Security in wireless body area networks: from in-body to off-body communications

Usman, Muhammad; Asghar, Muhammad Rizwan; Ansari, Imran Shafique; Qaraqe, Marwa

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2018.2873825

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Usman, M, Asghar, MR, Ansari, IS & Qaraqe, M 2018, 'Security in wireless body area networks: from in-body to off-body communications', *IEEE Access*, vol. 6, pp. 58064-58074.
https://doi.org/10.1109/ACCESS.2018.2873825

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 2, 2018, accepted September 19, 2018, date of publication October 4, 2018, date of current version October 29, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2873825

Security in Wireless Body Area Networks: From In-Body to Off-Body Communications

MUHAMMAD USMAN[1], (Member, IEEE), MUHAMMAD RIZWAN ASGHAR[2], IMRAN SHAFIQUE ANSARI[3], (Member, IEEE), AND MARWA QARAQE[1]

[1]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha 34110, Qatar
[2]Department of Computer Science, The University of Auckland, Auckland 1142, New Zealand
[3]School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K.

Corresponding author: Muhammad Usman (musman@hbku.edu.qa)

The publication of this article was funded by the Qatar National Library.

ABSTRACT Wireless body area networks (WBANs) play a vital role in shaping today's healthcare systems. Given the critical nature of a WBAN in one's health to automatically monitor and diagnose health issues, security and privacy of these healthcare systems need a special attention. In this paper, we first propose a novel four-tier architecture of remote health monitoring system and then identify the security requirements and challenges at each tier. We provide a concise survey of the literature aimed at improving the security and privacy of WBANs and then present a comprehensive overview of the problem. In particular, we stress that the inclusion of *in vivo* nano-networks in a remote healthcare monitoring system is imperative for its completeness. To this end, we elaborate on security threats and concerns in nano-networks and medical implants as well as we emphasize on presenting a holistic framework of an overall ecosystem for WBANs, which is essential to ensure end-to-end security. Lastly, we discuss some limitations of current WBANs.

INDEX TERMS WBAN, privacy, security, healthcare systems, remote monitoring, in-vivo communication, nano-networks, implants, wearables.

I. INTRODUCTION

Information and Communication Technologies (ICT) have radically changed the way the patients are treated in this modern era as they are able to receive improved healthcare services. Prior to the emergence of ICT, traditional healthcare systems have been used to provide healthcare services; however, traditional ways of healthcare management are unable to meet the healthcare needs of rapidly growing population of the world [1], [2]. Unfortunately, millions of people around the globe suffer from heart and chronic diseases: hypertension, diabetes, arthritis, asthma, cancer, Chronic Obstructive Pulmonary Disease (COPD), dementia and pain are prominent ones among many others. It is important to note that an early detection of a chronic disease helps healthcare professionals to provide necessary treatment in advance of potential complication(s), hence minimises expensive treatment [3].

In recent years, the need for a complete ecosystem for remote health monitoring systems has been increased, where a physician, using biomedical sensors, should not only monitor patients' physiological values but also must be able to treat or medicate abnormalities in those values remotely. Indeed, ICT can be integrated into traditional healthcare processes in order to develop an electronic healthcare system that can offer better healthcare services [4]. Such a new electronic healthcare system includes a successful integration of general communication networks, data analytics, and humans. Modern healthcare systems also include Wireless Body Area Networks (WBANs) where a set of sensors acquire health information such as heartbeat, blood pressure, blood sugar, or any deterioration in health of a patient. Such information can be potentially transmitted, utilizing communication technologies, to remote servers accessible by healthcare professionals for monitoring, diagnosis, or treatment purposes [5].

The biosensors in a traditional WBAN mainly include, but are not limited to, Implanted Cardiac Defibrillators (ICD), pacemakers, wearables for vital signs, neurostimulators, glucometers, oximeters, and others. The sensors are generally equipped with onboard radios to enable wireless data transfer from/to remote health monitoring units without sacrificing patient's mobility. It is reported that, in 2001, more than 25 million patients in the United States were using medical implants for their treatment and continuous health monitoring [6]. In the recent years, the field of remote healthcare monitoring has gone beyond the medical implants and wearables and entered into an emerging area of biomedical nano-networks. Due to their ability to reach the affected places deep inside the human body, the in-vivo nano-networks has revolutionized modern healthcare monitoring systems [7]. However, most of the works in the literature disregard in-vivo nano-networks when discussing WBANs. For instance, Venkatasubramanian *et al.* [8] define a WBAN as *"a network of economically powered, wireless, wearable, and implanted health monitoring sensors, designed to continually collect and communicate health information from the host they are deployed on"*, which only includes wearables and medical implants without any mention of nano-networks inside human body.

In this article, we present a holistic framework of a remote healthcare monitoring system that takes into account the nano-devices. In addition, we identify and review security and privacy requirements/challenges in such WBANs. We believe that despite the advances in medical implants and other biosensors, an average person's understanding of potential consequences of privacy and security on medical safety is still limited. Apart from the recent requirement of Food and Drug Administration (FDA) to address the privacy and security issues of medical devices for their complete life cycle [9], the manufacturers find no incentive in incorporating to ensure privacy and security in medical devices.

Although, the feasibility of security threats to wearables, medical implants, and nano-networks are debatable, consequences of a potentially insecure health monitoring system could be catastrophic. For instance, any vulnerability in the software or hardware of a remote health monitoring system can potentially breach the confidentially, integrity, and availability of the system in question. Hence, investigating end-to-end security of a complete health monitoring system is as important as the system itself. This end-to-end security ranges from the security of in-body communications (*i.e.,* nano-networks and implants) to off-body communications (*i.e.,* wearables, smartphones and medical server).

In this article, we divide the WBAN into four tiers based on their communication mechanisms. We discuss security requirements and challenges at these tiers and present some security threats. Particularly, we focus on tier-1 and tier-2 since the communication protocols at tier-3 and tier-4 are well established and the security threats and defenses at these two tiers have been widely discussed in the literature [10]–[14].

The contributions of this work are:

- We propose a holistic framework of a complete remote healthcare monitoring system including nano-networks inside a human body (see Fig. 1).
- We investigate current trends in the security of a WBAN, specifically, at tier-1 and tier-2, which mainly include nano-networks and medical implants, respectively.
- We provide a taxonomy of different entities in a remote healthcare ecosystem.
- We comprehend the communication technologies and trends at all tiers.
- We describe security requirements and challenges at tier-1 and 2 of a WBAN along with the potential solutions and future research directions.
- We discuss the limitation of current WBANs in addressing security and privacy issues.

