after presenting the very basics needed to understand MBAN concepts and their inherent challenges, the security and privacy requirements will be discussed. Given, that current MBAN applications are merely conceptual works or still in a research state, security has to be treated with special care, as there are still many unknowns. Thereby, the term security describes the protection of gathered data, whether in transit, in use or at rest. Privacy on the other hand refers to controlling the usage and collection of said data. When looking at the current research and already available commercial products, it seems that there is a clear focus on functionality and usability. However, given the nature of the processed data, especially by MBANs, security must not be left out of the equation.

3.1 Security requirements

The increasing volume of IoT devices in combination with the often extremely sensitive information pose an attractive attack surface for potential adversaries. When looking at MBANs, the so-called *Personal Health Information* (PHI) transported is of the highest level of sensitivity (according to the ISO/IEC 29100 standard), thus requiring not only increasing the needed level of technical controls to secure this data but also more trust from the user. If potential users of this technology cannot be absolutely sure that only authorized parties can access their PHI, general adoption and acceptance of this ecosystem will be low. There are already several methodologies and approaches on how to tackle security and privacy concerns in not only medical applications but IoT devices in general.

The most fundamental principle is the so-called *CIA Triad*, where secure systems handling information have three properties. Figure 1 shows how different types of attacks on a network can act upon the core principles, which are discussed in the following:

- **Confidentiality (SR1):** Data confidentiality can be compared to privacy, meaning that certain information should only be available to certain people. It is preventing unauthorized users to access the data, but at the same time authorized users should

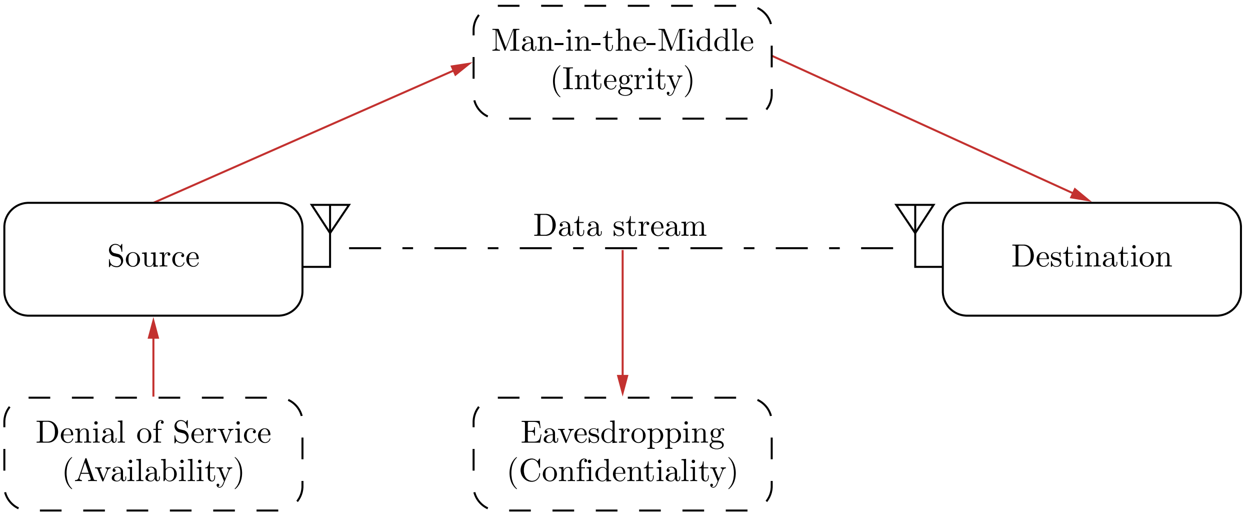


Figure 1: Possible attacks on the functionality of the CIA Triad, recreated from [30]

be enabled access. PHI is the most sensitive kind of information available. If leaked, it can have a variety of social and economic repercussions for the victim. A common practice is to categorize the data by its level of sensitivity and implement more or less stringent security controls accordingly. The most common control implemented to ensure confidentiality of data is encryption.

- **Integrity (SR2):** means that the processed data is stored and transported in a way that is intended and modification to that data is authorized. By protecting data from alteration, trustworthiness and accuracy is ensured. Falsified information can have serious consequences. For example, if falsified information is sent to the medical professional, he might wrongfully decide to deliver a treatment, even though in reality it would not be necessary. Some common controls to achieve integrity are access control mechanisms, hash based or cryptographic checksums and version control.
- **Availability (SR3):** Given the criticality of the data processed by an MBAN, it must be accessible to authorized users at all times. *Denial of Service* (DoS) attacks (e.g. jamming, flooding, . . .) can make data unavailable, which can lead to failure of delivering treatment, potentially causing a life threatening situation for the patient.

However, the CIA Triad is too broad for creating an in-depth framework to describe security and privacy concerns related to the MBAN nodes introduced in section 2.1. The several additional requirements such a network must fulfill in order to be considered as secure are listed below. Figure 2 gives a complete overview on the security requirements of MBANs.

- **Authentication (SR4):** Nodes within a MBAN must have the ability to identify the sender and verify if the data received is from a trusted source and not from a false

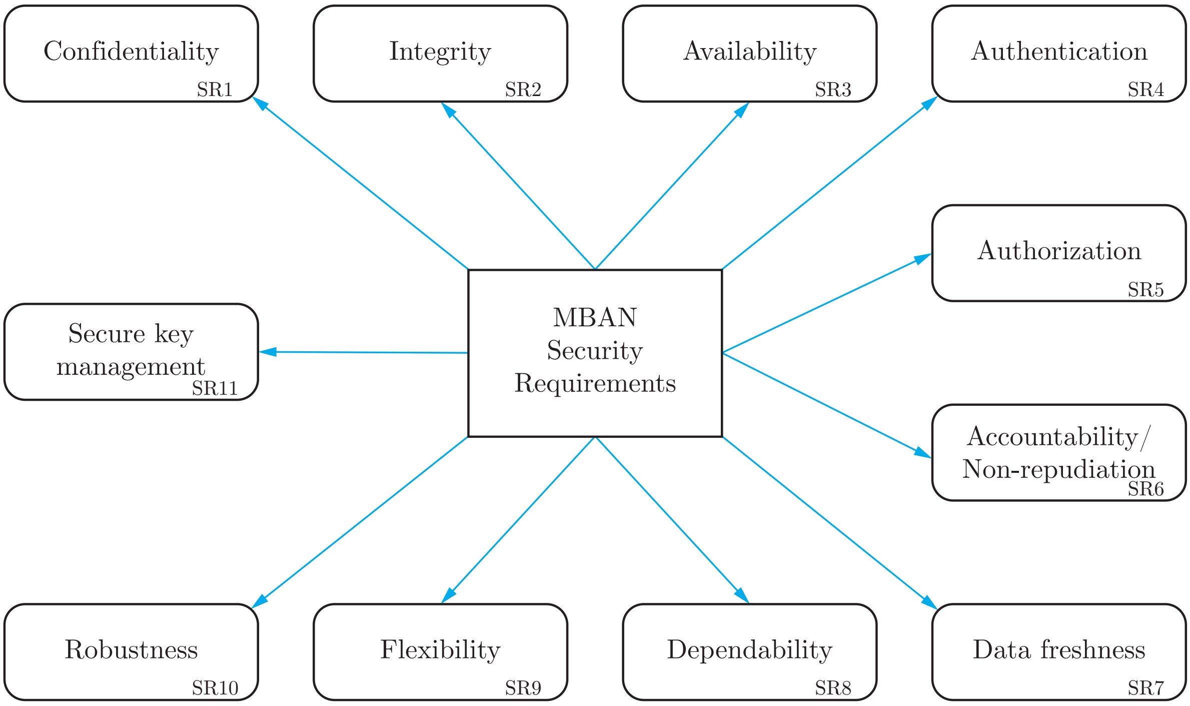


Figure 2: A comprehensive overview of MBAN security requirements

adversary. Authentication mechanisms in MBANs have to be highly energy efficient and guarantee anonymity of the sender. One way to achieve this is to generate a so-called *Message Authentication Code* (MAC) with a private key. If the receiving node can calculate the exact same MAC with the associated public key stored in an *Access Control List* (ACL), it is guaranteed that the message originates from an authenticated source. Some of the several other proposed techniques include: biometric features, certificate-less authentication, elliptic curve cryptography (ECC) systems, ID-based systems and many more [31].

- **Authorization (SR5):** After successfully authenticating the identity of the sender, it has to be decided which actions can be performed and which resources can be accessed. Authorization is needed to decide on who can access and manipulate data in the medical database, but also to decide data access within the MBAN. Clusters of sensors for instance sometimes need to retrieve different data than the rest of the nodes in the network, giving them a different authorisation level [32].

- **Accountability and Non-repudiation (SR6):** Given the sensitivity of the processed data, it has to be visible who has access and and who can manipulate it. Data users (e.g. patients, medical professionals, . . .) need to be held accountable in case they abuse their privilege to carry out unauthorized actions [33]. Additionally, they must not be able to refute the fact that they were the ones tampering with the data.

- **Data freshness (SR7):** Data freshness ensures the integrity and confidentiality of transmitted information, by ensuring old data is not recycled and data frames are valid [34]. When certain identifiers of transmitted data are not unique and get reused, there is danger that someone records said data and replays it at a later point in time. While the replayed data would still be authenticated, the actual body of the message could be altered and send unwanted commands to network nodes. Roy et al. [35] proposed an implemented data freshness in their trust evaluation model by considering a transmission delay. If the delay is greater than a set boundary, the model assumes that the message has been tampered with. This technique is referred to as *strong freshness*; a model where only the data frames are observed is considered as implementing *weak freshness* [34].

- **Dependability (SR8):** Dependability is a critical concern in MBANs, as it guarantees retrievability of data even in case of failures or malicious node modification. A failure to retrieve the correct data can interfere with the ability to deliver correct treatment to the patient. One possibility to address this issue is error-correcting code techniques [36]. Even though this is a pressing issue in designing secure and reliable MBANs, it has not received much attention yet [37].

- **Flexibility (SR9):** The MBAN needs to be able to change access rights depending on the circumstance and environment the network is in, i.e. the network must be context aware. On the one hand, the network needs to adapt to changing access points and control units (e.g. changing topology when the main CCU, like a cellphone is not in reach). On the other hand, in emergency or other situations, where a new individual needs to make changes to the data (e.g. emergency doctors), proper access needs to be granted and access control lists need to be updated. This is very challenging, since malicious actors could impersonate a new doctor and grant themselves access to the network, therefore proper controls need to be in place.

- **Robustness (SR10):** This means that the MBAN has to be resilient against attacks over all layers of security. Furthermore, the impact that an attack has on the network should be at a minimum, guaranteeing continuation of function and operability.

- **Secure key management (SR11):** Most MBAN systems rely on some kind of private key, which is used for encryption, authentication and integrity checks. The main challenge is that those private keys must be generated by using truly random numbers to alleviate the risk of key replication and be stored in a way inaccessible to any person other than the MBAN user. A novel idea in MBANs is to use the physiological signals to generate those keys. Thwerefore, the most prominent method is to use the randomness of RR-Intervals of an ECG signal to establish a key generation and exchange protocol [38]. So-called *Public Key Infrastructures* (PKI) embed the private keys in a certificate, issued by a trusted *Certificate Authority* (CA). However, traditional certificates use a lot of memory space, making them a sub-optimal choice for most MBAN nodes. Many alternatives to classical PKIs have been suggested, like TinyPK, μPKI and L-PKI, where the latter is considered most suitable for WBANs in general [32]. Also certificateless solutions have been proposed [39], [40].

3.2 Privacy requirements

As mentioned previously, privacy of patient-related data must be guaranteed at all times to increase user trust and acceptance. Before deployment of MBAN applications, some important issues, like how data is stored, who has access to the patient's medical records, how data is handled in emergencies and many more must be tackled [41]. Several regulations are in place to ensure privacy of medical data the *General Data Protection Regulation* (GDPR) in Europe and the *Health Insurance Portability and Accountability Act* (HIPAA) in the USA provide a solid framework to correctly handle healthcare-related information, including both civil and criminal consequences [34]. In addition to the existing frameworks, MBAN applications that handle *Personal Identifiable Information* (PII) have to comply to the following principles, as proposed by [42]:

- The volume of raw data collection and the overall data volume requested by applications must be minimised, e.g. lower sampling rate, amount of data, recording duration etc.
- Individual users should not be identified, unless there is an explicit need.
- Collected information should be stored in a confined manner and as short as possible, keeping the retention period to a minimum.
- As much data as possible should be anonymized, minimizing the amount of exposed PII.
- Data should be low in granularity and encrypted when at rest.

However, it is important to note that being compliant to privacy regulations does not equal being secure. Data stored in MBANs may be leaked by physically compromising the system or independent nodes. Therefore, the security requirements from 3.1 and privacy requirements need to have a symbiotic relationship.

3.3 Security discrepancies

Although security is a crucial aspect in designing any kind of MBAN, it cannot be the main concern of the technology. Security needs to be an assisting metric that supports functionality, usability and safety. After all a technology is not used because it is secure, but because it can add value to existing processes or even revolutionise the way things are done. That is why there are several discrepancies between security and characteristics that make systems more vulnerable.

3.3.1 Security versus Usability

When looking at the responsibilities accompanied by MBAN applications it is of utmost importance that there is as less margin for user mistakes as possible. Meaning, that user interactions should be fool proof, as most of the times input is not provided by experts. For instance, when implementing node pairing mechanisms in MBANs, the bootstrap has to involve some manual interaction. More specifically, directly applying device pairing requires $O(n^2)$ human interactions [33]. Omitting this human component from the process can degrade security of the whole pairing process.

3.3.2 Security versus Accessibility

Imagine a scenario where a patient, equipped with an MBAN is brought into a nearby hospital during an emergency situation. The patient is unconscious and is unable to unlock his CCU or respond at all. Additionally, legit emergency staff is not authenticated and authorized to make any changes to the MBAN setup, so they are unable to help the patient. This is a scenario, where security is actually detrimental to the well-being of the patient. Therefore, controls need to be implemented to grant accessibility whenever needed. As one can imagine, there is a fine margin between the right amount of accessibility and security and finding the sweet spot is a very challenging task. Access should be granted to the right people but implementing to loose security protocols can potentially broaden the attack surface for adversaries.

3.3.3 Security versus Resource Limitations

Like already mentioned previously, MBAN nodes have very limited resources that need to be distributed between value adding functionality, maintenance functions and security controls. A strong security control, i.e. one that shows capabilities to fulfill the requirements of sections 3.1 and 3.2, also needs correspondingly high amounts of resources. This issue is especially pressing in MBAN applications, where nodes are very often not rechargeable and need to be replaced when out of battery [43].

3.4 Threat landscape

In order to design secure MBANs, it is necessary to exactly know the attack surface offered to an adversary. Since no system will ever be 100% secure and new vulnerabilities will always be found, attack methods are constantly evolving. As one can imagine, there are several possibilities to categorize the plethora of existing attacks. In MBANs, the attack surface can be split into horizontal and vertical panes, giving the attacker a two-dimensional selection. There are three distinct horizontal entry points, which coincide with the three tiers introduced in section 2.2. Each point of entry in the horizontal pane is accommodated by a vertical pane, which consists of the seven-layer *OSI* model [32]. Figure 3 shows the possibilities an attacker has to enter the network.

Using the entry points identified in figure 3, the exact attack surface for an MBAN can be discussed. Those attacks appear at the hardware, software and network protocol stage of each element in the corresponding tier.

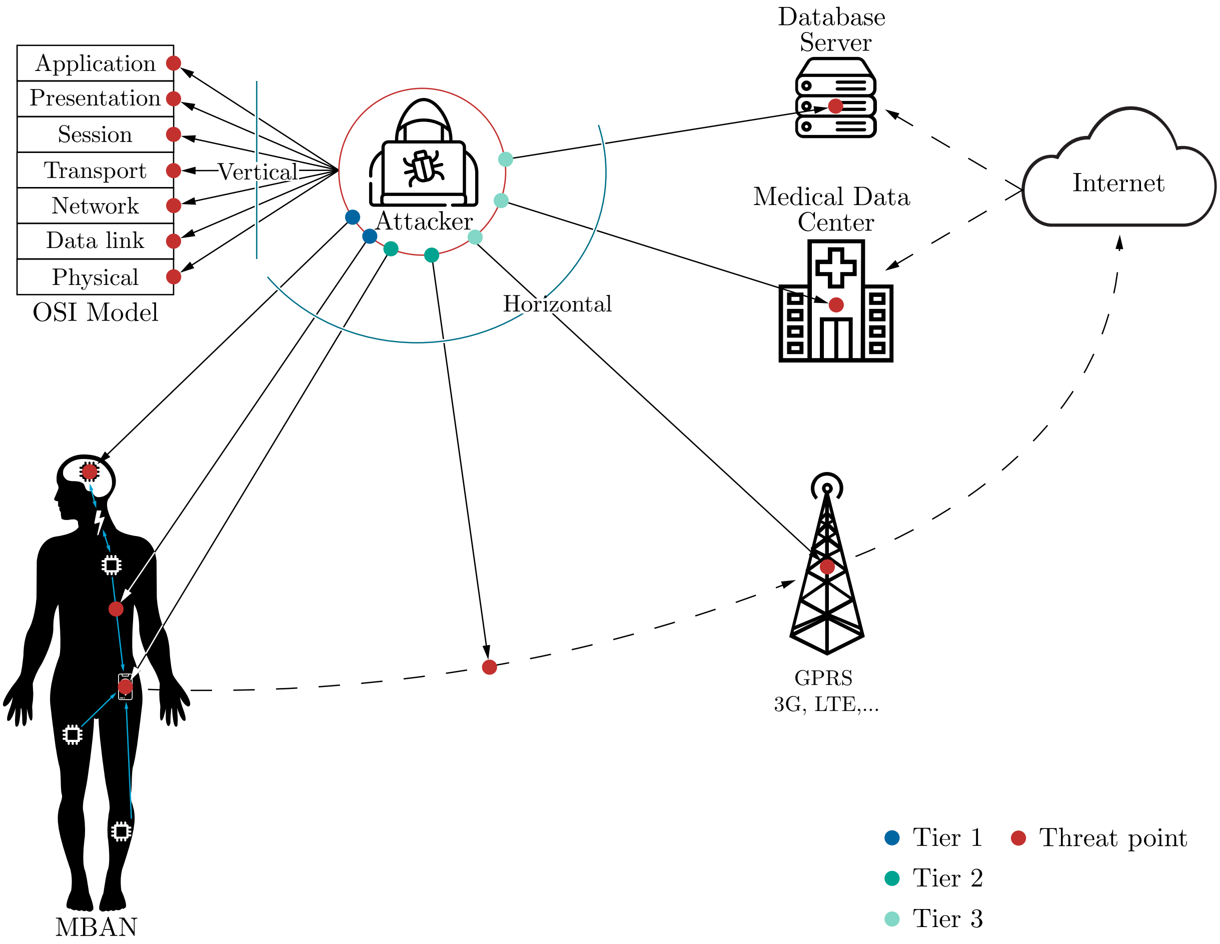


Figure 3: An overview of the entry points into a Medical Body Area Network offered to an attacker.

