Access Control Schemes for Implantable Medical Devices: A Survey

Longfei Wu, Xiaojiang Du, *Senior Member, IEEE*, Mohsen Guizani, *Fellow, IEEE*, and Amr Mohamed, *Senior Member, IEEE*

***Abstract*—Implantable medical devices (IMDs) are electronic devices implanted within human body for diagnostic, monitoring, and therapeutic purposes. It is imperative to guarantee that IMDs are completely secured since the patient's life is closely bound to the robustness and effectiveness of IMDs. Intuitively, we have to ensure that only the authorized medical personnel and IMD programmer can access the IMD. However, in recent years, several attacks have been reported which can successfully compromise a number of IMD products, e.g., stealing the sensitive health data and issuing fake commands. Up to now, there is no commonly agreed and well-recognized security standards and the protection of IMD is still an open problem. In this paper, we present a comprehensive survey of the existing literature on IMD security, with a focus on the access control schemes to prevent unauthorized access. Specifically, we first reviewed the security incidents, IMD threat model and the development of regulations for IMD security. Next, we classified existing IMD access control schemes based on architecture, type of keys used, access control channel, and logic. We also analyzed how different access control models can be adopted to secure IMD. Besides, we particularly discussed the viability of online authentication and low/zero power authentication in the IMD context.**

***Index Terms*—Access control, implantable medical devices (IMDs), survey.**

I. Introduction

NOWADAYS, the lives of millions of patients rely upon implantable medical devices (IMDs) implanted within their bodies to treat a variety of diseases and conditions such as cardiac arrhythmias, diabetes, Parkinson's disease, or for cosmetic purposes. According to the Transparency Market Research's report [1], the U.S. IMDs market is expected to be worth $73,944.3 million by 2018. The IMDs are small in size and thereby resource constrained in terms of computational power, storage and battery. Unlike other electronic devices, the battery recharge or replacement for IMDs requires invasive surgery. Some researchers have been seeking the feasibility to incorporate the wireless charging technology (e.g., magnetic resonance) into IMDs [2], [3], but it is in the very early stages and still faces significant regulatory hurdles [4]. Despite being very promising, the wireless charging enabled IMD product will not be released to the market, without many years of reliability testing (e.g., interference with other metal devices) and clinical trials (e.g., effect on human organs and tissues). Hence, at the current stage, reducing energy consumption is still one of the top priority in IMD design. Usually, IMD batteries should last from 5 to 10 years, which greatly limits the complexity of security mechanisms to be performed. For example, complicated cryptographic computations and long-range wireless transmissions are all considered unaffordable.

The IMDs are facing a range of malicious attacks launched by external adversaries and unintentional mistakes in software or firmware design. Modern IMDs are equipped with a radio transceiver to communicate with an external device generally known as "programmer." An authorized IMD programmer can issue commands to change the IMD configuration settings (e.g., parameter and dosage) and extract the medical data. Some IMDs are connected to the hospital networks or the Internet, hence can be remotely monitored and operated by the doctors. However, the wireless communication and networking capabilities in IMDs are the major source of security risks. Due to the openness of the wireless channels, all transmitted packets can be captured by nearby eavesdroppers. This cannot only expose patient privacy like the presence of IMD and its model, but also lead to other classic wireless attacks such as forging, tampering, and replying the messages. Additionally, if the IMD supports remote access by the doctor or the hospital, cyber attacks targeted at the hospital network/server may steal the patient data or the credentials. Therefore, the development of lightweight but effective access control scheme for IMDs is highly desired.

Security and privacy issues have been reviewed in several existing works [5]–[12]. In this paper, we conduct a comprehensive survey specifically on the access control scheme for IMDs. We also studied some authentication schemes for resource-limited body area networks (BANs) and secret key sharing methods for smartphones, which can potentially be adopted for IMD access control. This paper first summarizes

Manuscript received January 15, 2017; revised April 29, 2017; accepted May 14, 2017. Date of publication May 25, 2017; date of current version October 9, 2017. This work was supported by the Qatar National Research Fund (a member of Qatar Foundation) under Grant NPRP 8-408-2-172. *(Corresponding author: Xiaojiang Du.)*

L. Wu was with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19123 USA. He is now with the Department of Mathematics and Computer Science, Fayetteville State University, Fayetteville, NC 28301 USA.

X. Du is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19123 USA (e-mail: dux@temple.edu).

M. Guizani is with the Department of Electrical and Computer Engineering, University of Idaho, Moscow, ID 83844 USA.

A. Mohamed is with the Department of Computer Science and Engineering, Qatar University, Doha 2713, Qatar.

Digital Object Identifier 10.1109/JIOT.2017.2708042

the IMD security incidents of unauthorized access reported in recent years, and discusses the threat model IMD is facing and the current regulations on IMD security. Then, the existing IMD access control schemes are classified into four categories in terms of the access control architecture and the type of keys being used, including direct access control with preloaded keys, direct access control with temporary keys, indirect access control via a proxy, and anomaly detection-based schemes. Next, we present how different types of access control models can be applied to the IMD context. Finally, we discuss the viability of using online authentication server and embedding low-power (zero-power) authentication in IMD.

II. Background

IMDs, like other wireless computing devices, can be vulnerable to security breaches. This vulnerability increases as IMDs are increasingly connected to the Internet, hospital networks, and to other medical devices (e.g., IMD programmer and smartphone).

A. IMD Security Incidents

Halperin *et al.* [13] presented the vulnerabilities of a commercial implantable cardioverter defibrillator (ICD). Equipped with an oscilloscope and a software radio, they managed to reverse-engineer the ICD's communications protocol and obtain the personal information of the patient and the ICD. Furthermore, they also launched active attacks to change the therapy settings and drain the battery more rapidly. Similarly, eavesdropping attacks and active attacks can also compromise commercial glucose monitoring and insulin delivery system [14]–[16]. After reverse-engineering the communication protocol and packet format, they were able to impersonate the doctor and alter the intended therapy by replaying and injecting messages with a software radio. A security professional Barnaby Jack has also revealed serious security flaws in IMDs, and demonstrated how an adversary can remotely take full control of insulin pump, pacemaker and ICD [17].

Even though IMD manufacturers are supposed to take responsibility for the security incidents and vulnerabilities in their products, they are unwilling to include strong security mechanisms since these changes will result in additional cost and time to the market. In 2014, an independent security researcher Billy Rios discovered 100 vulnerabilities in the communications system in the PCA 3 Lifecare infusion pump software by medical device company Hospira (HSP), which allows a hacker to tap into the pumps and change the amount of medication they've been set to dispense. Rios notified Hospira, but the company failed to respond to him. Hospira stayed silent on the issue until another researcher Jeremy Richards publicly disclosed the vulnerability in April 2015 [18]. The U.S. Food and Drug Administration (FDA) and the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team sent out advisories notifying hospitals of the danger of Hospira pumps, and encouraging the transition to alternative infusion systems [19].

B. IMD Threat Model

Two types of adversaries can be involved in an attack targeted at IMD.

1) *Passive Adversary:* A passive adversary can only eavesdrop on the wireless channel and listen to the messages exchanged between the IMD and the IMD programmer. Given an unencrypted radio channel, a passive attack can break the confidentiality and the authentication. Specifically, it can determine whether a person is carrying an IMD or not; obtain the type, model, and serial number of the IMD; intercept the unencrypted data and disclose private information about the patient, such as the name, age, conditions, ID, health records, etc.
2) *Active Adversary:* After analyzing and reverse-engineering the communication protocol between the IMD and the programmer, an active adversary is able to tamper their messages and send unauthorized commands to the IMD (e.g., changing the configurations and parameters). The active attack could result in fatal threat to the patient.

