Finger-to-Heart (F2H): Authentication for Wireless Implantable Medical Devices

Guanglou Zheng, *Member, IEEE*, Wencheng Yang, Craig Valli, Li Qiao, Rajan Shankaran, Mehmet A. Orgun, *Senior Member, IEEE*, and Subhas Chandra Mukhopadhyay, *Fellow, IEEE*

***Abstract*—Any proposal to provide security for implantable medical devices (IMDs), such as cardiac pacemakers and defibrillators, has to achieve a trade-off between security and accessibility for doctors to gain access to an IMD, especially in an emergency scenario. In this paper, we propose a finger-to-heart (F2H) IMD authentication scheme to address this trade-off between security and accessibility. This scheme utilizes a patient's fingerprint to perform authentication for gaining access to the IMD. Doctors can gain access to the IMD and perform emergency treatment by scanning the patient's finger tip instead of asking the patient for passwords/security tokens, thereby, achieving the necessary trade-off. In the scheme, an improved minutia-cylinder-code-based fingerprint authentication algorithm is proposed for the IMD by reducing the length of each feature vector and the number of query feature vectors. Experimental results show that the improved fingerprint authentication algorithm significantly reduces both the size of messages in transmission and computational overheads in the device, and thus, can be utilized to secure the IMD. Compared to existing electrocardiogram signal-based security schemes, the F2H scheme does not require the IMD to capture or process biometric traits in every access attempt since a fingerprint template is generated and stored in the IMD beforehand. As a result, the scarce resources in the IMD are conserved, making the scheme sustainable as well as energy efficient.**

***Index Terms*—Biomedical informatics, network security, implantable medical devices (IMDs), fingerprint authentication, biometrics.**

Manuscript received March 29, 2018; revised July 24, 2018; accepted August 7, 2018. Date of publication September 10, 2018; date of current version July 1, 2019. *(Corresponding author: Guanglou Zheng.)*

G. Zheng, W. Yang, and C. Valli are with the Security Research Institute, Edith Cowan University, Perth WA 6027, Australia (e-mail: g.zheng@ecu.edu.au; w.yang@ecu.edu.au; c.valli@ecu.edu.au).

L. Qiao is with the School of Engineering and Information Technology, University of New South Wales, Canberra ACT 2610, Australia (e-mail: l.qiao@adfa.edu.au).

R. Shankaran is with the Department of Computing, Macquarie University, Sydney NSW 2109, Australia (e-mail: rajan.shankaran@mq.edu.au).

M. A. Orgun is with the Department of Computing, Macquarie University, Sydney NSW 2109, Australia, and also with the Faculty of Information Technology, Macau University of Science and Technology, Taipa 999078, Macau (e-mail: mehmet.orgun@mq.edu.au).

S. C. Mukhopadhyay is with the Department of Engineering, Macquarie University, Sydney NSW 2109, Australia (e-mail: subhas.mukhopadhyay@mq.edu.au).

Digital Object Identifier 10.1109/JBHI.2018.2864796

I. Introduction

WIRELESS communication technologies have been increasingly incorporated into healthcare and medical devices in order to facilitate more efficient and convenient forms of medical treatment with timely responses to the patients [1]. In particular, modern Implantable Medical Devices (IMDs), including cardiac pacemakers, Implantable Cardioverter-Defibrillators (ICDs) and neurostimulators, all feature wireless communication support [2], [3]. An external device, called a radiowave programmer, communicates with the IMD via the wireless channel. By adding the wireless module, doctors can fine-tune therapy related parameters in the IMD and retrieve critical data for health monitoring purposes. Recent studies, however, have demonstrated successful attacks on IMDs that can not only compromise the confidentiality of medical data but may even trigger malicious actions in the IMD which could potentially harm a patient harm and may even cause death [4]–[6].

A unique challenge in the IMD security design is a trade-off between *security and accessibility* [7]–[9]. A security scheme designed for an IMD must not hinder access to the IMD for medical treatment, especially in an emergency scenario. A conventional symmetric key based scheme, which requires the key to be deployed beforehand, is not viable here. This is because the emergency treatment to a patient is provided by the nearest first-aid responders or doctors and, moreover, there is no guarantee the access to the Internet is available in an emergency scenario. Therefore, it is very challenging to deploy the key at any doctor's end who requires emergency access to the IMD in a timely manner.

Most recently several biometric based schemes have been proposed to address the unique challenge between security vs. accessibility for the IMD [7], [10]. In a medical emergency when there is no security credential pre-deployed, doctors can gain access to the IMD by measuring intrinsic characteristics of the patient's body. Currently, electrocardiogram (ECG) signal-based security schemes have been widely studied for securing the IMD in which a doctor can gain access to a patient's IMD by measuring *real-time* ECG signals of the patient, e.g., the H2H scheme proposed by Rostami *et al.* [7], the IMDGuard scheme proposed by Xu *et al.* [10] and key distribution schemes [11]. Furthermore, ECG-based key distribution schemes, which are proposed to secure wireless body area networks (WBANs), can also be applied to the IMDs [12], [13].

However, in all these ECG-based schemes, the IMD has to capture and process biometric traits every time a secure access attempt is done and this requires a large amount of resources in the IMD. As analyzed in Section II, the biometric trait process includes five steps: ECG signal capture, signal pre-processing, ECG fiducial point detection, random binary sequence generation and other security related computations. Executing all these five steps in every access attempt is a heavy resource-consuming task for the IMD, since the IMD is a tiny wireless device with limited resources. Its battery is normally non-rechargeable and non-replaceable, and is expected to last 5-10 years [3], [6]. Therefore, the resource consumption becomes the major concern if applying the ECG-based security schemes to the IMD.

In order to reduce the consumption of resources within the IMD, in this paper, we propose a novel biometric based IMD security scheme, named Finger-to-Heart (F2H), which uses fingerprints instead of ECG signals to secure the IMD. In the F2H scheme, the IMD does not need to capture or process the biometric traits in every access attempt. The patient's fingerprint is captured and processed beforehand, and thereafter a fingerprint template is generated and stored in the IMD before the implantation. Consequently, an IMD security scheme which utilizes fingerprints exhibits a considerable improvement in terms of the resource consumption when compared to the ECG-based IMD security schemes. The contributions of the paper are summarized below:

- We present the motivations for our research by comparing ECG-based and fingerprint-based IMD security schemes in Section II. The fingerprint-based security scheme does not require the IMD to capture or process biometric traits in every access attempt and thus performs better in terms of resource usage when compared to the ECG-based schemes.
- We propose a system architecture which can underpin the F2H scheme for securing the IMD (Section III), and present an improved Minutia Cylinder-Code (MCC) based fingerprint authentication algorithm for this F2H scheme (Section IV). In order to conserve resources in the IMD, we propose to improve the MCC algorithm by reducing the length of each MCC feature vector and the number of query feature vectors.
- We evaluate the matching performance of the proposed IMD authentication algorithm (Section V). Experiments show that the size of MCC features can be reduced significantly, resulting in a significant reduction of resource consumption in the IMD in terms of memory and available computational power.

Section VI performs a security analysis of the scheme. Current research on IMD security is reviewed and analyzed in Section VII. The final section summarizes our research contributions with some concluding remarks.

II. Motivations

ECG signal-based security schemes have been widely proposed to secure IMDs [7], [10], [11]. However, these ECG-based schemes require a large amount of IMD resources to process biometric traits every time when an access attempt is made. Fig. 1 shows biometric processing steps in both the ECG signal-based and the fingerprint-based security schemes. In order to compare both types of schemes, a common process flow is extracted with five steps: biometric trait capture, pre-processing, feature extraction, feature processing and security related computations.