- **Direct attack on MBAN nodes:** This attack vector offers an adversary the opportunity to directly interact with a node. Thereby, the firmware, software or hardware of each node can be vulnerable, due to insecure software practices, unpatched firmware or faulty hardware design. Those vulnerabilities can be used to gain complete control over the node, leaving the entire application vulnerable to exploitation.

- **Attacks on intra-MBAN communication protocols:** Although most standard protocols used for this type of communication (e.g. Bluetooth, ZigBee, Ant, ...) are under vigorous testing and hardening, there is still a continuing flow of vulnerabilities being discovered. Sophisticated attacks on those protocols might include exploiting improper configurations, or not properly implemented security features.

- **Attacks on the CCU:** The control unit is most often the central node of the network, making it the most attractive entry point for potential attackers. To be able to process and access the data, applications installed on personal devices often possess elevated privileges, which can be abused if the application is not compliant to regulations or does not implement state-of-the-art security controls.

- **Attacks between CCU and gateway:** The connection between the control unit and the gateway is also vulnerable to interfering attacks, if not properly secured and configured. Various exploits can be applied to steal or modify transmitted, sensitive information.

- **Attacks between gateway and internet:** This connection is a popular target for attackers, as it is accessible from the outside world. Normally this link is protected by state-of-the-art security protocols, like SSL/TLS and IPSec. As those protocols are not MBAN specific they will be treated as a black box.

- **Attacks on medical servers and data centres:** Stored data on medical servers and in data centres has to be protected by various security controls. An attacker could attempt to infiltrate the data storage or cloud servers directly and steal sensitive information of multiple patients. But like in the previous attack vector, this area of the network should be secured by adequate access control mechanisms, robust encryption protocols and proper authentication and will thus be treated as a black box.

Once the correct entry point is chosen, two kinds of actions can be initiated, namely, active and passive attacks. In passive attacks data is only received and not written to the data stream. They do not facilitate changes to the data in the network, making them less intrusive. Active attacks on the other hand read and write to the data stream, possibly causing data corruption or Denial of Service. From an attacker's point of view both attack types have their advantages. Results obtained by active attacks might be more valuable and impactful, passive attacks are often very stealthy and hard to detect.
In fact, there are several ways in which attacks on MBANs can be classified. Alsubaei et al. [44] introduces a taxonomy of attack types on IoMT devices, which is shown in figure 4.

In the following, in-depth attack scenarios in tier-1 will be discussed, as the other tiers mostly rely on already established and well tested protocols.

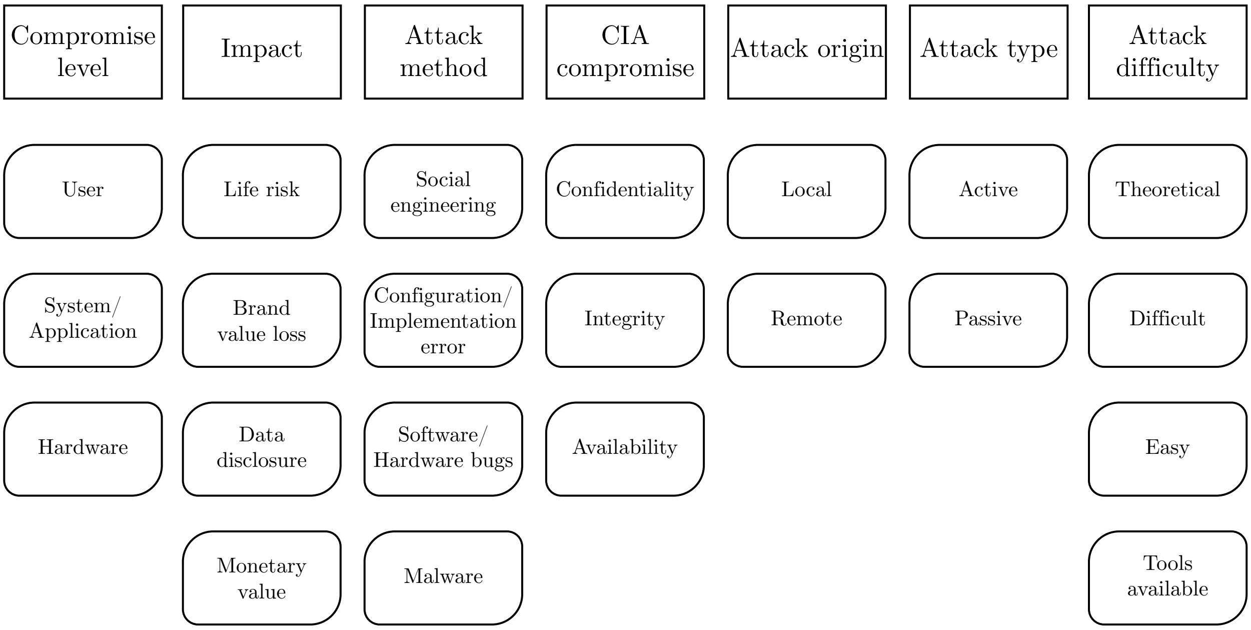
To get an up-to-date overview of the demonstrated attacks that have been conducted, on MBAN nodes of all of the categories presented in section 2.1, table I shows vulnerabilities in a variety of applications. As can be seen, the attack surface that is offered by those applications includes vulnerabilities on all levels of the OSI model. The most common attack methodologies that can be abused by potential adversaries will be explained in the following.

3.4.1 Physical layer attacks

Physical layer attacks involve interaction with the raw bit-stream of electronic signals. Most attacks usually involve transmitting signals in the same bandwidth as the original, thereby

Table I: A complete overview of demonstrated attacks on nodes typically used in MBAN applications.

MBAN node	Type	Functionality	Attack type	Layer	Vulnerability	Exploit
Animas OneTouch Ping Insulin Pump [45]	Semi-Invasive	Actuator	Eavesdropping	Transport	Packets between remote node and pump are sent in clear text.	An attacker can eavesdrop the traffic transmitted by the device and capture packets containing blood glucose and insulin dosage data.
			Impersonation	Transport	The CRC32 key used for pairing and authentication is statically used, and transmitted in the clear.	Attackers can sniff the CRC32 key and impersonate the remote node. This would allow them to remotely administer doses of insulin.
			Replay	Network	Communication between the pump and the remote node do not have any kind of replay protection (e.g. sequence numbers, packet identifiers, timestamps,. . .).	An attacker could capture commands sent to the pump and replay them at a later point in time, without specific knowledge about the packet structure.
Older generation ICDs [46]	Implantable	Hybrid	DoS	Data link	The short-range communication protocol is sent over the air in clear text and can be reverse engineered.	The wake-up protocol of the ICD can be exploited to continuously activate the RF module and thereby draining the battery of the device.
Newer generation ICDs [47]	Implantable	Hybrid	Replay/Spoofing	Transport	By intercepting the long-range communications between the ICD and the programming wand, messages can be reverse engineered due to the device relying on "security-through-obscurity". Intercepted messages always have the same header.	Intercepted messages can be eavesdropped by an attacker wearing a backpack with the right equipment and eavesdrop the data. This data can then be replayed at a later point in time, while being relatively close to the patient (e.g. in public transport).
			Eavesdropping	Transport	Sensitive patient data transmitted over the air is "obfuscated" by using a static Linear Feedback Shift Register (LFSR) sequence.	Attackers can passively eavesdrop the channel while an ongoing transmission and possibly gather private information about the patient. Eavesdropped information can potentially track, locate and identify patients.
			Impersonation/ DoS	Data link	The device does not immediately go to "sleep" mode after finishing communications, but to "standby" mode for five minutes. While in "standby", the device can be activated by sending a message, which is always the same.	It is possible for an attacker to impersonate the device programmer and repeatedly send "wake-up" calls to drain the battery or block legitimate traffic to depreciate patient safety.
FitBit fitness tracker [48]	Wearable	Sensor	Man-in-the-Middle	Application	Login credentials are sent in plain text and just secured by HTTPS without MITM protection.	Through modification of the smartphone app, attackers can associate trackers to another FitBit account and steal trackers.
			Firmware customization	Application	The BLE connection has Generic Attribute Profile (GATT) enabled, making it possible to remotely flash custom firmware on the device.	Custom firmware can override security protocols, making it possible to leak sensitive data to an attacker.
Hospira Symbiq infusion system [49]	Semi-Invasive	Actuator	Tampering/ Modification	Application	Pumps do not check incoming updates for authenticity. Corrupted libraries can be uploaded through the hospital network.	An attacker could transmit malicious commands to the infusion system, potentially directing the pump to perform unanticipated actions.
Hermes medical shoe [50]	Wearable	Sensor	Tampering/ Modification	Transport	The pressure sensor data and time between transmissions can be altered with sufficient access to the platform.	An attacker could tamper with the original data to interfere the diagnostic decision making process.
Drop sensor infusion pumps [51]	Semi-Invasive	Actuator	Sensor Spoofing/ DoS	Physical	Drop sensors are susceptible to signal injection of a spoofing signal using the same physical quantity. Alarm systems can be bypassed by using the right signal patterns.	By injecting an external high power signal into the drop sensor, the output can go into saturation, causing the drop counting mechanism to fail.



Compromise level	Impact	Attack method	CIA compromise	Attack origin	Attack type	Attack difficulty
User	Life risk	Social engineering	Confidentiality	Local	Active	Theoretical
System/ Application	Brand value loss	Configuration/ Implementation error	Integrity	Remote	Passive	Difficult
Hardware	Data disclosure	Software/ Hardware bugs	Availability			Easy
	Monetary value	Malware				Tools available

Figure 4: A taxonomy of possible attacks on an MBAN.

increasing the noise or changing signal phase. Attacks in the physical layer include:

Jamming Jamming or radio frequency interference uses, as the name suggests, radio frequencies that coincide with the signal frequency of the attacked node to interfere with and disturb transmitted signals. Thus, making the node inaccessible through wireless means, which is why this procedure is categorised as a Denial of Service attack. This method is however not capable of blocking large networks [7], but given the average size of MBANs, it is perfectly able to disrupt the network's function and induce packet loss.

Tampering and Impersonation In some scenarios an attacker might have physical access to the node, thus, creating the possibility to physically alter or even replace the node by an illegitimate one. The latter is called an impersonation attack, where the illegitimate node is modified in such a way that the network still accepts it, while enabling the attacker complete control over the device. Sometimes it is also possible to access sensitive information stored on the node, e.g. cryptographic keys or other PII.

Firmware modification Another way an attacker might exploit a node he has physical access to is to modify the installed firmware. Updates to this firmware are an essential part of device maintenance, especially for wearable devices. If an attacker is able to reverse engineer the firmware, he might be able to find and bypass all security checks that prove the legitimacy of an update. This would enable him to flash custom firmware onto the device, in which backdoors and malicious capabilities can be embedded.

3.4.2 Data link layer attacks

The data link layer is about transmitting frames (logical bits), which include information like the device's MAC address. This layer is especially prone to DoS attacks that can be classified as [32]:

Collision If an attacker finds the frequency with which data is transmitted by a node of the network, the data stream can be disrupted. By broadcasting on the same frequency, valid and invalid data packets collide, resulting in changes of the bit sequence, which in turn invalidate the data packet. Finding the exact frequency is most often a trivial task, furthermore invalid data packets can be sent from a significant distance, making it ever more important to implement adequate security controls like error-correcting codes [32].

Resource exhaustion If an attacker is causing a continuous stream of collisions, the node uses up energy for every wrongfully received transmission. If this is procedures is applied for a sufficient period of time, the node's energy resources will be depleted, resulting in packet loss and subsequent disruption of the communication link.

Unfairness If an attacker can intercept and manipulate the MAC layer priority mechanism, it is possible to give a particular node in the network a higher precedence rating than other nodes. This can be used to let nodes miss their transmission deadline and degrade the communication channel's capacities [32].

3.4.3 Network layer attacks

The network layer receives service requests, including packet source and destination information from the transport layer and forwards those packets to the data link layer. The routing protocols used can be exploited in many ways by potential adversaries. However, since most MBAN systems use a star or tree topology, in which a routing protocol is not needed, this type of attacks are only applicable for a small portion of MBAN applications.

Figure 5 shows an overview of internal, as well as external attacks carried out against the network layer of MBANs [52].

Internal attacks primarily concern matters of nodes within the network, either manipulating an existing or introducing a rogue node. Existing nodes may contain cryptographic keys that can be used to decipher sensitive information transported in the network. As malicious nodes are, if properly configured, trusted by the network it is a challenging task to discover not only the node itself but also the data transmitted by it [52]. In contrast, external attacks are launched from the outside and do not require any knowledge of the network's internal information, such as node identity or cryptographic keys [52]. Both internal and external attacks can act on every corner of the CIA Triad, more in-depth mechanisms will be explained in the following.

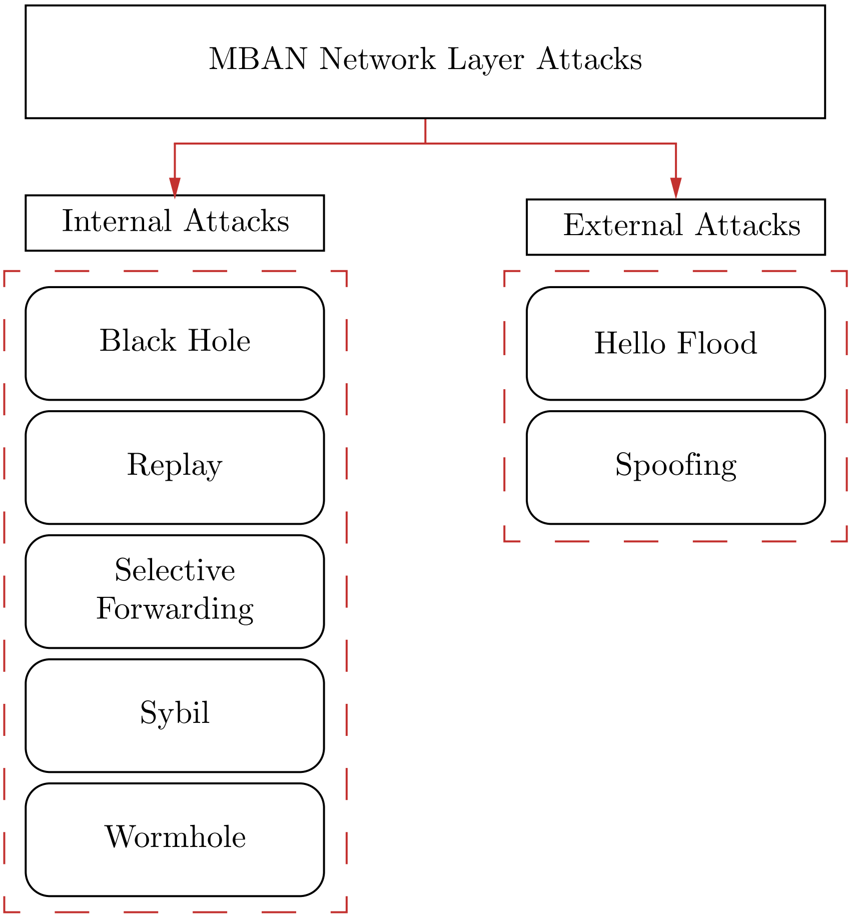


Figure 5: An overview of MBAN attacks on the network layer level.

3.4.3.1 Internal attacks

Black Hole When an attacker is able to introduce a malicious node into the MBAN, it is possible to configure it in a way that the routing protocol perceives it as a highly attractive data link (e.g. promoting zero-cost routines to adjacent nodes [41]). This results in a deception of the routing protocol, which rightfully redirects all traffic to the malicious node, as redirecting traffic to other nodes seems more costly. Subsequently, the malicious node drops all data packets, so that valid nodes in the network do not receive any more data. This causes operational functionality of the entire network to plummet.

Replay If information transmitted by MBAN nodes use static or predictable identifiers, it is prone to replay attacks. By intercepting and capturing information transmitted by the device an attacker can store the data packets on his device and, if needed, re-transmit the captured data at a later point in time. Thereby, the data packets can either be used for authentication purposes or to directly send commands to the node, granting the attacker illegitimate access.

Selective Forwarding In principle a selective forwarding attack is the same as a black hole attack. The only difference is that some selected data packets are allowed to proceed, while others are being dropped. Since the attacker is in full control of the malicious node, it is also possible to change routing information of the intercepted packets, which can be used to redirect them to wherever the attacker pleases. This kind of attacks are very hard to recognize and detect, as packet loss can also occur naturally through collisions and errors.

Sybil After successfully replicating a target node, an attacker can forge identifying data (e.g. MAC addresses, IP addresses, public keys, . . .) of valid nodes, so that it illegitimately expresses multiple identities, thus materialising itself in multiple locations at the same time. This kind of attack can then be used to either steal sensitive information from the network or attack the access point by sending huge amounts of data from the forged nodes and exhaust the network's bandwidth.

Wormhole By deploying two distant nodes into the existing network, it is possible for an attacker to create a tunnel between those two devices and control the routing process. In order for this to work, one of the malicious nodes has to advertise itself as low-cost for the routing protocol. This is typically achieved by claiming that the shortest routing path is through the malicious entity. This part of the two-ended wormhole now overhears the traffic of the network and subsequently forwards it via a high-quality wireless connection to the second malicious node, where similar procedures as in selective forwarding and black hole attacks can be employed.

3.4.3.2 External attacks

Hello Flood By adding a malicious node to the network and requesting routing information of all nodes an attacker is able to communicate with the entire network. This ability can be exploited by repeatedly sending useless messages to all nodes of the network with the help of high-power transmitters [32], thereby flooding the communication channels and exhausting the network's capabilities. Those useless messages can come in the form of *HELLO* packets, which occupy the buffer and cause subsequent packet loss in the node [53].

Spoofing In a spoofing attack the information that the routing protocol uses is falsified, in order to redirect data packets to another destination or to make the protocol believe that the packet originated from a different source. This type of attack is very prevalent on the network layer, as it does not require direct interaction with nodes. It much rather attacks the transmitted information directly, potentially giving attackers the opportunity to modify the routing topology to complicate the network [54].