A standard assumption in current literature is that the adversary will not approach the patient or make physical contact, deterred from leaving criminal evidence such as fingerprint, witness, or video taken by the surveillance camera. In this sense, the simple proximity-based access control scheme plus a lightweight key generation mechanism (generate a shared key between the IMD and the programmer to encrypt the communication) is sufficient to secure the IMD. However, Rushanan *et al.* [5] remarked that this adversarial model neglects subtle classes of attacks by people known to the victim. We also consider that the attack can be launched automatically through the wireless channel without manual operation and physical contact, which means the adversary can pretend to be a pedestrian happened to walk by. Besides, the adversary in the close range may be just a colluder collecting the basic information of the IMD (e.g., model and serial number) or amplifying the wireless signal, while the active adversary is launching sophisticated attack far away.

Existing access control schemes for IMD have been focusing on two general attack models. In the first type of attacks, an unauthorized programmer aims to obtain access to medical data stored in the IMD, send malicious commands, or change the device configurations. In the second type of attacks, an unauthorized programmer repeatedly connects with the target IMD, triggering the continuous execution of authentication computations in order to drain its battery. In addition, this may also result in the denial-of-service which can prevent authorized emergency treatments.

C. IMD Regulations on Cybersecurity

FDA is the governmental agency that supervise and regulate the medical device industry. FDA has been keeping an eye on the security incidents of medical devices. In order to improve the IMDs security and ensure that patients are safe, FDA has provided guidelines regulating medical device cybersecurity. In October 2014, FDA released the guidance on the Premarket Submissions for Management of Cybersecurity

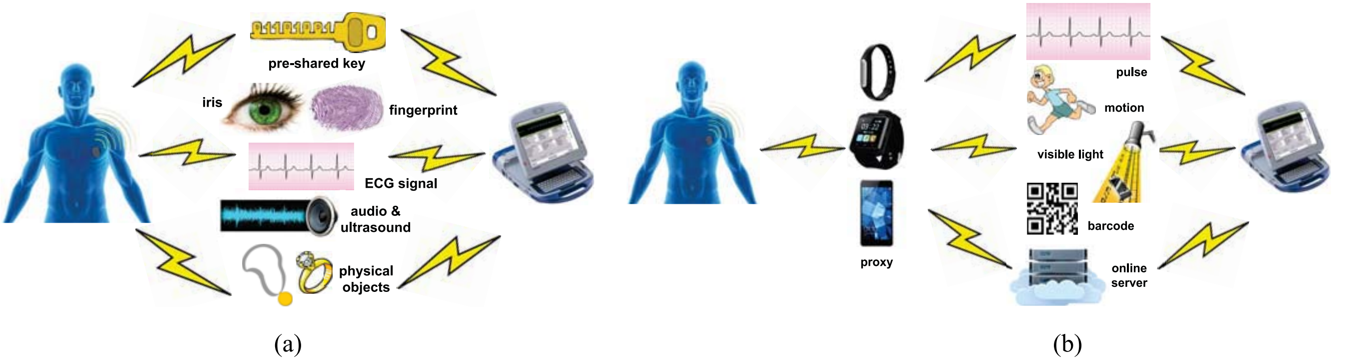

Fig. 1. IMD access control architecture. (a) Direct access control. (b) Indirect access control via a proxy.

in Medical Devices [20], and the more recent draft guidance of Postmarket Management of Cybersecurity in Medical Devices is released in January 2016 [21]. The premarket submission guidance provides recommendations to consider and document in FDA medical device premarket submissions to provide effective cybersecurity management and to reduce the risk that device functionality is intentionally or unintentionally compromised. To guard against vulnerabilities, the FDA urges manufacturers to consider cybersecurity during the design and development phase of the medical device. It also recommends manufacturers establish a cybersecurity vulnerability and management approach as part of their software validation and risk analysis. The draft guidance of postmarket management in cybersecurity encourages manufacturers to implement an effective cybersecurity risk management program for both premarket and postmarket lifecycle phases. Specifically, it highlights that manufacturers should maintain an ongoing process of monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they have entered the market. Additionally, it outlines the steps manufacturers should take to continually address cybersecurity risks with their devices.

However, these guidelines are mostly only recommendations and not legally binding. There is no validation and verification of the new IMD products (software and hardware) and their cybersecurity documentations by a trusted agency. The protection of IoT devices still relies on the research and development team of each individual manufacturer.

III. Classification of IMD Access Control Schemes

We categorize existing IMD access control schemes in four perspectives: the access control architecture, the type of keys (secrets) used to secure the communication channel, the access control channel, and the access control logic. The details are listed as follows.

1) *Access Control Architecture:* The programmer can communicate with the IMD directly for access control [Fig. 1(a)], or a proxy device can perform the access control scheme on behalf of the IMD [Fig. 1(b)]. Obviously, the proxy-based scheme can offload many of the communication, computation, and storage overheads to the proxy, which can be either a specialized authenticator or a general electronic device like the smartphone.
2) *Type of Keys:* The direct and indirect access control between an IMD and a programmer can use either the preloaded long-term "permanent" keys, or the temporary keys generated from the same source simultaneously. A special case is the anomaly detection-based access control, which may not require the use of keys at all.
3) *Access Control Channel:* The access control can be performed over the regular wireless channel (used for normal operation and communication), or take advantage of out-of-band auxiliary channels, such as audio, visual, human body movements, etc.
4) *Access Control Logic:* For IMD access control using the preloaded keys, the access control logic is simply the key matching; while for IMD access control using temporary keys, the access is determined by the physical channel characteristics utilized in the key generations. The common agreed assumption is that the adversary cannot approach the patient within the security range, thereby is not able to access these physical channel characteristics and steal the temporary key; for the anomaly detection-based access control, it checks if the programmer attempts to perform actions that do not comply with the normal pattern (trained from historical records).

Next, we review the existing IMD access control schemes, and divide them into four general categories, namely direct access control with preloaded keys, direct access control with temporary keys, indirect access control via a proxy, and anomaly detection-based schemes. Table I summarizes the IMD access control schemes surveyed in this paper, together with their features, including access control channel, access control logic, accessibility during emergency, sensors required for the IMD, and the programmer, respectively.

A. Direct Access Control With Preloaded Keys

Some schemes utilize a long-term permanent key that has been preloaded into the IMD for access control. Based on how the preloaded key is distributed to an authorized programmer, these schemes can be divided into two groups.

Earlier research attempts consider that the key has been predistributed to IMD programmers. One of the access control schemes proposed in [13] assumes that there is a common

TABLE I
SUMMARY OF EXISTING ACCESS CONTROL SCHEMES

Category		Access control channel	Access control logic	Accessibility during emergency	Sensors required for IMD	Sensors required for programmer
Direct access control with pre-loaded keys	[13], [14], [22]	regular channel	key matching	✓	–	–
	[23]	regular channel	key matching	✓	–	fingerprint and iris collector
	[24]	regular channel	key matching	✓	–	barcode scanner
Direct access control with temporary keys	[25]–[34]	regular channel	proximity	✓	ECG collector	ECG collector
	[14], [35]	human body	proximity	✓	electrode	electrical signal generator
	[36]	physical vibration	proximity	✓	accelerometer	vibration generator, speaker
	[13], [37]	audio / ultrasonic	proximity	✓	sound transmitter / microphone	microphone / sound transmitter
	[38], [39]	NFC channel	proximity	✓	NFC chip	NFC chip
Indirect access control via a proxy	[40]–[43]	regular channel	signature verification	✓	–	–
	[44]* [45]*	regular channel	proximity	✓	–	accelerometer
	[46]*	visual channel	proximity	✓	–	barcode scanner / display
	[47]*	visual channel	proximity	✓	–	LED receiver
Anomaly detection	[48]–[53]	-	anomaly detection	✓	sound detector [51]	–

∗ means the original design is not for IMD, but can be adopted or modified to work for IMD access control

master key K_M for all commercial programmers, and each IMD I has a device-specific key $K = f(K_M, I)$ (f is a cryptographic function). To access a given IMD I, the programmer first requests its identity I and a nonce N, then it computes the key $K = f(K_M, I)$ and the response $R = RC5(K, N)$. Finally, the IMD will verify the response it received from the programmer. However, it is not realistic to require all IMD manufacturers to use a common master key. In addition, the leak of the master key will threaten the safety of all IMDs and programmers.

