Implantable Medical Devices; Networking Security Survey

Siamak Aram[1, 2*], Rouzbeh A. Shirvani[1], Eros G. Pasero[2], and Mohamd F. Chouikha[1]
[1]Department of Electrical and Computer Engineering
Howard University, Washington DC, US
siamak.aram@howard.edu, rouzbeh.asgharishir@bison.howard.edu, mchouikha@howard.edu
[2]Department of Electronics and Telecommunications
Polytechnic University of Turin, Turin, Italy
{siamak.aram, eros.pasero}@polito.it

Abstract

The industry of implantable medical devices (IMDs) is constantly evolving, which is dictated by the pressing need to comprehensively address new challenges in the healthcare field. Accordingly, IMDs are becoming more and more sophisticated. Not long ago, the range of IMDs' technical capacities was expanded, making it possible to establish Internet connection in case of necessity and/or emergency situation for the patient. At the same time, while the web connectivity of today's implantable devices is rather advanced, the issue of equipping the IMDs with sufficiently strong security system remains unresolved. In fact, IMDs have relatively weak security mechanisms which render them vulnerable to cyber-attacks that compromise the quality of IMDs' functionalities. This study revolves around the security deficiencies inherent to three types of sensor-based medical devices; biosensors, insulin pump systems and implantable cardioverter defibrillators. Manufacturers of these devices should take into consideration that security and effectiveness of the functionality of implants is highly dependent on the design. In this paper, we present a comprehensive study of IMDs' architecture and specifically investigate their vulnerabilities at networking interface.

Keywords: implantable medical devices, security, wireless sensor network.

1 Introduction

Modern technologies have completely reshaped healthcare industry with providing variety of medical services to patients. New medical policies call for miniaturization of implantable devices so that they could meet body requirements while measuring different health parameters and performing various analyses.

Wireless Sensor Network (WSN) based systems can realize long-distance signal transmission so as to make it possible for doctors to follow up patients' health conditions remotely. By exploiting capabilities of wireless medical devices physicians are able to conduct real-time monitoring without causing any inconvenience for their patients.

Implantable devices are studied and analyzed based on a taxonomy called "Nano-medicine" [25] as shown in Figure 1. In this figure we scrutinized mentioned category to two main subcategories: "Implantable Sensors" and "Sensory Aids".

In medicine, sensing is a method which allows obtaining more accurate and immediate data for conducting medical diagnostics [61]. One of the recent developments of modern nanotechnology are "wearable" or "implantable" sensors which monitor health conditions and obtain medical data of high accuracy.

Journal of Internet Services and Information Security (JISIS), volume: 6, number: 3 (August 2016), pp. 40-60

[*]Corresponding author: Laboratorio di Neuronica , Dip. Elettronica e Telecomunicazioni - Politecnico di Torino c.so Duca d. Abruzzi 24 10129 Torino - Italy, Tel: +39-011-564-4065

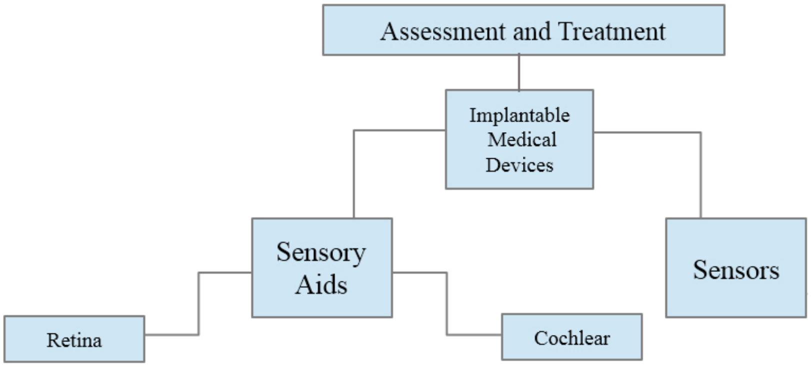


Figure 1: Implantable Medical devices Taxonomy

Additionally, along with rapid progress in the area of nano science development of technology for restoration of sight and hearing has also accelerated. Newly available technological solutions encouraged creation of miniature "sensory aid" devices with increased power capacity. The principle of sensory aid devices' operation is as follows: lost sense is being restored by electric systems that convey the data gathered by the sensors directly to the nervous system of a patient.

The convenient size of a sensor can widely expand the range of its possible applications. Likewise, vital body parameters including pulse, temperature and blood glucose can be monitored daily by sensor microchips [19]. Enhancement of micro-electro-mechanical systems (hereinafter - MEMS), progress in developing digital electronics and new opportunities of wireless communication cumulatively allow for substantial expansion of the range of implantable and indwelling medical sensor-based tools [29]. Assuming that, the devices appropriate for implantation in the human body hereby have become the key focus area for many scientists [19, 25].

The improved connectivity between implantable devices and a medical center equipment has both advantages and disadvantages. On one hand, it sufficiently facilitates regulating the course of patient's treatment. On the other hand, health data may be easily intercepted during the transmission from implant to authorized medical instruments. Such established vulnerability has been affirmed, and a range of security and privacy concerns have hereby arisen. *In view of the urgency to respond to new threats in the IMDs sphere, this survey is to compare, analyze and summarize main vulnerabilities in the interconnection network of the implantable devices.*

The security structure of wireless protocols such as ZigBee [62], Wi-Fi [27] and Bluetooth [42] for a long time has been the key area of focus for developers and security systems' specialists.

If the security standards are not observed properly malware and operational failures of wireless technology caused by security breaches are inevitable. Similarly, the rising use of Bluetooth [15] and other protocols of this kind doubles the risk of attacks on the devices' security system. Thus, to help prevent emerging security threats entire wireless network should be constantly monitored against the risks and equipped with new defense techniques. Main threats/attacks impacting on wireless networks are as follows:

- Jamming
- Interception of transmitted data
- Modifying the data in the course of transmission
- Data leaks to unauthorized persons

Attacks on wireless protocols may be performed both from short and long distances. Considering that long-range attacks require intricate equipment, and, therefore, are particularly dangerous to the integrity of the system, these threats should be investigated with more precision [60]. The scientists have defined at least 16 types of wireless security risks [42]. Apart from general risks, there also exist protocol-specific threats. For example, ZigBee networks, mainly intended for remote control operations, have certain drawbacks in the stack of the protocol. Based on ZigBee's inherent vulnerabilities, cyber criminals are able to substitute the data contained in the packets and, consequently, modify the entire network.

In view of the above, Section 3.1 of this work is dedicated to the security issues related to implantable medical devises. With view to developing efficient solutions against these threats, we find it necessary to concentrate on peculiarities of protocols incorporated into implants. The survey on the aforementioned protocols is presented in Section 6, while their comparative analysis is contained in Section 3. Respectively, the paper is summarized and concluded in the Sections 4 and 5.

2 Medical devices and embedded systems

Nowadays, embedded systems are regarded as an innovative and lightweight technical solution. Major benefits of embedded systems are as follows: connectivity, productive performance and cheap cost of components. All these advantages make embedded systems widely applicable in an array of fields, including the industry of implantable devices [47].

Today, all embedded systems have complex architecture which consolidates their functionality and robustness. In particular, set of sensors incorporated in the system enables multitasking, thus improving the network's performance time. Advanced processors utilized by embedded systems do not require excessive amounts of energy. Taking advantage of this feature, developers can expand the range of embedded systems' capabilities. The framework of modern medicine has taken advantage of computing devices integration. A variety of electronic medical tools are now being employed to address the needs of healthcare system. For example, continuous and automatic management of health conditions would not be possible without involvement of implantable medical devices (IMDs). IMDs are a type of medical devices embedded inside the human body for medical intervention.