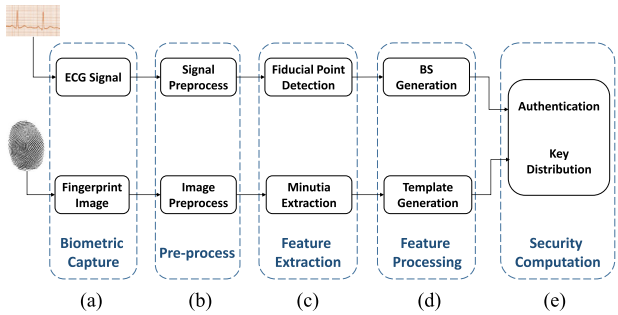

Fig. 1. Biometric processing steps in both the ECG-based and the fingerprint-based security schemes. BS = binary sequence.

A. ECG-based IMD Security

Using steps shown in Fig. 1, key features of ECG based IMD security schemes are summarized below:

a) *Biometric capture:* At the beginning of each secure access attempt, the IMD and the programmer synchronize with each other and capture real-time ECG signals from the body of the patient. Normally, ECG signals are required to be sampled by each device in cycles of 30–60 seconds.

b) *Pre-processing:* The preprocessing of ECG signals is carried out to make the sampled ECG signal ready for extracting features from the signal. This preprocessing includes steps of denoising, removal of baseline wander and power line interference [14].

c) *Feature extraction:* Features on an ECG signal normally refer to ECG fiducial points, especially R peaks in each heartbeat. In the feature extraction step, fiducial points can be detected and recorded by using discrete wavelet transforms. As studied by Zheng *et al.* [15], fiducial points used for the security applications include peak values of P wave, T wave and QRS complex in one heartbeat cycle.

d) *Feature processing:* ECG fiducial points cannot be used for securing IMDs directly. In this step, binary sequences (BSes) are generated by using the detected fiducial points with a random BS generation algorithm [15].

e) *Security Computation:* ECG BSes can be used for authentication or symmetric key distribution between the IMD and the programmer. In the authentication protocol, the programmer sends out the BS that it has generated to the IMD in order to authenticate itself to the IMD as well as to gain access to the IMD. Alternatively, the BSes can be exploited to distribute the key from the IMD to the programmer by using the fuzzy commitment scheme [11].

It is evident from the above discussion that the IMD has to follow all the five steps to capture and process the ECG signals in order to perform security related computations. However, the IMD is a tiny wireless device implanted in the patient's body and its battery is required to have a long lifetime. We can conclude from the analysis that requiring the IMD to capture and process ECG signals frequently can deplete its battery power rapidly thereby reducing the IMD lifetime.

B. Fingerprint-based IMD Security and Comparison

The five steps shown in Fig. 1 are also used in a fingerprint based security scheme to process a fingerprint image and generate features for authentication or key distribution purposes:

- *Biometric capture and preprocessing:* A fingerprint scanner captures a fingerprint image and pre-processes it. The preprocessing includes segmentation, orientation estimation, ridge enhancement and thinning of the image.
- *Feature extraction:* A minutia extractor extracts minutiae, including ridge endings and bifurcations, from the pre-processed image. The minutiae are used to distinguish different users [16].
- *Feature processing:* In order to achieve an alignment-free fingerprint matching process, local structures are established by using feature representation methods, e.g., the minutia cylinder-code [17].
- *Security Computation:* A fingerprint template is generated and stored in the IMD. In an authentication protocol, the programmer scans the patient's fingerprint every time an attempt to access the IMD is initiated and obtains a query which is to be sent to the IMD for the authentication purpose.

Nonetheless, in each access attempt, the IMD does not need to follow all these five steps. Especially it needs not to perform the biometric capturing and feature extraction. This is because, before the IMD implantation operation, a fingerprint template is generated from the patient's fingerprint of good quality and is stored in the IMD. In each access attempt, the IMD only needs to receive a query from an external programmer to execute security related computations. This means that the IMD only needs to process *Step (e) Security Computation* in Fig. 1 in each and every access attempt.

We conclude from the analysis that, for every secure access attempt made, the ECG-based IMD security schemes require the IMD to execute all the five steps in Fig. 1. In contrast, the fingerprint-based IMD security scheme only requires the IMD to execute one step with the other four steps completed before the IMD is implanted in the body. Therefore, the fingerprint-based IMD security scheme has an enormous advantage in terms of energy conservation in the IMD when compared to the ECG based approaches.

III. Securing an IMD With Fingerprints

In this section, we present a system architecture which can support the aforementioned Finger-to-Heart IMD security scheme. The advantages of using this architecture are highlighted.

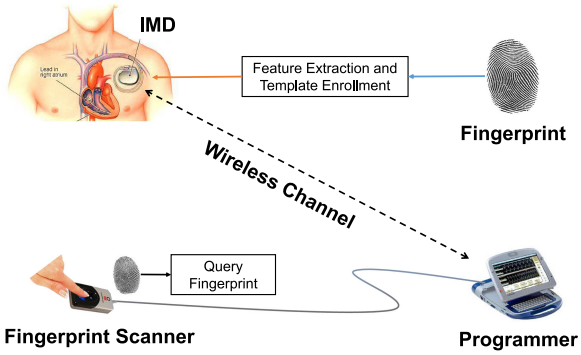

Fig. 2. The architecture of the fingerprint-based IMD security scheme.

A. System Architecture

A system architecture for supporting the application of fingerprint-based security schemes to an IMD is illustrated in Fig. 2. An IMD is implanted in the body of a patient. An external programmer can communicate with the IMD via the wireless channel. Both the IMD and its corresponding programmer form an IMD system.

In order to apply the fingerprint-based IMD security schemes, the following functions and hardware have to be added to an existing IMD system:

- *Add-on components for an IMD:* (a) the IMD memory space for storing the fingerprint template which is generated from the patient's fingerprint image and (b) a security function for verifying the template features against query features which are received from a programmer.
- *Add-on components for a programmer:* (a) a fingerprint scanner integrated with an existing programmer, as shown in Fig. 2, and (b) a function for extracting minutiae and generating query features from the fingerprint image.
- A wireless communication protocol for exchanging security-related messages between the IMD and the programmer. These messages include handshake messages for setting up a connection, query features sent from the programmer to the IMD and messages to convey to the programmer the outcome of the security protocol.

This architecture requires the programmer to extend its hardware by adding a fingerprint scanner, which is not a major concern in the design since the programmer is an external device and is not restricted in terms of size and power. Meanwhile, the IMD needs additional memory space for storing the template but does not require any other extra hardware. Query features of a patient's fingerprint is transmitted from the programmer to the IMD via an authenticated, encrypted channel. In order to achieve a better performance of the whole system, a crypto processor can be used in the IMD and the programmer. This can help to protect fingerprint template and query data against tampering and offer advantages in process speed and power consumption.

B. Fingerprint Authentication

In a fingerprint-based authentication scheme for securing an IMD, the fingerprint template of a patient is stored in the IMD.