Li *et al.* [14] proposed a rolling code-based authentication scheme, in which the insulin pump and the programmer share an encryption key used to encrypt the sequence number. The access is permitted if the difference of the sequence number is within a certain range. Liu *et al.* [22] introduced the idea of adding an extra wake-up circuit before the main circuit of the IMD, which is implemented using the passive RFID technology and is able to harvest energy from the incoming signal to perform a lightweight verification of the wake-up authentication code. The main circuit will be waked up only if the wake-up code is verified, so as to defeat resource depletion attacks. However, both schemes assume that the programmer and the IMD have preshared the rolling code/wake-up code/encryption key. Considering that the patient may need emergency treatment in different hospitals, clinics, and even ambulances, it is not feasible to store such secrets of all IMDs in a single programmer.

Other researchers propose that the IMD programmer obtains the key right before it attempts to access an IMD, either by using the physical characteristics of the human body or an item possessed by the patient. Hei and Du [23] embedded the patient's biometric features into the IMD for access control, including the fingerprints, iris and height. To make the verification of bio-features lightweight, the first level of protection only verifies the type of fingerprint (arch, loop, or whorl), iris color, and patient height. The second level of verification is more precise, which utilizes the iris data for access control. To reduce the overhead, their iris matching scheme only compares part of the iris code (sampled from the iris images). Denning *et al.* [24] proposed the use of visual objects to carry the key to the IMD. Specifically, the operator of the IMD programmer needs to first find the password engraved on a medical alert bracelet, the password tattooed as a visible 2-D barcode or as a ultra-violet visible 2-D barcode. The major disadvantage of these methods is that the adversary may obtain the bio-features and printed code stealthily, and hence can access the IMD with a legitimate programmer.

The most significant deficiency of access control schemes using the predistributed permanent key is its coarse-grained access control. In real life, the patient carrying an IMD may need treatment by medical personnel other than the primary care physician, e.g., when traveling out of hometown or getting injured in a traffic accident. Such access is supposed to be one-time only, but instead the programmer used in these scenarios gains unlimited access unless the preloaded key is replaced. However, the revocation process of the key is too hard to implement considering the amount of medical entities to be notified. Suppose a programmer is hacked or stolen by an adversary (i.e., the key is leaked), the IMD will be exposed to malicious attacks. All such worries can be mitigated if a temporary key is used instead.

B. Direct Access Control With Temporary Keys

In contrast to the usage of a preloaded key for access control, most existing schemes employ a pair of temporary keys generated/distributed on the fly during the access control process. Specifically, one category of such schemes requires the IMD and the programmer to extract certain features from the same source simultaneously, and generate the temporary keys based on these common features, respectively. The other category of schemes only needs one device to generate the key, then the key is distributed to the other device. After the key generation/distribution is completed, it can be used to establish an encrypted communication channel.

The reliability of the temporary key-based access control depends on the safety of the cryptographic key generation and distribution procedures. That is, the temporary key generation and distribution must be performed in proximity to the IMD, while the adversary cannot approach the patient to measure the source where the key is generated from, or eavesdrop on the transmission of the key. Various proximity-based methods can be used, e.g., biometrics, wireless signals, audio, etc. However, in practice, adversaries may resort to all kinds of approaches to get the temporary key. For example, they may deploy hidden monitoring equipment near the patient (instead of being presence themselves), or develop advanced techniques to extend the attack range.

1) Biometrics: Physiological values like the electrocardiogram (ECG or EKG) are popular sources used in existing biometrics-based schemes. ECG signal has two major advantages.

a) A fairly high level of randomness that the adversaries cannot predict.
b) ECG signal is measured in high accuracy only if the device is in physical contact with the patient.

The use of physiological values to secure the communications in BANs was first introduced in [25]. They proposed to use the pseudo-random number extracted from the biometric traits for the encryption and decryption of the temporary key during transmission. The differences of physiological signals measured by different sensors (at different locations of human body) are modeled as communication error. A simple error-correction scheme based on majority decoding is employed to alleviate this problem. Venkatasubramanian *et al.* [26] found that although the majority decoding can correct the presence of a few differences in feature vectors obtained from the physiological signal, it cannot handle reordering of the presence of additional features (in one of the sensors). They addressed this drawback with a cryptographic construct named fuzzy vault. As pointed out in [27], an adversary may infer the legitimate points and identify the polynomial used in the vault. The intuitive method to reduce the probability of breaking a vault is to increase the number of chaff points. However, the increase of the vault size also rises the collision rate between the features generated by one sensor and the chaff point generated by another sensor, which will lead to a false rejection. Instead of using error correction codes or reconstructing polynomials, Hu *et al.* [27] proposed the ordered-physiological-feature-based key agreement (OPFKA) leverages the fact that the generated features are ordered and known only to the respective sensor itself, and employs simple noisy data as chaff points to provide enhanced security. However, a design weakness resulting from the use of hashing in its second step is revealed in [28], which generates a small hash range and allows an adversary to greatly narrow down its search space in a brute-force attack against the key. Additionally, OPFKA is also vulnerable to an adaptive attack in which an adversary simulates a programmer to extract the key from the IMD.

Bao *et al.* [29] studied the potential to perform entity authentication in body area sensor network (BASN) using the heart rate variability (HRV), which is a readily available feature that can be easily measured in several kinds of physiological signals, such as ECG and photoplethysmogram (PPG). The heart rate can be estimated by the inverse of the time interval between the peaks of adjacent waves in ECG, or the time interval between the peaks of adjacent pulses in PPG. The difference between successive beat-to-beat heart rate is a measure of HRV. To constrain the errors among the generated encryption keys caused by the variations of measurements at different parts of the body, a fuzzy commitment is applied in [54]. Their follow-up work [30] uses the interpulse interval (IPI) as the biometric trait for the authentication and key transmission in BASN, and evaluates the performance of IPI by comparing the error rates under different conditions. However, two principal drawbacks of the above works are presented in [31].

1) The measurement of IPI values may vary due to the sensor deployment location.
2) Using these IPI-based methods to generate a 128-bit key in real-time takes around half a minute, which may not be feasible for authentication.

To overcome these deficiencies, the scheme proposed in [31] performs fast Fourier transform on the EKG signal and the coefficients are concatenated to form a feature vector. The feature vector is then quantized into a binary stream with exponential quantization functions, to produce a key with higher level of entropy. Seepers *et al.* [32] demonstrated that authentication using multiple less-entropic keys may alleviate the effects of intersensor variability and increase the key strength. They introduce the intermultipulse interval, which considers the time difference between two nonconsecutive heart beats, and is able to enhance the key strength at the cost of an extended key-generation time.