The remainder of the article is organized as follows. Section II presents a complete ecosystem of a WBAN and remote healthcare monitoring system. Security requirements, challenges at different tiers of a WBAN, and their potential solution are described in Section III. Section IV provides a discussion on future directions. Finally, Section V concludes the article.

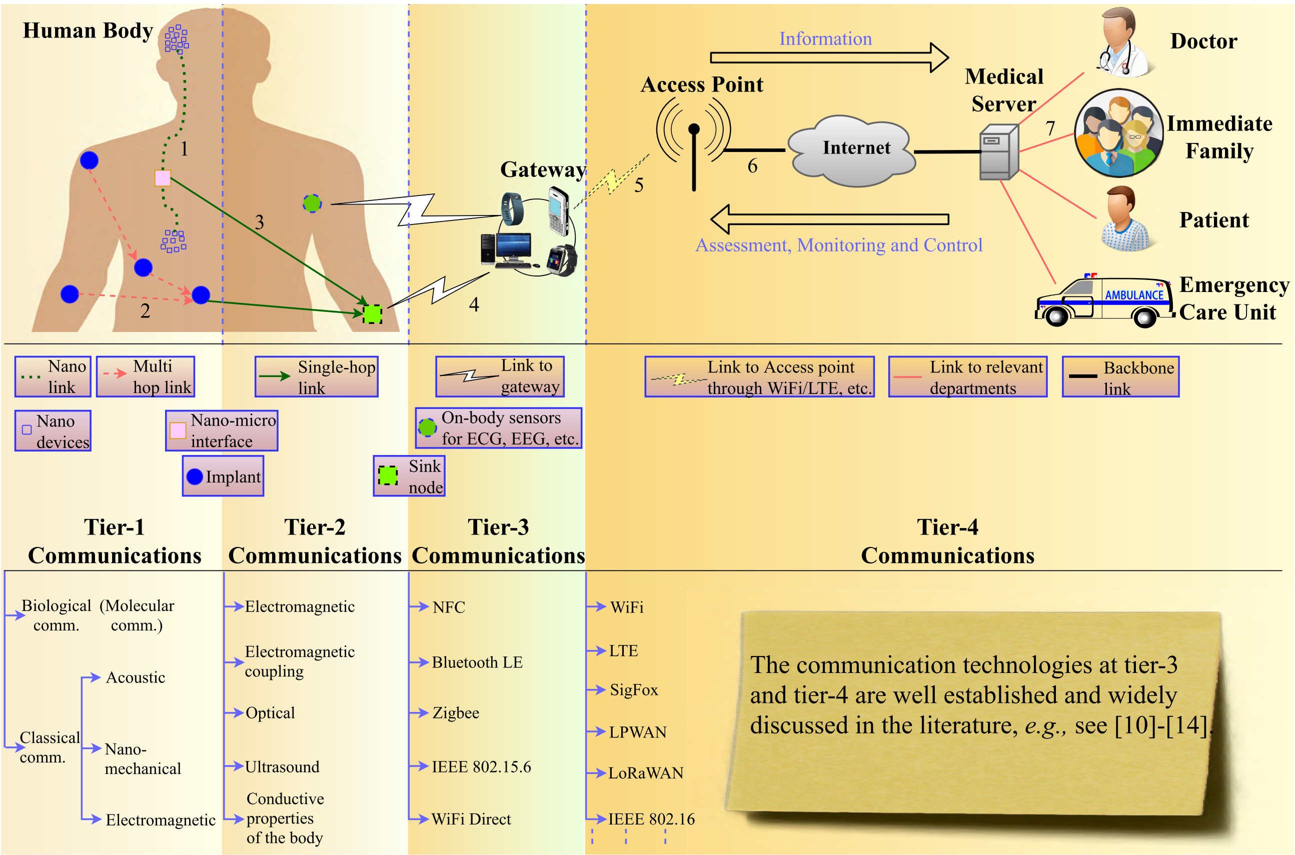
II. WIRELESS BODY AREA NETWORKS

A WBAN is a set of wireless biosensor network nodes (such as wearables, medical implants, and nano-nodes) connected through a star or multi-hop topology. These nodes are typically placed on a human body, implanted in the body, or even swallowed to monitor the vital signs and physiological signals without interrupting the daily routine of a patient. These physiological signals include, but are not limited to, Electrocardiography (ECG), Electroencephalography (EEG), Galvanic Skin Response (GSR), blood flow, glucose level, blood pressure, and blood oxygen level. With the advent of nanotechnology, a natural progression of WBANs is nano-health systems, which is composed of nano-sensors able to perform simple tasks such as computing, sensing, actuation, communication, and storage. Hence, a complete ecosystem of a WBAN, including in-vivo nano-nodes and remote healthcare monitoring system, is presented in Fig. 1.

A. WBAN ARCHITECTURE

Fig. 1 presents a complete architecture of WBAN including in-body, on-body, and off-body communications. In-body communications involve implants and nano-devices placed inside a human body. On-body communications involve the devices placed on the body such as wearables and other sensors for ECG, EEG, blood glucose, and blood pressure monitoring. The interaction of any device outside a human body is categorized as off-body communications. The entities in Fig. 1 can be defined as follows:

- **Nano-devices:** Nano-devices are one of the smallest entities in the healthcare ecosystem able to perform very basic functions at nano-scale, such as computing, data storage, sensing, actuation, and communications [15].
- **Nano-links:** These are communication links between nano-devices and nano-micro interfaces.
- **Nano-micro Interface:** This interface connects nano-devices inside human body to a sink node, which finally connects them to off-body devices.
- **Implant:** This represents a medical device implanted inside human body for monitoring certain diseases, vital signs, or even biometric identification.
- **Sink Node:** Sink node acts like a data hub in WBANs that collects data from different in-body devices to relay it to the medical server and vice versa. In this work,



The communication technologies at tier-3 and tier-4 are well established and widely discussed in the literature, *e.g.*, see [10]-[14].

FIGURE 1. A complete ecosystem of a WBAN and remote healthcare system: WBAN communications can be divided into 4 tiers. At tier-1, both the sender and the receiver reside inside human body (communication links are labeled with 1 and 2). Tier-2 includes the cases when at least one of the communicating devices resides inside human body (communication links are labeled with 3). Moreover, we categorize tier-3 as when at least one of the communication devices is an off-body device (communication links are labeled with 4). Lastly, all communications beyond the gateway are categorized as tier-4 (communication links are labeled with 5 and beyond). In this work, we mainly focus on security requirements of tier-1 and tier-2 communications. Security threats and defenses at tier-3 and tier-4 have been well investigated in numerous works as we can see in the literature [10]–[14].

at some places, we also used the term programmer node (a term sometimes used in the literature for the device that controls and communicates with the medical implants) interchangeably with the sink node.

- **On-body Sensors:** This includes different sensors placed on the skin or inside clothes of a human body to measure and monitor different vital signs such as ECG, EEG, blood pressure, blood glucose, and blood oxygen level.
- **Gateway:** This represents a gateway device employed to connect the WBAN with the medical server. It can be a smartphone or any other device such as a computer or an Internet-of-Things (IoT) device that is directly connected to a base station using, *e.g.,* 3G/4G.
- **Access Point:** This represents a cellular base station or a WiFi access point to route sensor's traffic to the medical server.
- **Medical Server:** This is a database, which stores all information of sensors for further actions and analysis of the data. It can include real-time monitoring of vital signs and virtual clinics wherein patients and physicians can connect online and alert about critical notifications to doctors or immediate family members for a potentially life-threatening condition.

B. DATA COMMUNICATIONS IN WBANS

We divide the ecosystem of remote healthcare monitoring system into four tiers. Each tier has its own protocols, security requirements, data rates, and communication range. Before evaluating end-to-end security requirements of this ecosystem, we first need to understand the communication protocols at each tier.

1) TIER-1 COMMUNICATIONS

We define tier-1 as all in-body communications, *i.e.,* both the sender and the receiver reside inside a human body. The examples include the communications between nano-devices and nano-micro interfaces inside a human body. The communication links labeled number 1 and 2 in Fig. 1 lie in this tier. The communications at this level can be realized by two categories. One is the classical communications, which can be realized by downscaling the existing communication paradigms of general wireless communications to nano-scale. While, the other is biological communications (*a.k.a.* molecular communications) that use molecules to encode, transmit, and receive the information. These categories are shown in Fig. 1. A short survey of these communication protocols is presented in [16]. There is no standard Medium Access Control (MAC) layer protocol at this level.

The classical communications could further be classified into three categories: *acoustic ultrasonic* communications, *nano-mechanical* communications, and *electromagnetic* communications at terahertz frequencies. Acoustic waves at ultrasonic frequencies can be generated by small pressure variations in a medium (*i.e.,* human tissues). The data rate depends on the properties of the surrounding tissues, operating frequency, and the properties of nano-devices. Hogg and Freitas, Jr., [17] observed a data rate of 10^4 bits/s. Nano-mechanical communications are based on the physical contact between the sender and the receiver [18]. Electromagnetic communications utilize classical radio transmission methods using nano-scale antennas at terahertz frequency band.

2) TIER-2 COMMUNICATIONS

Tier-2 represents communications between on-body and in-body devices. The example is the communications between implants and a sink node placed on a human body. The communication link labeled number 3 in Fig. 1 lies in this category. At this level, different communication paradigms are proposed at the physical layer (see Fig. 1). The most common ones are the wireless Radio Frequency (RF) communications and electromagnetic coupling. Concerning RF communications, the implants can use three different frequency bands defined as Wireless Medical Telemetry Services (WMTS), unlicensed Industrial, Scientific, and Medical (ISM), and Medical Implant Communication Service (MICS) [19]. The frequency bands in WMTS includes 608 - 614, 1395 - 1400, and 1427 - 1432 MHz, ISM includes 2.4 - 2.4835 GHz, and MICS includes 402 - 405 MHz. On the other hand, electromagnetic coupling works on the principle of transformer wherein the transmitter and the receiver are coupled by the magnetic flux through coils.

Other common communication paradigms include optical and ultrasound communications. Some works in literature also propose human body as a communication channel at this level [20].

3) TIER-3 COMMUNICATIONS

Tier-3 represents the communications between on-body and off-body devices. The example is the communications between a sink node or on-body sensors and the gateway or smartphone. The communication links labeled number 4 in Fig. 1 lie in this category. At physical layer, RF is mainly utilized for communication. The MAC layer protocols are well defined at this level. To this end, the protocols presented in Fig. 1, such as Near Field Communication (NFC) (13.56 MHz), bluetooth Low Energy (LE) (2.4 GHz), Zigbee (2.4 GHz), and WiFi Direct (2.4 GHz) are generally utilized.

Some works propose to use human body as a communication channel utilizing conductive properties of the body as a communication medium between on-body devices and the gateway, provided that the gateway is physically touching the body [21], [22]. The latest standard at this level is the IEEE 802.15.6 that aims to provide a reliable and low power communication within the surrounding area of a human body.

4) TIER-4 COMMUNICATIONS

This includes all communications beyond the gateway. The communication protocols at this level are well defined from physical layer to the top layers. The communication links marked number 5 and onwards in Fig. 1 lie in this category. At this stage, there are many options for BANs to connect with the medical server. The gateway can get connected to the medical server via 3G/4G or WiFi links or even through other communication protocols defined for wireless sensor networks, such as SigFox, Low Power Wide Area Network (LPWAN), and IEEE 802.16.

III. SECURITY REQUIREMENTS AND CHALLENGES IN WBANs

The general security requirements for a WBAN remains the same at all tiers of communications. However, the scale of communications and possible security threats change at every tier. This is due to the different paradigms of communications and different capabilities of devices at each tier. For instance, at tier-1, the computational, storage, and memory size of a device are extremely limited and the communication paradigm changes from classical RF to molecular communications. To realize the end-to-end security paradigm for a complete remote healthcare ecosystem, each tier of communications must be potentially explored for possible security threats and their solutions. However, in this work, we mainly focus on tier-1 and tier-2 disregarding tier-3 and tier-4 as they have widely been discussed in the literature [10]–[14].

Below, we list down the general security requirements of a remote healthcare ecosystem at all tiers of communications that should hold for the entire life cycle of devices, including their appropriate disposal after life expiry.

- **Confidentiality:** The contents of the data must be exposed to authorized personnel only who must be authenticated by some mechanism prior to accessing the data. Moreover, the confidentiality of the data must be ensured at rest (*i.e.,* storage) and in transit (*i.e.,* during transmission).
- **Integrity:** Data and the device information must not be modifiable by any unauthorized entity. Moreover, the origin of the data must be verifiable.
- **Availability:** The data and the devices must be accessible to the authorized entities all the time; *i.e.,* the attacker must not be able to disrupt the communication or affect the devices negatively.

In what follows, we will discuss and analyze the aforementioned security requirements at tiers 1 and 2 of WBANs.

A. TIER-1 COMMUNICATIONS

As illustrated in Fig. 1, this is the new layer in WBANs. In what follows, we analyze security issues and possible solutions at this layer.