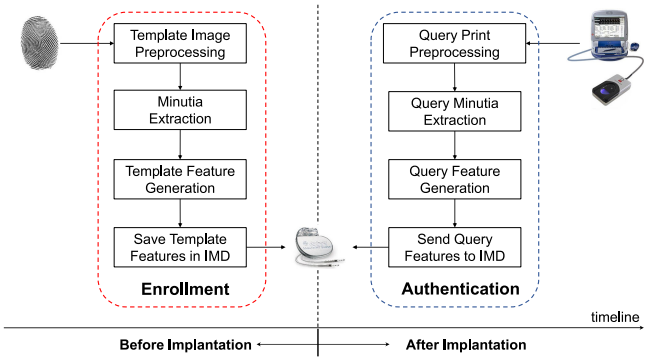

Fig. 3. A flow chat of the fingerprint-based authentication scheme for securing an IMD. The enrollment process is performed before the IMD implantation operation.

A programmer captures a fingerprint image of the patient and generates query features which are to be sent to the IMD for the purpose of authentication. The fingerprint-based IMD authentication scheme includes two phases: the enrollment phase and the authentication phase (shown in Fig. 3), which are described below.

- The *enrollment phase* is to register a patient's fingerprint template in an IMD for use in the authentication phase. A template is generated from a good quality fingerprint image which contains only refined discriminatory features. This enrollment phase is performed before the IMD is implanted in the patient's body by a cardiologist. Therefore, it does not consume resources of the IMD, especially computational resources and battery power.
- The *authentication phase* is to compare the template features against query features in the IMD and then determine whether the access to the IMD from an external programmer is to be permitted or not. In this phase, the programmer needs to capture the patient's fingerprint image and generate query features from it by using the same fingerprint processing algorithm as the one used in the enrollment phase.

If the authentication is successful, the IMD grants access permission to the programmer. The programmer can then read medical data from the IMD or adjust and fine-tune treatment parameters in the IMD [18]. Otherwise, the access to the IMD is blocked.

Each patient can register two fingers in his/her IMD: one as the primary and the other as the secondary. In case when the primary finger is not suitable for authentication (such as when the primary finger is hurt), then the doctor can use the patient's secondary finger for the authentication purpose.

This fingerprint-based IMD authentication scheme can support medical emergency access to the IMD. In an emergency, first-aid responders or doctors who do not possess the predeployed security key or credential of an IMD can still gain access to the IMD by capturing and processing the patient's fingerprint directly.

Fingerprint templates and the authentication algorithm can be stored and implemented in the IMDs in accordance with industrial standards, e.g., ISO/IEC/IEEE 21451-x family standards [19], [20]. A Transducer Electronic Data Sheet (TEDS) can be used to store these templates and the authentication algorithm. According to the standard, TEDS is used to provide machine-readable specification of the characteristics and algorithms for information processing for smart sensors. The fingerprint template can be stored in a removable and updatable memory since each patient's template needs to be registered in their own IMD. Meanwhile, the fingerprint authentication process algorithm could be saved in a read-only memory of an IMD. In this way, an IMD technician or clinician can configure the device with each patient's fingerprint in a clinic or hospital.

Nowadays the fingerprint authentication technology has been widely used to protect personal assets, national security and critical infrastructure, such as mobile phones, border protection and migration control and security sensitive buildings and environments [21]. Within these applications, people have the concern that whether adversaries could spoof a system with an artificial replica of a fingerprint and make it vulnerable to presentation attacks, since users could leave their fingerprints wherever they touch [22]. This is another key research area within the fingerprint authentication technology. Various Liveness Detection (LivDet) or presentation attack detection (PAD) methods have been proposed to counter attacks from spoof fingers, including software-based and hardware-based solutions [23]. Software-based solutions exploit information directly gathered from the fingerprint to detect liveness while hardware-based ones sense information in addition to the fingerprint image to detect liveness. These LivDet solutions can be incorporated into an IMD programmer to distinguish between live and fake biometrics and detect presentation attacks. This can enhance the security level of the F2H scheme.

C. Advantages of F2H Scheme

The IMD and the programmer form an asymmetric system in terms of resources. The IMD, as a medical device implanted in the body, has very limited resources with an extremely small size. However, the programmer, as an external device which is normally kept in a hospital or in a clinic setting, does not have severe resource limitations. Its battery can be charged frequently. The functions in the programmer, e.g., those relating to computations and communications, can be extended to adapt to changes in the IMD. Therefore, the analysis of any security scheme that is undertaken must focus on resource-related overheads at the IMD end rather than at the programmer end.

The fingerprint-based IMD security scheme brings about a significant improvement in biometric processes at the IMD end when compared with the ECG-based IMD security schemes, and thus conserves resources of the IMD. In this scheme, the IMD is required to allocate memory space to store a fingerprint template, execute a fingerprint matching function with the support of a wireless communication protocol in every secure access attempt. Compared to the ECG signal-based IMD security schemes, the fingerprint-based authentication scheme does not require the IMD to capture and preprocess the biometric, or to extract and process relevant features (as analyzed in

Section II). As a result, the resource consumption in the IMD is reduced significantly.

This IMD security scheme can be implemented with the concept of decoupled design proposed by Zheng *et al.* [3]. Since the authentication procedure with the IMD needs to be initiated at the beginning of every wireless communication session, this scheme can be further simplified to avoid overheads by implementing an additional security component in the IMD. This component returns a YES/NO result to decide whether the medical function of the IMD is to be executed or not. This decoupled design can reduce the complexity of the next generation IMDs, and thus reduce the risks of IMD malfunctions and recalls.

Deploying the fingerprint-based security scheme in the IMD could help IMD manufacturers to get their next generation IMD design approved speedily by government agencies. As a medical device, designing a new IMD product or making critical changes to an existing IMD product has to go through a rigorous government approval process by related agencies, e.g., the Food and Drug Administration (FDA) in the United States [3]. This process is normally long but mandatory. Nonetheless, since this fingerprint-based IMD security design does not require adding any extra hardware to the IMD, it can help manufacturers to speed up the approval process, and thus may gain more popularity and its use may become more widespread.

IV. Fingerprint Authentication Algorithm

This section presents a fingerprint authentication algorithm which can implement the F2H system architecture (depicted in Fig. 2) to secure an IMD. In order to generate an alignment-free fingerprint template for automatic matching process, the state-of-the-art Minutia Cylinder-Code (MCC) representation [17], [24]–[26] is employed because of its better matching performance when compared to other well-known algorithms in use, e.g., nearest neighbor-based structures[27] and fixed radius-based structures [28].

A. MCC Representation

A minutia in a template, T, is a triplet, and can be denoted by $m = \{x_m, y_m, \theta_m\}$ where (x_m, y_m) is its location and $\theta_m (0 \leq \theta_m < 2\pi)$ is its direction. The MCC representation associates a 3D local structure, called a cylinder, to each minutia, m. This cylinder is created by encoding relative relationships between m and its neighboring minutiae within a fixed-radius, R, with its base aligned to the direction, θ_m. The cylinder is enclosed in a cuboid which is discretized into $N_C = N_S \times N_S \times N_D$ cells. Each cell is a small cuboid with a base $\Delta_s \times \Delta_s$ and a height Δ_D. A discretized cylinder is illustrated in Fig. 4. It is centered at a given minutia, m, with its base and height representing the relative spatial and directional information of a neighboring minutia, respectively.