Rostami *et al.* [33] investigated the impact of read error rates on the false positive and false negative rates of authentication. Based on statistical analysis of real-world data, they found that roughly four truly random and statistically uncorrelated bits can be extracted from the ECG wave of a single heartbeat, which can be used for strong IMD programmer authentication. Their test results show that the proposed scheme H2H does not reveal any statistically significant information regarding the key source. Zheng *et al.* [34] proposed an ECG multiple fiducial-points-based binary sequence generation (MFBSG) algorithm. The technique of discrete wavelet transforms is employed to detect the arrival time of fiducial points. The time intervals between them are then calculated and used as ECG features to generate temporary keys with low latency. MFBSG algorithm exploits five feature values from one heart beat cycle, hence can be up to five times faster than the existing solely IPI-based methods.

The challenges of using ECG signal for IMD access control include: 1) the measurements of physiological values may vary due to the sensor deployment location, especially when deployed at body regions yielding very noisy measurements like the muscular and skeletal bone [35] and 2) some physiological values may be remotely obtained by an adversary (e.g., recent works [55], [56] show that the cardiac pulse and respiration rate can be remotely measured via video camera).

2) Body-Coupled Communications: The second defense scheme in [14] introduces the idea of body-coupled communication, which uses the human body as the transmission medium, in contrast to the conventional over-the-air communication. Body-coupled communication can limit the communication range to the very close proximity of the human body, which raises the difficulty for the adversary to eavesdrop on the communication. Another advantage is that it may consume less power because the data are only sent around the body rather than through free space. Chang *et al.* [35] proposed to setup the body-coupled communication by injecting an artificial electrical signal below the action potential level of human body (i.e., the threshold voltage magnitude to trigger the body cell activity).

3) Vibration: Kim *et al.* [36] employed a vibration-based unidirectional side channel formed between the vibration generator in the programmer and the accelerometer in the IMD. The advantages of a vibration-based communication channel includes intrinsically short-range, requiring direct physical contact, and highly user-perceptible. Since the vibration has an acoustic side-effect, the speaker of an external device (programmer or smartphone) is used to generate a masking sound as a countermeasure against acoustic eavesdropping attacks.

4) Audio and Ultrasound: The second defense scheme presented in [13] is an audio channel-based key exchange method, in which the IMD generates a random value to be used as a session key and broadcasts it as a modulated sound wave. They assume that the amplitude of this sound wave is explicitly controlled such that it can be received and correctly demodulated by the programmer, while cannot be overheard and demodulated (from the noise) by an adversary out of a safety distance. However, their audio-based key exchange scheme is demonstrated to be weak. Halevi and Saxena [57] tested the capability of a passive adversary to eavesdrop on the audio-channel communication with a general-purpose microphone. The results show that attacks launched from a distance of up to 5–6 ft can achieve an overall accuracy of 97%–100%, which indicates that the audio channel is not resistant to eavesdropping attacks. Rasmussen *et al.* [37] introduced a distance-bounding protocol based on ultrasonic sound signals. The proposed protocol allows the IMD to compute the distance to the programmer since an attacker in larger distance cannot transmit faster than the speed of ultrasonic sound, regardless of the type of transceiver or antenna being used. However, they also indicate that without appropriate shielding, all devices using ultrasonic distance bounding are vulnerable to compromise by inducing signals in the ultrasonic circuitry.

5) Near Field Communication: Some previous research works [38], [39] propose to utilize the near field communication (NFC) to perform device pairing, which supports key exchange between an IMD and the programmer in short communication range (less than 6 cm). Hei *et al.* [38] also measured the round trip time to eliminate relay attacks. In addition, they considered the crowded scenarios where an adversary may place the malicious programmer within the NFC communication range and access the IMD. To prevent this issue, they designed a crowd detection algorithm using WiFi and the patient's smartphone (not for authentication purpose).

C. Indirect Access Control via Proxy

Since the battery capacity of IMD is limited, many existing works use an indirect access control between the programmer and the IMD with the assistance of an external device (proxy). The proxy is usually a wearable device or a smartphone which has more power and computational resources than the IMD. The communications between the IMD and the proxy are protected with the lightweight symmetric encryption and can be considered safe, while the access control is delegated to the proxy device. Hence, the proxy device is responsible for securing the IMD/BAN telemetry. It cannot only perform more complex and power-consuming access control scheme, but also equip and employ more sensors for the advanced and multifactor access control. Note that the usage of a proxy device may increase the vulnerability surface as well. For example, the adversary could launch attacks through malicious apps on the proxy smartphone or wearable device.

The proxy-based access control is designed to be disabled in special situations where the proxy is missing, so that medical personnel can still gain access to the IMD. In case of medical emergency when the patient is traveling and the local medical staff cannot be authenticated, the medical staff can simply put the proxy device out of the communication range to gain access to the IMD. Note that this type of schemes assume that the adversary cannot get close to the patient and physically remove the proxy without being caught.

1) Friendly Jamming-Based Schemes: Radio jamming refers to the deliberate use of radio noise or signals to disrupt communications (or prevent listening to broadcasts). However, using it properly can protect the confidentiality of sensitive communications in the presence of eavesdroppers, and block the packets sent by the adversary. Several work has adopted friendly jamming in the IMD access control.

Denning *et al.* [40] proposed to use an external device named Cloaker to proxy authorized communication to the IMD. Specifically, if the Cloaker is present, the IMD will simply ignore incoming communications from all other parties; while if Cloaker is not in vicinity, the IMD enters the "open-access" state in which it listens and responds to all incoming communication requests. This can guarantee that under emergency situations (e.g., Cloaker is lost or damaged), the authorized medical personnel can still access the IMD. However, the reliability of this scheme depends on IMD's knowledge of the presence of Cloaker. The adversary may exploit this fail-open protocol by jamming the discovery messages between the IMD and Cloaker, to convince the IMD of Cloaker's absence. To counter this jamming attack, several potential solutions are suggested, including communicating at nonpredictable and pseudorandom time intervals, using in-body signaling techniques, and using various transmit characteristics. For the authentication between the programmer and Cloaker, the Cloaker can be preloaded with the public keys of authorized external programmers. After a successful authentication, instead of letting the programmer and the IMD communicate directly, Cloaker serves as a message relay so that it can log all the communications between the programmer and the IMD for forensics and analysis purposes.

Another proxy-based authentication scheme IMDGuard is presented in [41], which leverages the external wearable device Guardian. Similar to Cloaker, Guardian serves as the authenticator if present; otherwise, the IMD is openly accessible (emergency mode). IMDGuard can avoid the periodic message broadcasting for the existence detection of Guardian, and is resistant to the spoofing attack in which the adversary jams all messages transmitted from the Guardian to spoof the IMD to enter the emergency mode. Specifically, a simple challenge-response verification is added to the beginning of the emergency mode access control, in which the IMD will send two portions of challenges separated by a fixed time of T. If Guardian is present but "hidden" by the jamming attack, it will realize that the IMD is being spoofed into the emergency mode when hearing the first portion of the challenge message. Then, Guardian will jam the second portion of challenge message. As a result, the programmer will be unable to return the correct answer and rejected by the IMD. Guardian authenticates a programmer by verifying its signature. Once successful, Guardian will issue a pair of temporary session keys to the IMD and the programmer for further direct communication. Rostami *et al.* [28] presented a simple man-in-the-middle attack targeted at the IMDGuard scheme, which takes advantage of a protocol flaw in the second round to recover an additional bit of information for each block. This attack can reduce the effective key length from 129 to 86 bits.

Gollakota *et al.* [42] focused on the confidentiality of the IMDs' transmissions and use *shield* to protect IMDs against commands from unauthorized parties without requiring any modification to the IMDs. Specifically, a personal base station *shield* is used to relay the communications between the IMD and an authorized programmer. Shield utilizes a novel full-duplex radio design with two antennas: 1) a jamming antenna and 2) a receive antenna. Such design allows it to simultaneously receive the IMD's signal and jam the IMD's messages, preventing others from decoding them while being able to decode them itself. Additionally, to defend against unauthorized access, Shield listens for unauthorized transmissions to the IMD and jams them. As a result, the IMD cannot decode the adversarial transmissions (commands).

However, Tippenhauer *et al.* [58] analytically and experimentally demonstrated the weakness of defense schemes based on friendly jamming. They constructed an MIMO-based attack that enables the attacker to recover communications protected by friendly jamming, thereby break the confidentiality provided by friendly jamming in all settings.

2) Gateway-Based Schemes: Zheng *et al.* [43] proposed a nonkey-based security scheme, named BodyDouble, for the emergency treatment on IMDs. This scheme employs an external authentication proxy embedded in the gateway. When an adversary launches attacks, the gateway will jam its request/command signal unless it can authenticate its identity (digital signature). The gateway will also pretend to be the wireless interface of the IMD so that the adversary is spoofed to communicate with the gateway instead of the IMD. In emergency situations, the IMD can be directly accessed by simply powering off or removing the gateway.

3) Mobile Device-Based Schemes: Modern mobile devices are equipped with a variety of sensors, which can be utilized to assist the generation/distribution of the temporary key.

Xu *et al.* [44] presented Walkie-Talkie, a shared secret key generation scheme using the user's walking characteristics (gait). One major challenge is that the accelerometer signal captured may be the aggregated signal of multiple actions (e.g., walking and swinging arms). To address this issue, Walkie-Talkie uses the blind source separation technique to separate the signals produced from gait and arm swing, and use the common gait signal to generate the temporary key. Yüzügüzel *et al.* [45] proposed to derive a shared secret (key) from a special type of shared motion—shaking of two devices which are held together. Ten different features are extracted from the accelerometer data after an implicit synchronization, followed by a computationally simple quantization method, namely the standard decimal-to-binary quantization. Similarly, the motion-based key generation methods can be adopted for IMD access control. Specifically, the proxy mobile device and the programmer are held together, and go through the same set of movements. A secured channel can be established since only the programmer next to the proxy has the shared key.

Zhang *et al.* [46] introduced SBVLC, a secure system for barcode-based visible light communication (VLC) between smartphones. This can also be used for temporary key distribution in IMD access control, in which the programmer displays a barcode containing the temporary key to the proxy, and the proxy scans and decodes the barcode to recover the key (or vice versa).

Li *et al.* [47] proposed an user-aided authenticated key agreement protocol for BAN using synchronous LED blinking sequences. In IMD context, the proxy mobile device can send a light beam containing the temporary key via its light sensor (e.g., LED flash), to the programmer placed in close vicinity. The VLC can be considered secure if the strength of the LED light is well-controlled so that only light receiver in proximity can successfully receive and decode. In addition, no human participation is required so that the VLC-based access control scheme can work for emergency situations.

D. Anomaly Detection

Anomaly detection is a special type of access control scheme that attempts to automatically identify resource depletion and unauthorized access. This is generally achieved by comparing with the normal patterns over time, such as physiological changes or IMD access patterns (e.g., commands, time, and locations). The advantage of anomaly detection-based schemes is that it employs temporal and location correlation. However, it may not achieve 100% accuracy since attacks compliant with the normal pattern will not be detected.

Hei *et al.* [48] proposed a novel support vector machine (SVM) based defense scheme to address resource depletion attacks. Specifically, the normal IMD access patterns are trained to build an SVM model, which is loaded into the patient's cell phone. The phone will perform an efficient classification algorithm to reject the unauthorized access. When the IMD detects an emergency (e.g., a heart attack), it will deactivate the SVM-based security scheme so that the emergency personnel can still access the IMD without being blocked.

Zhang *et al.* [49] presented a framework for securing IMDs based on wireless channel monitoring and anomaly detection. Their scheme utilizes an external security monitor named MedMon, which detects adversarial attacks that deviate from legitimate transmissions either in the physical signal characteristics or in the behavior. MedMon tracks all wireless communications of the IMD, and identifies physical anomalies using physical characteristics including the received signal strength indicator, time of arrival (TOA), differential TOA, and angle of arrival. It also keeps a record of the historical data and commands. When new commands/data are received, MedMon compares them to the historical records to decide whether they constitute a behavioral anomaly that may cause harm to the patient. When an anomaly is detected, MedMon can initiate either a passive defense by alerting the patient, or an active defense by jamming the transmissions from reaching the medical device. Likewise, Ankarali *et al.* [50] proposed a physical layer authentication technique for IMD with the help of a wearable external device (WED) attached to the patient body. In the initial setup, the IMD sends pilot signals. The WED will estimate the wireless channel and pre-equalizes the signal. However, assuming that an adversary cannot be closer to the IMD than the WED, the larger path loss and signal dispersion will lead to erroneous channel estimation. Hence, adversaries trying to control or mislead IMDs from relatively distant locations can be prevented.

Henry *et al.* [51] introduced an anomaly detection scheme that is specific to IMDs for diabetes treatment. They propose a system to forensically detect the patient's eating activity, based on bowel sound. The bowel sound detection sensor is integrated into an insulin pump system, and its data is used to determine if an incoming command could result in a security incident (e.g., an insulin bolus that can cause hypoglycemia). Similarly, Hei *et al.* [52], [53] proposed the patient infusion pattern-based access control scheme (PIPAC) for the wireless insulin pump system. Two attacks via wireless links are considered, including the single acute overdose and chronic overdose over a long time period. To defeat these attacks, PIPAC employs the supervised learning to learn the normal patient infusions pattern with the dosage amount, rate, and time of infusion. The generated regression models are used to dynamically configure a safety infusion range for abnormal infusion identification.

IV. Access Control Model

In this section, we look into the IMD access control design from the access control model itself. We found that most existing IMD access control schemes fall into proximity-based access control, identity-based access control, and risk adaptive access control.

A. Identity-Based Access Control

The identity-based access control is the simple mechanism that exists for authenticating a device/user based on the identity or password that they possess. In the electronic health record system proposed by Sun *et al.* [59], an online authentication server is used to authenticate the physician attempting to access (checking the ID). They also propose that the patient's trusted family members should be able to perform authorized operations on behalf of the patient in emergency situations. Lin *et al.* [60] designed CAM, a cloud-assisted privacy preserving mobile health monitoring system, which uses the identity-based encryption to protect private health data. Identity-based access control is a straightforward approach for IMD protection. Usually, the patient only allow people they trust to access his/her IMD, e.g., family doctor and relatives. The patient can add the trusted people into an access control list (probably assigning them different levels of privilege), and have the IMD verify the identity of the access requester. Some related works using this access control model [13], [14], [22]–[24] consider the basic case, in which there is only one password/secret, while in other works [40]–[43], the proxy delegates the authentication and verifies the digital signature of the requester.

B. Role-Based Access Control

In the role-based access control model, the requester's professional role will determine whether the access will be granted or denied. A patient can freely choose a set of roles that are allowed to gain access to the IMD, such as the emergency medical technician, family doctor, nurses, pharmacists, specialist, admin staff, relatives, and the patient himself/herself. The difference between the role-based access control and the identity-based access control is that the requester will not be identified even if the access is granted. Although dividing people into categories based on roles makes it more difficult to implement granular access control, the identity of the requester is not necessary in IMD context. For example, when the patient is unconscious and needs emergency treatment in a foreign country, the most urgent thing is to make sure that the access requester is a medical staff rather than his/her name. Li *et al.* [61] proposed to grant access rights to patient-related data based on their professional roles in wireless BAN (WBAN). Similarly, the role-based model can also be applied to IMD access control, which can effectively control which types of requesters are allowed to access.

C. Attribute-Based Access Control

The attribute-based access control is an access control model wherein the access control decisions are made based on a set of attributes associated with the requester, e.g., speciality, license validity, certification of operating this IMD model, etc. Attribute-based access control can be viewed as an extension of identity-based access control since the identity of the requester can be one of the attributes. Attribute-based encryption (ABE) is a one-to-many encryption method, which can guarantee that the ciphertext can only be decrypted by users who own a certain set of attributes. ABE is collusion-resistant so that colluding users cannot gain access by combining their associated attributes if none of them possesses a sufficient number of attributes to successfully decrypt the ciphertext alone. There are two major types of ABE schemes: 1) key-policy ABE (KP-ABE) [62] and 2) ciphertext-policy ABE (CP-ABE) [63]. In KP-ABE, users' secret keys are generated based on an access tree whose leaves are associated with attributes, and the data are encrypted over a set of attributes. In CP-ABE, users' secret keys are generated over a set of attributes and the ciphertext specifies the access tree (policy). Attributes have been employed in many research works [64]–[72], to control the access of medical data, body area sensor networks, cloud system. The attribute-based model is suitable for IMDs, which can provide a fine-grained access control over the requester's qualifications.

D. Risk Adaptive Access Control

The risk adaptive access control model is devised to bring real-time, adaptable, risk-aware into the decision making. Specifically, it considers the varying situational conditions and changing of security risks in accordance with the access control policy. The anomaly detection-based access control schemes [48]–[53] fall into this category, which constantly monitor any abnormal behavior or incident in the access to the IMD.

E. Proximity-Based Access Control

A large portion of the existing IMD access control schemes [13], [14], [25]–[39] are based on the physical proximity of the programmer to the IMD. That is, the programmer can generate the same key used to decrypt the communication only if it is in physical contact or close proximity with the patient. Proximity-based access control is reasonable under the premise that the adversary is deterred from getting near the patient.

V. DISCUSSION

A. Online Authentication

Nowadays, online authentication has been widely used by IT service providers. Although access to personal computing devices like phone and PC is authenticated locally, IMD is different in that it is not a strictly "personal" device and is supposed to be operated by clinicians. In emergency situations, the IMD should allow access by any eligible clinician. However, it is not practical to have the IMD to store the information used to verify all clinicians. Some previous works [59], [73] propose to use a dedicated authentication server of a governmental health agency or hospital, which requires either the IMD proxy or the programmer to be able to connect to the Internet to verify the access requester (for IMD proxy) or get permission to access (for programmer).

Besides, modern IMDs [74], [75] are designed to support remote monitoring and medical treatment over long-range, high-bandwidth wireless links, so that doctors can remotely monitor their patients' health status or adjust their treatments without requiring the patient to be physically present at the clinical environments. The remote access and reprogramming of the IMD via Internet requires the authentication to be made and a secure channel to be established [76], [77].

The disadvantage of online authentication is that Internet connection may not be always available. For example, when the patient needs medical treatment while traveling to depopulated zone. Hence, a secondary local access control scheme must be embedded in case of such special situations.

B. Low-Power and Zero-Power Authentication

To address the limitation of computational capacity posed by power supply, a group of research works focus on enabling powerless authentication on IMDs. Halperin *et al.* [13] proposed zero-power defense and zero-power notification mechanisms that harvest energy from an external source (i.e., RF signal sent by the IMD programmer) without drawing energy from the primary battery. They implemented the prototype on revision 1.0 of the wireless identification and sensing platform [78], a postage stamp-sized embedded system. Ellouze *et al.* [79] designed a powerless mutual authentication protocol with RF energy harvesting. Instead of using fixed preshared keys, their scheme extracts dynamic biometric keys from ECG signals collected at IMD and the programmer.

Xu *et al.* [80] propose to use physical unclonable functions (PUFs) to implement low power and robust IMD security schemes. PUFs are low power physical digital hardware systems that have very complex but stable input to output mappings. Its unclonability property ensures that even if an attacker steals the device, they cannot reproduce its functionality. Their system consists of two PUFs: one is integrated as a security circuit in IMD and the other one is an external device that only the programmer (e.g., doctor) has access to. The two PUFs are paired and matched before one is installed into the patient body, such that their input–output mappings are identical. That is, both devices can produce identical output streams for authentication and/or encryption when given the same inputs.

C. Network Security in Body Area Networks

The rapid growth in physiological sensors and low-power wireless communication has enabled a new generation of wireless sensor networks, for inexpensive and continuous health monitoring. These devices are called BANs, which can be either embedded inside the body, implants, or surface-mounted on the body. BANs can also be referred to as the WBANs or a body sensor networks (BSNs), which are essentially a wireless network of wearable computing devices. Several literatures [81]–[85] have studied the related network and security issues.

VI. CONCLUSION

This paper surveys the state-of-the-art approaches to enforce access control on IMDs. We roughly classified them into four different groups: direct access control with preloaded keys, direct access control with temporary keys, indirect access control via a proxy, and anomaly detection-based schemes. For each group, we presented the affiliated related works together with their advantages and deficiencies. Additionally, we studied how various access control models can be used to protect the IMD. Finally, the viability to use online authentication server and low-power (zero-power) authentication techniques are discussed.

REFERENCES

[1] *Implantable Medical Devices Market—U.S. Industry Analysis, Size, Share, Trends, Growth, and Forecast 2012–2018*, Transparency Market Res., Albany, NY, USA, 2013.

[2] R.-F. Xue, K.-W. Cheng, and M. Je, "High-efficiency wireless power transfer for biomedical implants by optimal resonant load transformation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 4, pp. 867–874, Apr. 2013.

[3] K. M. Silay, C. Dehollain, and M. Declercq, "A closed-loop remote powering link for wireless cortical implants," *IEEE Sensors J.*, vol. 13, no. 9, pp. 3226–3235, Sep. 2013.

[4] *Wireless Power Supplier WiTricity Expands Medical-Industry Footprint*, B Boston Assoc. Inc., Vernon, CA, USA, 2015. [Online]. Available: http://www.betaboston.com/news/2015/08/26/wireless-power-supplier-witricity-expands-medical-industry-footprint/

[5] 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. IEEE Symp. Security Privacy*, Berkeley, CA, USA, May 2014, pp. 524–539.

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

[7] Z. E. Ankarali *et al.*, "A comparative review on the wireless implantable medical devices privacy and security," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare Transforming Healthcare Through Innov. Mobile Wireless Technol. (MOBIHEALTH)*, Athens, Greece, Nov. 2014, pp. 246–249.

[8] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, "Ideas and challenges for securing wireless implantable medical devices: A review," *IEEE Sensors J.*, vol. 17, no. 3, pp. 562–576, Feb. 2017.

[9] R. Altawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.

[10] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design challenges for secure implantable medical devices," in *Proc. 49th Annu. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, 2012, pp. 12–17.

[11] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.

[12] A. Sawand, S. Djahel, Z. Zhang, and F. Nait-Abdesselam, "Toward energy-efficient and trustworthy ehealth monitoring system," *China Commun.*, vol. 12, no. 1, pp. 46–65, Jan. 2015.

[13] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE S P*, Oakland, CA, USA, 2008, pp. 129–142.

[14] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE HealthCom*, Columbia, MO, USA, 2011, pp. 150–156.

[15] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in *Proc. Black Hat USA*, 2011.

[16] E. Marin, D. Singelée, B. Yang, I. Verbauwhede, and B. Preneel, "On the feasibility of cryptography for a wireless insulin pump system," in *Proc. 6th ACM Conf. Data Appl. Security Privacy (CODASPY)*, New Orleans, LA, USA, 2016, pp. 113–120.

[17] B. Jack. (2013). *Implantable Medical Devices: Hacking Humans*. [Online]. Available: https://en.wikipedia.org/wiki/Barnaby_Jack#cite_note-medcity-11

[18] D. Goldman. (2013). *A Hacker Can Give You a Fatal Overdose*. [Online]. Available: http://money.cnn.com/2015/06/10/technology/drug-pump-hack/

[19] *Two Safety Communications on the Cybersecurity Vulnerabilities of Two Hospira Infusion Pump Systems*, FDA, Silver Spring, MD, USA, 2015. [Online]. Available: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm

[20] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, FDA, Silver Spring, MD, USA, 2014. [Online]. Available: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[21] *Postmarket Management of Cybersecurity in Medical Devices*, FDA, Silver Spring, MD, USA, 2016. [Online]. Available: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

[22] J.-W. Liu, M. A. Ameen, and K.-S. Kwak, "Secure wake-up scheme for WBANs," *IEICE Trans. Commun.*, vol. 93-B, no. 4, pp. 854–857, 2010.

[23] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proc. IEEE INFOCOM*, Shanghai, China, 2011, pp. 346–350.

[24] T. Denning *et al.*, "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, Atlanta, GA, USA, 2010, pp. 917–926.

[25] 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. ICPP Workshops*, Kaohsiung, Taiwan, 2003, pp. 432–439.

[26] 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.

[27] C. Hu *et al.*, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2274–2282.

[28] M. Rostami, W. Burleson, A. Juels, and F. Koushanfar, "Balancing security and utility in medical devices?" in *Proc. IEEE Design Autom. Conf. (DAC)*, Austin, TX, USA, 2013, pp. 1–6.

[29] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Proc. IEEE Conf. Eng. Med. Biol.*, Shanghai, China, 2005, pp. 2455–2458.

[30] 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.

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

[32] R. M. Seepers, C. Strydis, I. Sourdis, and C. I. D. Zeeuw, "Enhancing heart-beat-based security for mhealth applications," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 1, pp. 254–262, Jan. 2017.

[33] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM CCS*, Berlin, Germany, 2013, pp. 1099–1112.

[34] G. Zheng *et al.*, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 3, pp. 655–663, May 2017.

[35] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. L. Huang, "Body area network security: Robust key establishment using human body channel," in *Proc. USENIX HealthSec*, 2012, p. 5.

[36] Y. Kim, W. S. Lee, V. Raghunathan, N. K. Jha, and A. Raghunathan, "Vibration-based secure side channel for medical devices," in *Proc. IEEE Design Autom. Conf. (DAC)*, San Francisco, CA, USA, 2015, pp. 1–6.

[37] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. ACM CCS*, Chicago, IL, USA, 2009, pp. 410–419.

[38] X. Hei, X. Du, and S. Lin, "Poster: Near field communication based access control for wireless medical devices," in *Proc. ACM MobiHoc*, Philadelphia, PA, USA, 2014, pp. 423–424.

[39] B. Kim, J. Yu, and H. Kim, "In-vivo NFC: Remote monitoring of implanted medical devices with improved privacy," in *Proc. ACM SenSys*, Toronto, ON, Canada, 2012, pp. 327–328.

[40] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proc. USENIX HotSec*, San Jose, CA, USA, 2008, Art. no. 5.

[41] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, 2011, Shanghai, China, pp. 1862–1870.

[42] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM SIGCOMM*, Toronto, ON, Canada, 2011, pp. 2–13.

[43] G. Zheng, G. Fang, M. A. Orgun, and R. Shankaran, "A non-key based security scheme supporting emergency treatment of wireless implants," in *Proc. IEEE ICC*, Sydney, NSW, Australia, 2014, pp. 647–652.

[44] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication," in *Proc. ACM/IEEE IPSN*, Vienna, Austria, 2016, pp. 1–12.

[45] H. Yüzugüzel, J. Niemi, S. Kiranyaz, M. Gabbouj, and T. Heinz, "ShakeMe: Key generation from shared motion," in *Proc. IEEE Int. Conf. Pervasive Intell. Comput. (PICom)*, 2015, pp. 2130–2133.

[46] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: Secure barcode-based visible light communication for smartphones," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, 2014, pp. 2661–2669.

[47] 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. Sensor Netw.*, vol. 9, no. 2, 2013, Art. no. 18.

[48] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. IEEE GLOBECOM*, Miami, FL, USA, 2010, pp. 1–5.

[49] M. Zhang, A. Raghunathan, and N. K. 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.

[50] Z. E. Ankarali *et al.*, "Physical layer security for wireless implantable medical devices," in *Proc. IEEE 20th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Guildford, U.K., Sep. 2015, pp. 144–147.

[51] N. L. Henry, N. R. Paul, and N. McFarlane, "Using bowel sounds to create a forensically-aware insulin pump system," in *Proc. USENIX HealthTech*, Washington, DC, USA, 2013, p. 8.

[52] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky, "PIPAC: Patient infusion pattern based access control scheme for wireless insulin pump system," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 3030–3038.

[53] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky, "Patient infusion pattern based access control schemes for wireless insulin pump system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 11, pp. 3108–3121, Nov. 2015.

[54] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "A new symmetric cryptosystem of body area sensor networks for telemedicine," in *Proc. 6th Asian–Pacific Conf. on Med. and Biol. Eng.*, 2005.

[55] M.-Z. Poh, D. J. McDuff, and R. W. Picard, "Non-contact, automated cardiac pulse measurements using video imaging and blind source separation," *Opt. Exp.*, vol. 18, no. 10, pp. 10762–10774, 2010.

[56] F. Zhao, M. Li, Y. Qian, and J. Z. Tsien, "Remote measurements of heart and respiration rates for telemedicine," *PLoS ONE*, vol. 8, no. 10, 2013, Art. no. e71384.

[57] T. Halevi and N. Saxena, "On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping," in *Proc. ACM CCS*, Chicago, IL, USA, 2010, pp. 97–108.

[58] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Proc. IEEE S&P*, Berkeley, CA, USA, 2013, pp. 160–173.

[59] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in *Proc. 31st Int. Conf. Distrib. Comput. Syst.*, Minneapolis, MN, USA, Jun. 2011, pp. 373–382.

[60] H. Lin, J. Shao, C. Zhang, and Y. Fang, "CAM: Cloud-assisted privacy preserving mobile health monitoring," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 6, pp. 985–997, Jun. 2013.

[61] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.

[62] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Security (CCS)*, 2006, pp. 89–98.

[63] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy (SP)*, May 2007, pp. 321–334.

[64] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[65] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[66] Z. Guan, T. Yang, and X. Du, "Achieving secure and efficient data access control for cloud-integrated body sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, Jan. 2015, Art. no. 142.

[67] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-health wireless sensor networks," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Munich, Germany, Jul. 2012, pp. 1–7.

[68] M. Barua, X. Liang, R. Lu, and X. Shen, "PEACE: An efficient and secure patient-centric access control scheme for ehealth care system," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Shanghai, China, Apr. 2011, pp. 970–975.

[69] Z. Guan, J. Li, Z. Zhang, and L. Zhu, "Conditional ciphertext-policy attribute-based encryption scheme in vehicular cloud computing," *Mobile Inf. Syst.*, vol. 2016, Oct. 2016, Art. no. 1493290.

[70] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in *Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Security Privacy (HotWiSec)*, Budapest, Hungary, 2013, pp. 31–36.

[71] P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. Suarez-Tangil, "Secure publish-subscribe protocols for heterogeneous medical wireless body area networks," *MDPI Sensors*, vol. 14, no. 12, pp. 22619–22642, 2014.

[72] Z. Guan *et al.*, "An efficient traceable access control scheme with reliable key delegation in mobile cloud computing," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, p. 208, Dec. 2016.

[73] C.-S. Park, "Security mechanism based on hospital authentication server for secure application of implantable medical devices," *Hindawi BioMed Res. Int.*, vol. 2014, Jul. 2014, Art. no. 543051.

[74] *Medtronic MyCareLink Patient Monitor*. Accessed on Jun. 6, 2017. [Online]. Available: http://www.medtronicheart.com/

[75] *Biotronik Home Monitoring*. Accessed on Jun. 6, 2017. [Online]. Available: https://www.biotronik.com/en-us/products/services/home-monitoring/

[76] D. Vassis, P. Belsis, C. Skourlas, and G. Pantziou, "Providing advanced remote medical treatment services through pervasive environments," *Pers. Ubiquitous Comput.*, vol. 14, no. 6, pp. 563–573, 2010.

[77] E. Marin, "Secure remote reprogramming of implantable medical devices," COSIC, Kent, WA, USA, Internal Tech. Rep. 2485, 2014.

[78] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev, "A wirelessly-powered platform for sensing and computation," in *Proc. 8th Int. Conf. Ubiquitous Comput. (UbiComp)*, Orange County, CA, USA, 2006, pp. 495–506.

[79] N. Ellouze, M. Allouche, H. B. Ahmed, S. Rekhis, and N. Boudriga, "Securing implantable cardiac medical devices: Use of radio frequency energy harvesting," in *Proc. 3rd Int. Workshop Trustworthy Embedded Devices (TrustED)*, Berlin, Germany, 2013, pp. 35–42.

[80] T. Xu, J. B. Wendt, and M. Potkonjak, "Matched digital PUFs for low power security in implantable medical devices," in *Proc. IEEE Int. Conf. Healthcare Informat.*, Verona, Italy, Sep. 2014, pp. 33–38.

[81] X. Du and D. Wu, "Adaptive cell relay routing protocol for mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 55, no. 1, pp. 278–285, Jan. 2006.

[82] S. Liang and X. Du, "Permission-combination-based scheme for android mobile malware detection," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 2301–2306.

[83] X. Du, M. Shayman, and M. Rozenblit, "Implementation and performance analysis of SNMP on a TLS/TCP base," in *Proc. IEEE/IFIP Int. Symp. Integr. Netw. Manag.*, Seattle, WA, USA, 2001, pp. 453–466.

[84] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending DoS attacks on broadcast authentication in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 1653–1657.

[85] X. Du and F. Lin, "Designing efficient routing protocol for heterogeneous sensor networks," in *Proc. 24th IEEE Int. Perform. Comput. Commun. Conf.*, Phoenix, AZ, USA, Apr. 2005, pp. 51–58.

Longfei Wu received the B.S. degree in communication engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2012, and the Ph.D. degree in computer and information sciences from Temple University, Philadelphia, PA, USA, in 2017, under the supervision of Dr. X. Du.

He is currently a Professor with the Department of Mathematics and Computer Science, Fayetteville State University, Fayetteville, NC, USA. His current research interests include security and privacy issues of modern computing systems and devices, such as mobile devices, medical devices, and Internet of Things.

Xiaojiang Du (M'04–SM'09) received the B.S. and M.S. degrees from Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the M.S. and Ph.D. degrees from the University of Maryland at College Park, College Park, MD, USA, in 2002 and 2003, respectively, all in electrical engineering.

He is currently a Professor with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA, USA. He was an Assistant Professor with the Department of Computer Science, North Dakota State University, Fargo, ND, USA, from 2004 to 2009. His current research interests include security, wireless networks, and computer networks and systems. He has authored or co-authored over 200 journal and conference papers in the above areas.

Dr. Du was a recipient of the Excellence in Research Award in 2009 and over $3M research grants from the U.S. National Science Foundation, Army Research Office, Air Force Research Laboratory, NASA, the Commonwealth of Pennsylvania, and Amazon. He serves on the Editorial Boards of four international journals. He served as the Lead Chair of the Communication and Information Security Symposium of the IEEE ICC 2015, and the Co-Chair of the Mobile and Wireless Networks Track of the IEEE WCNC 2015. He was the Chair of the Computer and Network Security Symposium of the IEEE/ACM International Wireless Communication and Mobile Computing Conference from 2006 to 2010. He has been a Technical Program Committee member of several premier ACM/IEEE conferences, such as INFOCOM from 2007 to 2015, IM, NOMS, ICC, GLOBECOM, WCNC, BroadNet, and IPCCC. He is a Life Member of the ACM.

Mohsen Guizani (S'85–M'89–SM'99–F'09) received the B.S. (with Distinction) and M.S. degrees in electrical engineering and M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively.

He is currently a Professor and the ECE Department Chair with the University of Idaho, Moscow, ID, USA. He was the Associate Vice President of Graduate Studies with Qatar University, Doha, Qatar, the Chair of the Computer Science Department with Western Michigan University, Kalamazoo, MI, USA, and the Chair of the Computer Science Department, University of West Florida, Pensacola, FL, USA. He also served in academic positions with the University of Missouri–Kansas City, Kansas City, MO, USA, the University of Colorado–Boulder, Boulder, CO, USA, Syracuse University, and Kuwait University, Kuwait City, Kuwait. His current research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He has authored 9 books and over 400 publications in refereed journals and conferences.

Dr. Guizani was a recipient of the Best Teaching Assistant for two consecutive years at Syracuse University and the Best Research Award from three institutions. He currently serves on the Editorial Boards of several international technical journals and is the founder and the Editor-in-Chief of *Wireless Communications* and *Mobile Computing Journal* (Wiley). He guest edited a number of special issues in IEEE journals and magazines. He has also served as a member, the Chair, and the General Chair of a number of international conferences. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker from 2003 to 2005.

Amr Mohamed (S'00–M'06–SM'14) received the M.S. and Ph.D. degrees in electrical and computer engineering from the University of British Columbia, Vancouver, BC, Canada, in 2001 and 2006, respectively.

He was an Advisory IT Specialist with the IBM Innovation Centre, Vancouver, from 1998 to 2007, taking a leadership role in systems development for vertical industries. He is currently an Associate Professor with the College of Engineering, Qatar University, Doha, Qatar, and the Director of Cisco Regional Academy. He possesses over 20 years of experience in wireless networking research and industrial systems development. He has authored or co-authored over 120 refereed journal and conference papers, textbook, and book chapters in reputed international journals and conferences. His current research interests include networking and MAC layer techniques mainly in wireless networks.

Dr. Mohamed was a recipient of three awards from IBM Canada for his achievements and leadership and three Best Paper Awards from the 2015 IEEE/IFIP International Conference on New Technologies, Mobility, and Security, Paris, France. He has served as a Technical Program Committee (TPC) Co-Chair for workshops in the IEEE WCNC'16. He has served as the Co-Chair for technical symposia of international conferences, including Globecom'16, Crowncom'15, AICCSA'14, IEEE WLN'11, and IEEE ICT'10. He has served on the Organization Committee of many other international conferences as a TPC member, including IEEE ICC, GLOBECOM, WCNC, LCN, and PIMRC and as a Technical Reviewer for IEEE, ACM, Elsevier, Springer, and Wiley journals.