3.4.4 Transport layer attacks

The transport layer offers a relatively big attack surface for an adversary, as it handles protocols for the end-to-end communication between individual nodes. Some of the attacks include:

Data modification If the transmitted data is not properly secured by security mechanisms, an attacker might be able to modify data after capturing it. The intercepted and modified data can either be forwarded directly (Man in the Middle) or replayed at a later point in time (Replay). This type of attack can be used to send falsified information to the control unit, causing malfunction of the application, or bypass authentication schemes to get a foothold into the network. Since an attacker does not need to be in direct vicinity of the target, implementing encryption and up to date transport layer protocols is crucial.

Desynchronisation If an attacker is able to forge the sequence number or control flags of an intercepted message, he is able to repeatedly transmit the message to its destination, thereby causing a desynchronisation of the end point's sequence number. The node reacts by sending the message again and again, trying to correct errors which never really existed in the first place [41]. Slowly depleting the node's energy resources and eventually making the node unavailable [54].

Eavesdropping This is one of the most common attack methods available in an attacker's arsenal and is often one of the beginning steps of an attack. Eavesdropping is the simple interception of data sent over the air, which if not properly secured through encryption and authentication mechanism can give away sensitive information. Most often it is very easy to intercept this data through antennas, without the need of being in close proximity of the network. This low execution requirements make eavesdropping a real danger for most networks.

3.4.5 Session, Presentation and Application layer

Usually, the layered architecture of MBANs and WBANs treats the last three layers of the OSI model as one. On this level, user sessions and software applications are the main targets, with attacks that can be classified in either one of the layers:

Sideloading and Drive-by-Downloads If the MBAN relies on central coordinator units that run on app-based systems, a user might be tricked into downloading a malicious version of the control app from a third-party app store or website. The former would be called *Sideloading* and the latter would be classified as a *Drive-by-Download*. Once the malicious app is loaded onto the device, an attacker can exploit its elevated privileges and control the data received and transmitted by the coordinator. This attack is especially relevant, as central coordinators, such as mobile phones offer a huge attack surface to potential adversaries. Another aspect is that in this kind of attack a user's decision to download a malicious app can undermine the system's security. This added social engineering aspect tremendously increases the vulnerable surface of the entire network.

Reprogramming attack Instead of loading a malicious application from a third-party app store it might be possible to directly reprogram the already installed application, in order to embed malicious code that gives an attacker access to the network. For instance, Tiny OS's Deluge programming system, which is used by some IoMT applications, offer the opportunity to reprogram devices remotely [41]. Since those tools are designed to work within a trustworthy environment, an attacker might hijack this functionality and use it against the system [41].

Chapter 4

Introducing the IEEE 802.15.6 standard

According to IEEE 802.15 TG6 the aim of this standard is to govern communications inside and around the human body. One of the main challenges is the definition of new physical (PHY) and medium access control (MAC) layers for MBANs, as well as the definition of frequency bands, as the used frequency bands differ from country to country [55]. In the following the key concepts and features of this standard will be introduced.

4.1 IEEE 802.15.6 requirements

In order for the standard to become established and successful, it has to fulfill certain requirements. The most important of those requirements are listed below [1], [19], [55]:

- MBAN links should support bit rates ranging from 10 Kbps to 10 Mbps
- Each MBAN should be able to support at least 256 nodes
- The packet error rate (PER) needs to be under 10% and the latency should be less than 125ms for medical and 250ms for non-medical applications
- Nodes should be added and removed from the network in less than 3 s
- While the patient is moving, i.e. sitting, walking, twisting, turning, running, dancing, etc., every sensor node should be able to provide reliable data transmission without losing packets
- MBANs need to incorporate ultra wide band (UWB) transmission in order to be able to communicate with different environments
- Energy saving and self-healing properties need to be implemented

4.2 IEEE 802.15.6 basics

4.2.1 Frequency bands

Since generally speaking, most countries govern the licensing of certain frequency bands themselves it can become challenging to create a homogeneous landscape to minimise interference [56]. Figure 1 shows a brief overview of frequency bands used in MBAN applications.

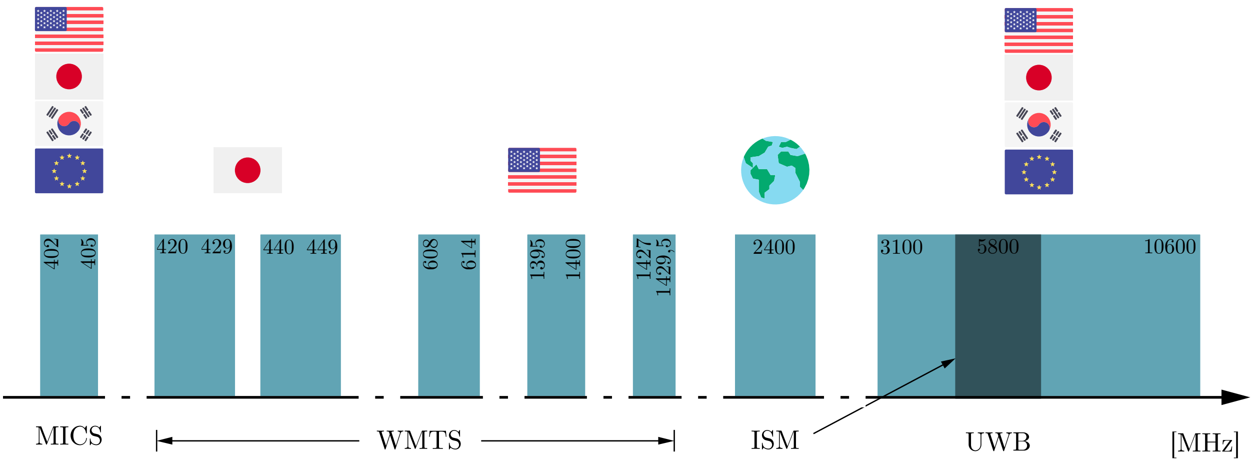


Figure 1: An overview of frequency bands used by MBANs, recreated from [55].

The most used frequency band is the spectrum used for industrial, medical and scientific (ISM) purposes. Both WiFi and Bluetooth mainly operate in the 2,4 GHz frequency band. Although this band supports very high data rates and is already standardised worldwide, there is a very high probability of interference. Two frequency bands specially licensed for medical applications are the *Medical Implant Communication Service* (MICS) and the *Wireless Medical Telemetry Services* (WMTS). Both do not support very high data rate applications [55], but the chance of interference is much lower than with the ISM band.

Another important aspect of any standard for a communication technology is the definition of communication layers. The actual number of those depends on the protocol and the application, but the two most essential layers are defined by IEEE 802.15.6 [57]. Those layers are the PHY and the MAC, which will be discussed in the following.

4.2.2 PHY layer

For binary data to be transmitted from node to node, a handling infrastructure needs to be created. This infrastructure is called the PHY, or physical layer. It is primarily responsible for establishing a reliable connection link between nodes, some tasks it performs are:

- Toggling of radio transceiver

- Data transmission and reception
- Perform clear channel assessment (CCA), i.e. checking if the communication channel is free

The standard supports PHYs in three different variants. Two mandatory ones, ultra wide band and human body communication and narrow band PHY as an optional layer. In the following a brief overview of the three operational PHY layers will be given, for a more in-depth explanation the reader may refer to Ullah et. al [58].

4.2.2.1 Narrow band PHY

The narrow band (NB) PHY's main goal is to establish communication with implanted in-body and wearable on-body nodes. The standard defines 230 physical channels and seven operation bands, alongside modulation techniques and data rates for a variety of frequency bands [59]. Mathew et al. [60]–[62] show how a NB transceiver could be implemented in hardware.

4.2.2.2 Ultra wide band PHY

The ultra wide band (UWB) PHY not only increases robustness, but it also aims to achieve low power consumption, high performance and low complexity. UWB is set to achieve data rates of up to 20 Mbps, which can be necessary for sensors monitoring multiple channels or high frequency signals, such as ECG or EMG. Also, video streams can be transported using this link, offering great advantages for endoscopic applications. In addition, it is compliant with the MICS power levels, making power exposure to the human body safer and the probability of interference lower [28], [58]. There are two different types of ultra wide band PHYs, namely impulse radio UWB (IR-UWB) and frequency modulation UWB (FM-UWB). They can operate in two distinct modes, default and high quality of service (QoS) mode. For this PHY, the standard defines 11 channels, which are divided into low band and high band groups [59]. Yuce et al. [63] confirm the feasibility of this approach, while Chávez-Santiago et al. [64] present an architecture for a MBAN using UWB technology.

4.2.2.3 Human body communication PHY

Human body communication (HBC) is physically realised using electric field communication (EFC). Instead of an antenna, the transmitter is implemented with digital circuits, thereby utilising two distinct technologies, namely, capacitive and galvanic coupling [65]. The RF-parts can also be omitted, making this technology very light-weight and low power. Although this technology does not see much real-life applications yet, it yields great possibilities and advantages in respect to the other PHYs. Seyedi et al. [66] gives a good overview on HBC also beyond the scope of IEEE 802.15.6, some of the mentioned advantages are listed here:

- **Less interference:** Since the transmitted signal is only propagating inside or directly on the body and the required frequency spectrum is way beneath the other communication types, the interference is by nature very low.

- **Low energy consumption:** As shown by Bae et al. [67] a HBC transceiver uses an energy of 0,24 nJ/b, which is an order of a magnitude lower than the energy consumption per bit of a UWB transceiver [68].
- **Reasonable data rate:** HBC offers a data rate of up to 10 Mbps, which is quite high compared to other communication protocols, like Bluetooth and ZigBee, but still lower than the 20 Mbps offered by UWB.

A possible disadvantage of this PHY is, that the sensor nodes constantly need to be in direct contact with the body, which is not always guaranteed with on-body devices like wristbands or watches.

4.2.3 MAC layer

Due to the variations in the nature of data being collected by MBANs, individual measurements need to be transmitted and processed on different channels. Therefore, the so-called *Medium Access Control* (MAC) layer is built on top of the PHY layer, with the aim to control channel access and allocate slots based on the category of collected data. Due to the multitude of restrictions faced upon when working with MBANs energy efficient slot allocation and access control management can become a challenging task. There were two basic design decisions made, one of them is a multiple access (MA) scheme and the other is a superframe structure, provided by the IEEE 802.15.6 standard [69].

The latter divides either the time axis or the channel into beacon periods or superframes of equal length, which contain allocation slots used to access the channel. Depending on the use case a central hub may transmit beacons of equal length to define superframe boundaries and allocate the slots. The superframe consists of different access phases, namely the exclusive access phases (EAPs), random access phases (RAPs), managed access phase (MAP) and the contention access phase (CAP) [58]. According to the standard the central coordinating hub has to allow three different access modes [28]:

- **Beacon mode with beacon period superframe boundaries:** Beacons are transmitted in active superframes by the hub.
- **Non-Beacon mode with superframe boundaries:** The operation of the hub is limited to MAPs only.
- **Non-Beacon mode without superframe boundaries:** In this mode only unscheduled allocations are provided by the hub.

Next to the access phases the standard also defines different mechanisms on how the data can access the channels:

- **Random access:** Slotted ALOHA or *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA)
- **Improvised and unscheduled**

- **Scheduled and scheduled polling**

In the slotted ALOHA mechanism nodes accessing the channel are assigned predefined user priorities (UP) which are used to classify and prioritize traffic [69]. CSMA/CA uses a sensing mechanism to find if nodes are already occupying the wireless channel. If that is the case, the CSMA/CA mechanism implements a random, short waiting period before sending the data until the channel frees up to avoid collisions. One can imagine that this access mechanism becomes more and more ineffective with the number of nodes, as the collision probability also increases. However, for a small number of nodes or networks with a low traffic volume, especially when strict timing constraints are in place, this method is greatly advantageous. A detailed review of the introduced principles can be found in [69].

There are also channel access mechanisms used by more common technologies outside of the IEEE 802.15.6 standard. The most popular are the already introduced CSMA/CA, as well as the *Time Division Multiple Access* (TDMA) mechanism [70]. Others include: *Collision Free Real Time Protocol* (CFRT), *Adaptive Data Transmission MAC* (AT-MAC), and *FrameComm* [71]–[73].

4.3 IEEE 802.15.6 security

The IEEE 802.15.6 standard does not only offer standardisation of MBANs' PHY and MAC layers, but also suggests controls that can be implemented to improve system security. It offers three distinct security levels, of which hubs (nodes managing the network's traffic) have to choose one during the security association:

Level 0 - Unsecured communication: If chosen, the network is left without any kind of security measures in place. Transmitted messages are sent in unprotected data frames without applying authentication procedures to protect confidentiality or integrity. The lack of privacy protection and security mechanisms leave the network wide open to a variety of attacks.

Level 1 - Authentication without Encryption: Here, security measures are implemented to guarantee only authenticated entities can receive, transmit or manipulate data frames. Message confidentiality and privacy are however not secured, as the data is not encrypted by any means.

Level 2 - Authentication and Encryption: This level combines the implemented authentication mechanisms with state-of-the-art encryption algorithms to protect the confidentiality and privacy of transmitted data. Therefore, this method offers the most extensive protection against attacks, resolving the problems of the lower security levels [58]. Some of the mitigated attack scenarios mentioned in the standard include message authenticity and integrity validation, confidentiality and privacy protection and replay defense.

While the first two levels may have certain use-cases, it is obvious that only level 2 can offer the desired security and privacy measures. Therefore, it is crucial that a well-designed MBAN system always chooses the highest security level available. The so-called *Security Suite Selector* (SSS) is thereby used to indicate which levels of security the connection should apply. It has bits for choosing the security level, the security association protocol and the used cipher function, as well as a bit to indicate if control frames to or from the sender need to be authenticated.

4.3.1 Security hierarchy and secured communication

Additionally, to the security levels introduced previously, the standard offers a clear guideline and implementation of how and when cryptographic keys are established and activated. Figure 2 shows the basic security hierarchy of IEEE 802.15.6, which is used to identify nodes and hubs. For this purpose, either a pre-shared or newly established master key (MK) is activated to open secure communications. In case of unicast communication, a pairwise temporal key (PTK) is created and shared once per session. For multicast communication on the other hand a group temporal key (GTK) is created and subsequently shared with the relevant group using the unicast method [55], [58].

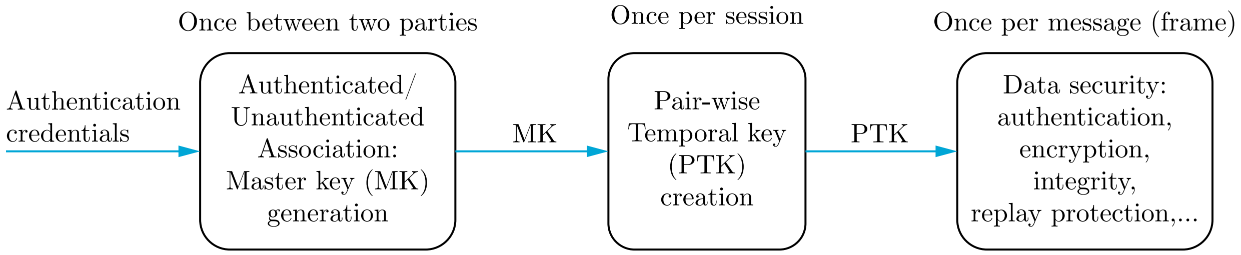

Once between two parties
Once per session
Once per message (frame)
Authentication credentials
Authenticated/ Unauthenticated Association: Master key (MK) generation
MK
Pair-wise Temporal key (PTK) creation
PTK
Data security: authentication, encryption, integrity, replay protection,...

Figure 2: Security hierarchy as specified in IEEE 802.15.6 [2]

Before establishing a secure communication to exchange data, a node-hub pair passes certain stages at the MAC level. Figure 3 shows the state diagram specified in the standard.

As can be seen, when establishing a secured communication MBAN nodes can be in four distinct stages:

Orphan: The goal of this initial stage is to activate a pre-shared or establish a newly created MK between a node and a hub. Additionally, if required, the two parties may authenticate each other before being raised into the *Associated* state. Thereby, communications between them are limited to Security Association and Control Unsecured frames. In case of failing to establish or activate a MK, the parties will remain in the *Orphan* state.

Associated: After successful establishment/ activation of a shared MK, the nodes are trying to create a shared PTK by exchanging PTK unsecured frames. In case of success,

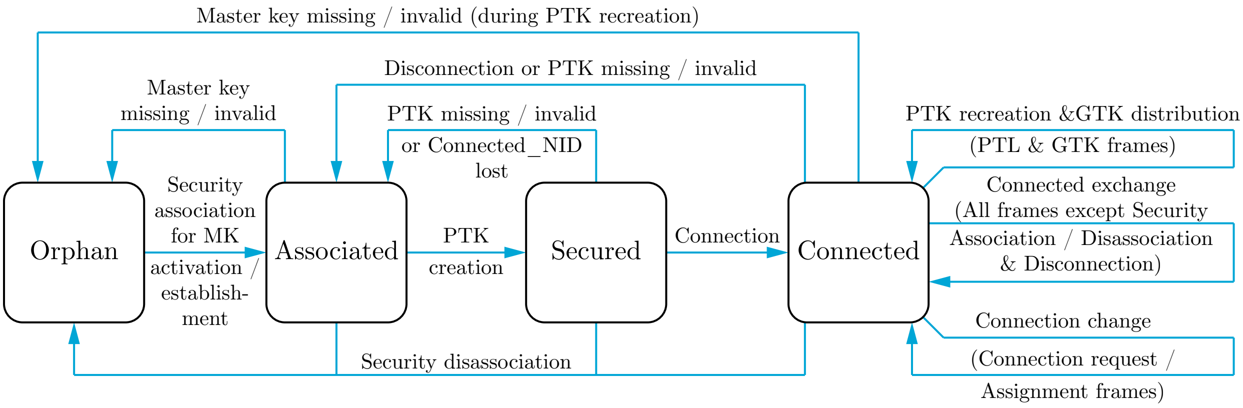

Master key missing / invalid (during PTK recreation)
Master key missing / invalid
Disconnection or PTK missing / invalid
PTK missing / invalid or Connected_NID lost
PTK recreation &GTK distribution
(PTL & GTK frames)
Connected exchange (All frames except Security Association / Disassociation & Disconnection)
Orphan
Security association for MK activation / establishment
Associated
PTK creation
Secured
Connection
Connected
Connection change
(Connection request / Assignment frames)
Security disassociation

Figure 3: IEEE 802.15.6 Mac layer security state diagram for secured communication [2]

both parties will advance into the *Secured* state. However, if they fail to create a PTK, both entities will remain in the current state. Furthermore, if their MK is missing or invalid, they transition back to the *Orphan* state, whereby each of the parties is allowed to transmit a Security Disassociation frame to its counterpart.

Secured: At this stage, node and hub are allowed to exchange Connection Request and Connection Assignment secured frames to establish a mutual connection and transition to the *Connected* state. If they fail to do so, both parties remain in the current state, if the PTK is missing or invalid, or the Nonce (Connected_NID) is lost they will transition back to the *Associated* state. To delete the current MK, both parties are allowed to send a Security Disassociation frame forcing the nodes to move back to the *Orphan* state.