Each cell in the cylinder can be represented by three indices (i, j, k) in the coordinate system. A cell is valid only when the projection of its center on the cylinder base is within the intersection of the base and a convex hull defined by the template T. For a valid cell (i, j, k), its relative direction (height), $d\varphi_k$, and relative location, $p^m_{i,j}$, to the center of the cylinder, m, can

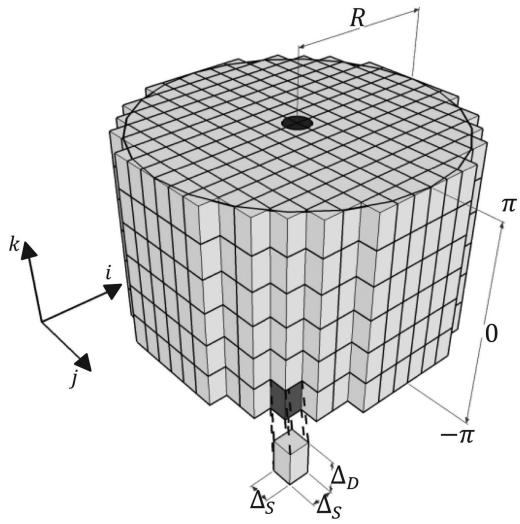

Fig. 4. A discretized cylinder associated to a given minutia in which each cell is a small cuboid with base $\Delta_s \times \Delta_s$ and height Δ_D [17].

be denoted by [17]:

$$\begin{cases} d\varphi_k = -\pi + (k - 0.5) \cdot \Delta_D \\ p^m_{i,j} = \begin{bmatrix} x_m \\ y_m \end{bmatrix} + \\ \qquad \Delta_S \cdot \begin{bmatrix} cos\ (\theta_m) & sin\ (\theta_m) \\ -sin\ (\theta_m) & cos\ (\theta_m) \end{bmatrix} \cdot \begin{bmatrix} i - \frac{N_S+1}{2} \\ j - \frac{N_S+1}{2} \end{bmatrix} \end{cases} \tag{1}$$

The MCC calculates a numerical value, $C_m(i, j, k)$, to represent a cell, (i, j, k), in the cylinder. This value represents the likelihood of finding minutiae which are close to the center of the cell in terms of location and direction. It is calculated by accumulating contributions from a minutia, m_p, in the neighborhood, $N_{p^m_{i,j}}$ of $p^m_{i,j}$ with a radius, $3\sigma_S$, denoted by:

$$\begin{cases} C_m(i, j, k) = \Psi(v, \mu, \tau) = \frac{1}{1+e^{-\tau(v-\mu)}} \\ v = \sum\limits_{m_p \in N_{p^m_{i,j}}} \left(C^S_m(m_p, p^m_{i,j}) \cdot C^D_m(m_p, d\varphi_k) \right) \end{cases} \tag{2}$$

where $C^S_m(m_p, p^m_{i,j})$ represents the spatial contribution of m_p to the cell (i, j, k) while $C^D_m(m_p, d\varphi_k)$ is the directional contribution. $\Psi(v, \mu, \tau)$ is a sigmoid function controlled by two parameters, μ and τ.

In the bit-based implementation process, $\Psi(v, \mu, \tau)$ is defined as 1 if $v \geq \mu$. Otherwise, it is defined as 0. So, the cell value, $C_m\{i, j, k\}$, is represented by one bit value. By combining all cell values in a cylinder, a binary feature vector, C_m, is formed to represent the local structure associated with the minutia, m. The length of C_m is the same as the number of cells in the cylinder.

Given two sets of minutiae: one is a template set, $T = \{m_{t_1}, m_{t_2}, \ldots, m_{t_{n_A}}\}$, and the other is a query, $Q = \{m_{q_1}, m_{q_2}, \ldots, m_{q_{n_B}}\}$. Then MCC representation for the

template and the query can be denoted by,

$$C_{m_T} = \left\{C_{m_{t_1}}, C_{m_{t_2}}, \ldots, C_{m_{t_{n_A}}}\right\} \tag{3}$$

$$C_{m_Q} = \left\{C_{m_{q_1}}, C_{m_{q_2}}, \ldots, C_{m_{q_{n_B}}}\right\} \tag{4}$$

C_{m_T} is stored in the IMD as a template before the implantation while C_{m_Q} is generated by the programmer in each authentication attempt.

B. Local Similarity and Matching

All potential minutia pairs between T and Q can be denoted by,

$$P = \{(m_{t_\zeta}, m_{q_\eta})\}, (1 \leq \zeta \leq n_A, 1 \leq \eta \leq n_B) \tag{5}$$

Two cylinders are associated with each pair of minutiae and can be represented by two binary feature vectors, $C_{m_{t_\zeta}}$ and $C_{m_{q_\eta}}$, respectively. The local similarity score between these two minutiae can be calculated by,

$$\gamma(m_{t_\zeta}, m_{q_\eta}) = 1 - \frac{\|C_{m_{t_\zeta}} \oplus C_{m_{q_\eta}}\|}{\|C_{m_{t_\zeta}}\| + \|C_{m_{q_\eta}}\|} \tag{6}$$

where $\|.\|$ is a 2-norm of a vector.

In order to indicate the overall similarity between T and Q, a global similarity score is obtained with the help of the local similarity scores for minutia pairs in P. In this scheme, the mean of top n_P local similarity scores is used to represent the global similarity between T and Q, denoted by,

$$\gamma(T, Q) = \frac{\sum_{s=1}^{n_P} \gamma_s}{n_P} \tag{7}$$

where $\gamma_1, \gamma_2, \ldots, \gamma_{n_P}$ are the top n_P local similarity scores. When selecting the top n_P scores, the same minutia is not considered more than once. If $\gamma(T, Q)$ is larger than a pre-defined threshold, γ_{thd}, T and Q are considered to match each other, which means the external programmer is successfully authenticated by the IMD. Otherwise, the authentication fails and thus the programmer cannot gain access to the IMD.

C. MCC Improvement for IMDs

As mentioned before, an IMD has extremely limited resources, including memory, power, computation and communication resources. In order to conserve the resources in the IMD, the improvement of the MCC algorithm is essential. The resource consumption of the MCC-based authentication algorithm in the IMD is caused by the consumptions of memory, computations, communications and power.

The memory overhead of the IMD is primarily determined by the the number of features in the template and the query, and the length of each binary feature vector, C_m, denoted by,

$$O_m = g_m(n_A, n_B, N_C) \tag{8}$$

Where O_m represents the overhead of memory and g_m is a positive correlation function. n_A and n_B represent the number of minutiae in the template and the query, respectively. N_C is the length of the binary feature vector which equals to the number of the cells in each cylinder.

The major part of the communication overhead in the IMD is caused by receiving query features from the programmer. So, the IMD communication overhead can be denoted by,

$$O_{comm} = g_{comm}(n_B, N_C) \tag{9}$$

Where O_{comm} is the communication overhead and g_{comm} is a positive correlation function representing the relationship between (n_B, N_C) and O_{comm}.

The major computation overhead in the IMD arises from the calculation of local similarities. According to equations (5) & (6), this overhead can be denoted by,

$$O_{comp} = g_{comp}(n_A \times n_B, N_C) \tag{10}$$

Where O_{comp} is the computation overhead and g_{comp} is a positive correlation function.