1) SECURITY CHALLENGES

Functionally, a nano-network at this tier behaves similar to a Wireless Sensor Network (WSN). The security challenges faced by WSNs can be extended to the nano-domain keeping in mind the extremely limited resources of nano-networks. A survey on security issues in WSNs is given in [23] wherein Djenouri *et al.* summarize security challenges in WSNs. Dressler and Kargl [18], on the other hand, elaborate on these challenges in the framework of nano-communications. In what follows, a summary of security requirements and challenges in nano-networks inside a human body is presented [18].

a: KEY MANAGEMENT

Key management remains a primary challenge in nano-networks. The problem is the distribution of key among the nano-devices, whether it will be a pre-distribution of the key deployment or a pro-active key distribution wherein key is exchanged after node deployment or an on-demand key exchange during the communication procedure after the node deployment. The pre-distribution of the key may seem one of the viable solutions in the in-body nano-environment, where on-demand key distribution may not be feasible due to limited online access to nano-devices. However, this technique requires storing large set of keys in each nano-device, *e.g.,* a key for pair-wise communications between neighboring nodes, a key for multicast among selective nodes, and a key for broadcast across the whole nano-network. This might not be feasible at the nano-scale where nodes have ultra limited storage capacities.

Another challenge is the structure of the key being shared among nano-devices. In the nano-domain, one option of encryption can be the biochemical cryptography wherein a key can be a molecular configuration or a chemical reaction inside a body. In this regard, some authors propose Deoxyribonucleic Acid (DNA) nano-structures for data encryption in nano-networks. DNA encryption is not only an emerging area of research to preserve genetic privacy in DNA sequencing but also laid down a foundation for the field of bio-molecular computing [24].

b: SCALABILITY

In-vivo nano-communications will pose various challenges in terms of the scale of the network. On one hand, nano-devices will have extremely limited resources in terms of their communication range, processing power and memory, and storage capacities; on the other hand, the presence of a large number of these nodes inside human body will make it exceptionally challenging to propose communications and security architectures. The security algorithms designed for WSNs cannot be directly transferred to nano-domains due to entirely different communication environment and protocols. Moreover, energy consumption of those cryptographic protocols in WSNs makes them inappropriate for the nano-domain.

Keeping in view the size of the nano-network and nano-devices, shorter key lengths might be appropriate at nano-scale. However, sending very little information (*e.g.*, few bits of data) through nano-devices might need alternate solutions to classical cryptographic algorithms, as the key length in this case might exceed the actual data itself.

c: AUTHENTICATION

At nano-scale, authentication of nano-devices inside human body remains an open research challenge. The classical cryptographic ways of authentication might be too expensive to run on nano-machines. This remains valid for all types of communication possibilities at nano-scale (see Fig. 1, tier-1 communications). For instance, in the case of classical communications, the classical cryptographic algorithms are relatively easier to adopt as compared to molecular communications [18], provided they meet the communication and computational requirements of nano-networks and nano-devices. However, in the case of molecular communications, the problem becomes more severe wherein for every single bit of transmission, there is an associated tiny molecule to carry the information [18].

As mentioned earlier in this section, the emerging field of biochemical cryptography, *i.e.,* the use of biological molecules such as DNA and Ribonucleic Acid (RNA) as a source of encryption, can better fit the security needs of molecular communications at nano-scale. However, it comes with entirely new challenges for the researchers investigating communications security. For instance, some molecules may react spontaneously leading to uncontrollable situations in nano-networks. In this regard, the researchers must work closely with biochemists to investigate innovative ways of encrypting nano-communication utilizing biological molecules.

2) POSSIBLE SECURITY THREATS

At the scale of nano-communications inside human body, it is not simple to list the possible vulnerabilities a patient might be exposed to by a threat actor. However, in what follows, we list down some of the possible attacks at tier-1 of WBANs.

a: DENIAL OF SERVICE

In nano-communications, the Denial of Service (DoS) attack refers to the blockage of communications among nano-devices or with the devices at tier-2 of WBANs, eventually compromising the availability of the network. Th DoS attack is generally initiated by flooding interference among nano-devices/molecules inside human body or by jamming the communication links between tier-1 and tier-2.

Avoiding DoS attacks in nano-networks is not an easy task. One strategy to prevent such an attack in nano-networks can be to establish an intrusion detection mechanism for in-vivo nano-networks. A kind of artificial immune system can be added to patient's body that not only can save the system to go into fail mode but also can handle the intruding nodes. However, introducing this kind of system inside human body may harm the real immune system of the body or may react or attack the legitimate nano-machines, inserted to treat certain disease(s) in a patient.

Moreover, the solutions proposed in the WSN literature or the prevention of DoS attacks can be investigated to check their applicability to nano-networks especially in the cases of molecular communications. A survey on such techniques is provided in [25].

b: DATA TAMPERING

Data tampering is an act of manipulating, modifying, or editing data through unauthorized means, eventually compromising the integrity of the network. Unlike WSNs, nano-networks operate inside human body and are not exposed to open environments. Therefore, device tampering is potentially challenging in in-vivo nano-networks. However, it is quite possible that an adversary introduces some illegitimate nano-devices inside human body that can substantially intercept the communications between the nano-devices, modify the data, and/or change its destination.

To protect nano-networks from data tampering, the first defense can be to block the entry of an unauthorized node inside human body. This can be achieved by enforcing the use of the prescribed medications only. Taking non-prescribed medicine from unauthorized sources can potentially increase the chances of introduction of illegitimate nodes. To cope with this, nano-devices must enforce a strict authentication procedure prior to establishing a communication link with any node inside human body.

In communication technologies, spread spectrum techniques, which are used to meet the bandwidth demands of users, provide higher level of security by potentially decreasing the chances of interference and interception at the nodes. For instance, in the Frequency Hoping Spread Spectrum (FHSS), the nodes continually keep on changing their transmission frequency. Hence, it becomes quite challenging for an attacker to intercept and keep track of the current frequency.

One may investigate the adoption of a similar communication paradigm at nano-scale to avoid the possibility of legitimate nodes, or communications in general, being compromised. However, the spread spectrum techniques require complex infrastructure at both the transmitter and the receiver ends. Nevertheless, the technique can still be investigated in the context of nano-molecular communications. Instead of hopping the frequency, the information can be carried by hopping the molecules themselves. The possibility of generating various molecular structures can be intensely investigated in close collaboration with biochemists.

The solutions proposed in the WSN literature for the prevention of data tampering attacks can be investigated to check their applicability to nano-networks especially in the cases of molecular communications. A survey on such techniques is provided in [26].

Some other active attacks that might affect confidentiality, integrity, and availability of the nano-networks include, but are not limited to, masquerade, brute-forcing, replay, misdirection, and blackholes attacks. These attacks are partially discussed in [18]. However, we believe that the prevention techniques of all these attacks at nano-scale still remains an open research challenge.

B. TIER-2 COMMUNICATIONS

Bearing in mind the nature of communication protocols at this tier (see Fig. 1), in what follows, we analyze security issues and possible solutions.

1) SECURITY CHALLENGES

Prior to analyzing security challenges of aforementioned protocols at tier-2, it seems logical to understand the function of these protocols. The protocols such as WMTS, ISM, and MICS were designed to replace the wired telemetry system to give patients a freedom to move freely with sensors and get monitored while performing daily life activities. In WMTS, a patient wears a small radio transmitter (possibly on the wrist), which acts as an intermediate node to relay information to the gateway. The device named as *sink node* in Fig. 1 represents a WMTS relay node. More specifically, a licensed MICS band is recommended for implant communication in WBAN [3]. The communication range varies from few centimeters to 2 meters [3], depending upon the type of the technology utilized (see tier-2 communications in Fig. 1 for possible communication options).

In most of the aforementioned systems, the adversary needs to be very close to the patient's body. Particularly, in the case of communications using conductive properties of the body, the adversary needs a physical contact with the patient's body. Moreover, unlike nano-devices, the network topology at this tier is a star topology wherein tier-2 nodes connect with the sink node (or a programmer in some cases) using one of the aforementioned communication technologies. Specifically, medical implants send their data to the sink node, which is connected to a medical server through a gateway.

The security challenges for a general star type (client-server) network have been extensively studied in the literature (*e.g.*, see [27], [28]). However, tier-2 communications in WBANs use different protocol settings and the security solutions presented in the literature can not be directly applied. More importantly, the protocols at this tier are not well established nor well studied in the literature. Particularly, the security of such protocols is rarely investigated in the literature and the device manufacturers do not consider security while designing such devices. Consequently, it becomes very easy for an attacker to get access to an implanted medical device. One important example to note here is the incident wherein the wireless interface of the pacemaker on vice president Dick Cheney got disabled [29].

In what follows, we elaborate security challenges and possible attacks at this tier of WBANs.

a: KEY MANAGEMENT

Managing the distribution of the key among the tier-2 nodes remains an open research challenge. Some potential options can be: i) a pre-deployment key distribution wherein a set of keys is stored in the nodes before deployment, ii) a pro-active key distribution wherein the key is exchanged after node deployment, or iii) an on-demand key exchange wherein the key is exchanged during the communication procedure post node deployment. Additionally, in order to decide the key management, one needs to consider the node's capabilities in this tier. The devices in this tier include implants and other medical devices that communicate with the sink node. The storage, processing, and communication capabilities of these devices are better than nano-devices but they are still extremely limited to apply complex cryptographic techniques for key management.

Some out-of-band key exchange protocols are proposed in the literature [30], [31] including physiological values [8], [32]–[34], such as using Inter Pulse Interval (IPI) [35], [36], Photoplethysmogram (PPG), and ECG [37]–[39] of the human body.

b: AUTHENTICATION

The limitation of computational resources in medical implants at tier-2 restricts the use of cumbersome cryptographic methods, such as Diffie-Hellman authentication and other asymmetric and symmetric authentication procedures. However, some works in the literature propose out-of-band authentication for the implants. The idea is to utilize auxiliary channels that work outside the data communication channel, such as a human contact or audio and visual channels [30], [31], [40], [41]. The out-of-band authentication circumvents the need for trusted third parties and pre-distribution of the keys. In addition, certain out-of-band authentication schemes, such as physiological biometrics limit the eavesdropping attacks due to personalized nature of these authentication schemes.

A typical example of the out-of-band authentication in medical implants is the work presented in [30] wherein the authors utilize a low-frequency audio channel to transmit the key generated by a tier node utilizing a zero-power Radio-Frequency Identification (RFID) device. Whenever there is a key exchange between the implant and the programmer/sink, the patient is alerted through a vibration generated by a piezo element attached to the RFID device. However, the problem with this scheme is the possibility of hearing the piezo sound at a distance quite near the patient (*e.g.*,/ 1m), which may lead to passive attacks such as eavesdropping. For instance, an adversary may use general purpose microphone in the vicinity of the patient to receive the piezo sound and consequently overhear the communications.

The limited power supply of implants and other tier-2 devices obstructs the use of state-of-the-art cryptographic authentication schemes. The external power sources such as the one presented in [42] may solve power consumption issues but may create serious security concerns. The live connection between the implant and the power source may provide an advantage for the adversaries to compromise the implant if the security concerns are not addressed properly.

2) POSSIBLE SECURITY THREATS

In the following, we discuss some of the possible security vulnerabilities and attacks that implants and other medical devices at tier-2 of WBANs can be exposed to.

a: DENIAL OF SERVICE

At tier-2, the DoS may refer to the cases when the legitimate communications between implants and the sink are disrupted or the implant's or sink's power is needlessly depleted. The DoS attack may lead to serious physical problems to the patients. For instance, in the case of an emergency, the legitimate commands sent by a doctor may not reach the implant that may cost patient's life.

A strategy to avoid DoS attacks in medical implants can be to detect the anomalous behavior that may automatically identify malicious communications and resource depletion. For this purpose, some works in the literature propose to use physical characteristics of the transmitted signal such as received signal strength, angle of arrival, time of arrival, and time difference of arrival. Particularly, Zhang *et al.* propose an external device [43] that can examine the aforementioned physical characteristics and anomalous transmission.

The solutions proposed to prevent DoS attacks in WSNs in the clustering environment can be adopted in implants. Clustering in the WSNs represents a network setting wherein WSN nodes group together to form a cluster and one node acts as a cluster head. This cluster head can virtually represent a sink node in the WBAN and the cluster members can be virtually represented by medical implants. A survey on DoS attacks in such a network setting is presented in [44]. The survey provides an analysis of various different DoS attacks at different layers along with some mitigations.

b: DATA TAMPERING

Data tampering in medical implants and other tier-2 devices is about manipulating or modifying the data through illegitimate means, compromising eventually the integrity of the WBAN. Unlike nano-networks, the nodes in this tier are somewhat exposed to adversaries with a potential likelihood of these nodes/data being tempered or compromised. Practically, Halevi and Saxena [45] successfully compromised a medical implant provisioned with acoustic signal, based on the out-of-band authentication system, from a distance of 0.9 meters and an average key retrieval correctness of 99.88%. Other out-of-band authentication schemes [8], [30]–[34] may also be compromised, thus instigating data tampering attacks. The details of such attacks can be found in [30] and [46]–[48].

To protect the communication channel of medical implants and their stored data from being tampered or disclosed, cryptographic measures (both symmetric and asymmetric) may sound a feasible solution [49]–[51]. However, these solutions may deplete the battery of implants if adopted to secure the wireless telemetry between implants and the sink node. The power saving solutions such as [42] may need to be further investigated in the perspective of security of implants. Moreover, cryptographic solutions for medical implants have already been criticized and challenged by the research community for their usability and reliability. For instance, the use of cryptographic mechanisms will force patients to replace the implant by undergoing a surgery to make the implant more secure, given that it was functioning properly.

Camara *et al.* provide a deep insight of possible security attacks at tier-2 of WBAN [52]. However, the prevention techniques of different attacks at this tier still remains an open challenge.

IV. DISCUSSION AND FUTURE DIRECTIONS

This section discusses research challenges faced by data scientists and researchers investigating security and privacy issues in WBANs.

A. LACK OF PHYSICAL ACCESS

Given the critical nature of medical devices such as implants, the primary challenge is the lack of their access to researchers wherein they can evaluate and asses the risk of an attack and the effectiveness of its defense. Some of those devices require justification and a prescription from a physician. For instance, Medtronic sells their insulin pumps to patients only when it is prescribed by a physician. The problem becomes worse when it comes to medical implants such as implantable cardiac defibrillators and others. Besides, the firmware configuration of those devices is neither public nor shared with the research community, which makes it quite challenging for researchers to examine these devices for potential vulnerabilities in their firmware. However, the authors in [53] were successful in identifying vulnerabilities in the firmware of Automatic External Defibrillator (AED) by reverse engineering the device.

In the case of nano-communications, it becomes more challenging to fully realize a real in-vivo nano-network to investigate security and privacy issues. Particularly, for molecular communications, the results generated from experimental environments such as human tissue simulator and artificial blood, may not be reproduced in the real in-vivo networks. It can be interesting to investigate if the calibrated saline solution used to simulate physiological signal [54] may also be used for testing in-vivo nano-communications.

B. SCARCITY IN RESOURCES

Resources scarceness in the in-vivo and in-vitro medical devices, such as sink nodes, medical implants, and nano-nodes is a well-known problem in WBANs, which restricts them to use state-of-the-art cryptography mechanisms. Several solutions are proposed in the literature to enhance the life time of medical implants. These solutions include, but are not limited to, investigating various types of batteries [55]–[57], harvesting energy from the surroundings of implants [58], [59], and obtaining energy from external sources for battery-less implants [42], [60], [61]. The work presented in [42] is the most recent solution in this regard wherein an external power source keeps battery-less implants alive deep inside human body. However, all of the aforementioned solutions do not intend to make implants powerful enough to run cryptographic schemes proposed for general purpose networks. They merely increase the lifespan of an implant, while the computational and storage capacity of these devices remains minimal.

The solutions, such as [42], further expand security challenge in a sense that an adversary may pretend to be a legitimate power source to get access to the implant. Alternatively, an adversary can interfere the communications between the power source and the implant and can potentially block it, endangering the life of the patient. Technically, empowering implants from an external source is a powerful concept but needs further comprehensive investigations to secure the power transfer and communication links. One research direction is to investigate solutions where most of the computational burden is placed towards external power source, thus resulting implant to consume as less energy as possible during the authentication procedure. To this end, a couple of solutions are proposed in the literature [30], [62] but requiring further investigation.

The case of in-vivo nano-networks is more complicated wherein the nano-nodes have extremely limited power and computational resources. However, the security solutions investigated for the case of external power supply can be easily extended to nano-networks, where an external source can meet the power, computational, and security demands of nano-networks.

C. BIG DATA CHALLENGE

Recently, Rizwan *et al.* [16] have drawn attention of research community towards an emerging research field, *i.e.,* big data perspective of nano-communication and its impact on the overall healthcare system. Given the scale of nano-communications and its relation with the big data [16], security and privacy issues become even more challenging not only inside human body but also during data storage and processing by medical servers. Losing this data to an adversary may cause serious privacy concerns to the patients. This stresses the need for an end-to-end security system for WBANs where security and privacy challenges are ensured at all tiers.

V. CONCLUSIONS

In this work, we discussed the current and future research trends in WBANs and remote healthcare monitoring systems. First, based on the communication of medical devices, we divide a WBAN into four-tiers, including in-vivo nano-communications. Subsequently, we provided a taxonomy of entities involved in remote healthcare monitoring systems. Then, we analyzed security requirements and challenges faced by the medical devices at each tier of communications. Particularly, we focused on the challenges to ensure confidentiality, integrity, and availability at all tiers of communications in WBANs. Specifically, we identified the complex situation of nano-networks with extremely limited resources and capabilities. Last but not least, we highlighted several areas of research to ensure end-to-end security and pointed out some limitations in the current WBANs.

REFERENCES

[1] Q. H. Abbasi, M. U. Rehman, K. Qaraqe, and A. Alomainy, *Advances in Body-Centric Wireless Communication: Applications and State-of-the-art*. Stevenage, U.K.: Institution of Engineering and Technology, 2016.

[2] N. Kalid, A. A. Zaidan, B. B. Zaidan, O. H. Salman, M. Hashim, and H. Muzammil, "Based real time remote health monitoring systems: A review on patients prioritization and related 'big data' using body sensors information and communication technology," *J. Med. Syst.*, vol. 42, p. 30, Feb. 2018.

[3] M. N. Islam and M. R. Yuce, "Review of medical implant communication system (MICS) band and network," *ICT Express*, vol. 2, no. 4, pp. 188–194, Dec. 2016.

[4] G. Quaglio *et al.*, "E-health in Europe: Current situation and challenges ahead," *Health Policy Technol.*, vol. 5, no. 4, pp. 314–317, 2016.

[5] M. Usman, M. R. Asghar, and F. Granelli, *5G and D2D Communications at the Service of Smart Cities*. Hoboken, NJ, USA: Wiley, 2017.

[6] A. Pope *et al.*, *Innovation and Invention in Medical Devices: Workshop Summary*. Washington, DC, USA: National Academies Press, 2001.

[7] Q. H. Abbasi, A. A. Nasir, K. Yang, K. A. Qaraqe, and A. Alomainy, "Cooperative *in-vivo* nano-network communication at terahertz frequencies," *IEEE Access*, vol. 5, pp. 8642–8647, 2017.

[8] K. K. Venkatasubramanian and S. K. Gupta, "Physiological value-based efficient usable security solutions for body sensor networks," *ACM Trans. Sensor Netw.*, vol. 6, no. 4, 2010, Art. no. 31.

[9] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. US Food Drug Admin. Others, Annapolis, MD, USA, Oct. 2015.

[10] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[11] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[12] A.-S. K. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Boca Raton, FL, USA: CRC Press, 2016.

[13] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[14] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[15] Q. H. Abbasi *et al.*, "Nano-communication for biomedical applications: A review on the state-of-the-art from physical layers to novel networking concepts," *IEEE Access*, vol. 4, pp. 3920–3935, 2016.

[16] A. Rizwan *et al.*, "A review on the role of nano-communication in future healthcare systems: A big data analytics perspective," *IEEE Access*, vol. 6, pp. 41903–41920, 2018.

[17] T. Hogg and R. A. Freitas, Jr., "Acoustic communication for medical nanorobots," *Nano Commun. Netw.*, vol. 3, no. 2, pp. 83–102, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1878778912000154

[18] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Commun. Netw.*, vol. 3, no. 3, pp. 151–160, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1878778912000294

[19] S. Ullah *et al.*, "A comprehensive survey of wireless body area networks," *J. Med. Syst.*, vol. 36, no. 3, pp. 1065–1094, Jun. 2012. [Online]. Available: http://dx.doi.org/10.1007/s10916-010-9571-3

[20] J. E. Ferguson and A. D. Redish, "Wireless communication with implanted medical devices using the conductive properties of the body," *Expert Rev. Med. Devices*, vol. 8, no. 4, pp. 427–433, 2011.

[21] M. S. Wegmueller *et al.*, "An attempt to model the human body as a communication channel," *IEEE Trans. Biomed. Eng.*, vol. 54, no. 10, pp. 1851–1857, Oct. 2007.

[22] A. R. Ansari and S. Cho, "Human body: The future communication channel for WBAN," in *Proc. 18th IEEE Int. Symp. Consum. Electron. (ISCE)*, Jun. 2014, pp. 1–3.

[23] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 4, pp. 2–28, 4th Quart., 2005.

[24] K. Halvorsen and W. P. Wong, "Binary DNA nanostructures for data encryption," *PLOS ONE*, vol. 7, no. 9, pp. e44212, 2012, doi: 10.1371/journal.pone.0044212.

[25] S. Patil and S. Chaudhari, "DoS attack prevention technique in wireless sensor networks," *Procedia Comput. Sci.*, vol. 79, pp. 715–721, Jan. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916002258

[26] K. Xing, S. S. R. Srinivasan, M. J. M. Rivera, J. Li, and X. Cheng, "Attacks and countermeasures in sensor networks: A survey," in *Network Security*. Berlin, Germany: Springer, 2010, pp. 251–272.

[27] K. P. Mahaffey *et al.*, "Multi-factor authentication and comprehensive login system for client-server networks," U.S. Patent 9 374 369 B2, Jun. 21, 2016.

[28] M. Bloch, R. Narasimha, and S. W. McLaughlin, "Network security for client-server architecture using wiretap codes," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 404–413, Sep. 2008.

[29] G. Kolata, "Of fact, fiction and cheney's defibrillator," *New York Times*, Oct. 2013. [Online]. Available: https://www.nytimes.com/2013/10/29/science/of-fact-fiction-and-defibrillators.html

[30] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 129–142.

[31] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2010, pp. 917–926.

[32] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2274–2282.

[33] K. K. Venkatasubramanian and S. K. Gupta, "Security for pervasive health monitoring sensor applications," in *Proc. 4th Int. Conf. Intell. Sens. Inf. Process. (ICISIP)*, Oct./Dec. 2006, pp. 197–202.

[34] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proc. Int. Conf. Parallel Process. Workshops*, Oct. 2003, pp. 432–439.

[35] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. 2013 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1099–1112.

[36] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[37] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–68, Jan. 2010.

[38] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2008, pp. 1–7.

[39] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proc. IEEE INFOCOM Workshops*, Apr. 2008, pp. 1–6.

[40] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Trans. Sen. Netw.*, vol. 9, no. 2, pp. 18:1–18:35, Apr. 2013, doi: 10.1145/2422966.2422975.

[41] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud and clear: Human-verifiable authentication based on audio," in *Proc. 26th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2006, p. 10.

[42] Y. Ma, Z. Luo, C. Steiger, G. Traverso, and F. Adib, "Enabling deep-tissue networking for miniature medical devices," in *Proc. ACM SIGCOMM Conf.*, New York, NY, USA, Aug. 2018, pp. 417–431.

[43] M. Zhang, A. Raghunathan, and N. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.

[44] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervas. Comput.*, vol. 7, no. 1, pp. 74–81, Jan./Mar. 2008.

[45] T. Halevi and N. Saxena, "On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 97–108.

[46] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Services (Healthcom)*, Jun. 2011, pp. 150–156.

[47] M. Rostami, W. Burleson, A. Juels, and F. Koushanfar, "Balancing security and utility in medical devices?" in *Proc. 50th Annu. Design Autom. Conf.*, May/Jun. 2013, pp. 1–6.

[48] P. Bagade, A. Banerjee, J. Milazzo, and S. K. S. Gupta, "Protect your BSN: No handshakes, just namaste!" in *Proc. IEEE Int. Conf. Body Sensor Netw. (BSN)*, May 2013, pp. 1–6.

[49] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices," in *Proc. IEEE 5th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, Mar. 2011, pp. 6–9.

[50] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography," in *Proc. Int. Conf. Anti-Counterfeiting Secur. Identificat. Commun. (ASID)*, Jul. 2010, pp. 1–6.

[51] K. Singh and V. Muthukkumarasamy, "Authenticated key establishment protocols for a home health care system," in *Proc. IEEE 3rd Int. Conf. Intell. Sensors, Sensor Netw. Inf. (ISSNIP)*, Dec. 2007, pp. 353–358.

[52] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Inform.*, vol. 55, pp. 272–289, Jun. 2015.

[53] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song, "Take two software updates and see me in the morning: The case for software security evaluations of medical devices," in *Proc. HealthSec*, 2011, p. 6.

[54] *Active Implantable Medical Devices-Electromagnetic Compatibility-EMC Test Protocols for Implantable Cardiac Pacemakers and Implantable Cardioverter Defibrillators*, document ANSI/AAMI PC69: 2000, Association for the Advancement of Medical Instrumentation, 2007.

[55] M. Nathan, "Microbattery technologies for miniaturized implantable medical devices," *Current Pharmaceutical Biotechnol.*, vol. 11, no. 4, pp. 404–410, 2010.

[56] D. C. Bock, A. C. Marschilok, K. J. Takeuchi, and E. S. Takeuchi, "Batteries used to power implantable biomedical devices," *Electrochim. Acta*, vol. 84, pp. 155–164, Dec. 2012.

[57] K. Dong, B. Jia, C. Yu, W. Dong, F. Du, and H. Liu, "Microbial fuel cell as power supply for implantable medical devices: A novel configuration design for simulating colonic environment," *Biosensors Bioelectron.*, vol. 41, pp. 916–919, Mar. 2013.

[58] H. S. Kim, J.-H. Kim, and J. Kim, "A review of piezoelectric energy harvesting based on vibration," *Int. J. Precis. Eng. Manuf.*, vol. 12, no. 6, pp. 1129–1141, 2011.

[59] S. Almouahed, M. Gouriou, C. Hamitouche, E. Stindel, and C. Roux, "Self-powered instrumented knee implant for early detection of postoperative complications," in *Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC)*, Apr./Sep. 2010, pp. 5121–5124.

[60] N. P. Willis, A. F. Brisken, M. W. Cowan, M. Pare, R. Fowler, and J. Brennan, "Optimizing energy transmission in a leadless tissue stimulation system," U.S. Patent 8 718 773 B2, May 6, 2014.

[61] B. C. Tran, B. Mi, and R. S. Harguth, "Systems and methods for controlling wireless signal transfers between ultrasound-enabled medical devices," U.S. Patent 8 369 960 B2, Feb. 5, 2013.

[62] Q. Yang, S. Mai, Y. Zhao, Z. Wang, C. Zhang, and Z. Wang, "An on-chip security guard based on zero-power authentication for implantable medical devices," in *Proc. IEEE 57th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2014, pp. 531–534.

MUHAMMAD USMAN (S'14–M'17) received the B.E. degree in electronics engineering from the School of Electrical Engineering and Computer Science, National University of Science and Technology, Pakistan, in 2004, the M.S. degree in telecommunication engineering from the University of Trento, Italy, in 2014, the M.S. degree in computer networks from the Sant'Anna School of Advanced Studies, Pisa, Italy, in 2014, and the Ph.D. degree in information and communication technologies from the University of Trento in 2017. He was a Visiting Researcher with Texas A&M University at Qatar in 2017. He is currently a Post-Doctoral Researcher at Hamad Bin Khalifa University, Doha, Qatar. His research interests include wireless body area networks, cyber security, software-defined networks, and device-to-device communication in 5G and beyond networks.

MUHAMMAD RIZWAN ASGHAR received the M.Sc. degree in information security technology from The Eindhoven University of Technology, The Netherlands, in 2009, and the Ph.D. degree from the University of Trento, Italy, in 2013. As part of his Ph.D. programme, he was a Visiting Fellow at the Stanford Research Institute, CA, USA. He was a Post-Doctoral Researcher with international research institutes, including the Center for IT-Security, Privacy, and Accountability (CISPA), Saarland University, Germany, and CREATE-NET, Trento, Italy. He is currently a Senior Lecturer with the Department of Computer Science, The University of Auckland, New Zealand. His research interests include access control, cyber security, privacy, and consent management.

IMRAN SHAFIQUE ANSARI (S'07–M'15) received the B.Sc. degree (Hons.) in computer engineering from the King Fahd University of Petroleum and Minerals (KFUPM) in 2009 and the M.Sc. and Ph.D. degrees from the King Abdullah University of Science and Technology (KAUST) in 2010 and 2015, respectively. He was a Visiting Scholar with Michigan State University, East Lansing, MI, USA, in 2009, and a Research Intern with Carleton University, Ottawa, ON, Canada, in 2010. From 2015 to 2017, he was a Post-Doctoral Research Associate with Texas A&M University at Qatar. From 2017 to 2018, he was a Lecturer with the Global College of Engineering and Technology, University of the West of England, Bristol, U.K. Since 2018, he has been a Lecturer with the University of Glasgow, Glasgow, U.K.

Dr. Ansari has been affiliated with IEEE and IET since 2007 and has served in various capacities. He has been serving on the IEEE Communication Society Young Professionals Board since 2016. He is part of the IEEE 5G Tech Focus Publications Editorial Board since 2017. He has served on IET Communities Committee-Europe, Middle-East and Africa for a complete term from 2010 to 2013 and has been re-elected to serve for another term from 2015 to 2018. He is serving on the IET Satellite and Systems

Applications (SSA) Technical Professional Network (TPN) for the term 2016–2019. He is an active reviewer for various IEEE TRANSACTIONS and various other journals. He has served as a TPC for various IEEE conferences. He was a recipient of appreciation for an Exemplary Reviewer for the IEEE WIRELESS COMMUNICATIONS LETTERS (WCL) in 2014 and 2017, a recipient of appreciation for an Exemplary Reviewer for the IEEE TRANSACTIONS ON COMMUNICATIONS in 2016, a recipient of the TAMUQ Research Excellence Award 2016 and 2017, a recipient of Recognized Reviewer Certificate at the Elsevier *Optics Communications* in 2015, a recipient of Recognized Reviewer Certificate at OSA Publishing in 2014, a recipient of Post-Doctoral Research Award (first cycle) at the Qatar National Research Foundation in 2014, a recipient of the KAUST Academic Excellence Award in 2014, and a recipient of the IEEE Richard E. Merwin Student Scholarship Award in 2013.

He has authored/co-authored over 65 journal and conference publications. He has co-organized the GRASNET'2016, 2017, and 2018 workshops in conjunction with the IEEE WCNC'2016 and 2017 and the IEEE Globecom 2018. His current research interests include free-space optics, channel modeling/signal propagation issues, relay/multihop communications, physical layer secrecy issues, full-duplex systems, and secure D2D applications for 5G+ systems, among others.

MARWA QARAQE received the degree *(summa cum laude)* from Texas A&M University at Qatar in 2010 and the M.Sc. and Ph.D. degrees in electrical engineering from Texas A&M University, College Station, TX, USA, in 2012 and 2016, respectively. She is currently an Assistant Professor with Hamad Bin Khalifa University, Doha, Qatar.

Her current research interests lie in the area of predictive data analytics and machine learning, particularly in the health domain, and wireless body-area communication. Throughout her academic career, she has received several awards. She was a recipient of the first place in the Qatar Foundation Annual Research Forum in the Health and Biomedical Sector in 2013. Throughout her Ph.D. career, she has received several Al-Thanaa awards from the Qatar Foundation for her high academics and excellence in research. She was also a recipient of the Richard E. Wing Award for Excellence in Student Research in 2012. During her master's degree, she was a recipient of the Texas A&M University's Diversity Fellowship. She also received three Scholarships for High Academic Achievement from 2007–2010.