Connected: This is the final stage of the security association procedure, the node and hub are connected and allowed to transmit any secured frames - except Security Association secured frames - to each other. The connected node holds an assigned Connected_NID, a wake-up arrangement and optionally scheduled and unscheduled allocations for abbreviated node addressing and desired wake-up. In case of a missing or invalid PTK both parties must return to the *Associated* state. To revoke the established connection and remove the current Connected_NID, wake-up arrangement and scheduled/ unscheduled allocations, both nodes are allowed to send a Disconnection frame to move back to the *Associated* state. To completely reset the connection the current MK is deleted, forcing the nodes to move back to the *Orphan* state. Thereby, both parties are allowed to send a Security Disassociation frame.

4.3.2 Security association and disassociation protocols

In order to establish a secure, mutual connection between nodes in the network, the standard offers five distinct *Authenticated Key Exchange* (AKE) and *Password Authenticated*

Key Exchange (PAKE) protocols for association, namely: unauthenticated, pre-shared MK, public-key hidden, display authenticated, and password authenticated association. Furthermore, the standard employs a protocol for the disassociation procedure and one for PTK creation/ GTK distribution. Whereby, association and disassociation describe the mechanisms of exchanging and erasing master and pair-wise temporal keys between a node and a hub, respectively. Protocols typically consist of a three-phase handshake, namely, request, response and activate (or erase). In this context, we call the party sending the first frame the Initiator I and its counterpart the Responder R.

The security association and disassociation phases, except the MK pre-shared association, implement a *Diffie-Hellmann* key exchange mechanism, which uses *Elliptic Curve Cryptography*, more specifically the P-256 curve from the FIPS Pub 186-3 secure hash standard, which is characterised by:

$$y^2 = x^3 + ax + b \ (mod\ p), with\ a, b \in GF(p) \tag{1}$$

$$4a^3 + 27b^2 \neq 0 \tag{2}$$

where (x,y) are points on the elliptic curve, (a,b) are coefficients, p is an odd prime number and GF(p) is a prime finite field.

If transported in a secure mode, message frames are encrypted using AES-128 in counter with cipher block chaining (CCM) mode, where a 13-octet nonce, containing both high and low order sequence numbers is required for each session to synchronise frames in order to mitigate replay attacks and guarantee data freshness [58]. Alternatively, the standard also offers the option to encrypt messages using the slower 128-bit Camellia cipher. However, this cipher does not offer any obvious advantages over its counterpart, using it may even bare some risks, as it is far less tested and established.

Throughout all of the protocols presented in the standard, association happens by exchanging so-called *Security Association frames*. Those frames include amongst other things the SSS to indicate which protocol should be employed, as well as the addresses of I and R. They also include bits for indicating the association status, which can be set as one of five states [2]:

- 0 - Joining the security association procedure
- 1 - Aborting the security association procedure with a different security suite selector
- 2 - Aborting the security association procedure due to lack of needed security credential
- 3 - Aborting the security association procedure due to temporary lack of resources
- 4 - Aborting the security association procedure due to security policy restrictions as imposed by the administrator/owner of this hub on the communications in its BAN

After receiving an Security Association frame, R immediately sends an Immediate Acknowledge (I-Ack) message to let I know that the message has been received and provide a time stamp for slot allocation. In the following the seven protocols described in the standard will be introduced and explained.

I - MK Pre-shared association: As already mentioned previously, this procedure does not employ a Diffie-Hellmann key-exchange protocol, as the corresponding secret MK is already pre-shared between node and hub. Since the MK is only activated and directly used for PTK creation, there is - according to the standard - no danger of impersonation attacks in the PTK creation procedure.

After receiving a Security Association frame, which is always initiated from the node, the hub answers with a second likewise frame to establish a secured connection or abort the session. If the first frame indicates that a connection should be established, the hub activates its pre-shared MK. Accordingly, if the node receives a frame from the hub, which indicates that a connection shall be established, the node activates its pre-shared MK. In both cases, the true identity of the sender is treated as unauthenticated.

Subsequently, both parties proceed to create the PTK and mutually authenticate each other using the previously activated, pre-shared MK.

II - Unauthenticated association: A big advantage of unauthenticated association is that there is no need for human intervention or a shared secret.

Again, only the node may initiate the association procedure by sending a Security Association frame, including the SSS, its Public Key (PK$_I$) and some other values to the hub. Upon receiving the frame, the hub answers with a similar frame, including its Public Key (PK$_R$). Subsequently, both parties compute a Diffie-Hellmann key and two distinct keyed hash-functions (KMACs), which are then transmitted in another Security Association frame. After each of the parties has received the newly computed KMAC and compared it to its own, the MK is activated. This happens only in case that the aforementioned check is successful, otherwise both nodes may abort the association procedure and the node may re-initiate it with a different SSS. Furthermore, if during the entire procedure a received PK turns out to be invalid, both node and hub can abort the procedure.

III - Public-Key hidden association: During this protocol, the node transmits its public key to the hub prior to the association procedure, typically through an OOB channel. As mentioned in the standard, this should mitigate the risk of an impersonation attack. After completing the transmission of its PK, only the node may initiate the association procedure, which is basically the same as in Protocol II, with the only difference that in the node's Security Association frames the PK is set to zero.

IV - Password authenticated association: Upon beginning the association procedure, the user must provide a secret password (PW), in this case a positive integer according to IEEE Std 1363-2000 to the node. This password is then used to compute a scrambled version PK_I' of the node's PK, by calculating $PK_I' = PK_I - Q(PW)$, where $Q(PW) = (Q_x, Q_y)$ is a function that builds a relationship between the given password and a point on the elliptic curve. Thereby, $Q_x = 2^{32} + PW + M_x$, where M_x is the smallest non-negative integer such that Q_x is the X-coordinate of a point on the elliptic curve and Q_y is an even, positive integer. After scrambling its PK, the node transmits it - alongside other values - to the hub. The hub also sends a Security Association frame, including its PK and unscrambles the node's public key by calculating $PK_I = PK_I' + Q(PW)$. Subsequently, both parties compute KMACs, which are then transmitted and compared. If the comparison is valid both parties proceed to activate the MK, thereby completing the association procedure. If at some point during the procedure a PK turns out to be invalid, the procedure can be aborted by both parties. Furthermore, if the hub sets the abortion flag in one of its Security Association flags, cancelling the course of action, the node may re-initiate the association procedure at a later point in time.

V - Display authenticated association: Similarly, to Bluetooth's numeric comparison, protocol V of the standard also bets on comparing a five digit number before activating the MK. Therefore, both node and hub need to be equipped with a display and either one of them must have some means to verify the equality of the displayed numbers. According to the standard, this mitigates the risk of man-in-the-middle attacks.

Before exchanging any frames, the node computes a *Witness A*, by - amongst other things - using a selected 128-bit nonce and its public key PK$_I$. Subsequently the node sends the first Security Association frame, which includes the newly computed *Witness A* and PK$_I$ to the hub, which reacts by answering with the second Security Association frame, including PK$_R$. Now, both parties compute two distinct KMACs and sequentially transmit and check their validity. After receiving the fourth Security Association frame, the hub independently computes a second witness, *Witness B* and compares it to *Witness A* received in the first frame. If any of the previously checks fail, the association protocol will be aborted. However, if all checks succeed, both parties calculate a five-digit integer and display it on their screen. If the user confirms that both displays are showing the same number, the MK is activated, and the association procedure is completed.

VI - PTK creation and GTK distribution: After successfully activating the 128-bit MK using one of the five association protocols, node and hub need to agree on a mutually shared PTK to secure the frames transferred between them. The PTK creation procedure may be initiated by either one of them and starts by sending a PTK frame, including both addresses, an individually, beforehand selected nonce, and PTK control bits. Those PTK control bits include the PTK creation status, which can be set as either one of the following states:

- 0 - Joining the PTK creation procedure
- 2 - Aborting the PTK creation procedure due to lack of shared master key
- 3 - Aborting the PTK creation procedure due to temporary lack of resources

- 4 - Aborting the PTK creation procedure due to security policy restrictions as imposed by the administrator/owner of this hub on the communications in its BAN

If the state is set to anything other than state 0, the Responder may abort the PTK creation procedure.

Subsequently, KMACs are computed, exchanged and compared by both parties. If all validations succeed, both hub and node proceed to compute and activate a secret PTK, by computing a cipher-based hash function (CMAC), including the previously established MK.

After agreeing on a secret PTK, the hub may initiate a GTK distribution procedure, where it transmits the GTK secured by the PTK to desired nodes.

VII - Disassociation: The security disassociation procedure implemented in the standard is fairly simple and effective. Either one of the participating parties may initiate the security disassociation to nullify the existing connection between them. After successfully sending a Security Disassociation frame, the sender deletes all information about the MK and the established PTK from its internal memory. Subsequently, the same is done by the receiver of the message.

4.3.3 Vulnerabilities and weaknesses

Like with any novel technology, establishing a reliable and secure framework around it needs to be an iterative process of improvement, as new zero-day vulnerabilities will most likely be found, even in protocols that have undergone extensive testing and validation. For instance, in 2014 the *Heartbleed* bug has been discovered in the *OpenSSL* protocol, one of the most widely used cryptographic software libraries to date. This bug allowed anyone on the internet to read the memory of systems protected by this protocol.

The IEEE 802.15.6 standard is no exception to this. Although, it offers an immense potential for future MBAN applications, there are still some key weaknesses that need to be addressed.

The standard is based on an MBAN architecture where a hub is the central coordinator of the network. All nodes are directly connected to the hub, creating a star topology. The problem is that the central coordinator represents a single point of failure (SPOF), meaning that if the hub is not able to communicate with the nodes, the network stops functioning as a whole. For an attacker with malicious intent this offers the opportunity to exhaust the hubs resources, by sending it a large number of invalid frames. As the hub needs to be equipped with superior computing, memory and energy resources, it is most likely not implanted in the body, making it even more accessible to the outside world. Physical theft or damage to the hub could have the same Denial of Service effect. The standard does not offer any kind of DoS protection; hence, it does not guarantee the required availability and robustness of the network.

There have also been found several severe vulnerabilities in the standard's association protocols, which will be discussed in the following. Toorani was the first one to recognize those vulnerabilities, the following analysis will mostly be based on his works [3], [74].

Protocol I The problems with this protocol lie not in the association procedure itself, but much rather in the ways the MK is shared between parties beforehand. If the key includes a default value it would make it vulnerable to key-guessing attacks. Another common problem with this method is the key-management process. The manufacturer has to generate and track MKs for all nodes and hubs they produce. Furthermore, when solely using this protocol, a dynamic and seamless addition of new nodes to the network will not be possible without the need of interaction with someone authorized to pre-share keys. This might become a problem in future MBAN applications, where it maybe is not sustainable to plan the entire network beforehand as more functionality might be added over time, making Plug-and-Play a hard requirement.

Protocol II As one can imagine, unauthenticated association does not provide extensive security features to protect the network from malicious attacks. Even though it might seem convenient to employ this association protocol, it leaves the system wide open to possible intrusions. As mentioned in the standard, the increased usability of this method leads to the system being vulnerable to impersonation attacks, as the lack of authentication mechanisms and forward secrecy enable anyone to establish a connection to the MBAN network. An Attacker could either impersonate node or hub, or even both at the same time to establish a MITM.

Protocol III This protocol is basically the same as protocol II with the only difference, that the node transfers its public key to the hub over an OOB channel. This procedure is based on a so-called *Security-through-Obscurity* approach, which means that the given security implementations are solely based on trying to hide and obscure the information to be protected. In this case, if an adversary plans on attacking the network, the node's PK might be intercepted by eavesdropping on the OOB channel. If in addition to that the private key of the hub is compromised, an attacker might impersonate the hub and illegitimately receive sensitive information from nodes. The fact that the OOB channel is only used for transmitting the PK from one node to the other seems unusual. Normally, the channel is used to host the entire association procedure, securing the process from adversaries. In this case, even if an attacker could eavesdrop the public key during the association protocol, only if malicious packages can be injected into the communication channel an attack would be successful. The standard does not specify details of the OOB band channel, making it important for the designer to implement well-known and secure concepts.

Protocol IV The password authenticated association relies on the user to enter a secret password into an input field of the node. Thereby it is assumed, that the node has some kind of input capabilities, which is problematic for implantable nodes for obvious reasons. The protocol itself was also found to be vulnerable to impersonation and offline dictionary attacks and does not provide forward secrecy. By eavesdropping both PK_I' from the first association frame transmitted by the node and PK_I from the following association frames, an adversary can reconstruct the function $Q(PW) = PK_I - PK_I'$. As the attacker now essentially has all the variables that are used for verification during the association procedure, the MK can be calculated, thereby successfully being able to impersonate the node. Although, this attack could potentially be mitigated by implementing an infrastructure that uses digital certificates, the protocol would still be vulnerable to a key compromise impersonation attack. By compromising the hub's secret key, the attacker could impersonate the hub and share a MK with the node, without the need of knowing the secret password. Additionally, digital certificates have a rather expensive toll on computational and memory resources of the network's nodes, which is why they are not recommended for MBAN applications.

In case an attacker eavesdrops messages between hub and node during a single protocol iteration, it is possible to obtain PK_I and PK'_I. Like already mentioned, the function $Q(PW) = Q(Q_x, Q_y)$ can now be calculated. Since $Q_x = 2^{32}PW + M_x$ and Q_x is now known to the attacker, this function can be used to verify the secret password. By brute forcing sequential values into this function, the adversary can now find the password through trial and error, without the need of an active connection to the network.

Protocol V Like the previous protocol, the display authenticated association implemented in the standard relies on a crucial assumption. Namely, that both parties have some kind of display to show a five-digit number used for validation. While this may be possible for some nodes, this is absolutely not suitable for implantable nodes. Furthermore, the hub needs a means to input a validation that confirms that both displays show the same value. It is assumed that users are trustworthy in confirming that both displays actually show the same number. Nodes also have to be trustworthy, in that the number shown on the display is actually the value computed during the association procedure and is not altered by an external, malicious party.

Besides those obvious weaknesses, the protocol is vulnerable to an impersonation attack and does not provide forward secrecy. However, the impersonation attack would still need physical interaction with the hub, to validate the numbers shown on the displays.

Protocol VI Although no exploitable vulnerabilities have been found in this protocol so far, the security of the PTK creation solely relies on the security of the previously computed MK. This means that this protocol is only as secure, as the security association protocols used to calculate the MK beforehand. By exploiting one of the previous vulnerabilities, an attacker will also be able to compromise the PTK creation procedure.

Protocol VII Like the previous protocol, security of the disassociation is also solely dependent on the security of the security association protocols. As the MK is the only secret parameter used by this protocol, any attacker that is able to compute a CMAC including the MK might initiate the disassociation procedure, thereby erasing MK and PTK from memory and pushing both parties back into the *Orphan* state.

Toorani also points out, that although the standard mentions that public keys need to be validated, the explanation of this validation is missing. In elliptic curve cryptosystems it is absolutely crucial to validate the ephemeral keys, as the values used for during the computation must be within certain boundaries. According to Toorani public key validations must include [3]:

- PK $\neq O$
- PK$_x$, PK$_y$ $\in$ GF(p)
- PK$_x$ and PK$_y$ must satisfy the defining elliptic curve equation

Here, O denotes a point at infinity on the elliptic curve.

If validations are left out, protocols II-V show additional vulnerabilities that could lead to impersonation and invalid-curve attacks. The former is initiated if an attacker chooses O as their public key. This simple trick would allow them to bypass authentication procedures and calculate a valid MK.

Chapter 5

Assessing and analysing the IEEE 802.15.6 standard

To assess the IEEE standard's weaknesses and short-comings in a broad number of dimensions, a structured, analytical method of analysis is needed. In this chapter such a method is introduced and subsequently demonstrated following the goal to give sound recommendations on how to improve the standard in future iterations.

5.1 Introducing the assessment procedure

The main goal of this analysis is to derive recommendations to refine and enhance the existing IEEE 802.15.6 standard. Thereby, a structured approach has to guarantee an extensive oversight of not only security, but also additional dimensions. To achieve that, additionally to the security requirements (SRx) defined in section 3.1, supplementary physical requirements are introduced. To get a better overview, figure 1 illustrates the relationship between all of the different requirements introduced in this chapter.

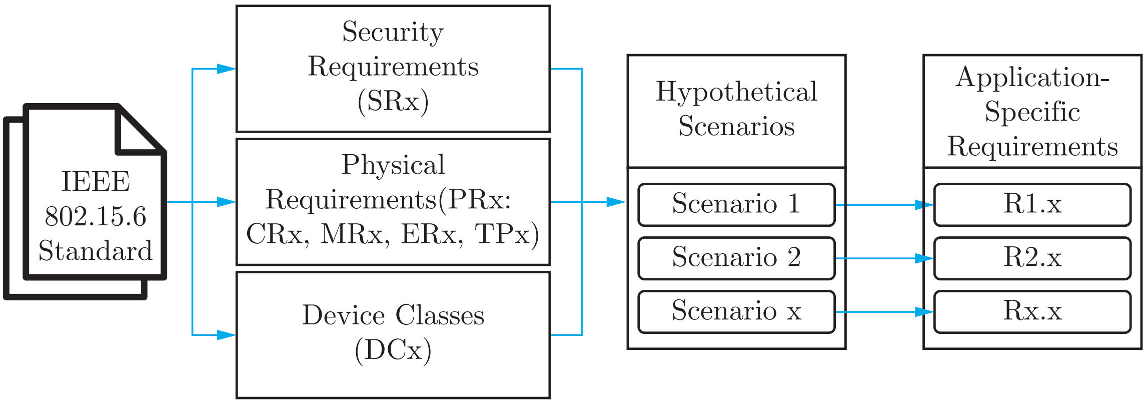

IEEE 802.15.6 Standard
Security Requirements (SRx)
Physical Requirements(PRx: CRx, MRx, ERx, TPx)
Device Classes (DCx)
Hypothetical Scenarios
Scenario 1
Scenario 2
Scenario x
Application-Specific Requirements
R1.x
R2.x
Rx.x

Figure 1: An overview of the different requirements used in this analysis procedure.

The IEEE 802.15.6 standard acts as the basis for this whole procedure. In order to be considered as secure, per the definition of this thesis, it has to fulfill a number of defined security requirements SRx (see section 3.1), supplementary physical requirements including a set of topologies PRx and cover the entire range of device classes DCx (i.e. the node types based on implementation from section 2.1). As seen in figure 2, the physical requirements PRx include the following areas: computational capacities CRx, memory capacities MRx, energy resources ERx and topology TPx.

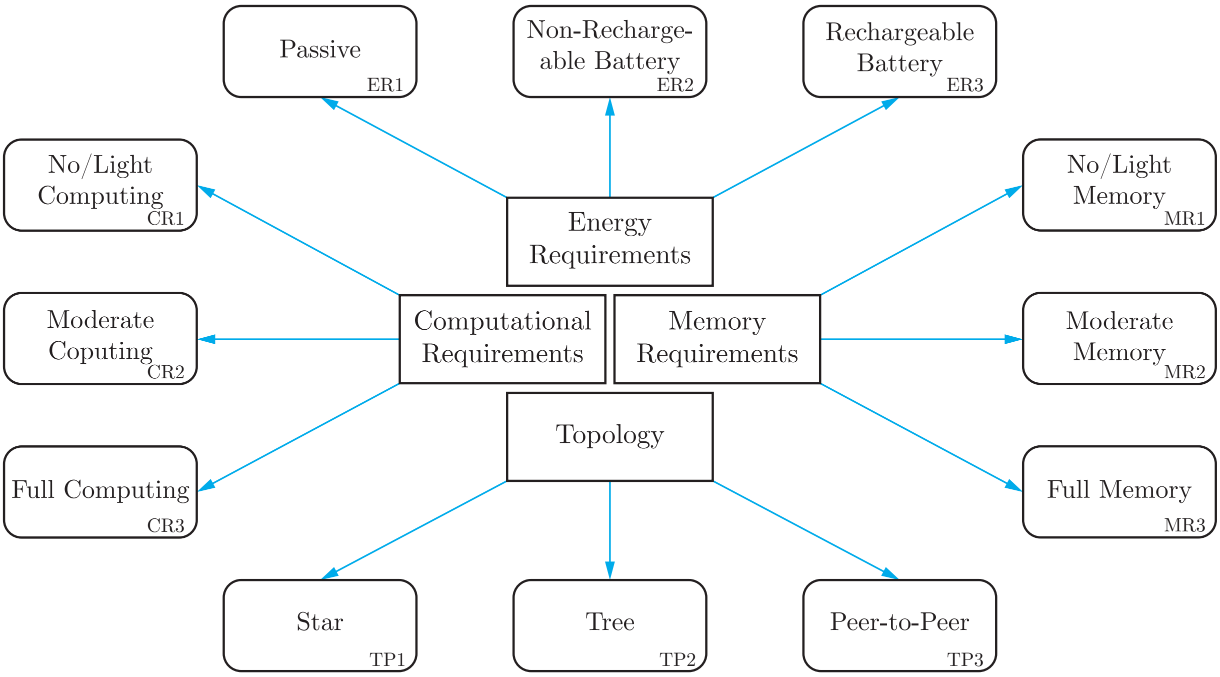


Figure 2: An overview of supplementary physical requirements (PRx) used in the assessment procedure.

The reason for including this additional set of PRx is that only including the SRx does not provide the whole picture. Each SRx has a specific impact on how the standard needs to treat hypothetical applications. The defined supplementary PRx capture that impact, thereby guaranteeing exhaustiveness of the analysis.

As seen in figure 1 the next step is to design rational and useful hypothetical scenarios covering the entire spectrum of defined requirements (i.e. SRx, PRx and DCx). Therefore, a two-dimensional matrix, as seen in Table I, is created. This matrix connects the range of requirements and the specific components (i.e. nodes) of each scenario. Only if the scenarios collectively require the fulfillment of each requirement and include all of the DCx, they can be considered as collectively exhaustive.

After the design of the scenarios is complete, for each scenario a number of application-specific requirements (Rx.x) are formulated (see the last step in figure 1). The application-specific requirements (Rx.x) are once again connected to the previous requirements (SRx and PRx) by using a similar matrix than the one seen in table I. This creates the possibility to

Table I: A preview of the matrix used to design exhaustive hypothetical scenarios in a structured manner.

		DC1	DC2	DC3	DC4		ER1	ER2	ER3	MR1	MR2	MR3	CR1	CR2	CR3	TP1	TP2	TP3		SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9	SR10	SR11
Scenario 1																														
	Invasive Sensor	●					●			●				●							●	●	●			●	●		●	
	Wearable CCU			●					●			●			●	●				●	●	●	●	●	●	●	●	●	●	●
	Semi-Invasive Actuator		●						●			●		●						●	●	●	●	●	●	●	●	●	●	●
Scenario 2																														
	...																													
	...																													
Scenario ...																														
	...																													

validate that the newly formulated application-specific requirements are covering the entire range of relevant dimensions, guaranteeing a comprehensive foundation for the subsequent in-depth analysis of the standard. The matrix including the application specific requirements (Rx.x) can be seen in Table II. Once again, only if all of the requirements (SRx and PRx) are collectively included in the application-specific requirements (Rx.x) the subsequent analysis can be considered as complete. Whether the list of Rx.x is complete or not does not matter in the context of this analysis, as long the Rx.x of each scenario collectively cover all of the requirements. To indicate to which degree the standard is fulfilling each requirement (SRx and PRx), the table is color coded in the following way:

- Red: The standard does not satisfy this requirement
- Yellow: The standard partly satisfies this requirement
- Green: The standard satisfies this requirement

The analysis is conducted by taking each of the application-specific requirements and assessing if the standard fulfills it. Prospective findings that appear during the in-depth analysis are documented, connected to the specific requirements and clustered into the following categories:

- Physical and organisational findings (PO.Fx)
- Cryptography, confidentiality and integrity findings (CC.Fx)
- Authentication and authorisation findings (AA.Fx)
- Other findings (O.Fx)

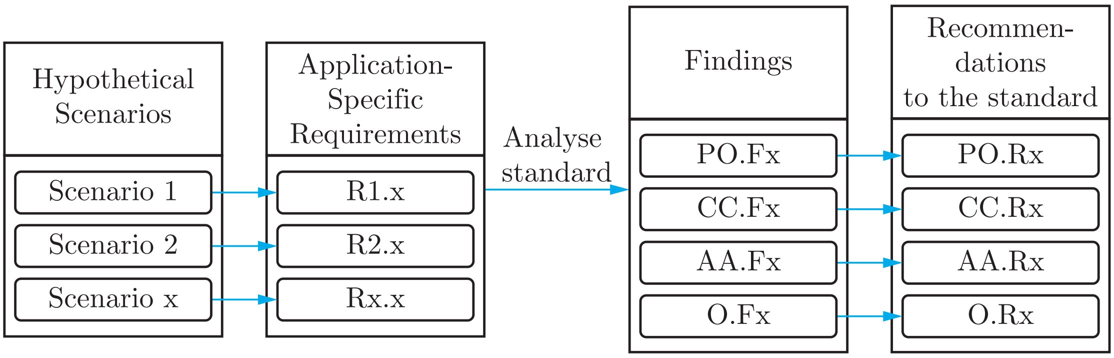


Figure 3: An Overview of the relationship between application-specific requirements (Rx.x), findings and recommendations to the standard.

Once the analysis is completed, recommendations on how to correct each of the prospective findings in order to improve the existing standard are given (PO.Rx, CC.Rx, AA.Rx and O.Rx). An overview of the relationship between Rx.x, findings and recommendations can be seen in figure 3.

Table II: An example of the matrix used to check if the created application-specific requirements (Rx.x) cover all of the dimensions.

		SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9	SR10	SR11	ER1	ER2	ER3	MR1	MR2	MR3	CR1	CR2	CR3	TP1	TP2	TP3
Scenario 1																								
	R1.1							🟩●																
	R1.2											🟨●												
	R1.3																		🟩●					
	R1.4																🟥●							
	R1.5												🟥●											
	...																							
Scenario 2																								
	R2.1	🟩●	🟨●	🟩●																				
	...																							
Scenario ...																								
	...																							

5.2 Designing the hypothetical scenarios

Since we have already defined all of the necessary requirements (SRx, PRx and DCx), designing the hypothetical MBAN scenarios is the first step of the process. While it is possible to create completely fictional scenarios which cover all of the necessary dimensions, this section concentrates on designing real-life, actively researched applications. It has to be mentioned, that although the following scenarios are currently being actively researched, there are still major issues to be addressed before they become feasible. However, in the context of this thesis it is assumed that the issues related to the basic functionality have been solved, as the main focus lies on the IEEE 802.15.6 standard and its analysis. In the following a number of hypothetical scenarios ordered by decreasing complexity will be introduced.

5.2.1 Scenario 1: Neural Dust

The concept of smart dust has been around for over 20 years and the initial thought behind it is still relevant. The principal idea is to establish a network of thousands of free-floating, independent, micron-sized sensor and actuator nodes (resembling the "dust") spread across the brain (neural dust) or in the intestines (body dust) for monitoring and stimulating purposes [75]. The neural dust concept is revolutionizing the way we think about traditional brain machine interfaces (BMIs), especially when thinking about chronic and long-term treatment. Increased biocompatibility by massively decreasing the form factor and adding encapsulation, eliminating wired connections and removing the necessity of a battery for implantable nodes make this technology so interesting. There are two main use cases that have been proposed for neural dust applications. On the one hand, sensory nodes can be implanted in the cortex to chronically record extracellular electrophysiological activities, which can then be sent to a medical server for further diagnostics. On the other hand, sub-cortically implanted actuator nodes may be used for deep-brain stimulation to treat a variety of diseases, like Alzheimer's and epilepsy. In the following, said sensor and actuator nodes implanted into the brain will also be referred to as *dust particles* or *dust nodes*. Figure 4 shows the basic topology of the used hypothetical neural dust scenario.

The created scenario is based on the well-established conceptual research of Seo et al. [75], which consists of three stages of communication. Multiple transceivers implanted beneath the dura mater communicate with, and power dust particles implanted into the brain's cortex and sub-cortex via ultrasound signals. The dust particles either read out electrophysiological signals or deliver stimulating signals to the tissue for deep brain stimulation. The backscattering of the incoming ultrasound waves of each individual particle is then again received by the sub-dural transceivers. Through the use of artificial intelligence, each particle's signal can not only be differentiated and uniquely identified by certain traits, but also simultaneously record multiple free-floating nodes [76]. In terms of security, the ultrasound communication between dust nodes and sub-dural transceivers does not employ any encryption algorithms, as assuming that the dust nodes can handle complex computations is unrealistic. The dust nodes rely on the inherent security of the ultrasound channel, which is secured through the touch-to-access principle. Siddiqi et al. recently validated the inherent

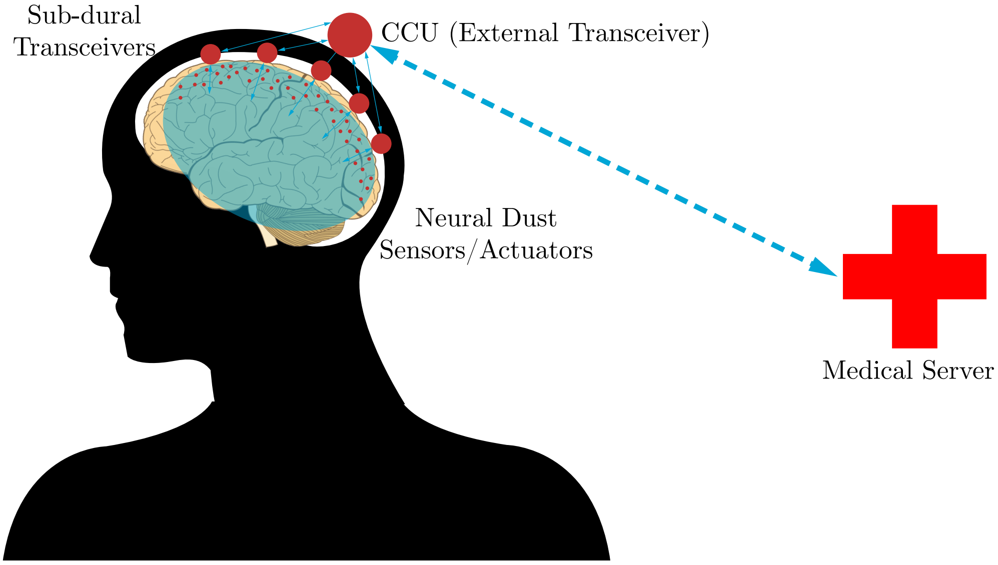


Figure 4: An overview of Scenario 1: Neural dust sensors and actuators spread across the brain, communicating with sub-dural transceivers that relay data to and from an external transceiver

security of this channel [77]. the Hence, an adversary has to get in contact with the patient to initiate an attack. In this scenario this is considered as a secure approach, as the cost for an attacker to come in physical contact with the patient and initiate a successful attack are unreasonably high when compared to other possibilities to do harm.

The sole purpose of the sub-dural receivers is, however, to relay information between the correct particles and a wearable, external receiver acting as the CCU. Although they are only used as relay nodes within the network, they have some computational and memory capacities to be able to compute various protocols. Furthermore, it is assumed, that the CCU has the computational means to coordinate the entire network's functionality and to establish a WiFi connection to a nearby router, eliminating the need for a personal device (e.g. mobile phone, smart watch). As sub-dural transceivers and CCU are separated by the skull, which blocks and attenuates ultrasound waves, a custom wireless protocol is used instead for communication. The wireless communication protocol utilizes a RF-channel that transmits data and simultaneously powers the sub-dural transceiver. In contrast to the communication between dust nodes and sub-dural transceivers, the communication between the sub-dural transceivers and the CCU is fully encrypted at all times.

Application-specific requirements:

- **R1.1:** Consider the passive, ultra-low resource character of dust particles and sub-dural transceivers (ER1, MR1, CR1)
- **R1.2:** Support the network's tree (extended two-hop star) topology (TP2)

- **R1.3:** Be scalable enough to support the great number of implantable sensor and actuator nodes (SR9)
- **R1.4:** Sufficiently encrypt messages between CCU and sub-dural transceivers at all times (SR1, SR2)
- **R1.5:** Support mutual authentication between CCU and sub-dural transceivers (SR4, SR6)
- **R1.6:** Guarantee that security keys can only be generated and used by legitimate parties (SR1, SR11)
- **R1.7:** Support sufficient flexibility that the network still functions if dust nodes or a sub-dural transceiver fails or is under DoS attack (SR3, SR8, SR10)
- **R1.8:** Ensure data frames are protected with non-repeating sequence numbers to mitigate the risk of eavesdropping and replay attacks (SR1, SR2, SR7)
- **R1.9:** Ensure messages can only be delivered to dust nodes via legitimate sub-dural transceivers (SR4, SR5)

5.2.2 Scenario 2: Leadless Cardiac Pacemaker

Conventional cardiac pacemakers are amongst the most used IMDs to date. The numbers of successful implantation of those devices are expected to keep rising, given the increasing age of the population and the rise in chronic diseases that come with it. Usually, they consist of a subcutaneous generator pocket alongside a transvenous lead for cardiac sensing and stimulation. Although this technology is widely established as the standard treatment for symptomatic bradyarrhythmias, in up to 12% of patients short term and in 6% long-term complications, like pneumothorax, cardiac occlusion, pocket hematoma, lead perforation, fracture and dislodgement can still occur [78]–[80].

Leadless cardiac pacemakers (LCPs) are trying to mitigate the risks associated with conventional pacemakers by decreasing the overall size and invasiveness of the components. Currently, there are two clinically available systems, namely the Nanostim Leadless Cardiac Pacemaker, by Abbott and the Micra Transcatheter Pacing System, by Medtronic. Both are completely self-contained and capable of providing single-chamber right ventricular pacing, sensing and rate response delivery [79]. However, those solutions currently show some functional limitations, as there are no capabilities for Cardiac Re-synchronisation Therapy (CRT) [81].

According to Tjong et al., in the future, LCPs will have an increased number of wirelessly interconnected components that are capable of not only pacing and CRT, but also leadless defibrillation therapy [79]. They will consist of multiple leadless pacers, heart rate sensors, pressure monitors and can also be combined with other novel devices and therapies. Currently, efforts are being made to combine LCPs and subcutaneous Implantable Cardioverter-Defibrillators (s-ICDs) into a single, interconnected ecosystem [82]. Figure 5 shows the basic topology of the created hypothetical scenario.

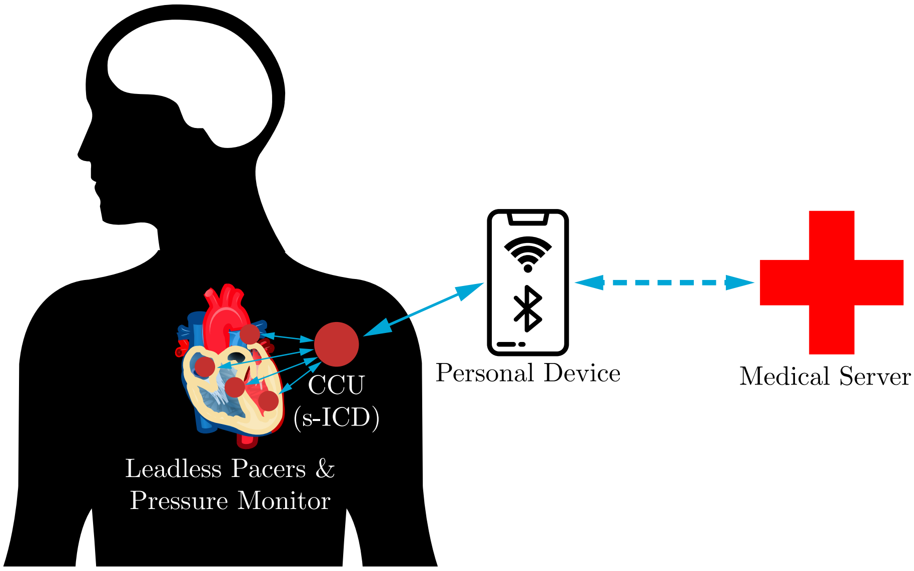


Figure 5: An overview of Scenario 2: A permanent LCP combined with an s-ICD that functions as the network's coordinator

As one can see, scenario 2 consists of multiple leadless pacers in the right atrium, both ventricles, a pulmonary artery pressure monitor and an interconnected s-ICD. Given their capabilities to record the heart rate and deliver treatment in the form of electrical impulses, leadless pacers are considered as hybrid devices, while the blood pressure monitor is a pure sensor. The s-ICD's device generator is used as the central coordinator for the entire LCP-network, as it offers the greatest resource capacities. It is not only positioned subcutaneously but also extra thoracic, making it relatively easy to access for reprogramming and replacing in case of device failure. Due to the generator being the network's coordinator and all the other nodes directly communicating with it, the network is arranged in a star-topology. For safety and resource purposes it is not assumed that the CCU will directly handle beyond-MBAN communications. Therefore, there is a possibility for the CCU to connect to a wearable or ambient personal device (e.g. mobile phone, smart watch, bedside reader, ...), which connects the network to the internet to transmit recorded medical data to a clinical server for further processing. The network's topology would in this case remain unchanged, as the PDA is treated as a mere relay node that connects the MBAN to the outside world. If the personal device is dysfunctional or not within communication range, recorded data is stored in memory until a secure connection to the personal device is established once again. The nodes and coordinator communicate with each other using intra-body communication. It is assumed that the implanted nodes have enough computational capabilities to encrypt the intra-body communication.

Application-specific requirements:

- **R2.1:** Consider moderate resource character of implantable nodes (ER2, MR2, CR2)

- **R2.2:** Support the network's star topology (TP2)
- **R2.3:** Make certain that keys stored on personal device are only accessible by authorized entities (SR5, SR11)
- **R2.4:** Dynamically associate/disassociate personal device to CCU, as the PDA will not always be in reach (SR9)
- **R2.5:** Make sure only registered PDAs can establish a connection to CCU (SR4, SR5, SR6)
- **R2.6:** Encrypt communication between implanted nodes, CCU and PDA (SR1, SR2)
- **R2.7:** Ensure mutual authentication between implanted nodes and CCU, and between CCU and PDA (SR4, SR6)
- **R2.8:** Support high availability and robustness of the system, given the high criticality of its function (SR8, SR9, SR10)
- **R2.9:** Ensure data frames are protected with non-repeating sequence numbers to mitigate the risk of eavesdropping and replay attacks (SR1, SR2, SR7)
- **R2.10:** Offer possibility to employ different short-range communication technologies for different parts of the communication (SR9)

5.2.3 Scenario 3: Artificial Pancreas

Type 1 diabetes is one of the most common chronic diseases to date. If blood glucose levels remain unmanaged a variety of micro- and macro-vascular diseases, like cardio-vascular or renal failure, limb amputations, vision loss or nerve damage can occur [83]. Despite intensive research, only reactive interventions are available and feasible to date. The most common is to manually administer insulin to lower blood glucose levels. Therefore, blood sugar is measured by pricking the finger to analyse a drop of blood, subsequently, glucose is manually administered by either an insulin pen or a pump. There are two types of issues with this traditional method: (a) Pricking the finger is rather uncomfortable and only gives information about the blood sugar levels at one specific point in time and (b) manually administrating insulin is error-prone, ineffective and inconvenient. However, two particular recent technological advancements in this field have enabled this process to be fully automated. *Continuous glucose monitors* (CGM) can be used to continuously measure real-time values of blood glucose levels. Usually, a CGM consists of a sensor to measure blood glucose levels placed just beneath the skin and a wireless rechargeable transmitter that is fastened on top to send collected data to the outside world. There are already several commercial products, such as the Medtronic Guardian Connect or the Dexcom G6 CGM system, which are both placed on the stomach. The second advancement are so-called *closed-loop insulin pumps* which are able to autonomously administer insulin without the need of any user intervention. An extension of that is a system that can administer both insulin and glucagon to also raise blood glucose levels if needed. Such systems are called *bihormonal insulin pumps* or sometimes also *artificial pancreata* since they essentially mimic the pancreas' function. While there is a lot of active research around those types of insulin pumps, no commercial systems exist to date.

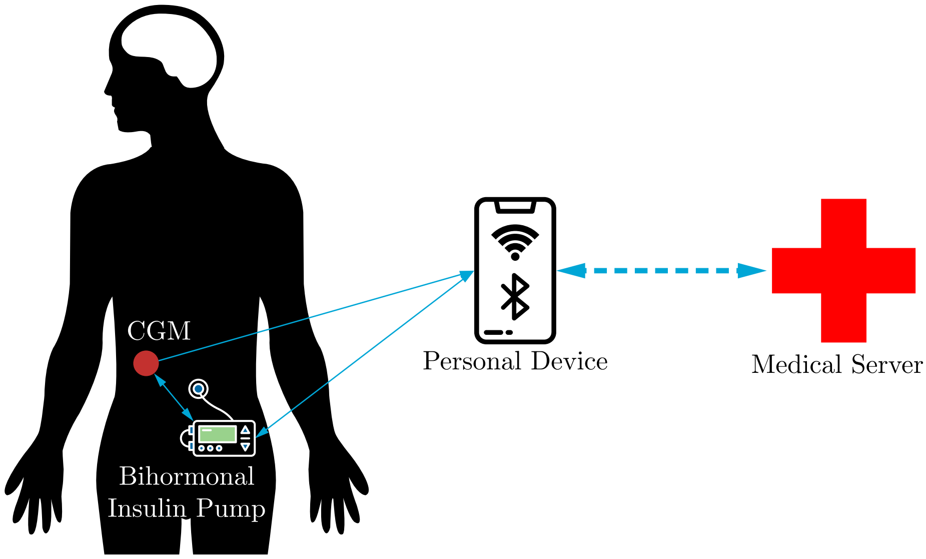


Figure 6: An overview of Scenario 3: A CGM system recording real-time blood glucose levels that transmits data to a closed-loop bihormonal insulin pump and a personal device for relaying data to a medical server.

In this scenario the functionality of a CGM and that of an artificial pancreas is combined in order to create an ecosystem to continuously monitor and regulate blood glucose levels. This ecosystem is visualised in Figure 6.

The CGM system records real-time blood sugar levels and transmits the data to a closed-loop bihormonal insulin pump, as well as a personal device (e.g. Smart Phone or Smart Watch). Besides the obvious functionality of the pump, it also provides extended memory capacities to store collected medical data if the personal device is not in reach. If the personal device connects at a later point in time the pump transmits the historical and current dosage data, as well as other stored medical data received from the sensor. It also acts as the network's central coordinator, handling security processes, medium access and power management. The personal device is used twofold: (a) It processes the received medical data and conveniently displays it, creating the opportunity for the patient to better understand how the body reacts to meals and physical exercise and evolve healthy habits (b) It acts as relay node to transmit data to a medical server for further processing and deeper analysis. The network is arranged in a peer-to-peer fashion, as each of the individual nodes need to be connected to each other to exchange data.

Application-specific requirements:

- **R3.1:** Consider high resource character of implantable nodes (ER3, MR3, CR3)

- **R3.2:** Support network's peer-to-peer topology (TP3)
- **R3.3:** Ensure full, heavy encryption of the peer-to-peer connections (SR1, SR2)
- **R3.4:** Guarantee that only an authenticated and authorised personal device can connect to the network (SR4, SR5)
- **R3.5:** Protect pump and CGM from DoS attacks, given the importance of their function (SR3, SR8, SR10)
- **R3.6:** Ensure the data transmitted by the CGM is up-to-date and not tampered with (SR2, SR7)
- **R3.7:** In case of a battery change the links need to dynamically associate/disassociate to each other (SR9)
- **R3.8:** Make sure keys are safely stored on each node and properly managed by the CCU (SR11)
- **R3.9:** Transmitted data needs to be clearly connected to the sender to prevent injection attacks (SR6)

To get a quick overview, table III summarizes the key-features of both hypothetical scenarios introduced in this section.

All of the introduced scenarios represent promising future applications that offer a variety of exciting functionalities and treatments. They collectively cover a wide range of possible challenges the IEEE 802.15.6 standard needs to address, table IV shows that the created scenarios cover the entire range of previously defined dimensions.

Furthermore, the three scenarios offer a unique set of application-specific, security and functional requirements which need to be fulfilled to ensure a secure and safe operation for future patients. Table V shows that the defined requirements are collectively exhaustive.

It is important to mention that the introduced scenarios offer a realistic enough subset of the entire range of possible applications to cover the needs of this analysis. The selected scenarios are merely a means to the end of analysing the IEEE standard, meaning that they are not the only scenarios to cover the defined range of requirements (SRx and PRx). This represents a heuristic bottom-up method to standardise the entire field based on a chosen subset. Furthermore, it is also not claimed that the use-cases are equally weighted by importance, however, the standard should treat all of the possible MBAN implementations regardless of popularity.

In the next step, it will be assessed if the standard does indeed fulfill all of the defined requirements or if there is still room for improvement, by exposing it to each one of the hypothetical scenarios' application-specific requirements.

Table III: Summary of the key-features of the three introduced hypothetical, futuristic application scenarios

	Scenario 1	Scenario 2	Scenario 3
Description	Cortically and sub-cortically implanted untethered, micron-sized sensors and actuators, communicating with sub-dural transceivers via ultrasound and backscattering that relay data to a wearable external transceiver. The external transceiver acts as CCU and has WiFi capabilities.	Leadless cardiac pacemaker network capable of CRT and bradycardia pacing therapy, combined with an s-ICD. The s-ICD's device generator acts as the CCU that collects and relays data and instructions from implanted nodes to a personal device.	Artificial pancreas system with a CGM transmitting blood glucose levels to a bihormonal insulin pump as well as a personal device. The pump acts as the network's CCU and coordinates the peer-to-peer connection between nodes.
Node functionality	Sensors: EMG signals, recording of extra-cellular activities Actuators: Deep brain stimulation Relay: Sub-dural transceivers CCU: External transceiver	Sensors: Heart rate, blood pressure Actuators: Leadless pacer (Vagus nerve) Hybrid: Leadless pacer (right atrium, right ventricle, left ventricle) Relay: Personal device (mobile phone, smart watch, etc.) CCU: s-ICD device generator	Sensor: Continuous Glucose Monitor (CGM) Actuator CCU: Bihormonal, closed-loop insulin pump Relay: Personal device (mobile phone, smart watch, etc.)
Network topology	Tree	Star	Peer-to-Peer
Number of nodes	Sensors/actuators: > 1000 Relay nodes: 5 CCU: 1	6	3
Node size	Sensors/Actuators: micron-sized Relay: mm-sized CCU: ca 5 cm	Sensors/Actuators: ca. 1 cm CCU: ca. 5 cm	Sensor: 3 cm Relay: ca. 5 cm CCU: ca. 5 cm
Node implementations	Invasive: Sensors, Actuators, Relay Wearable: CCU	Invasive: Sensors, Actuators, Hybrids, CCU Wearable/Ambient: personal device	Semi-Invasive: Sensor, Actuator CCU Ambient: personal device
Communication technologies	Dust particles to sub-dural nodes: ultra-sound and backscattering Sub-dural nodes to CCU: RF communication with custom wireless protocol CCU to router: WiFi	In-body nodes to CCU: intra-body communication CCU to PDA: RF communication with custom wireless protocol PDA to medical server: WiFi, GPRS	All nodes: RF communication with wireless protocol (Custom, Bluetooth, ZigBee, etc.)
Transmission distance	max. 10 cm	In-body nodes to CCU: 5 - 15 cm CCU to PDA: 0,1 - 5 m	Sensor to CCU: 20 - 30 cm Sensor CCU to personal device: 0,1 - 5 m
Complexity	very high	moderate	low

Table IV: The three hypothetical scenarios are covering the entire range of relevant dimensions on top of the already defined security requirements, guaranteeing their exhaustiveness.

		DC1	DC2	DC3	DC4		ER1	ER2	ER3	MR1	MR2	MR3	CR1	CR2	CR3	TP1	TP2	TP3		SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9	SR10	SR11
Scenario 1 Neural Dust																														
	External Transceiver (CCU)			●					●		●				●		●			●	●	●	●	●	●	●	●	●	●	●
	Sub-dural Transceivers (Relay Nodes)	●					●			●				●						●	●	●	●			●	●	●	●	
	Dust nodes (Sensors/Actuators)	●					●			●			●							●	●					●				
Scenario 2 Leadless Cardiac Pacemaker																														
	s-ICD Device Generator (CCU)	●						●			●			●			●			●	●	●	●	●	●	●	●	●	●	●
	Mobile Phone/PDA (Relay Node)				●				●			●			●					●	●		●	●	●	●		●	●	●
	Leadless Pacers (Hybrid)	●						●			●			●						●	●	●	●		●		●		●	
	HR & BP Monitor (Sensor)	●						●			●			●						●	●	●	●			●	●		●	
Scenario 3 Artificial Pancreas																														
	CGM (Sensor)		●						●		●			●			●			●	●	●	●	●		●	●	●	●	●
	Bihormonal Insulin Pump (CCU/Actuator)		●						●			●			●					●	●	●	●	●	●	●	●	●	●	●
	Personal Device (Relay Node)				●				●			●			●					●	●		●	●	●	●		●	●	●

Table V: This matrix shows how the application-specific requirements (Rx.x) correlate with the security and physical requirements (SRx and PRx).

		SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9	SR10	SR11	ER1	ER2	ER3	MR1	MR2	MR3	CR1	CR2	CR3	TP1	TP2	TP3
Scenario 1																								
	R1.1												●			●			●					
	R1.2																						●	
	R1.3									●														
	R1.4	●	●																					
	R1.5				●		●																	
	R1.6	●										●												
	R1.7			●					●		●													
	R1.8	●	●					●																
	R1.9				●	●																		
Scenario 2																								
	R2.1													●			●			●				
	R2.2																					●		
	R2.3					●						●												
	R2.4									●														
	R2.5				●	●	●																	
	R2.6	●	●																					
	R2.7				●		●																	
	R2.8								●	●	●													
	R2.9	●	●					●																
	R2.10									●														
Scenario 3																								
	R3.1														●			●			●			
	R3.2																							●
	R3.3	●	●																					
	R3.4				●	●																		
	R3.5			●					●		●													
	R3.6		●					●																
	R3.7									●														
	R3.8											●												
	R3.9						●																	

5.3 Putting the IEEE 802.15.6 standard to the test

The assessment will follow a clear and structured procedure, where the application-specific requirements are tested against the standard one-by-one. Eventual abnormalities will be documented and inserted in the color-coded requirements matrix defined in section 5.1 (as previewed in table II).

Scenario 1: Neural Dust

R1.1: The IEEE 802.15.6 standard claims to be designed for low power devices, supporting data rates up to 10 Mbps, while keeping the specific absorption rate (SAR) to a minimum. On a MAC level, the standard provides recommendations for power management of nodes, where those have the ability to be put into a hibernation and sleep mode for energy saving purposes. Although, sub-dural transceivers and implanted dust nodes are of passive nature, this is still relevant for the external transceiver, as it is battery powered and the main source of energy for the entire intra-MBAN network. That means that if the external transceiver is not powering the sub-dural transceivers via RF power transfer, the underlying nodes are always in a hibernation/sleep state. At the PHY layer the standard offers the possibility to employ UWB communication, which is a proven technology for ultra-low power devices. Specifically, UWB-RFID is a promising technology for the communication between external and sub-dural transceiver. However, it is still not clear if the sub-mm sized sub-dural transceivers and the even smaller dust nodes have enough overhead to compute the standards protocols and features.

R1.2: The standard dictates the network topology by limiting the number of hubs in a BAN to a single one. The topology discussed in the standard is a star with the possibility to employ a two-hop star extension, which is needed for this scenario.

R1.3: The maximal number of nodes supported by the standard is specified in the parameter *mMaxBANSize*, which is equal to 64. Considering that a neural dust application must support thousands of individual dust particles, this number is not sufficient. The standard does not specify where this limitation comes from, it can only be assumed that computational and memory resources of the CCU might be seen as limited in that they cannot support a higher number of nodes.

R1.4: To see if the standard fulfills this requirement, certain assumptions about the computational capacities of the sub-mm, sub-dural transceivers have to be made. Although the transceiver's form factor is in a range where Moore's law limits their computational capacities, it is assumed that in contrast to the micron-sized dust nodes they still have sufficient processing power to handle complex cryptographic algorithms. As discussed in chapter 4.3.2, the IEEE standard employs association protocols based on ECC. For encryption, AES-128 is used, which is a state-of-the-art encryption algorithm without any currently known vulnerabilities. The Camellia-128 cipher function offers a solid alternative even though it is inferior to the AES-128 algorithm in terms of speed. There are, however, readily available larger key sizes (e.g. 192, 256 bits), which drastically improve security that are not mentioned in the standard. In the future it might be necessary to fall back on those larger key sizes to guarantee message security. Given that the transceivers can handle the computational overhead needed for calculating the needed algorithms, this requirement can be considered as fulfilled.

R1.5: The standard mentions mutual authentication for two of the five association protocols, namely the MK pre-shared (Protocol I) and the Display authenticated (Protocol IV) protocol. Protocol IV, however, is not valid in this specific scenario, as the CCU does not have a display to authenticate the 5-digit number. Protocol I ensures mutual authentication by using the pre-shared, readily activated MK, while simultaneously initiating the PTK creation procedure. The exact workings of the mutual authentication procedure are not mentioned in the specifics of the standard. For the remaining 3 protocols the standard does not specifically mention mutual authentication, which is why this requirement is only partly fulfilled.

R1.6: The standard uses a variety of keys, e.g. PK, MK, PTK, GTK to handle association and authentication. Thereby, secure key management is crucial to mitigate the risk of keys being compromised. There are detailed protocols to generate, distribute, refresh and revoke keys offered and employed by the standard.

R1.7: In case of node failure, a protocol must be in place to communicate the occurrence of a failure to the hub and in sequence further to the medical server, where actions can be decided. Failure of individual dust nodes might be tolerable to a certain degree, without having to initiate intervention procedures. Thereby, the standard must account for changes in the network topology and computational overhead of the network's nodes. The standard does not specify what happens if a node disconnects in case of failure, in fact, node failure is not mentioned at all. Additionally, the standard does not include measures to improve dependability in terms of security.

R1.8: To ensure message freshness and protect against replay attacks, the standard implements a so-called *low-order security sequence number* and a *high-order security sequence number*. If a frame is secured with the same PTK or GTK, the value of the low-order number increments by one. This is also true for re-transmission of previous frames. If a node or hub receives frames that would lead to the high-order SSN to wrap around zero, it will be discarded. The same will happen if the value of the low-order SSN of the current frame is not higher than that of the previous frames.

R1.9: The security paradigm mentioned in the standard offers the possibility to authenticate control type frames during security frame exchanges between external and sub-dural transceivers. As mentioned in chapter 4.3, the SSS can be used to specify if either level

1 or level 2 of the security levels shall be employed. The main tool of authentication are Cipher-based message authentication codes (CMACs) algorithms, as specified in the NIST Special Publication 800-38B, which are then derived to compute KMACs and a MK. CMACs are considered to be energy efficient and memory saving, if the authenticated messages are in the range of one or two blocks, which is very small [84]. The presence of the MK assures that only authorized entities are able to verify the computed authentication codes.

Scenario 2: Leadless Cardiac Pacemaker

R2.1: For this scenario, the low-power measures and protocols offered by the standard are considerate of the application-specific restrictions. The individual, implanted nodes have sufficient capabilities to handle complex computations, like processing the electric field communication that is used for the human body communication PHY in the standard. Additionally, the power management options provided by the standard (i.e. nodes being able to hibernate/sleep) aid to save power resources if there is no need for the nodes to transmit or receive data.

R2.2: As already mentioned in the previous scenario, the standard supports networks with a star topology, meaning this requirement is satisfied.

R2.3: As already established in the previous scenario, the standard does not offer any recommendations on how to securely store generated keys. In this scenario the CCU is implanted beneath the patient's skin, enabling the device a certain degree of inherent security. Even though - given the increased difficulty to access the device - key management measures for keys stored on the CCU are less stringent, this is not the case for key stored on the personal device. Here, very strict security controls have to be in place to ensure keys are not stolen and used for malicious purposes.

R2.4: The association and disassociation frames specified in the standard are employed to regulate connections between a hub and accompanying nodes. Based on the so-called connection status field, connection requests are categorized and decided if a connection can be established or if it shall be terminated. While this is sufficient in most situations, the standard does not treat cases where nodes unexpectedly or abruptly terminate an already established connection, e.g. through failure or an empty battery, thus, not having an opportunity to send a disconnection frame. It does, however, support dynamic association by sending connection request frames if the PDA is in reach.

R2.5: Although the standard has protocols in place to ensure a hub-node pair follows a specific security hierarchy when initially establishing a mutual connection, basically any node following the specified frame formats can initiate a connection. If the node follows the specified processes to generate a SSS, as well as a valid public key and other security frames, there is nothing stopping a malicious actor to connect a node to the network, as no access control list or other medium to track legitimate nodes is discussed by the standard. Hence, this requirement is not satisfied.

R2.6: The AES-128 and Camellia-128 ciphers offered by the standard are a valid choice to encrypt messages between hub and nodes. Furthermore, the ECDH key exchange protocols, although computationally expensive, are an established method to exchange keys in a secure way. When looking at the security paradigm, only if security level 2 (authentication and encryption) is chosen at the beginning of the security association procedure frames will be encrypted.

R2.7: As already discussed when assessing the first scenario, the standard only specifically mentions mutual authentication for the association protocols I (MK Pre-Shared) and IV (Display Authenticated). Once a PTK is established between a hub-node pair, the origin (i.e. the sender's address) is corroborated using CCM mode of the AES algorithm is used every time a message is transmitted. On the control frame level, frames are also authenticated using AES in CCM mode, as well as message integrity codes (MICs), as they are called in the standard.

R2.8: Although the standard provides measures to increase robustness at a bit-level (e.g. bit interleaving prior to modulation), as well as at the PHY and frequency band level (e.g. UWB, FM-UWB), it does not discuss robustness against security threats. There are no controls in place to detect or actively prevent intrusion in the network, neither is protection against DoS attacks considered which can have a detrimental effect on the system's availability. Furthermore, the standard does not at all discuss the threat landscape or possible attack scenarios in order to improve availability and robustness, which is why this requirement is considered as not satisfied.

R2.9: As already mentioned in the previous scenario, the security sequence number used in the standard aid to protect messages from replay attacks and ensure data freshness. Hence, this requirement can be considered as satisfied.

R2.10: The three distinct PHYs employed by the standard, namely narrowband, ultra wideband and human body communication are not restricted to a specific communication technology, as long as the high-level technology is able to process the PHY-specific requirements. It lies within the design of the standard to offer a common foundation for novel or already established communication technologies to build upon. Therefore, this requirement can be considered as satisfied.

Scenario 3: Artificial Pancreas

R3.1: As already mentioned in previous requirements, the standard is designed for ultra-low power devices, with data rates of up to 10Mbps. Given the high resource capabilities of the devices used in scenario 3, the protocols of the standard can be easily computed and handled in terms of resource allocation. Hence, this requirement is fulfilled by the standard.

R3.2: The standard only mentions that a star topology is used for medium access. Additionally, a two-hop star extension can be employed. The peer-to-peer topology of scenario 3's network is not discussed, which is why this requirement is not fulfilled.

R3.3: The standard offers three security levels from which the application's designer can choose from. Here, only level 2 offers the possibility to transmit messages in secured authenticated and encrypted frames. At MAC level, messages are encrypted by using one of the two ciphers: (a) AES-128 in CBC mode and (b) the Camellia-128 forward cipher function. Both are considered state-of-the-art heavy encryption ciphers, meaning that this requirement is fulfilled.

R3.4: Entity authentication is defined as corroborating the identity of a node or a hub during a security association procedure. This offered by four of the five association protocols introduced in the standard. However, when it comes to authorisation the standard fails to introduce a mechanism (e.g. access control lists, . . .), meaning this requirement is only fulfilled in parts.

R3.5: The main focus of the standard in terms of robustness lies on measures to reduce transmission errors and interference. There are no mentions of DoS protection or any other controls to harden the system against security attacks, meaning it is up to the designer whether dependability measures shall be implemented or not.

R3.6: In the standard a secure frame is described as one that has authenticity, integrity, confidentiality (if required) and replay protection. The frame body consists of three parts, a low-order security sequence number, a message integrity code (MIC) and the actual frame payload. The low-order security sequence number is set to zero if the current frame is secured with a PTK/GTK that has never been used and is incremented by one from its last value if the frame uses the same PTK/GTK, is from the same sender and contains a valid MIC. This procedure guarantees message freshness and integrity. However, the sequence number is sequential, which could theoretically be exploited by guessing the next value. Hence, this requirement is only partly fulfilled.

R3.7: As seen in figure 3 of chapter 4.3.1 MBAN nodes can send disassociation frames, no matter the current state they are in. Once each one of the parties receives such a frame, the current security association and the security keys are revoked, and the connection is transferred back to the Orphan state. However, the standard does not specify what happens if there is a sudden loss of connection, e.g. the battery fails. Hence, this requirement is only fulfilled in parts.

R3.8: The standard successfully implements the following important aspects of key management: generation, refreshing, agreement, distribution and revocation. However, as discussed in section 4.3.3 vulnerabilities mainly in the key distribution have been discovered. Those vulnerabilities pose a major issue for secure key management. Furthermore, the standard does not mention how keys should be secured when at rest, opening possibilities for attacks on the physical nodes.

R3.9: The sender's and the recipient's identity are always linked to a frame on the MAC level. There, respective IDs are transmitted in the MAC header, alongside the BAN ID. This ensures that it is always known which node sent a frame, clearly connecting it to the sender. However, if an attacker could compromise a node or maybe place a rogue node into the network (e.g. by exploiting the vulnerabilities discussed in section 4.3.3), the sender's ID could in theory be spoofed.

Table VI summarizes the standard's fulfillment of the application-specific requirements of the hypothetical scenarios. As one can see, several areas of shortcomings of the standard have been identified by following the structured analysis procedure. In the next step the findings will be summarised and organised in order to give recommendations on how to close the gap between requirements and the standard.

5.4 Findings of the analysis

The most important findings of the in-depth analysis in the previous section will be documented here. As already discussed in section 5.1, the findings will be clustered into three main categories, namely physical, organisational and security findings. Table VII gives a general overview of how the findings connect to the application-specific requirements.

Physical and organisational findings

- **PO.F1:** Although the standard is designed for ultra-low power devices, it does not consider passive devices that have no computational capabilities at all.
- **PO.F2:** While there is a whole list of possible reasons why an incoming connection request gets rejected (as specified in the connection status field encoding), there is no discussion what happens if a node abruptly disconnects due to device failure or DoS.
- **PO.F3:** The standard only supports a maximal number of nodes of up to 64 (mMaxBAN-Size). This number might not be sufficient for future applications. Furthermore, it is not mentioned where this limit comes from.
- **PO.F4:** The only network topology introduced in the standard is a star with the possibility of a two hop star extension. Peer-to-peer topologies and ad-hoc connections are not discussed.

Table VI: This matrix identifies the areas where the standard does not fulfill the formulated application-specific requirements (Rx.x) and, hence, the overall requirements (SRx and PRx). (Red: The standard does not satisfy this requirement, Yellow: The standard partly satisfies this requirement, Green: The standard satisfies this requirement)

		SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9	SR10	SR11	ER1	ER2	ER3	MR1	MR2	MR3	CR1	CR2	CR3	TP1	TP2	TP3
Scenario 1																								
	R1.1												🟨			🟨			🟨					
	R1.2																						🟩	
	R1.3									🟥														
	R1.4	🟩	🟩																					
	R1.5				🟨		🟨																	
	R1.6	🟩										🟩												
	R1.7			🟥					🟥		🟥													
	R1.8	🟩	🟩					🟩																
	R1.9				🟩	🟩																		
Scenario 2																								
	R2.1													🟩			🟩			🟩				
	R2.2																					🟩		
	R2.3					🟥						🟥												
	R2.4									🟨														
	R2.5				🟥	🟥	🟥																	
	R2.6	🟩	🟩																					
	R2.7				🟨		🟨																	
	R2.8								🟥	🟥	🟥													
	R2.9	🟩	🟩					🟩																
	R2.10									🟩														
Scenario 3																								
	R3.1														🟩			🟩			🟩			
	R3.2																							🟥
	R3.3	🟩	🟩																					
	R3.4				🟨	🟨																		
	R3.5			🟥					🟥		🟥													
	R3.6		🟨					🟨																
	R3.7									🟨														
	R3.8											🟥												
	R3.9						🟩																	

Table VII: This table shows the connection between findings of the in-depth analysis of the standard and the defined application-specific requirements (Rx.x).

	Physical and organisational findings					Cryptography, confidentiality and integrity findings				Authentication and authorisation findings			Other findings		
	PO.F1	PO.F2	PO.F3	PO.F4	PO.F5	CC.F1	CC.F2	CC.F3	CC.F4	AA.F1	AA.F2	AA.F3	O.F1	O.F2	O.F3
R1.1	●							●							
R1.2															
R1.3			●												
R1.4						●									●
R1.5										●	●				
R1.6													●		
R1.7		●													
R1.8									●						
R1.9							●								
R2.1															
R2.2															
R2.3													●		
R2.4															
R2.5												●			
R2.6						●									●
R2.7															●
R2.8														●	
R2.9									●						
R2.10															
R3.1															
R3.2				●											
R3.3						●									●
R3.4												●			●
R3.5														●	
R3.6									●						
R3.7		●													
R3.8													●		
R3.9															

- **PO.F5:** The BAN introduced in the standard must have one and only one hub. Networks that require more than one hub (for instance as a passive back-up) are therefore not covered by the standard.

Cryptography, confidentiality and integrity findings

- **CC.F1:** The AES and Camellia ciphers used for encryption are only issued with a key size of 128 bits. However, there are already more secure, bigger key-sizes available, which should be employed instead whenever possible.
- **CC.F2:** The standard uses CMACs according to the NIST special publication 800-38B, which are energy efficient and memory saving for messages in the range of less than or equal to 2 blocks [84]. For longer messages, there are more energy efficient alternatives of which there is none offered.
- **CC.F3:** For applications that use an ultrasound channel for communication and devices that do not have sufficient processing power to compute complex security algorithms, the standard does not mention the need for security by design.
- **CC.F4:** The low-order security sequence number functioning as replay protection and guaranteeing message freshness is always incremented by one for every new frame. This is - in terms of security - not recommendable, as attackers could easily predict the sequential numbers and bypass this security control.

Authentication and authorisation findings

- **AA.F1:** For the MK-pre shared association protocol (protocol I) the standard mentions a mutual authentication procedure based on the pre-shared MK. It does, however, not specify the inner workings of this procedure.
- **AA.F2:** For the public-key hidden association protocol (protocol III) the standard fails to specifically mention mutual authentication.
- **AA.F3:** It is not sure how the standard maintains which nodes are allowed access in to the network. It does not mention an *Access Control List* (ACL) where identifying information about nodes with access is stored. Any node with the correct formal requirements (e.g. frame structure, SSS, valid PK, ...) can establish a connection with the hub.

Other findings

- **O.F1:** Although the standard offers various protocols for secure key management, it fails to discuss how security keys should be stored on devices that allow physical access by an attacker.

- **O.F2:** The standard does not deploy sufficient measures to protect the network against DoS attacks, nor to improve the overall dependability in terms of security of the system.
- **O.F3:** The security of the standard mainly revolves around authentication and encryption. Broader topics, like for instance overall threat surface and possible attack scenarios are not part of the discussion.

5.5 Recommendations to the standard

The last step of the procedure is to translate the findings from the previous section into concrete recommendations on how to fix the identified issues. Thereby, for each finding in the different categories a recommendation will be given.

Physical and organisational recommendations

- **PO.R1:** In order to encompass the entire range of possible device categories, the standard needs to extend its scope from extremely low power devices to include passive devices. Therefore, a specific section on how to handle the specific requirements of passive devices has to be added in the following chapters:
  - *4. General framework elements:* This chapter explains the framework elements within the defined scope, which does not include passive devices. Within all of the subsections in this chapter a paragraph needs to be added introducing the relevant framework elements that consider the resource capabilities of passive devices.
  - *10. Human body communications PHY specification:* Since most of implantable, passive devices rely on human body communication, a section needs to be added explaining in detail the communication of passive devices on a PHY level.
- **PO.R2:** Section *6.4.3 Node disconnection* specifies that if a node receives a Connection Assignment frame indicating that a connection request was rejected for some reason, the node sends a Disconnection frame. The possible reasons for a rejected connection request are listed in *Table 12 - Connection status field encoding.* An entry needs to be added to this table stating that a connection request was rejected because the device is not reachable. Whether this is due to device failure, or a DoS attack does not matter in this context. In addition to that, an explanation to what happens if the node can no longer communicate with the previously connected device needs to be added within section *6.4.3*.
- **PO.R3:** An explanation of where the limitation of a maximum node count of mMaxBANSize needs to be added in chapter *4.2 Network topology* or as an addition to *Table 24 - MAC sublayer parameters.* The limitation on the node count is not sufficient for some future-applications, which is why a detailed explanation would help to add transparency.

- **PO.R4:** The standard needs to include an alternative peer-to-peer topology to the star network introduced in chapter *4.2 Network topology*. Additionally, the standard needs to either extended the existing protocols and procedures to support multiple topologies, or new protocols need to be introduced.

- **PO.R5:** The standard needs to consider the scenario when a new hub gets added to the network or the current hub is replaced. Therefore, the restriction in the first paragraph of chapter *4.2 Network topology* needs to be lifted and the introduced topology needs to be extended.

Cryptography, confidentiality and integrity recommendations

- **CC.R1:** In *Table 7 - Cipher Function field encoding* of chapter *4.3.2.3.4 Cipher function* additional entries for the 256-bit versions of both forward cipher functions should be added. Furthermore, chapter *7. Security services* needs to include a one-liner introducing the possibility to use the larger key sizes.

- **CC.R2:** In chapters *7.1 Security association and disassociation* and *7.2 PTK creation and GTK distribution* the definitions of the CMAC used to compute KMACs needs to be extended to include more energy efficient CMAC alternatives for messages that are longer than 2 blocks.

- **CC.R3:** In chapter *7. Security services*, a paragraph needs to be added stating that for devices communicating via an ultrasound channel, the developer needs to ensure the inherent security of the link (security by design), if conventional cryptography is not possible.

- **CC.R4:** In chapter *5.2.2.1 Low-Order Security Sequence Number*, paragraph *b)* it should not be stated that the low-order security sequence number is incremented by one. To improve security the numbers should be incremented by a non-predictable value, e.g. starting at a random point that changes for every session or incrementing the sequence number by random values bigger than one.

Authentication and authorisation recommendations

- **AA.R1:** In chapter *7.1.1 Master key pre-shared association* it is mentioned that hub and node perform mutual authentication with each other, while simultaneously advancing to the PTK creation procedure. Here, a paragraph explaining the inner workings of the mutual authentication procedure has to be added.

- **AA.R2:** In chapter *7.1.3 Public key hidden association* the standard needs to specifically mention that mutual authentication is guaranteed, in case the association procedure is successful.

- **AA.R3:** In chapter *7. Security services* the standard needs to introduce and discuss a means to store and track created and established keys to guarantee only registered devices can enter the network. The concept of an access control list - managed by the hub - can be used to keep track of authorisation of individual nodes.

Other recommendations

- **O.R1:** In chapter *7. Security services* a section on best practices and recommendations on how to securely store security keys when at rest needs to be included. This is especially important for nodes that are physical accessible, e.g. semi-invasive, wearable and ambient nodes.
- **O.R2:** In chapter *7. Security services* best practices and recommendations on how to harden the BAN against DoS attacks need to be introduced in a separate sub-chapter.
- **O.R3:** The standard needs to include recommendations on how to effectively reduce the threat surface of a MBAN. Therefore, a sub-chapter including preferences on how to reduce the threat surface needs to be added to chapter *7. Security services*.

Chapter 6

Conclusion

This thesis is focused on improving security for future Medical Body Area Network (MBAN) applications by assessing the security posture of the IEEE 802.15.6 standard, which aims to govern such networks. Therefore, a structured procedure to analyse the governing standard was introduced and applied. This resulted in a number of various recommendations to the standard, which could be implemented to improve its security.

This chapter aims to conclude this work and is structured in the following way: Section 6.1 gives a retrospective overview of this thesis, section 6.2 summarises contributions made by this work and section 6.3 discusses future work and possible next steps.

6.1 Thesis overview

To achieve the overall goal of increasing the security of the IEEE 802.15.6 standard, this thesis had two key objectives: (a) Establishing a structured analysis procedure and (b) Using that procedure to find shortcomings in terms of security and giving recommendations on how to fix them.

The main difficulty of creating a structured assessment procedure was to ensure that the analysis would be collectively exhaustive, covering all of the necessary dimensions. As device and network security are dependent on the node type, the analysis needed to encompass more than just the scope of security itself. Therefore, not only security requirements, but also a number of physical requirements that represent distinct node types were taken into consideration.

By using a matrix which guarantees collective exhaustiveness, the requirements were materialised into three distinct hypothetical scenarios. While this process would allow for the creation of completely fictional scenarios which still cover the requirements, the three scenarios created in this thesis are based on active research and real-life applications. Given the exhaustiveness of the introduced procedure, those scenarios represent the entirety of the MBAN application spectrum. However, it is not being said that those are the only scenarios that are feasible. It is up to the researcher to select a relevant set of applications that collectively cover the defined range of dimensions.

The created scenarios are used as a means to translate the security and physical requirements into application-specific requirements, which can be used to assess the IEEE 802.15.6 standard. They are a set of challenges for each hypothetical scenario that the standard needs to encompass. By using a matrix that checks if the application-specific requirements cover all of the security and physical requirements, exhaustiveness is once again guaranteed.
The assessment of the standard was conducted by taking each of the application-specific requirements per hypothetical scenario and analysing if the standard fulfills it. Thereby, gaps between the requirements and the standard were identified and summarised into findings of four categories (physical and organisational; cryptography, confidentiality and integrity authentication and authorisation, other). Those findings were then analysed and specific recommendations on how to improve the standard in terms of security were formulated and clustered in the same categories.

6.2 Contributions

The following contributions were made by this thesis:

- An overview of Medical Body Area Networks (MBANs), including all the most important building blocks was given.
- An overview of the current IEEE 802.15.6 standard with a focus on the security features and vulnerabilities was given.
- A structured procedure to exhaustively analyse the IEEE 802.15.6 standard in terms of security was introduced. Thereby, a set of security and physical requirements were introduced and, following the procedure, hypothetical scenarios were designed.
- The IEEE 802.15.6 standard's security posture was analysed and gaps between the standard and the defined requirements were found and summarised as findings.
- Specific recommendations on how to improve the security posture of the IEEE 802.15.6 standard were given and clustered into four distinct categories.

6.3 Future work and next steps

Concluding this work, an extensive analysis of the IEEE 802.15.6 standard was conducted, resulting in a number of findings and recommendations. Those recommendations aid to improve the security posture of the standard, making future WBAN and MBAN applications governed by this standard more secure. Before this becomes a reality, the following next steps need to be taken:

- The introduced assessment procedure is designed in a way that is not specific to the IEEE 802.15.6 standard. Since the formulated security and physical requirements are valid for other non-MBAN applications as well, the procedure should be applied to standards similar to IEEE 802.15.6, like for instance IEEE 802.15.4.

- During this research many security issues not only regarding the IEEE 802.15.6 standard but also MBAN applications in general were raised. This gained knowledge can contribute to improving the overall security posture of MBANs and, as a next step, should be applied to future MBAN applications.
- Now, after conducting an in-depth analysis of the standard and formulating specific recommendation on how to improve it in terms of security, the obvious next step is to propose the recommendations to the standard's body. However, before doing so, it is necessary to validate the recommendations and if needed, conduct more research to further specify them.

Bibliography

[1] "Chapter 7 - wban: Driving e-healthcare beyond telemedicine to remote health monitoring: Architecture and protocols," in *Telemedicine Technologies*, H. D. Jude and V. E. Balas, Eds., Academic Press, 2019, pp. 89–119, ISBN: 978-0-12-816948-3.

[2] "Iso/iec/ieee international standard - information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 15-6: Wireless body area network," *ISO/IEC/IEEE 8802-15-6:2017(E)*, pp. 1–274, 2018. DOI: `10.1109/IEEESTD.2018.8323448`.

[3] M. Toorani, "Security analysis of the ieee 802.15. 6 standard," *International Journal of Communication Systems*, vol. 29, no. 17, pp. 2471–2489, 2016.

[4] Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji, and H. Wu, "A survey of routing protocols in wban for healthcare applications," *Sensors*, vol. 19, no. 7, p. 1638, 2019.

[5] I. U. K. Aqeel-ur-Rehman and A. Y. Khan, "A review on authentication schemes for wireless body area networks,"

[6] M. Roy, C. Chowdhury, and N. Aslam, "Designing transmission strategies for enhancing communications in medical iot using markov decision process," *Sensors*, vol. 18, no. 12, p. 4450, 2018.

[7] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks," *Journal of medical systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[8] R. Pan, D. Chua, J. S. Pathmasuntharam, and Y. P. Xu, "A wban based cableless ecg acquisition system," in *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, IEEE, 2014, pp. 910–913.

[9] T.-Y. Kim and E.-J. Kim, "Multi-hop wban configuration approach for wearable machine-to-machine systems," *Multimedia Tools and Applications*, vol. 75, no. 20, pp. 12 859–12 878, 2016.

[10] R. Punj and R. Kumar, "Technological aspects of wbans for health monitoring: A comprehensive review," *Wireless Networks*, vol. 25, no. 3, pp. 1125–1157, 2019.

[11] J. Mahapatro, S. Misra, M. Manjunatha, and N. Islam, "Interference mitigation between wban equipped patients," in *2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN)*, 2012, pp. 1–5.

[12] T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in wban: Analysis and open research issues," *Wireless Networks*, vol. 20, no. 8, pp. 2165–2199, 2014.

[13] Bluetooth, 2020. [Online]. Available: `https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/radio-versions/`.

[14] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards," *Computer communications*, vol. 30, no. 7, pp. 1655–1695, 2007.

[15] Y. Kim, S. Lee, and S. Lee, "Coexistence of zigbee-based wban and wifi for health telemonitoring systems," *IEEE journal of biomedical and health informatics*, vol. 20, no. 1, pp. 222–230, 2015.

[16] A. Groner and K. Grippe, "The leadless pacemaker: An innovative design to enhance pacemaking capabilities," *Journal of the American Academy of PAs*, vol. 32, no. 6, pp. 48–50, 2019.

[17] M. Hadjem, O. Salem, F. N. Abdesselam, and A. Mehaoua, "Early detection of myocardial infarction using wban," in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, IEEE, 2013, pp. 135–139.

[18] M. Hadjem, O. Salem, and F. Naıt-Abdesselam, "An ecg monitoring system for prediction of cardiac anomalies using wban," in *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*, IEEE, 2014, pp. 441–446.

[19] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications surveys & tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[20] G. Huzooree, K. K. Khedo, and N. Joonas, "Data reliability and quality in body area networks for diabetes monitoring," in *Body Area Network Challenges and Solutions*, Springer, 2019, pp. 55–86.

[21] N. Escobar Cruz, J. Solarte, and A. Gonzalez-Vargas, "Automated epileptic seizure detection system based on a wearable prototype and cloud computing to assist people with epilepsy," in *Applied Computer Sciences in Engineering*, J. C. Figueroa-García, J. G. Villegas, J. R. Orozco-Arroyave, and P. A. Maya Duque, Eds., Cham: Springer International Publishing, 2018, pp. 204–213, ISBN: 978-3-030-00353-1.

[22] M. Wu and J. Luo, "Wearable technology applications in healthcare: A literature review," *Online J Nurs Inform*, vol. 23, 2019.

[23] Y. Choi, Y.-M. Jeon, L. Wang, and K. Kim, "A biological signal-based stress monitoring framework for children using wearable devices," *Sensors*, vol. 17, no. 9, p. 1936, 2017.

[24] M. G. R. Alam, E. J. Cho, E.-N. Huh, and C. S. Hong, "Cloud based mental state monitoring system for suicide risk reconnaissance using wearable bio-sensors," in *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication*, 2014, pp. 1–6.

[25] J. Saha, S. Biswas, T. Bhattacharyya, and C. Chowdhury, “A framework for monitoring of depression patient using wban,” in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, IEEE, 2016, pp. 410–415.

[26] R. A. Khan and A.-S. K. Pathan, “The state-of-the-art wireless body area sensor networks: A survey,” *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, p. 1 550 147 718 768 994, 2018.

[27] L. Haoyu, L. Jianxing, N. Arunkumar, A. F. Hussein, and M. M. Jaber, “An iomt cloud-based real time sleep apnea detection scheme by using the spo2 estimation supported by heart rate variability,” *Future Generation Computer Systems*, vol. 98, pp. 69–77, 2019.

[28] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, and M. S. Islam, “A comprehensive review of wireless body area network,” *Journal of Network and Computer Applications*, vol. 143, pp. 178–198, 2019.

[29] D. P. Tobón, T. H. Falk, and M. Maier, “Context awareness in wbans: A survey on medical and non-medical applications,” *IEEE Wireless Communications*, vol. 20, no. 4, pp. 30–37, 2013.

[30] M. A. El-Bendary, *Developing security tools of WSN and WBAN networks applications.* Springer, 2015.

[31] B. Narwal and A. Mohapatra, “A review on authentication protocols in wireless body area networks (wban),” in *2018 3rd International Conference on Contemporary Computing and Informatics (IC3I)*, IEEE, 2018, pp. 227–232.

[32] R. Doss, S. Piramuthu, and W. Zhou, *Future Network Systems and Security.* Springer, 2016.

[33] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” *IEEE Wireless communications*, vol. 17, no. 1, pp. 51–58, 2010.

[34] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications,” *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113–122, 2017.

[35] S. Roy and S. Biswas, “A novel trust evaluation model based on data freshness in wban,” in *Proceedings of International Ethical Hacking Conference 2018*, Springer, 2019, pp. 223–232.

[36] J. Li, K. Ren, B. Zhu, and Z. Wan, “Privacy-aware attribute-based encryption with user accountability,” in *International Conference on Information Security*, Springer, 2009, pp. 347–362.

[37] S. Khan and A. K. Pathan, “Wireless networks and security,” *Springer*, vol. 10, pp. 978–3, 2013.

[38] A. Sammoud, M. A. Chalouf, O. Hamdi, N. Montavont, and A. Bouallegue, “A new biometrics-based key establishment protocol in wban: Energy efficiency and security robustness analysis,” *Computers & Security*, p. 101 838, 2020.

[39] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, “Certificateless remote anonymous authentication schemes for wirelessbody area networks,” *IEEE Transactions on parallel and distributed systems*, vol. 25, no. 2, pp. 332–342, 2013.

[40] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, “Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks,” *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[41] B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, *Handbook of Computer Networks and Cyber Security*. Springer, 2020.

[42] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, “Review of security and privacy for the internet of medical things (iomt),” in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, IEEE, 2019, pp. 457–464.

[43] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, “Ideas and challenges for securing wireless implantable medical devices: A review,” *IEEE Sensors Journal*, vol. 17, no. 3, pp. 562–576, 2016.

[44] F. Alsubaei, A. Abuhussein, and S. Shiva, “Security and privacy in the internet of medical things: Taxonomy and risk assessment,” in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, IEEE, 2017, pp. 112–120.

[45] T. Beardsley, *R7-2016-07: Multiple vulnerabilities in animas onetouch ping insulin pump*, Oct. 2016. [Online]. Available: `https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/`.

[46] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, IEEE, 2008, pp. 129–142.

[47] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, “On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them,” in *Proceedings of the 32nd annual conference on computer security applications*, 2016, pp. 226–236.

[48] J. Classen, D. Wegemer, P. Patras, T. Spink, and M. Hollick, “Anatomy of a vulnerable fitness tracking system: Dissecting the fitbit cloud, app, and firmware,” *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 1, pp. 1–24, 2018.

[49] U. Food, D. Administration, *et al.*, “Cybersecurity vulnerabilities of hospira symbiq infusion system: Fda safety communication,” *Silver Spring, Maryland (www. fda. gov/MedicalDevices/Safety/AlertsandNotices/ucm456815. htm)*, 2015.

[50] R. Yan, T. Xu, and M. Potkonjak, “Semantic attacks on wireless medical devices,” in *SENSORS, 2014 IEEE*, IEEE, 2014, pp. 482–485.

[51] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, "This ain't your dose: Sensor spoofing attack on medical infusion pump," in *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016.

[52] Y. A. Qadri, R. Ali, A. Musaddiq, F. Al-Turjman, D. W. Kim, and S. W. Kim, "The limitations in the state-of-the-art counter-measures against the security threats in h-iot," *Cluster Computing*, pp. 1–19, 2020.

[53] K. Arya and R. Gore, "Data security for wban in e-health iot applications," in *Intelligent Data Security Solutions for e-Health Applications*, Elsevier, 2020, pp. 205–218.

[54] S. S. Javadi and M. A. Razzaque, "Security and privacy in wireless body area networks for health care applications," in *Wireless networks and security*, Springer, 2013, pp. 165–187.

[55] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of ieee 802.15. 6 standard. applied sciences in biomedical and communication technologies (isabel)," in *2013 3rd International Symposium on Rome*, 2010.

[56] A. W. Astrin, H.-B. Li, and R. Kohno, "Standardization for body area networks," *IEICE transactions on communications*, vol. 92, no. 2, pp. 366–372, 2009.

[57] IEEE, *Ieee 802.15 wpan™ task group 6 (tg6) body area networks*, Jun. 2011. [Online]. Available: `http://www.ieee802.org/15/pub/TG6.html`.

[58] S. Ullah, M. Mohaisen, and M. A. Alnuem, "A review of ieee 802.15. 6 mac, phy, and security specifications," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, p. 950 704, 2013.

[59] M. Li and M. Zhuang, "An overview of physical layers on wireless body area network," in *Anti-counterfeiting, Security, and Identification*, IEEE, 2012, pp. 1–5.

[60] P. Mathew, L. Augustine, D. Kushwaha, D. Vivian, and D. Selvakumar, "Hardware implementation of nb phy baseband transceiver for ieee 802.15. 6 wban," in *2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom)*, IEEE, 2014, pp. 64–71.

[61] P. Mathew, L. Augustine, T. Devis, *et al.*, "Hardware implementation of (63, 51) bch encoder and decoder for wban using lfsr and bma," *arXiv preprint arXiv:1408.2908*, 2014.

[62] P. Mathew, L. Augustine, D. Kushwaha, V. Desalphine, and A. D. Selvakumar, "Implementation of nb phy transceiver of ieee 802.15. 6 wban on fpga," in *2015 International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI-SATA)*, IEEE, 2015, pp. 1–6.

[63] M. R. Yuce, H. C. Keong, and M. S. Chae, "Wideband communication for implantable and wearable systems," *IEEE transactions on microwave theory and techniques*, vol. 57, no. 10, pp. 2597–2604, 2009.

[64] R. Chávez-Santiago, A. Khaleghi, I. Balasingham, and T. A. Ramstad, "Architecture of an ultra wideband wireless body area network for medical applications," in *2009 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies*, IEEE, 2009, pp. 1–6.

[65] S. A. Salehi, M. A. Razzaque, I. Tomeo-Reyes, and N. Hussain, "Ieee 802.15. 6 standard in wireless body area networks from a healthcare point of view," in *2016 22nd Asia-Pacific Conference on Communications (APCC)*, IEEE, 2016, pp. 523–528.

[66] M. Seyedi, B. Kibret, D. T. Lai, and M. Faulkner, "A survey on intrabody communications for body area network applications," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 8, pp. 2067–2079, 2013.

[67] J. Bae, K. Song, H. Lee, H. Cho, and H.-J. Yoo, "A low-energy crystal-less double-fsk sensor node transceiver for wireless body-area network," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 11, pp. 2678–2692, 2012.

[68] D. Lachartre, B. Denis, D. Morche, L. Ouvry, M. Pezzin, B. Piaget, J. Prouvée, and P. Vincent, "A 1.1 nj/b 802.15. 4a-compliant fully integrated uwb transceiver in 0.13 μm cmos," in *2009 IEEE International Solid-State Circuits Conference-Digest of Technical Papers*, IEEE, 2009, pp. 312–313.

[69] F. Ullah, A. H. Abdullah, O. Kaiwartya, S. Kumar, and M. M. Arshad, "Medium access control (mac) for wireless body area network (wban): Superframe structure, multiple access technique, taxonomy, and challenges," *Human-centric Computing and Information Sciences*, vol. 7, no. 1, p. 34, 2017.

[70] G. Fang and E. Dutkiewicz, "Bodymac: Energy efficient tdma-based mac protocol for wireless body area networks," in *2009 9th international symposium on communications and information technology*, IEEE, 2009, pp. 1455–1459.

[71] E. Farella, A. Pieracci, L. Benini, L. Rocchi, and A. Acquaviva, "Interfacing human and computer with wireless body area sensor networks: The wimoca solution," *Multimedia Tools and Applications*, vol. 38, no. 3, pp. 337–363, 2008.

[72] Z. Li, G. Zhang, and W. J. Li, "An adaptive data transmission scheme for wireless body area networks," in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, IEEE, 2012, pp. 399–403.

[73] J. Benson, T. O'Donovan, U. Roedig, and C. J. Sreenan, "Opportunistic aggregation over duty cycled communications in wireless sensor networks," in *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, IEEE, 2008, pp. 307–318.

[74] M. Toorani, "On vulnerabilities of the security association in the ieee 802.15. 6 standard," in *International conference on financial cryptography and data security*, Springer, 2015, pp. 245–260.

[75] D. Seo, J. M. Carmena, J. M. Rabaey, E. Alon, and M. M. Maharbiz, "Neural dust: An ultrasonic, low power solution for chronic brain-machine interfaces," *arXiv preprint arXiv:1307.2196*, 2013.

[76] R. M. Neely, D. K. Piech, S. R. Santacruz, M. M. Maharbiz, and J. M. Carmena, "Recent advances in neural dust: Towards a neural interface platform," *Current opinion in neurobiology*, vol. 50, pp. 64–71, 2018.

[77] M. A. Siddiqi, R. H. S. H. Beurskens, P. Kruizinga, C. I. De Zeeuw, and C. Strydis, "Securing implantable medical devices using ultrasound waves," *IEEE Access*, pp. 1–1, 2021. DOI: `10.1109/ACCESS.2021.3083576`.

[78] J. E. Poole, M. J. Gleva, T. Mela, M. K. Chung, D. Z. Uslan, R. Borge, V. Gottipaty, T. Shinn, D. Dan, L. A. Feldman, *et al.*, "Complication rates associated with pacemaker or implantable cardioverter-defibrillator generator replacements and upgrade procedures: Results from the replace registry," *Circulation*, vol. 122, no. 16, pp. 1553–1561, 2010.

[79] F. V. Tjong and V. Y. Reddy, "Permanent leadless cardiac pacemaker therapy: A comprehensive review," *Circulation*, vol. 135, no. 15, pp. 1458–1470, 2017.

[80] D. J. Cantillon, D. V. Exner, N. Badie, K. Davis, N. Y. Gu, Y. Nabutovsky, and R. Doshi, "Complications and health care costs associated with transvenous cardiac pacemakers in a nationwide assessment," *JACC: Clinical Electrophysiology*, vol. 3, no. 11, pp. 1296–1305, 2017.

[81] A. Joury, T. Bob-Manuel, A. Sanchez, F. Srinithya, A. Sleem, A. Nasir, A. Noor, D. Penfold, R. Bober, D. P. Morin, *et al.*, "Leadless and wireless cardiac devices: The next frontier in remote patient monitoring," *Current Problems in Cardiology*, p. 100 800, 2021.

[82] F. V. Tjong, T. F. Brouwer, L. Smeding, K. M. Kooiman, J. De Groot, D. Ligon, R. Sanghera, M. Schalij, A. Wilde, and R. Knops, "Combined leadless pacemaker and subcutaneous implantable defibrillator therapy: Feasibility, safety, and performance," *Ep Europace*, vol. 18, no. 11, pp. 1740–1747, 2016.

[83] C. Bommer, V. Sagalova, E. Heesemann, J. Manne-Goehler, R. Atun, T. Bärnighausen, J. Davies, and S. Vollmer, "Global economic burden of diabetes in adults: Projections from 2015 to 2030," *Diabetes care*, vol. 41, no. 5, pp. 963–970, 2018.

[84] M. A. Simplicio Jr, B. T. De Oliveira, C. B. Margi, P. S. Barreto, T. C. Carvalho, and M. Näslund, "Survey and comparison of message authentication solutions on wireless sensor networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1221–1236, 2013.