Since g_m, g_{comm} and g_{comp} are all positive correction functions between inputs and outputs, the overheads of the MCC-based IMD authentication algorithm can be improved by reducing the inputs n_A, n_B and N_C. In order to maintain the matching performance, reducing the number of feature vectors in the template, n_A, is not recommended. However, reducing the number of feature vectors in the query, n_B, can reduce the overheads of O_m, O_{comm} and O_{comp}, simultaneously. Therefore, in the improved MCC, only a few feature vectors, n_S $(n_S \leq n_B)$, are selected from the query feature set, C_{m_Q}, and are sent to the IMD from the programmer in each authentication attempt. The selection of the query feature vectors is performed in the following way:

a) The programmer captures the patient's fingerprint image and extracts a query minutia set, Q. Then the programmer applies the MCC algorithm to associate each minutia with a cylinder to generate a set of query feature vectors, C_{m_Q}.
b) The programmer calculates the central point of the query minutiae, $P_{cm} = (x_{cm}, y_{cm})$, where x_{cm} and y_{cm} are the mean of x-axis and y-axis values of all minutiae in Q, respectively.
c) The programmer selects a subset from Q with n_S minutiae which are spatially closest to the center, P_{cm}, denoted by $Q_s = \{m_{s_1}, m_{s_2}, \ldots, m_{s_{n_S}}\}$. The Euclidean distance between a minutia, $m = \{x_m, y_m, \theta_m\}$, and the template center, P_{cm}, is calculated to decide which minutia is closer to the center, denoted by $d(m, P_{cm}) = \sqrt{(x_m - x_{cm})^2 + (y_m - y_{cm})^2}$.
d) The query feature vector of each minutia in Q_s is selected from C_{m_Q} and forms a subset of query features, C_{m_s}. This query feature subset is then sent to the IMD for authentication purposes.

Although the subset, C_{m_s}, has only n_S MCC representations, it contains information of more than n_S minutiae. This is because an MCC cylinder associated to a minutia encloses minutiae in that minutia's neighborhood within a fixed-radius R.

Furthermore, decreasing the length of each feature vector, N_C, can help to reduce both the size of the template and the query. Nevertheless, decreasing N_C should not compromise the fingerprint matching performance for securing the IMD. In order

to evaluate the matching performance of the algorithm with different N_C values, extensive experiments are performed by varying N_S and N_D in Section V-C.

V. Experimental Evaluation

In this section, fingerprint matching experiments are conducted in order to evaluate the performance of the improved MCC algorithm. In order to conserve resources in the IMD, we propose to improve the MCC on two aspects: by reducing the number of cells in a cylinder and by reducing the number of MCC feature vectors in the query template.

A. Experimental Setup

By following the prescribed methods of research in [17], [29], the MCC-based IMD authentication scheme is evaluated on public fingerprint databases, with fingerprint images from the FVC2002 DB1, DB2 and DB3 [30]. This database contains images captured from 100 different fingers and each finger has eight different fingerprints. Fingerprint minutiae are extracted from finger images by using Verifinger 4.0 from the Neurotechnology [31].

The FVC2002 test protocol [32] is adopted in the experiments:

- Each fingerprint template in the database is matched against the remaining ones of the same finger to compute the False Non Match Rate (FNMR). If the template T_1 is compared against T_2, the symmetric one (i.e., T_2 against T_1) is not executed to avoid correlation in the matching scores. The total number of genuine tests is: $((8 * 7)/2) * 100 = 2,800$.
- The first template of each finger in the database is matched against the first sample of the remaining fingers in A to compute the False Match Rate (FMR). If the matching T_1 against T_2 is performed, the symmetric one (i.e., T_2 against T_1) is not executed to avoid correlation. The total number of imposter tests is: $((100 * 99)/2) = 4,950$.

The matching score is set to zero if there is any failure in the matching process. The performance of the scheme is evaluated by indicators below:

- Equal Error Rate (EER): the error rate when the FNMR equals the FMR.
- FMR_{1000}: the lowest FNMR when FMR $\leq 0.1\%$.
- FMR_{100}: the lowest FNMR when FMR $\leq 1\%$.

B. Fingerprint Minutiae Extraction

In the experiments, minutiae are extracted from each fingerprint image, including their location and orientation information. An example of the minutia extraction process is shown in Fig. 5 and described below:

- Fig. 5(a) shows that minutiae, including ridge endings and bifurcations, are detected and located on a fingerprint image.
- Fig. 5(b) is a fingerprint minutia template which contains location and orientation information of each minutia.

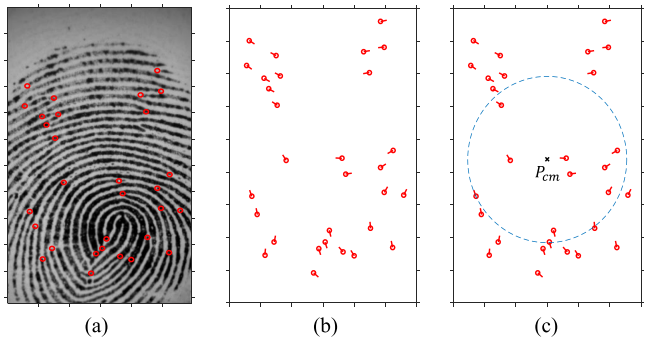

Fig. 5. Extracting minutiae from a fingerprint image. (a) Minutiae (including ridge endings and bifurcations) located on a fingerprint image. (b) Extracted minutiae template with location and orientation information. (c) n_S selected minutiae which are spatially close to the center of the minutiae template, P_{cm}.

- In Fig. 5(c), the center of the minutia template, P_{cm}, is calculated and located on the template. A subset with n_S selected minutiae (enclosed in a circle) is created and used for selecting query feature vectors in the IMD authentication scheme.

When applying the improved MCC algorithm to secure the IMD, the programmer follows the processes from Fig. 5(a) to Fig. 5(c) in each authentication attempt. A subset with n_S minutiae is created in order to select partial MCC query features which are to be sent to the IMD for authenticating the programmer.

C. Experiments: Cylinder Dimension Reduction

As analyzed in Section IV-C, reducing the length of each feature vector, N_C, can simultaneously reduce the overheads of memory, communications and computations in the IMD. The length of the feature vector is determined by the dimension of the cylinder, $N_C = N_S \times N_S \times N_D$. On the other hand, the reduction of the length of MCC feature vectors should not compromise the fingerprint matching performance. In order to achieve this trade-off, we conduct a series of experiments by varying the N_S and N_D values, with other parameters configured according to Table 2 in [17]. The EER results in the experiments are shown in Table I.

Each row in the table shows the EER values in a series of tests when N_D is set as a constant while N_S varies from 1 to 16. As highlighted in each row, the best results are normally achieved when $N_S \geq 10$. However, it is also shown that the EER is around 2% when $N_S \geq 6$. To achieve the trade-off between the size of each MCC feature vector and the matching performance, comparisons are conducted below. In the series of tests when $N_D = 3$, the EER is reduced by 9.74%, from 1.54% ($N_S = 10$) to 1.69% ($N_S = 6$). But, the size of each MCC feature vector is reduced by 64%. Similarly, when $N_D = 6$, the size of each MCC feature can be reduced by 84% while the EER is reduced by 23.91%, from 1.38% ($N_S = 15$) to 1.71% ($N_S = 6$). Therefore, setting $N_S = 6$ reduces the size of the MCC feature vector significantly while the matching performance can still be maintained at an acceptable level (2%). It also shows that the EER

TABLE I
FINGERPRINT MATCHING PERFORMANCES IN EXPERIMENTS BY VARYING N_S AND N_D VALUES, WITH EER IN PERCENTAGE VALUES (%)