Although implantable devices so far have met wide approval of the professionals, several limitations in the design and structure of IMDs still impede further expansion of the implant market. Hence, development of completely new technique is strongly required to prevent any undesired external impact on IMDs. In view of this necessity, members of computer security community teamed up with biomedicine specialists to create security defense for implanted devices [1]. The manufacturers of the implants have been instructed by the FDA to treat the risk of potential cyber security breaches with explicit attention. It is also recommended that cybersecurity measures be taken at every stage of the implant's life circle [3].

Robust security of the IMDs should be ensured at all stages of their exploitation, including the stages of their injection into human body and removal from it.

To discover previously unknown vulnerabilities in the system, the most suitable items per category should be selected and carefully studied. This evaluation has to be based on the most appropriate values according to the researcher's choice.

2.1 Designing challenges

The main goals of IMD designers are to improve reliability of device and enhance its safety features, meanwhile reducing its power consumption and usage costs. At the same time, basic data privacy and security of the device should not be overlooked at the device's development stage. Oddly enough, developers have not paid enough attention to security and privacy elements in IMDs and mainly focused on enhancement of devices' interface and technical capacities.

The history of implant therapy dates back to 1958 when the pacemaker was placed inside a human body for the first time [59]. In the early years of implantation practice the manufacturers primarily focused their efforts on enhancing battery power of the implants, wireless communication or testing new materials that could be used in implant production. Back then, cyber-crimes were rare and there was no urgency or priority to equip implants with a strong security system [31]. However, the advent of modern technology, apart from bringing enormous benefit to the society, has also created new opportunities for hackers or attackers. It turned out that IMDs, which have become more interconnected now, have no effective defense system to withstand recently emerged security threats. Hereby, there is a serious need for finding effective security solutions for IMDs in order to protect health and privacy of implant bearers.

Considering that IMDs have immediate contact with the patient's organism, all IMDs are subject to stringent safety and effectiveness checks to assure strict compliance with standards and requirements accepted in biomedicine. IMDs producers have traditionally agreed on that the structure of the implants may not be complicated by any security addition that could slow down the technical approval process. However, this general approach needs to be reconsidered in response to new risks. Among the existing deficiencies of IMDs, weak control system is the most critical factor in destabilizations of device's functioning. A single threat model cannot be adopted for all IMDs: each and every implant is designed to serve a different purpose, hence, vulnerabilities and deficiencies of the devices largely vary.

Errors in the design of the device itself may eventually result in security vulnerabilities, as well. This is the case with implantable cardioverter defibrillators, insulin pump systems and subcutaneous biosensors. In purpose of highlighting the significance of harmonizing the design of the IMDs with its security, basic design concerns of these three devices are discussed in the following [14]:

2.1.1 Insulin pump

The insulin pump device is an open-loop system, where private information and control signals are reflected in its remotely controlled interface. Accordingly, wireless connectivity issues of IMDs increase likelihood of security failures [14]. Manufacturers' negligence in this regard exposes insulin pumps to various security risks.

2.1.2 Defibrillator

As opposed to the insulin pump, the defibrillator is a close-loop system. The main security problem here relates to the battery of the implant. The studies prove that batteries in defibrillators may not always preserve the necessary low-power state [14]; More precisely, the sensing system of a defibrillator randomly reacts to the signals of the device's in-built radio for reporting the patient's conditions. Simultaneously, the battery switches to the high-power mode and the overall consumption of power by the device drastically increases.

2.1.3 Biosensors for data acquisition

One of the broadest categories of IMDs is biosensors. Unlike both defibrillators and insulin pumps, biosensors apply advanced signal processing techniques and transfer higher range of signals. Inherent security threats for biosensors are not typical of any other implants. For example, minor wireless transmissions with unstable frequency may negatively impact the biosensors' security.

2.2 Mapping imds to embedded systems

One of the biggest challenges in security today is to establish what makes the software in our operating systems and applications, hardware and networking so vulnerable in terms of their security. To achieve great resilience in IMDs, embedded device and systems need many considerations leading to secure system design and development maturity.

Generally, the internal structure of IMDs involves sensors, radios, actuators, batteries, CPUs etc. Yet, notwithstanding the primary purpose of the implants, which is to contribute to treatment's efficacy, the implants may also leak patients' private information to unauthorized persons. In this regard, it is vital that the security system of the implants be equipped with new instruments safeguarding privacy of the implant-bearer. Though, this objective is often impeded by the impossibility strike a balance between the strength of encryption and moderate power expenditures of the implant. Luckily, there is fair chance to avoid the impediments by taking due measures as early as at the stage of IMD's designing [28]. Relying on the descriptions of IMDs' types elaborated in the previous section, we identified a number of aspects which play the key role in mapping the implants to embedded structures. These specific features are also demonstrated in the relevant tables which will be provided below in Figure 2 [14] as a general block diagram.

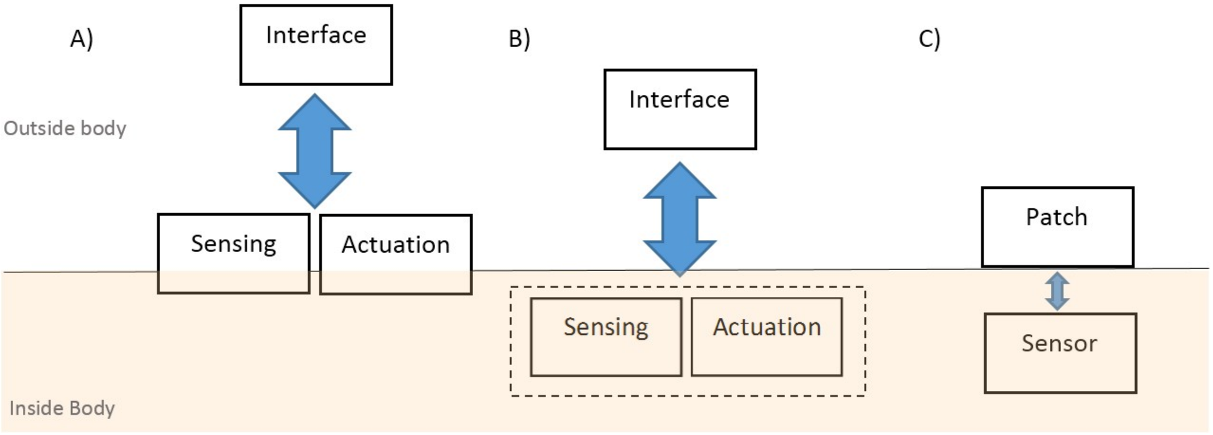


Figure 2: Block diagram of the implantable medical devices, A) Insulin pump and B) Cardiac defibrillator (ICD) and C) Biosensor

The pump system is structured as follows: Personal diabetes manager, which is a tool for performing remote calculations of insulin dosages required by patient, is linked to the pod with a built-in pumping device. In turn, it may be inferred from Figure 2 A that the pumping mechanism referred to above is composed of a number of varying components, such as infusion set, system for control, insulin reservoir, interface and sensing part. After the sets for infusing insulin are submerged under the skin of a diabetic patient, the pump reservoir starts injecting insulin dosages into the patient's organism. Then, the patient may make all necessary insulin dose adjustments via the pump's control system and its sensing components. For patients' convenience, the manufacturers equipped the insulin pump with an interface which allows a hand-held operation of the device by the patient or medical center.

As regards the structure, insulin pumps are similar to cardiac defibrillators which are also fully implantable into the human body (Figure 2 B).

Figure 2 C presents an overview of implantable biosensors. The main purpose of implantable biosensors is to routinely gather biological data on patient's health conditions and transfer it to other connected devices for further storing and analyzing . Depending on the sphere of application, biosensors may be

both low-rate and high-rate [39].

2.2.1 Insulin pump

Implantable category embraces the type of pumps which are intended to be introduced into the human body for therapeutic purposes (i.e. regular injections of life-supporting medicines). As a matter of fact, implantable pumps are slightly different from the ordinary insulin infusion devices, widely applicable in the medical sphere [58]. Main purpose of implantable insulin pump is to regulate the glucose level in the patient's blood by continuous insulin injections.

It is a known fact that nowadays a lot of different hardware for embedded systems is available in the market. Considering that, many researchers have been working primarily on comparison of various types of hardware rather than focusing on its constituent parts. For instance, [9] shows design and architecture elements of an insulin pump as an embedded system. General available insulin pump distributes insulin dosages automatically in the accord with the limited daily amount of insulin (Total delivery limit of the day, hereinafter - "TDD").

As a sample, the device in [55] consists of a glucometer and a pump: Insulin pump is controlled by MS3P430 unit responsible for the graphic LCD and keyboard. RTC guarantees operating the device in real time modes. EEPROM stores the date on the events and system updates. Power module of the device activates cell batteries' voltage. Insulin pumps of such kind are compatible with LEDs, buzzer, vibrator mode.

2.2.2 Implanted defibrillator

The ID (Implanted Defibrillator) is composed of two basic constituent elements namely leads and a pulse generator.

Speaking of pulse generators as element of the ID, these mechanisms have at least three core components: namely capacitor, battery, and central processing unit. Sometimes, pulse generators may be also powered and controlled by minicomputers. Nonetheless, in the prevailing number of cases main energy supply of ID is provided by the battery. When the cardiac arrest happens, the capacitor must immediately apply strong electric shock to the heart. It should be noted that, defibrillation cannot be effectively performed by employing the battery alone. High-energy impulse is indeed generated by the capacitor connected to the battery and its circuit.

All the data logs on patients health conditions collected in the course of ID's operation are stored in the processing unit. Therefore, the processing unit is often referred to as control center of the device. Currently there exist three types of ICDs: Single chamber, Dual chamber and Biventricular [6] . Particular type of implant is recommended for the patient upon assessment of the individual needs and evaluation of prescribed treatment.

2.2.3 Biosensors

Biosensors are employed to identify and quantify the analyte interest. Samples can be extracted from water, food, blood, or urine. Mainly, biosensor architecture involves biological recognition elements which can interact with the chosen analytes. To enable converting analyte into a signal, biological recognition element must be brought in direct contact with the transducer [23, 24].

The set of security challenges pertinent to biosensors requires consideration of specific countermeasures. And since biosensors are exposed to uncommon threats, solutions cannot be easily derived [16].

3 Communication vulnerabilities

Figure 3 overviews the FCC standards and technologies for short and long range devices and applicable US regulations which are explained and listed in [11]. FCC classified WSN-based medical systems into two groups: short-range devices and long-range devices. During the long-range transaction data is received by remote monitoring station, whereas short-range transactions are intended for locally based receivers. Recently, FCC revised its standards for medical devices to keep up with the technological progress. Thus, wireless medical products are released to US market only having been authorized by FDA and certified in FCC. With regard to the fact that wireless systems incorporate radio technology, all such devices fall under the scope of FCC's regulation that are listed in Figure 3.

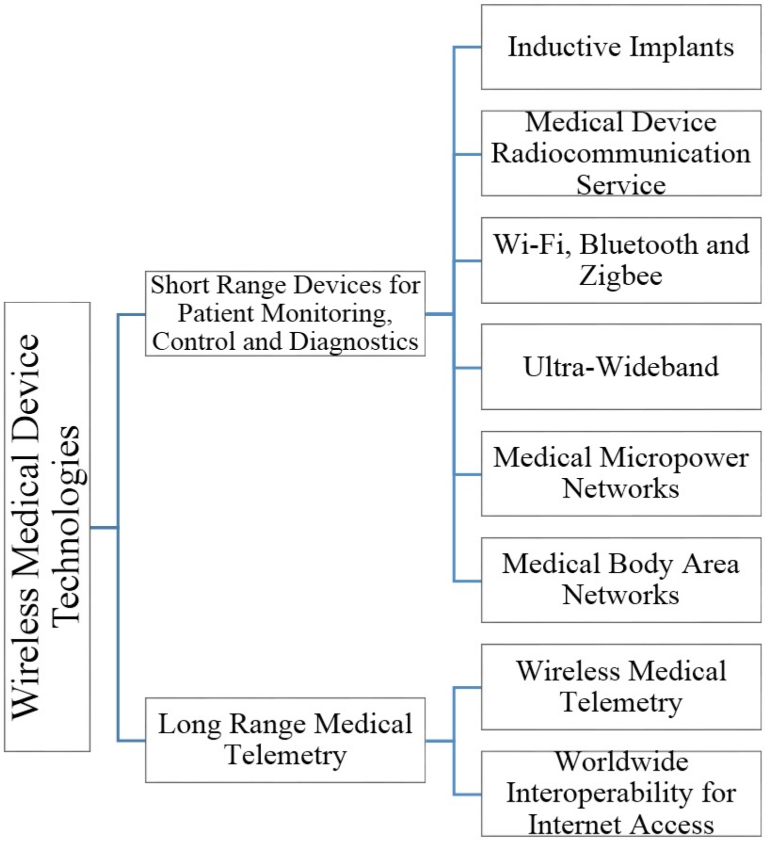

Wireless Medical Device Technologies
Short Range Devices for Patient Monitoring, Control and Diagnostics
Long Range Medical Telemetry
Inductive Implants
Medical Device Radiocommunication Service
Wi-Fi, Bluetooth and Zigbee
Ultra-Wideband
Medical Micropower Networks
Medical Body Area Networks
Wireless Medical Telemetry
Worldwide Interoperability for Internet Access

Figure 3: Wireless Medical Device technologies' category

As stated in [11], prior to development of the Wireless Medical Telemetry, which was coordinated by FCC, IEEE became pioneers of the newly-emerged LAN market. In particular, IEEE proposed 802.11 LAN standard, designed to suit the needs of ISM (Industrial Scientific and Medical) band at 2.4 GHz. Whereas the initial variants of 802.11 standard were only capable of conducting short range transmissions (for example, data exchanges between medical systems within one hospital), further versions of this LAN standard could be applied for transmitting signals at much longer ranges and varying rates of data. Based on the 802.11 standard's broad functionality, it stands a chance to be acknowledged as the most popular and effective tool for telemetry data operations.

As it is known, both Zigbee and Bluetooth protocols demonstrate best efficiency in transmitting data at short ranges and with low expenditures of power.

In contrast to Bluetooth, which is usually used for facilitating connection between a receiver and base, Zigbee protocols are mainly devised for managing a chain of interconnected system. Accordingly, groups of implants may as well be controlled with the aid of Zigbee.

3.1 Security and privacy

Currently, the most common security issues that may threaten stability and reliability of the systems are as follows: emergent threats, lack of access control, encryption failures, human factor, foundation and design shortages of hardware, insufficient privacy policy and discrepant software specifications [54]. The more complex is the structure and role of the equipment, the more specific threats are likely to emerge in the process of its functioning. In [18], the main focus is placed on the factors which affect security of the implantable medical devices and so far, three main sources of security errors were identified:

- Fundamental tensions: the core problem lies in the conflict of privacy enhanced access control and overall utility of the implant. Due to the strength of implant's cryptography there arises risk of doctors' failure to gain immediate access to the implant in the case of near-death conditions or other emergency situations. In [26] the authors' attention was given to the utility and safety goals pursued by IMDs manufacturers and their probable conflict with the security and privacy systems of these devices.

- Software risks: software vulnerabilities have many underlying causes, and from time to time some of them emerge due to incoherent co-functioning of hardware and software of the implant or because of software complexities [34].

- Human factors: system security is frequently affected by the incorrect application of its features by system's users. For instance, users ignoring basic commands such as security warnings risk destabilizing the entire system as well as exposing it for further dangers [53].

Owing to rapid development of the sensor-based medical technology, biomedical community is now prompted to seek solutions for the problems which were initially encountered only in connection with the security instruments. The authors in [18] are opined that the best result as regards this objective will be achieved through establishing collaboration between biomedical engineers and the security researchers. Apart from the aforementioned constrains, IMDs do not differ much from other network computing devices, therefore, basic security and privacy risks apply to IMDs as like to any other device. This poses a challenge to device designers who are now struggling to adapt available security mechanisms to the biomedical domain.

In order to maximize safety and privacy of the IMDs and BANs (Body area networks), security instruments are recommended for incorporation into all stages of the devices' life circle. Three main pillars of security system in IMDs and BANs are the following: confidentiality, integrity and availability. However, other supportive security goals may also be mentioned in the same line. Even though these objectives bear some resemblance with long established confidentiality principles, the authors in [47] believe that comprehensible treatment of privacy will be achieved only by adopting complex cross-domain approach.

3.1.1 ZigBee

Recently, there appeared an innovative up-and-coming standard known under the marketing name ZigBee. The newly emerged technology enables rapid wireless communication at a reduced energy cost. One of the most attractive features of ZigBee is its compatibility with multiple types of sensor-based instruments including low-power networks.

Another important feature of ZigBee is its strong security system which incorporates a wide range of advanced functions, such as, for example, complicated set of cryptographic tools, valuable cipher algorithms and newly developed control tools.

Noting the novelty of ZigBee, it is not surprising that several impediments of the instrument have been already determined by the specialists. The security system of ZigBee critically requires several enhancements, which will be considered below:

- Firstly, there have arisen several problems as regards onboard keying material. In lieu of certain deficiencies overlooked by the developers the node does not simultaneously turn off along with termination of the networks' operation [62, 48]:
    - Same Key in Multiple ACL Entries
    - Network Shared key
- Another stringent issue is the lack of storage space which closes off possibilities of equipping the device with the data on its specifications. Still, such information may be required to safeguard effective application of the tool.
- Finally, despite the fact that ZigBee was designed as the next generation tool, the problem of power limitations, typical of all WSNs, is recurrent in ZigBee as well. Having extended the battery life of the device up to two years, the developers compromised ZigBee's energy capacity. As a result, many heavy data-based operations will not be supported by ZigBee unless its power consumption capabilities are expanded [41]. Also, ACL state is properly maintained even during power interruptions, Notwithstanding that, communication insecurities are most likely to occur in two following states [48]:
    - Power Failure
    - Low Powered Operation

3.1.2 Bluetooth

Security violations in the wireless environment have become more common with the rapid increase in usage of Bluetooth-based devices. With regard to this tendency, the architecture of Bluetooth-based devices should incorporate novel solutions to withstand any security failures.

Table 2 contains the results of the assessment on the standards associated with the security of Bluetooth transmissions.The studies reflected in the table encompasses evaluation of such components of Bluetooth security mechanisms as basic security frameworks, validation of the codes, principles of data encryption, management of the keys and approvals of the data transferring.

In general, the systems of Bluetooth security are considered to be solid relatively safe. However, more remote transmissions via Bluetooth might be impeded if the scheme for location of Bluetooth-connected devices is not planned well enough. Other disadvantages related to the Bluetooth connections are as follows : impossibility to change the key of the unit, improper supervision, problems with the PIN code, lack of regularity in the number era.

3.1.3 Wi-Fi

Usually, security in Wi-Fi networks is achieved on account of cryptography and related methods. Essentially, there are two pillars of Wi-Fi security, namely, privacy and authentication mechanisms. It should

Table 1: Security of ZigBee network's vulnerabilities and proposed solution

Reference	Problem	Solution
[46]	Vulnerability of ACK Authenticity And Data Authentication	Proposed protocol based on Message Authentication Code (MAC) and encryption ACK of packet by AES
[50]	Confidentiality data in home automation, Authentication home user	Proposed Attribute Based Proxy Re-encryption (ABPRE) model
[51]	Vulnerability In Authentication	Proposed the Key management based on Hummingbird
[12]	Vulnerability in key distribution	Proposed Multiple Key Protocol based on AES-128 CCM and ECC
[50]	Vulnerability in key distribution	Proposed an application of attributed-based cryptography mechanism
[33]	Vulnerability in Key distribution of new joining node	Proposed the novel security mechanism based on Elliptical Curve Identity Cryptography
[35]	Vulnerability in key storage and key distribution	Proposed the Efficient Group Key Management
[17]	Vulnerability in key distribution	Proposed Key Management based on Elliptic Curve Diffie Hellman and SubMAC
[52]	Vulnerability of ZigBee security in application layer	Proposed model that introduced a MSG frame on the APS
[37]	Complexity and high power mechanism	Propose Application Frame work based on data integrity
[22]	Vulnerability in devices that leaving the network	Proposed Home Certification Authority (HCA).

be considered that these principles apply to Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) [27]. Privacy method can be summarized as restriction of access to the network for unauthorized users. Authentication method presupposes preliminary input of secret code by users before connecting to the network.

- Breaking Confidentiality in Wi-Fi [27]

  Encrypting application level data is a popular method of ensuring confidentiality protection. WEP, which is the common security tool, has 7 glaring vulnerabilities:

Table 2: Vulnerability Analysis of the Bluetooth Standard [38, 44]

Vulnerabilities	Attack/Risk	Countermeasure/Solution
The quality of pseudorandom number	Pseudorandom number Generator	Statistical tests to detect non-repeating and randomly generated requirement
PIN key is too short or zero	Easy to guess PIN key	Increase the PIN code length
Need to physically enter PIN code to the device	Inconvenient PIN code input	Application level key agreement software
Initialization of key is too weak	Depend on both RAND and PIN which are both unsafe	New strong initialization key scheme
Unit key is reusable	Calculate encryption key OR impersonate other devices with their unit key	Use unit key as input to generate random key
Shared master key	Impersonating or disclosing	Change broadcast scheme
No user authentication	Device Embezzling	User Authentication
Repeating attend for authentication	Disabling Authentication attempts from legitimate devices	Encrypting device address
Weak E0 stream cipher	Shortcut attack ; guess the content of E0	Replace the cipher with the other advanced scheme
Negotiable key length	Encryption abort	Globe agreement on minimal key length
Leak support for legacy applications	Security manager stands idle, no security for legacy applications	Add a Bluetooth-aware "adapter" application for legacy application
No separately defined authorization for services.	No service related flexible device trusting assignment	Modify security manager and the registration processes
Unidirectional access check but bidirectional traffic	Malicious verifier attacks claimant by nasty messages	Access check at all the phases and mutually. Check consistent data flaw direction.

1. The RC4 algorithm for key scheduling may be decoded by hackers
2. Passphrase seeded WEP key may be accessed via a dictionary brute-force attack.
3. Familiar (Initialization Vector) IV/key sequence databases may be used for various decryptions of packets.
4. Plaintext attacks may be conducted inductively
5. WEP is decodable through double encryption.
6. Hackers are able to redirect encrypted data to externally controlled IPs
7. WEB keys may be verified offline.

- Breaking Authentication in Wi-Fi

  There are two authentication modes:

  1. Open System: access point is made available to all users benefiting from Wi-Fi network.
  2. Shared Key: network is accessed exclusively by inputting the key, which is the same for all users.

  Here, we will not concentrate on the issues related to open system authentication in view of the fact that it incorporates a null authentication mechanism. As opposed to open authentication, shared key authentication is based on an ordinary scheme of challenge and nonce. When the connection is attempted by user, clear text random string of challenge-text is generated. At the access point, user must decrypt the nonce using the registered web key. The key is then processed by the system and in case the response of the access point is positive, access will be allowed.

  Encrypted and non-encrypted networks may be equally accessed with the aid of shared key method. The shared key is a compulsory requirement for access to the network even when it is not encrypted. Necessity to observe this requirement is explained by the fact that non-encrypted network responds to the access key input by sending clear-text.

3.1.4 UWB

Not long ago, incorporation of UWB radio technology into wireless devices was licensed in the US by the legislators [10]. Some of the complications that occur with UWB devices include standardization problems and regulatory non-compliance. Another issue requiring focus is the need to meet the energy constraints during performance of UWB physical layer. At the same time, the energy costs must be sufficient enough to: a) sustain running of MAC mechanisms b) providing reliable connectivity to backbone systems c) enable ad hoc communication.

Currently, there is a wide range of accessible UWB tools. Existing types of these devices vary from vehicular radar systems, systems for communicating and systems for measurements to imaging systems (i.e. surveillance tools, radars, medical systems, instruments for wall-imaging and others)[45]. Transmitting via UWB are well suited for WSNs because UMB's bandwidth allows establishing effective physical layer security. UWB radio signals are hard to detect at large distances and are often mistaken for white noise. Consequently, WSN transmissions conducted by UWB signals are more protected from interceptions. At the same time, UWB transmissions do not guarantee any better security against close distance attacks. In this regard, there arises need for a new security tool that can be deployed at all layers of WSNs [32].

4 Analysis and comparison

The samples of commercial implanted insulin pump, defibrillator and biosensor prototypes are contained in Table 3. The parameters that are listed in the table are based on common modules and features of these three prototypes. The devices considered in this study mostly have the following constituent elements: control unit, memory, interface, power supply unit and communication unit. The general abstract on the architecture of these devices is contained in Figure 4.

ZigBee, Bluetooth, Wi-Fi and UWB comparison is listed in Table 4. In view of considerable power constraints, Bluetooth and ZigBee based systems are generally installed in portable devices for short range applications. As a result, stable operation of the devices may be maintained at a low energy cost. At the same time, the life of device's battery remains unaffected.

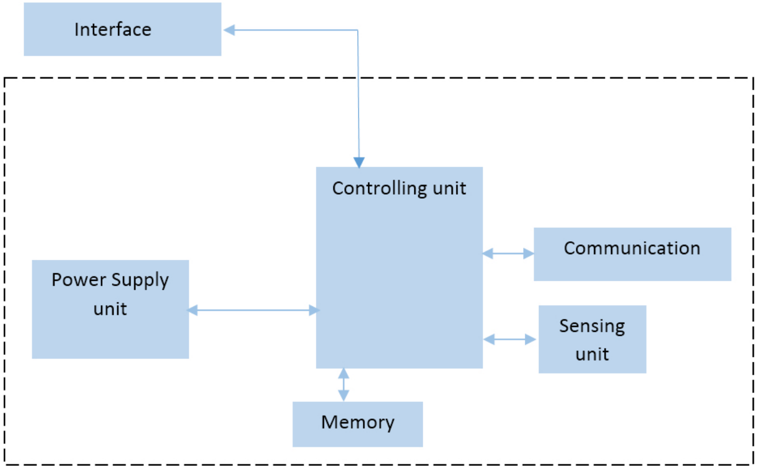


Figure 4: General abstract architecture

In total, reasonable energy consumption of Bluetooth and ZigBee, as it shown in Table 4, provides better compatibility with small-sized devices rather than Wi-Fi, which requires substantial supply of power.

Table 3: Commercial implanted insulin pump, defibrillator and biosensor prototypes hardware elements

Reference	Control Unit	Memory	Battery	Communication	Type
[55]	MSP430	EEPROM	Cell battery	Bluetooth	IP
[49]	MEMS-based	EEPROM	lithium-ion	-	IP
[2]	MEMS-BASED	-	Wireless power rechargeable RF COIL	RF	IP
[4]	PC/104	-	External battery pack and high efficiency step-down DC/DC converter / eight C and eight AA Alkaline batteries	PCMCIA card carrier with a wireless radio LAN adapter	ID
[56]	CC2430 wireless microcontroller	4-kB block of non-volatile	specific battery developed by Tadiran Batteries in a 1520 package, providing 360 mAh and supplying current spikes up to 750 mA	ZigBee	BS

In [20] the authors compared energy consumption of ZigBee and Bluetooth in the period of the cyclic sleep. It should be mentioned here that in general obtaining the information on power costs during sleeping mode is not possible. Yet, approximate energy consumption may be calculated based on cumulative factors including but not limited to sleep currents, data rate, average transmits and receiving.

The assessment was conducted with regard to the following parameters:

1. Time required for reconnecting the system upon termination of sleeping mode
2. Extent of RF module's sleeping between specific data transferring.

As a result, it was determined that Bluetooth allowed saving more energy in the sleeping mode. However ZigBee-based tool was the swiftest one as regards configuring the system at the time of cyclic sleep. It was also established during the experiment on the protocols that power capacity of the devices could be potentially influenced by the locations of transmitter and receiver, variations in packet sizes, characteristics of hubs and others.

Mechanisms for authentication and encryption are retained in all 3 protocols. AES block cypher with CTR and CCM based on 32-bit and 16-bit CRC is typical for ZigBee. In the same vein, Bluetooth systems adopt E0 steam cyphers and 16-bit CRC. Encryption and integrity of 802.11 systems is supported by a RC4 stream and CRC-32 checksum. The focus will be now made on major drawbacks of these systems. Based on conclusions of cryptanalysts, researchers established that WEP keys could be hacked with no difficulty if matching software is applied. Accordingly, the solutions were to install WPA2 to the system, thus upgrading WEP. Despite that, CCM and AES Block cipher were not subjected to any subsequent alterations [36].

Also the table presents summary of the main differences existing among the four protocols. Each protocol is based on an IEEE standard. Obviously, UWB and Wi-Fi provide a higher data rate, while Bluetooth and ZigBee give a lower one. In general, the Bluetooth, UWB, and ZigBee are intended for WPAN communication and may transmit data at distances up to 10 m, while Wi-Fi is oriented to WLAN and allows conduction of long-range transactions over distances up to 100m. The maximum number of devices belonging to the network's building cell is 8 for a Bluetooth and UWB piconet, over 65000 for a ZigBee network, and 2007 for a structured Wi-Fi.

Proper choice of protocols and tools for communication should be based on multiple parameters. As per [21], network solutions may be selected according to the those criteria.

Also, human factors and peculiarities of design should be taken into consideration at the primary stages of building BAN systems.

5 Discussion and conclusion

The extensive progress in designing sophisticated IMDs requires these instruments to be able to establish a safe connection between the implant and external devices. This type of connection proves to be effective only at low frequencies of a carrier. Consequently, the carrier frequency may be gradually increased if it is required [5]. As a highly innovative application, 400 MHz Medical Implant Communication Service (MICS) band [7] may be used for extending the communication range during interaction of implant with other equipment. It should be mentioned that MICS was devised for specific applications in metrology and medicine fields.

[30] presents the results of the study on a) compatibility of various implants' design with the human organism, and b) the correlation between the size/position of body and the propagation of waves generated by the implant. These two parameters, along with other factors presented in Section 2.2, affect the designing of IMDs.

Analysis of IMDs designing parameters and characteristics elaborated in this work suggests the need for reconsideration of security for medical applications. Table 5 demonstrates the results of comparative analysis between Medical BAN and other WSNs.

Table 4: ZigBee, Bluetooth, Wi-Fi and UWB comparison

Standard	UWB	Bluetooth	ZigBee	Wi-Fi
IEEE spec.	(Low-Rate) 802.15.3a	802.15.1	802.15.4	802.11a/b/g
Max signal rate	110 Mb/s (10m) 200 Mb/s (4m)	1 Mb/s	250 Kb/s	54 Mb/s
Nominal range	10 m	10 m	10 - 100 m	100 m
Number of RF channels	(1–15)	79	1/10; 16	14 (2.4 GHz)
Max number of cell nodes	8	8	$>$ 65000	2007
Encryption	AES block cipher (CTR, counter mode)	E0 stream cipher	AES block cipher	RC4 stream cipher (WEP),AES block cipher
Authentication	CBC-MAC (CCM)	Shared secret	CBC-MAC (ext. of CCM)	WPA2 (802.11i)
Data protection	32-bit CRC	16-bit CRC	16-bit CRC	32-bit CRC
Security protocols /Models	-	Security Modes	“High security mode” and “ Standard security mode”	WEP and WPA
POWER - transmit (TX)	˜ 227.3	54	24.7	219
POWER - Receive (RX)	˜ 227.3	47	27	216
Cost	Low	Low	Ultra Low	High

Table 5: The comparative analysis between Medical BAN and other Wireless Sensor Networks

	Medical BAN	General WSN
Common features	Limited resources: battery, computation, memory, energy efficiency, Diversity coexistence environment	
Security	Must be re-considered	Required security
Networking	Small scale	Small and Large scale
	Pre-planned network	Pre-planned or/and Random distribution network
Range	Short range	Short and/or long range

[40] overviews several characteristics which ensure the secure operation of WSN and its constituent elements. One of the critical threats for wireless sensor networks is the series of attacks performed on the system by accessing the gateways to sensor nodes or sensor nodes themselves. Thus, in order to safeguard the WSN from external risks each and every node of the network should be secured individually. Additionally, it is necessary to detect and report failing nodes before their destructive impact destabilizes the whole system. Healing the affected network can be achieved by relying on group key distribution

techniques. Such techniques largely enhance security mechanisms of WSNs without overlapping the energy costs limit. Other techniques such as establishing one shared key make the system vulnerable to hacking, whereas individual keys are more secure but also consume more power. Besides, it should be noted that medical area demands frequent reporting on possible node failures in order to prevent future emergency situations.

Usefulness of wireless security standards is usually determined in the process of the system's practical application. For instance, it may be estimated during the use of the system that its security measure doubles total energy costs, or, on the contrary, assists in maintaining moderate energy expenditure. In this regard, it is nearly impossible to make fair comparison between ZigBee, UWB, Bluetooth and Wi-Fi as regards the benefits of security standards adopted by these systems; since they have variable characteristics and, thus, require different vulnerability solutions. On the whole, UWB is considered as more favorable option for applications that process high rate data, while ZigBee or Bluetooth prove most effective when trained against low rate data [57]. Consequently, in section 3 we focused on short-distance transmissions in the range between 1 and 75 meters performed by inductive implants.

As per the guidelines imposed by FDA, wireless protection mechanisms employed by the medical device that contain (i) key secrecy, (ii) encryption, and (iii) control of access to protected data should correspond to security threats [8].

In this respect, three most common security issues are as follows: jamming, eavesdropping and impersonation. These risks are mainly associated with the lack of effective defense mechanisms and problems with the design of the devices. Hereby, the designers of new wireless medical devices need to upgrade the following parameters: a) reliability, b) battery longevity, c) adaptability, and d) availability [13]. To reach these goals, several issues linked to the IMDs' defense mechanisms should be elaborated in more details as indicated in Table 6:

Table 6: Conflicting requirements in IMD design and security [43]

IMD Needs	Security Needs
Limited energy consumption	Extra processing and signaling
Availability in emergencies	Protection against unauthorized access
No modification for implanted devices	Additional functionalities on IMD
Less software for low susceptibility against software bugs	Extra algorithms for security operations

In [40] the authors suggest Bluetooth as the solution which suits their research objectives. Accordingly, this study sought to provide comparison of medical WSNs' basic parameters with particular focus on communication platforms and their security. Indeed, the key advantages of Bluetooth are its modest size and extensive battery life. Such features are especially useful in providing regular medical monitoring: convenient size and ability of the sensor to retain its charge over sufficiently long periods facilitates patients' adherence to the treatment plan. Adopting the communication protocols built on IEEE 802.15 standard provides better compliance with the standards of the network such as required frequency and range. Insofar as it can be ascertained, Bluetooth-based low energy tools are fully compatible with individual Medical WSN systems in terms of the frequencies, latency and expected energy limits. With regard to the above facts, we may thus describe the perfect protocol as swift, scalable, low power consuming and robust.

The outcome of the study points out that to the current date, the pressing need for enhancing the security of wireless communication has been profoundly addressed in related scientific works. Further on, growing popularity of this scientific trend led to development of some feasible techniques to that extent. However, the rapid evolvement of the software utilized in building the IMDs is likely to trigger substantially new operational and security risks, which calls for more research in this area.

Additionally, the paper contains outlines as regards the peculiarities of three types of IMDs, which may be especially useful for scientists whose research interests include security and privacy protection of the implantable and wireless medical devices. The results of our scientific work also correspond with the computer science area, which suggests the possibility of future extensive cooperation between computer science specialists and researchers in the field of biomedics. We believe that combining the approaches available in these two areas may potentially speed up development of stronger and more complex security solutions.

References

[1] http://www.edn.com/common/jumplink.php?target=http%3A%2F%2Fwww.continuaalliance.org [Online; Accessed on August 5, 2016].

[2] https://www.academia.edu/4212752/MEMS-based_Implantable_Drug_Delivery_System [Online; Accessed on August 5, 2016].

[3] Content of premarket submissions for management of cybersecurity in medical devices–draft guidance for industry and food and drug administration staff. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm [Online; Accessed on August 5, 2016].

[4] An eight channel telemetry system for chronic ecg recording. http://baby.indstate.edu/isb/publications/15th_isob_proceedings/6/6.htm [Online; Accessed on August 5, 2016].

[5] Low-power medical implant communication service (mics) transceiver. https://www.mosis.com/files/research/2008/ncat_dogan_prop_0707.036.pdf [Online; Accessed on August 5, 2016].

[6] Patient specific implants. http://www.buzzle.com/articles/defibrillator-implant.html [Online; Accessed on August 5, 2016].

[7] Planning for medical implant communications systems (mics) related devices. http://acma.gov.au/webwr/radcomm/frequency_planning/spps/0306spp.pdf [Online; Accessed on August 5, 2016].

[8] Radio frequency wireless technology in medical devices. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf [Online; Accessed on August 5, 2016].

[9] Texas instruments infusion pump solutions. http://www.ti.com/solution/infusion_pump [Online; Accessed on August 5, 2016].

[10] Ultra wide band devices. Radio Spectrum Policy and Planning, Resources and Networks Branch, Ministry of Economic Development, New Zealand, April 2005. http://www.ieee802.org/18/Meeting_documents/2005_May/NZ%20UWB%20Eng%20Discussion.pdf [Online; Accessed on August 5, 2016].

[11] Wireless medical technologies: Navigating goverment regulation in the new medicatl age. Fish's Regulatory & Government Affairs Group White Paper, November 2013. http://www.fr.com/files/Uploads/attachments/FinalRegulatoryWhitePaperWirelessMedicalTechnologies.pdf [Online; Accessed on August 5, 2016].

[12] S. Al-alak, Z. Ahmed, A. Abdullah, and S. Subramiam. Aes and ecc mixed for zigbee wireless sensor security. *International Journal of Electrical, Computer, Energetic, Electronic and communication Engineering*, 5(9):1219–1223, 2011.

[13] Z. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan. A comparative review on the wireless implantable medical devices privacy and security. In *Proc. of the 2014 EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth'14), Athens, Greece*, pages 246–249. IEEE, November 2014.

[14] W. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In *Proc. of the 49th ACM/EDAC/IEEE Annual Design Automation Conference (DAC'12), San Francisco, CA*, pages 12–17. IEEE, June 2012.

[15] M. Castelluccio. A new bluetooth in 2016. *Strategic Finance*, 97(6):55, 2015.

[16] S. Cherukuri, K. K. Venkatasubramanian, and S. K. Gupta. Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In *Proc. of the 2003*

International Conference on Parallel Processing Workshops (ICPPW'03), Kaohsiung, Taiwan, pages 432–439. IEEE, October 2003.

[17] K. Choi, M. Yun, K. Chae, and M. Kim. An enhanced key management using zigbee pro for wireless sensor networks. In *Proc. of the 2012 International Conference on Information Networking (ICOIN'12), Bangkok, Thailand*, pages 399–403. IEEE, 2012.

[18] S. S. Clark and K. Fu. Recent results in computer security for medical devices. In *Wireless Mobile Communication and Healthcare - Revised Selected Papers from the 2nd International ICST Conference, MobiHealth 2011, Kos Island, Greece, October 5-7, 2011*, volume 83 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 111–118. Springer Berlin Heidelberg, 2012.

[19] A. Darwish and A. E. Hassanien. Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors*, 11(6):5561–5595, 2011.

[20] A. Dementyev, S. Hodges, S. Taylor, and J. Smith. Power consumption analysis of bluetooth low energy, zigbee and ant sensor nodes in a cyclic sleep scenario. In *Proc. of the 2013 IEEE International Wireless Symposium (IWS'13), Beijing, China*, pages 1–4. IEEE, April 2013.

[21] A. Devineni. *Performance evaluation of body area network using ZigBee protocol*. PhD thesis, San Diego State University, 2011.

[22] G. Dini and M. Tiloca. Considerations on security in zigbee networks. In *Proc. of the 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'10), Newport Beach, CA, USA*, pages 58–65. IEEE, June 2010.

[23] B. R. Eggins. *Biosensors: an introduction*. Springer-Verlag, 2013.

[24] R. Fogel and J. Limson. Developing biosensors in developing countries: South africa as a case study. *Biosensors*, 6(1):5:1–5:17, 2016.

[25] N. Gordon, U. Sagman, and C. N. Alliance. *Nanomedicine taxonomy*. Canadian Institutes of Health Research, 2003.

[26] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7(1):30–39, 2008.

[27] H. Helleseth. Wi-fi security how to break and exploit. Master's thesis, Department of Informatics, University of Bergen, Norway, June 2006.

[28] S. Hosseini-Khayat. A lightweight security protocol for ultra-low power asic implementation for wireless implantable medical devices. In *Proc. of the 2011 5th International Symposium on Medical Information & Communication Technology (ISMICT'11), Montreux, Switzerland*, pages 6–9. IEEE, May 2011.

[29] A. Inmann and D. Hodgins. *Implantable Sensor Systems for Medical Applications*. Elsevier, 2013.

[30] A. Johansson. *Wireless communication with medical implants: antennas and propagation*. PhD thesis, Lund University, 2004.

[31] Y.-H. Joung. Development of implantable medical devices: from an engineering perspective. *International neurourology journal*, 17(3):98–106, 2013.

[32] E. Karapistoli and A. A. Economides. Adlu: a novel anomaly detection and location-attribution algorithm for uwb wireless sensor networks. *EURASIP Journal on Information Security*, 2014(1):1–12, 2014.

[33] H. Kim, C. H. Kim, and J.-M. Chung. A novel elliptical curve id cryptography protocol for multi-hop zigbee sensor networks. *Wireless Communications and Mobile Computing*, 12(2):145–157, 2012.

[34] S. D. Kobes. Security implications of implantable medical devices. Master's thesis, Iowa State University, 2014.

[35] Y. Kwon and H. Kim. Efficient group key management of zigbee network for home automation. In *Proc. of the 2012 IEEE International Conference on Consumer Electronics (ICCE'12), Las Vegas, NV, USA*, pages 378–379. IEEE, January 2012.

[36] J.-S. Lee, Y.-W. Su, and C.-C. Shen. A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi. In *Proc. of the 33rd Annual Conference of IEEE Industrial Electronics (IECON'07), Taipei, Taiwan*, pages 46–51. IEEE, November 2007.

[37] H. Li, Z. Jia, and X. Xue. Application and analysis of zigbee security services specification. In *Proc. of*

the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC'10), Wuhan, China, volume 2, pages 494–497. IEEE, April 2010.

[38] B. K. Mandal, D. Bhattacharyya, and T.-h. Kim. A design approach for wireless communication security in bluetooth network. *International Journal of Security & Its Applications*, 8(2), 2014.

[39] M. Mark. *Powering mm-Size Wireless Implants for Brain-Machine Interfaces*. PhD thesis, University of California, Berkeley, 2011.

[40] A. Mathur and T. Newe. Comparison and overview of wireless sensor network systems for medical applications. In *Proc. of the 8th International Conference on Sensing Technology, Liverpool, UK*, pages 272–277, Sepember 2014.

[41] R. Meyer. Security issues and vulnerability assessment of zigbee enabled home area network implementations. Master's thesis, the faculty of the Department of Computer Science, California State University, USA, 2012.

[42] N. Minar and M. Tarique. Bluetooth security threats and solutions: a survey. *International Journal of Distributed and Parallel Systems (IJDPS)*, 3(1):86–94, 2012.

[43] L. OTT. The evolution of bluetooth® in wireless medical devices. Socket Mobile, Inc. White Papers, July 2010. `https://www.socketmobile.com/docs/default-source/white-papers/socket_bluetooth-medical_white-paper.pdf?sfvrsn=2` [Online; Accessed on August 5, 2016].

[44] J. Padgette, K. Scarfone, and L. Chen. Bluetooth security guide: Recommendations of the national institute of standards and technology. NIST Special Publication 800-121, Revision 1, June 2012. `http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf` [Online; Accessed on August 5, 2016].

[45] D. Porcino and W. Hirt. Ultra-wideband radio technology: potential and challenges ahead. *IEEE Communications Magazine*, 41(7):66–74, 2003.

[46] D. Rossi, M. Omana, D. Giaffreda, and C. Metra. Secure communication protocol for wireless sensor networks. In *Proc. of the 2010 East-West Design & Test Symposium (EWDTS'10), St. Petersburg, Russia*. IEEE, September 2010.

[47] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *Proc. of the 2014 IEEE Symposium on Security and Privacy (SP'14), San Jose, CA, USA*, pages 524–539. IEEE, May 2014.

[48] N. Sastry and D. Wagner. Security considerations for ieee 802.15. 4 networks. In *Proc. of the 3rd ACM workshop on Wireless Security (WiSe'04), Philadelphia, PA, USA*, pages 32–42. ACM, October 2004.

[49] L. Schetky, P. Jardine, and F. Moussy. A closed loop implantable artificial pancreas using thin film nitinol mems pumps. In *Proc. of the 2003 International Conference on Shape Memory and Superelastic Technologies (SMST'03), Pacific Grove, CA, USA*, pages 555–561, May 2004.

[50] H. Seo and H. Kim. Zigbee security for visitors in home automation using attribute based proxy re-encryption. In *Proc. of the 15th IEEE International Symposium on Consumer Electronics (ISCE'11), Singapore*, pages 304–307. IEEE, June 2011.

[51] S. Seshabhattar, P. Yenigalla, P. Krier, and D. Engels. Hummingbird key establishment protocol for low-power zigbee. In *Proc. of the 2011 IEEE Consumer Communications and Networking Conference (CCNC'11), Las Vegas, NV, USA*, pages 447–451. IEEE, January 2011.

[52] M. Sun and Y. Qian. Study and application of security based on zigbee standard. In *Proc. of the 3rd International Conference on Multimedia Information Networking and Security (MINES'11), Shanghai, China*, pages 508–511. IEEE, November 2011.

[53] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of ssl warning effectiveness. In *Proc. of the 18th USENIX Security Symposium (USENIX Security '09), Montreal, Canada*, pages 399–416. USENIX Association, August 2009.

[54] Trusted Information Sharing Network. User-access management: a defence in depth control analysis, June 2008. `http://www.tisn.gov.au/Documents/User-Access+Management++A+Defence+in+Depth+Control+Analysis.doc` [Online; Accessed on August 5, 2016].

[55] A. V, M. H. T. P, N. R, and R. A. Reliable and affordable embedded system solution for continuous blood glucose maintaining system with wireless connectivity to blood glucose measuring system. *IJCA Proceedings*

on Amrita International Conference of Women in Computing - 2013, AICWIC(2):36–43, January 2013.

[56] P. Valdastri, E. Susilo, T. Forster, C. Strohhofer, A. Menciassi, and P. Dario. Wireless implantable electronic platform for chronic fluorescent-based biosensors. *IEEE Transactions on Biomedical Engineering*, 58(6):1846–1854, 2011.

[57] P. Valdastri, E. Susilo, T. Forster, C. Strohhofer, A. Menciassi, and P. Dario. Wireless implantable electronic platform for chronic fluorescent-based biosensors. *IEEE Transactions on Biomedical Engineering*, 58(6):1846–1854, June 2011.

[58] P. R. van Dijk, S. J. Logtenberg, K. H. Groenier, J. W. Haveman, N. Kleefstra, and H. J. Bilo. Complications of continuous intraperitoneal insulin infusion with an implantable pump. *World journal of diabetes*, 3(8):142–148, 2012.

[59] N. van Hemel and E. van der Wall. 8 october 1958, day for the implantable pacemaker. *Netherlands Heart Journal*, 16(1):1–2, 2008.

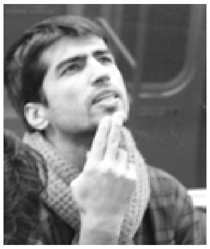
[60] D. Welch and S. Lathrop. Wireless security threat taxonomy. In *Proc. of the 4th Annual IEEE SMC Information Assurance Workshop (IAW'03), New York, USA*, pages 76–83. IEEE, June 2003.

[61] G.-Z. Yang and M. Yacoub. *Body sensor networks*. Springer, 2006.

[62] E. Yuksel, H. R. Nielson, and F. Nielson. *Qualitative and quantitative security analyses for zigbee wireless sensor networks*. PhD thesis, Technical University of DenmarkDanmarks Tekniske Universitet, Department of Applied Mathematics and Computer ScienceInstitut for Matematik og Computer Science, 2011.

Author Biography

Siamak Aram received his Master degree in Networking and Data Security from Sharif University of Technology in 2009. Further on, in 2011 Siamak Aram commenced his PhD Programme in Politecnico di Torino. Consequently, in July 2014 Siamak commenced another research mission in Howard University, Washington DC as a visiting scholar. From 2015 he has been a postdoctoral fellow at the school of Medicine in the University of Maryland in Baltimore and is now focusing on finding biomarkers for gambling problems.



Rouzbeh A. Shirvani is currently a PhD student in Electrical Engineering at Howard University. Prior to coming to Howard University he received his Master's degree from Sharif University of Technology and Bachelor's degree from Iran University of Science and Technology both in Electrical Engineering. His main research focus is in the area of Text/Speech/Image processing and data mining with focus on machine learning.

Eros G. Pasero is is Professor of Electronics at the Politecnico of Turin since 1991 after a four year appointment as Professor at the University of Roma, Electronics Engineering. He was also Visiting Professor at ICSI, UC Berkeley, CA in 1991, Professor of digital electronics and electronic systems at Tongji University, Shanghai, China in 2011 and Professor of digital electronics and electronic systems at TTPU (Turin Tashkent Politechic University), Tashkent, Uzbekistan since 2012. Prof. Pasero interests lie in Artificial Neural Networks and Electronic Sensors. He created in 1990 the Neuronica Lab where hardware neurons and synapses are studied for neuromorphic approaches; neural software applications are applied to real life proof of concepts. Innovative wired and wireless sensors are also developed for biomedical, environmental, automotive applications. Data coming from sensors are post processed by means of artificial neural networks. Prof. Pasero is now the President of SIREN, the Italian Society for Neural Networks; he was v. General Chairman of IJCNN2000 in Como, General Chairman of SIRWEC2006 in Turin. He holds 5 international patents (two were the first silicon European neurons and synapse together Texas Instruments). He was supervisor of tenths of international Ph.D and hundredths of Master students and he is author of more than 100 international publications. He is now involved in several funded research projects among which: AWIS (Airport Winter Information Systems), ITACA (coffee and hazelnuts quality assessment processes, THOR (electrical intelligent car), OPLON (remote control of at risk persons), MIE (Intelligent Suistanable Mobility), NEC (Neural Engineering and Computation Lab), MAKE LAB.

Mohamed F. Chouikha is a Professor and Chair of the department of Electrical and Computer Engineering at Howard University. Dr. Chouikha received his Ph.D. from the University of Colorado in Boulder. He is a Senior Member of IEEE with primary expertise in signal processing and in detection and estimation. During the last 28 years his research activity has been quite diverse. His funded research areas include sensory data fusion, adaptive signal processing, statistical machine learning with application to pattern recognition, human detection in infrared imaging, advanced perception for XUV, wireless communication and intelligent signal processing and control.