	N_S Value Varies from 1 to 16															
N_D	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	43.7	17.9	6.98	3.30	2.34	2.07	2.02	1.68	1.79	1.88	1.78	1.82	1.89	**1.61**	1.80	1.67
3	48.9	16.4	7.18	3.74	2.04	1.69	2.04	1.65	1.77	**1.54**	1.68	1.75	1.63	1.73	1.68	1.57
4	46.2	14.0	5.25	2.56	1.93	1.60	2.03	1.57	1.49	1.53	1.58	1.55	1.51	**1.47**	1.60	1.49
5	45.5	14.7	5.70	2.83	1.79	1.59	1.78	1.61	1.70	1.53	1.65	1.57	1.59	1.64	**1.50**	1.57
6	46.5	15.5	6.16	3.12	1.94	1.71	1.66	1.65	1.62	1.43	1.66	1.54	1.53	1.63	**1.38**	1.52

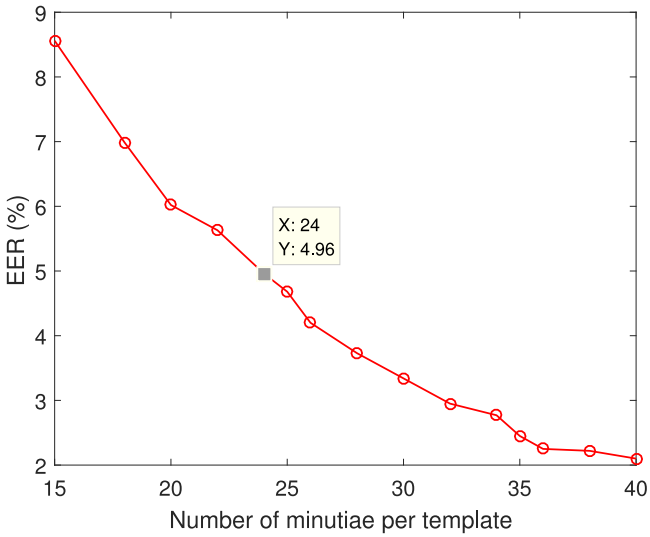

Fig. 6. EER varies along with the number of MCC feature vectors.

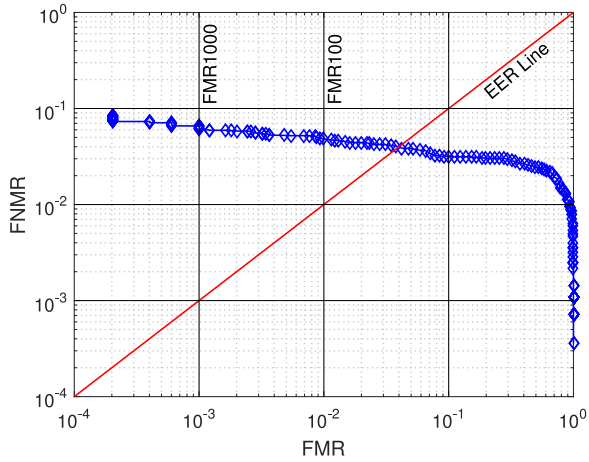

Fig. 7. Test results of FNMR and FMR on the FVC2002 DB1, with EER = 3.93% and FMR1000 = 6.57%.

values converge to below 2% for all N_D values. So, the smallest value of N_D is selected , that is, $N_D = 2$. Consequently, in the improved MCC algorithm, the optimal configuration is when $N_S = 6$, $N_D = 2$.

D. Experiments: Query Feature Number Reduction

In each authentication attempt, the programmer sends MCC query feature vectors, C_{m_Q} in Eq. (4), to the IMD. Reducing the number of feature vectors in C_{m_Q} brings down the size of messages in wireless transmission and therefore decreases the energy overheads associated with wireless transmission of these messages. If there are n_B minutiae in a query template, n_B MCC feature vectors are generated first. With the improved MCC algorithm, n_S ($n_S \leq n_B$) feature vectors are selected from the MCC feature set. Fingerprint matching tests by using a different number of MCC features in the query are conducted, with the matching performance shown in Fig. 6. The tests show that the EER can be maintained at less than 5% when no less than 24 MCC feature vectors are required in each query. Although using more query feature vectors can improve the matching performance, it consumes more resources in the IMD.

E. Performance of the Improved MCC Algorithm

According to experimental results presented in Sections V-C and V-D, the improved MCC algorithm for securing the IMD configures parameters as $N_S = 6$ and $N_D = 2$, and uses no more than 24 MCC feature vectors in each query. In order to evaluate the matching performance of the algorithm with these and similar parameter settings, extensive experiments are conducted on fingerprint databases, the FVC2002 DB1, DB2 and DB3, with the corresponding FNMR and FMR results shown in Fig. 7, Fig. 8 and Fig. 9, respectively. The EER values for tests running on these three databases are 3.93%, 4.95% and 5.81%, respectively. It shows that the EER of the improved MCC algorithm can be maintained at around 5% for all three tested databases, which is acceptable in fingerprint authentication applications. Therefore, this algorithm can be applied to secure an IMD.

Query features are the major part of the message sent out by the programmer and then received by the IMD. The size of the query features can be calculated by,

$$N_C \times n_B = (N_S \times N_S \times N_D) \times n_B \tag{11}$$

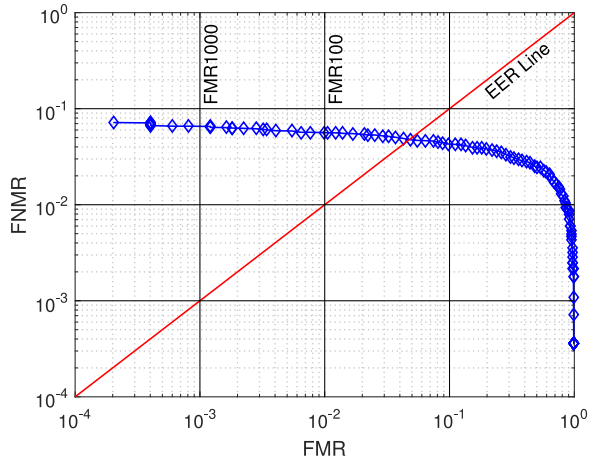

Fig. 8. Test results of FNMR and FMR on the FVC2002 DB2, with EER = 4.96% and FMR1000 = 7.11%.

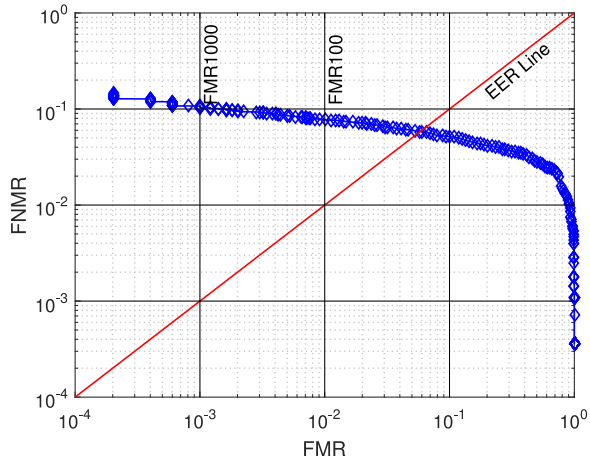

Fig. 9. Test results of FNMR and FMR on the FVC2002 DB3, with EER = 5.81% and FMR1000 = 10.7%.

In the *MCC16b* test presented in [17], parameters are configured as $N_S = 16$ and $N_D = 6$. If there are 40 MCC feature vectors in a query, the total number of bits of the query features is 61,440. With the improved MCC algorithm, parameters are configured as $N_S = 6$, $N_D = 2$ and no more than 24 feature vectors are selected from the MCC query feature set. So, the size of the query features sent to the IMD is less than 1,728 bits. Therefore, the size of the message in wireless transmission is reduced significantly by 97.2%. Meanwhile, the matching performance of the system is within an acceptable level (EER is around 5%). Even in comparison with the *MCC8b* test in [17], the size of the message is reduced by 88.8%.

In comparison to the ECG-based IMD authentication schemes, the memory consumption of the improved MCC in the IMD side is smaller. The major memory consumption in the IMD here is for storing the template and the query features, and can be calculated as around $(61,440 + 1728)$ bits $= 7.7$ KB. However, the ECG signal detection and encryption/decryption operations in the IMD in the ECG signal-based H2H scheme, according to Table 4 in [7], consumes 17 KB memory totally. Furthermore, in order to generate a 128-bit key, it requires at least 32 seconds to capture, detect and process ECG signals in the IMD before the authentication process. Therefore, the improved MCC-based fingerprint authentication scheme outperforms the ECG-based schemes in terms of resource usage while providing a robust mechanism to authenticate the IMDs.

VI. Security Analysis

In this section, we will first analyze the security performance of the proposed F2H IMD security scheme and then compare its security performance with the ECG signal-based IMD security schemes.

A. Scheme Security

Currently an IMD system faces critical security risks from two types of attackers: passive eavesdroppers and active adversaries [8], [11]. A passive eavesdropper wiretaps on the IMD's wireless channel and tries to capture private information related to the patient and his/her IMD. Moreover, an active adversary has the capability to send a command to control and manipulate the IMD with an off-the-shelf programmer, which may lead to fatal consequences. For example, a pacemaker or ICD could be configured maliciously to deliver lethal electric shocks to the patient's heart [6], [8], and an insulin pump can be hacked to deliver abnormal bolus insulin to the body of the patient. So, the active adversaries are more harmful to the patients than the passive ones. However, by using our proposed fingerprint-based IMD security scheme, these active adversaries can be blocked from accessing the IMDs at the beginning of each wireless communication session. This is because any programmer which wants to communicate with the IMD has to be authenticated first by the IMD with a security token which is the patient's fingerprint. If this authentication procedure fails, any following operation/s on the IMD, such as reading medical data or altering therapy related settings, cannot proceed. Therefore, with the use of the proposed fingerprint based IMD security scheme, the IMDs can be protected from the active adversaries.

The F2H IMD security scheme can help doctors access the IMD quickly in an emergency situation by pressing and scanning the patient's fingers, even if the patient is unconscious. Compared to the security key/password based schemes, this scheme does not require the patient to remember or tell doctors their IMDs' keys/passwords, making it viable for elderly patients and those with mental illnesses. So, it achieves the trade-off between security and accessibility, especially in an emergency situation. Furthermore, this IMD security scheme is built upon the improved MCC algorithm and can protect the IMDs against user impersonation attacks. As analyzed in the experiments, this scheme can maintain a low FMR on all three FVC2002 fingerprint databases, which guarantees a low rate to pass the IMD authentication procedure for an imposter using an impersonated fingerprint.

B. Comparison With ECG-Based Schemes

In comparison to the ECG signal based IMD security schemes proposed in [10], [11], this F2H scheme has a better matching

performance. The FNMR in this scheme can be maintained at around 5%. However, it is very challenging for the ECG-based schemes to achieve this performance. This is due to the fact that the fingerprint image is stable and can be captured more accurately than the ECG signals. ECG measurements need to use electrodes each of which consist of conductive electrolyte gel and a conductor, and detect tiny electrical changes on the skin. In a typical 12-lead ECG measurement, ECG outputs from each lead at the same time vary significantly, although the R peaks in each ECG waveform are roughly synchronized. This makes the accurate measurement of ECG signals more difficult than the fingerprints. Furthermore, in this scheme, the fingerprint template stored in the IMD is captured and processed before the implantation, and thus can achieve a reasonably good quality. However, the ECG signals in the IMD have to be sampled and processed in a real-time manner for each secure access attempt. Therefore, the biometric features used at the IMD end in this scheme can maintain a better quality of accuracy than the ECG-based security schemes.

VII. Related Work

The security issues of IMDs affect the safety and privacy of patients severely [33], [34]. According to recent vulnerability studies performed by Rios and Butts [4] and Halperin *et al.* [6], adversaries can attack a pacemaker or an ICD by using a software radio or even a commercial device programmer. By wiretapping the wireless channel, passive adversaries can obtain personal information of the patient, such as the name, the date-of-birth and medical recordings in the IMD [35]. Furthermore, active attackers can re-configure the pacemaker or ICD maliciously and deliver lethal electric shocks to the heart of the patient. Similarly, Li *et al.* [5] demonstrated successful attacks on a glucose monitoring and insulin pump system by using the Universal Software Radio Peripheral (USRP). The adversaries can compromise both the privacy and the safety of the patient, e.g., obtaining medical recordings and history, sending control commands to stop/resume insulin injection or forcing unwanted bolus injection into the patient's body. Therefore, it is imperative to design a security scheme which can protect the IMDs from potentially fatal cyber-attacks.

Physical layer security solutions, which are based on a wearable external device, have been proposed by various researchers to balance the trade-off between security and accessibility [8], [36]–[38]. For instance, Gollakota *et al.* [8] proposed to delegate the security of an IMD to an external jammer-cum-receiver device called the shield which can jam unauthorized messages sent to/from the IMD. It can be applied to protect patients who already have IMDs implanted in the body. Nonetheless, if this external device is not present, e.g., forgotten, lost, broken or stolen, the IMD becomes vulnerable to various cyber-attacks. An adversary may set up new wireless connections on a continual basis for a period of time to deplete the battery power of the shield since this shield needs to be activated to jam all messages sent to and from the IMD. In contrast, our proposed F2H scheme does not require an external security proxy and thus becomes more convenient for the patient. Furthermore, as explained in Section 7 in [8], this scheme relies on identifying a sequence to authenticate and authorize a programmer and block messages from active adversaries. According to this design, the ID sequence of an IMD can be made up from a known preamble, a header, the device's serial number and/or Federal Communications Commission IDentification (FCC ID). Such ID sequence, although it is unique, cannot be considered as a secret/key/password from the security point of view and cannot be updated if it is disclosed, which makes the system insecure. To address this shortcoming, Ankarali *et al.* [36] proposed a scheme which can authenticate the programmer (adversary) at the physical layer without using the ID sequence of an IMD. This goal is achieved during the channel estimation process. At the beginning of each communication session, the IMD transmits a pilot signal to the wearable security device for it to estimate the channel. The pilot signal can be received by an adversary as well from the wireless channel. However, compared to the wearable security device, e.g., the shield [8], the adversary is normally located far away from the patient's body. So, the pilot signal received by the adversary suffers higher power loss than that received by the shield, making it impossible to estimate the channel correctly between the IMD and the adversary.

On the other hand, some researchers proposed biometric-based security solutions to secure IMDs which are embedded in the IMD, not relying on a wearable security device, e.g., the ECG signal-based IMD security schemes which have been analyzed in Section II. Furthermore, Hei *et al.* [39] proposed to use an iris pattern-based verification scheme to provide access control to the IMD. The iris-based scheme requires scanning one or both the eyes which are sensitive organs of the patient. Therefore, the patient normally has more concerns if his/her eyes are scanned rather than the finger. Hei *et al.* [39] also described the use of fingerprint as the first-level access control for the IMD. However, the paper does not propose any fingerprint based authentication algorithm for IMDs. The study also does not conduct any analysis of fingerprint based security performance in the context of IMDs. To the best of our knowledge, this is the first research paper which proposes, designs and evaluates the fingerprint-based authentication algorithm to secure an IMD.

Some IMD security schemes are based on the programmer's proximity to the IMD [40]. An external programmer is allowed to have access to the IMD only when it is within a pre-defined secure range to the IMD. However, the proximity-based schemes can be breached when the adversary manages to get close to the patient in places such as in public transport or other public spaces. In order to support secure access to the IMD from a remote user, Wazid *et al.* [41] proposed a lightweight three-factor remote user authentication scheme in which a controller node of the IMD and the remote user can authenticate each other. Ellouze *et al.* [42] designed an IMD mutual authentication protocol which combines the radio frequency energy harvesting technique and the ECG signal based key generation technique.

Protecting the privacy and security of medical devices is mandated by government laws and regulations, e.g., the Health Insurance Portability and Accountability Act (HIPAA) and the European Union Directive 2002/58/EC [43]. The U.S. FDA issued a guidance for designing cybersecurity safeguards to pro-

tect medical devices [44]. In the design stage of medical devices, manufacturers are required to take into consideration the issues pertaining to cyber security.

VIII. Conclusion

A security scheme designed for IMDs should not impede immediate access to an IMD for medical treatment, especially in an emergency scenario. In order to address this challenge, biometric-based IMD security schemes are proposed, by use of which the doctors can gain access to the IMD by measuring characteristics of the patient's body. Currently, ECG signal-based security schemes have been widely studied to secure the IMD. However, these schemes require the IMD to capture and process real-time ECG signals in each and every access attempt, which can consume a considerable amount of resources in the IMD.

In order to reduce the resource consumption of biometric-based IMD security schemes, a Finger-to-Heart IMD authentication scheme is proposed in this paper. In the F2H scheme, the IMD does not have to capture and process biometric traits in every access attempt. A fingerprint template is generated beforehand and stored in the IMD for use before the implantation surgery. Therefore, the resource consumption of the F2H scheme is reduced significantly when compared to the ECG signal-based IMD security schemes. A minutia cylinder-code based fingerprint authentication algorithm is designed for the IMD. Since the IMD is a tiny wireless device and has limited resources, the MCC algorithm is improved by reducing the length of each MCC feature vector and the number of query feature vectors used for authentication. Extensive experiments show that the improved MCC algorithm reduces the size of messages in transmission along with the computational overheads significantly, and therefore offers practical and viable alternative to secure the IMDs.

References

[1] A. F. Demir *et al.*, "In vivo communications: Steps toward the next generation of implantable devices," *IEEE Veh. Technol. Mag.*, vol. 11, no. 2, pp. 32–42, Jun. 2016.

[2] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access control schemes for implantable medical devices: A survey," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017.

[3] 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.

[4] B. Rios and J. Butts, "Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies." 2017. [Online]. Available: http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html

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

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

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

[8] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, 2011.

[9] G. Zheng, G. Fang, M. Orgun, and R. Shankaran, "A non-key based security scheme supporting emergency treatment of wireless implants," in *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 647–652.

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

[11] G. Zheng, G. Fang, R. Shankaran, and M. A. Orgun, "Encryption for implantable medical devices using modified one-time pads," *IEEE Access*, vol. 3, pp. 825–836, 2015.

[12] K. Venkatasubramanian, A. Banerjee, and 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.

[13] S.-D. Bao, C. Poon, Y.-T. Zhang, and L. Feng Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 6, pp. 772–779, Nov. 2008.

[14] L. V. Rajani Kumari, Y. Padma Sai, and N. Balaji, *ECG Signal Preprocessing Based on Empirical Mode Decomposition*. New Delhi, India: Springer, 2016, pp. 673–679.

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

[16] A. K. Jain, J. Feng, and K. Nandakumar, "Fingerprint matching," *Computer*, vol. 43, no. 2, pp. 36–44, 2010.

[17] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.

[18] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan.–Mar. 2008.

[19] R. Morello, "Use of TEDS to improve performances of smart biomedical sensors and instrumentation," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2497–2504, May 2015.

[20] R. Morello and C. D. Capua, "An ISO/IEC/IEEE 21451 compliant algorithm for detecting sensor faults," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2541–2548, May 2015.

[21] W. Yang, S. Wang, G. Zheng, J. Chaudhry, and C. Valli, "ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures," *J. Supercomput.*, Jan. pp. 1–17, 2018.

[22] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, 2014.

[23] L. Ghiani, D. A. Yambay, V. Mura, G. L. Marcialis, F. Roli, and S. A. Schuckers, "Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015," *Image Vis. Comput.*, vol. 58, pp. 110–128, 2017.

[24] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible minutia cylinder-code representation," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1727–1737, Dec. 2012.

[25] R. Cappelli, M. Ferrara, and D. Maltoni, "Fingerprint indexing based on minutia cylinder-code," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 5, pp. 1051–1057, May 2011.

[26] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *Proc. Int. Conf. Biometrics Special Interest Group*, Sep. 2014, pp. 1–8.

[27] X. Jiang and W.-Y. Yau, "Fingerprint minutiae matching based on the local and global structures," in *Proc. 15th Int. Conf. Pattern Recognit.*, 2000, vol. 2, pp. 1038–1041.

[28] J. Feng, "Combining minutiae descriptors for fingerprint matching," *Pattern Recognit.*, vol. 41, no. 1, pp. 342–352, 2008.

[29] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1179–1192, Jul. 2014.

[30] Biometric System Laboratory, "FVC fingerprint databases," 2002. [Online]. Available: http://bias.csr.unibo.it/fvc2002/databases.asp

[31] NeuroTechnology Inc., "Verifinger SDK." [Online]. Available: http://www.neurotechnology.com/verifinger.html

[32] Biometric System Laboratory, "Fingerprint verification competition—Performance evaluation." 2002. [Online]. Available: http://bias.csr.unibo.it/fvc2002/perfeval.asp

[33] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.

[34] 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*, 2014, pp. 524–539.

[35] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare—Transforming Healthcare Through Innovations Mobile Wireless Technol.*, Nov. 2014, pp. 246–249.

[36] Z. E. Ankarali *et al.*, "Physical layer security for wireless implantable medical devices," in *Proc. IEEE 20th Int. Workshop Comput.-Aided Model. Des. Commun. Links Netw.*, Sep. 2015, pp. 144–147.

[37] 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.

[38] S. Kulaç, "Security belt for wireless implantable medical devices," *J. Med. Syst.*, vol. 41, no. 11, p. 172, Sep. 2017.

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

[40] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009, pp. 410–419.

[41] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.

[42] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Powerless security for cardiac implantable medical devices: Use of wireless identification and sensing platform," *J. Netw. Comput. Appl.*, vol. 107, pp. 1–21, 2018.

[43] Y. Poullet, "EU data protection policy. The directive 95/46/EC: Ten years after," *Comput. Law Security Rev.*, vol. 22, no. 3, pp. 206–217, 2006.

[44] US FDA, "Content of premarket submissions for management of cybersecurity in medical devices: Guidance for industry and food and drug administration staff," Oct. 2014. [Online]. Available: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf