Access Control for Implantable Medical Devices

Carmen Camara, Pedro Peris-Lopez, Jose Maria de Fuentes, and Samuel Marchal

***Abstract*—The telemetry incorporate in the new generation of Implantable Medical Devices (IMDs) allows remote access and re-programming without interfering with the daily routine of their holders. Despite the benefits of this new feature, such remote access raises new threats related to the access of unauthorized entities to IMDs. Cardiac implants represent the most deployed types of IMD nowadays. Current solutions, to control their remote access, usually use a single feature for authentication. However, this feature is easily replicable, making these authentication schemes vulnerable to attacks. To overcome this limitation, we propose in this article a distance bounding protocol to manage access control of IMDs: ACIMD. ACIMD combines two security mechanisms, namely, identity verification (authentication) and proximity verification (distance checking). The authentication mechanism, formally and informally verified, conforms to the ISO/IEC 9798-2 standard. The distance checking is performed using the whole Electrocardiogram (ECG) signal and relies on the correlation coefficient (comparing an external versus an internal ECG signal) in the Hadamard domain. We evaluate the accuracy and security of ACIMD access control using ECG signals of 199 individuals recorded over 24 hours while considering three adversary strategies. Our results show that ACIMD is 92.92% accurate.**

***Index Terms*—Implantable Medical Devices (IMDs), E-health, Remote Access, Cybersecurity, Distance Bounding**

I. Introduction

Significant advances have been made in the healthcare domain over the past years. In particular, providing new communication capabilities to medical systems and devices benefits all actors. Users can monitor their health status without interfering with their daily activities, the medical staff has fast remote access to medical data and can also quickly re-program these devices remotely. These new communication capabilities also reduce the global costs of healthcare operations [1].

Implantable medical devices (IMDs) are such an example of devices having remote communication capabilities, including access to telemetry data [2]. IMDs are electronic devices implanted within the body to treat a medical condition, to monitor a physiological organ and to actuate when necessary. IMDs can be categorized in four main classes [1]: cardiac implanted devices (pacemakers and implantable cardioverter defibrillators), neurostimulators, drug delivery systems, and biosensors.

IMDs communicate with an external device, called *Programmer*. As illustrated in Fig. 1 there are two alternatives for this communication. Until 2001, the connection between the IMD and the *Programmer* was exclusively supported via a cable and a band placed over the patient's body. In this case, a very short-range communication channel is established between both devices. Although the first designs date from the early 2000s, in the last decade the use of IMDs with telemetry has spread in hospitals around the world. To understand how it works, suppose the following example. Imagine a group of patients with an IMD (henceforth assume a pacemaker with no loss of generality) in the waiting room of a hospital. A doctor (cardiologist in our example) can be in an adjoining room. Under this scenario, each patient's pacemaker could send their electrocardiogram to the doctor (the specialist receives the data via the *Programmer*). Besides, the doctor could interact with each of the pacemakers and change some of their operating parameters. Therefore, the communication channel between the IMDs and the *Programmer* is bi-directional. In this regard, two properties have to be achieved to guarantee the security of this communication: (1) we must ensure that the *Programmer* is authorised to interact with the implant: *access control*, (2) the data at stake and transmitted through the insecure radio channel must only be accessible to the two legitimate communicating entities: *confidentiality*. In this paper, we focus on the provision of (1): *access control*. Interested readers may refer to [1] for a comprehensive survey on confidentiality issues.

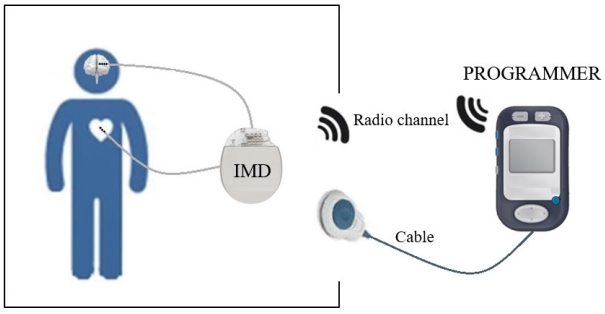

Fig. 1. Communication channels between an IMD and a *Programmer*

As mentioned the new generations of IMDs have wireless connectivity, which on the one hand allows more efficient management of the device, but on the other hand, opens the doors to many possible attacks. By merely eavesdropping on the channel the attacker could capture confidential information from the patient. From this passive attack, we could pass to more deadly active attacks that, for example, could change the reprogramming of the IMD or deplete its battery. The interested reader can find a detailed study of all possible attacks in [3]. In this vein, some researchers have shown that the security level of some IMDs is very low [2]. Besides, the

Carmen Camara, Pedro Peris-Lopez, Jose Maria de Fuentes are with the Depatment of Computer Science, Carlos III University of Madrid, Avda. de la Universidad 30, 28911, Leganés, Madrid (e-mail: macamara@pa.uc3m.es and {pperis,jfuentes}@inf.uc3m.es).

Samuel Marchal is with the Department of Computer Science, Aalto University, Konemiehentie 2, 02150 Espoo, Finland (e-mail: samuel.marchal@aalto.fi)

Pedro Peris-Lopez carried out a research stay at Aalto University (Konemiehentie 2, 02150 Espoo, Finland) during the development of this research.

FDA has recently alerted of several security vulnerabilities in commercial IMDs [4].

Motivated for all the above, in the literature, we can find a wide variety of proposals to increase the security of IMDs. We can categorize the existing solutions in four main classes, according to the taxonomy introduced in [1]: 1) auditing; 2) cryptographic primitives; 3) access control, and 4) anomaly detection. The auditing may help to chase away attackers since accesses and setting modifications are stored securely into a memory [5]. Regarding cryptography, we can find symmetric [6], asymmetric [7], and hybrid solutions to securize the wireless communication between the IMD and the *Programmer*. In general terms, the main drawback of each approach is that symmetric proposals have to deal with the key distribution problem, while asymmetric solutions face with the high consumption of resources and energy [8]. Because implants resources such as the memory and battery onboard are limited, malicious attackers may focus on misuse these resources. The combined use of pattern analysis and an alarm system is the most popular anomaly detection solution to combat this sort of attacks [9]. The principal limitation of this type of solutions is whether we can model all normal and abnormal (those that represent a possible attack) conditions. Finally, access control mechanisms guarantee that the requester (*Programmer*) has the necessary privileges to execute a particular action (e.g., reading memory, adjust configuration parameters) over the IMD. Within this category, the existing solutions are very diverse, including those based on access control lists and certificates or the ones based on role controls [10]. Besides, and since many researchers have studied ECG biometrics deeply in the last years due to its potential commercial applications, and in vein with this, some authors have recently proposed biometrics solutions for pacemakers based on both fiducial and non-fiducial features from an electrocardiogram [11]. Finally, other authors leave the access control responsibility to an adjacent device [12].

A. Access control: distance-based approaches

A particular branch in access control for IMDs is based on measuring the distance between this device and the *Programmer*. This technique is referred to as *distance bounding protocols* and requires the following three definitions [13]:

Definition 1.1 (Authentication): One party (P) is assured of both the identity of a second party (V) and her presence at the time of the protocol execution.

Definition 1.2 (Distance checking): One party (P) is assured of the distance (or a property derived from this) to a second party (V) at some point of the protocol execution. The area in which P is considered to be close enough to V is called Neighbourhood Area (NA).

Definition 1.3 (Distance bounding): It combines identity (authentication) and neighbourhood (distance checking) verifications. Regarding the distance between P and V, an upper-bound limit is often used.

Distance bounding protocols were proposed by Brands and Chaum (see Fig. 2 [14]). They were intended to cope with *mafia fraud* attacks (also known as man-in-the-middle, relay

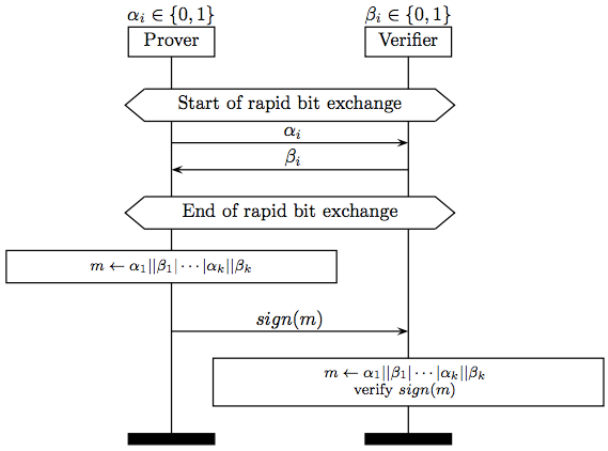

Fig. 2. Brands and Chaum Distance Bounding Protocol [14]

or chess grand-master attacks), which are based on the relaying of messages between dishonest entities [15]. Note that well-known and formally verified authentication protocols (e.g., Bellare-Rogaway protocol [16]) or "Chip and PIN" smartcard payments systems are vulnerable to relay attacks [13]. In particular, this kind of attacks lies in a man-in-the-middle attack between an honest verifier (V; e.g., IMD) and a legitimate prover (P; e.g., *Programmer*). The adversary is made up of two entities: a rogue prover ($\overline{P}$) and a rogue verifier ($\overline{V}$). $\overline{V}$ interacts with P and $\overline{P}$ communicates with V, respectively. In addition, rogue entities (i.e., $\{\overline{P}, \overline{V}\}$) forward the messages received from the legitimate entities (i.e., $\{V, P\}$) between each other.

Distance bounding protocols guarantee to the IMD that the connected *Programmer* is in its Neighbourhood Area (NA) and is not a distant third party. In general terms, we can compute the distance between a Verifier (P) and a Prover (P) in several ways. For example, the range can be calculated based on the received signal energy/power (RSS) [17]. Unfortunately, this sort of solutions is not reliable whether the adversary can increase the power of the emitted signals. Alternatively, we can upper bound the distance between P and V by measuring the time interval between sending a challenge and receiving its response. The security of these proposals relies on that P can only generate the responses after accepting the challenge, which is randomly generated by V. Distance bounding schemes commonly utilise this second approach. Particularly and as a consequence of the mushrooming of radio frequency identification (RFID) devices, large numbers of distance bounding protocols have appeared in the literature [13]. In the same line and the context of IMDs, for instance, Rasmussen *et al.* proposed a distance bounding protocol, which uses ultrasound signals to delimit the distance [18].

Besides, among the possible techniques, a promising approach is the use of a key derived from an internal (measured by the IMD) and external (recorded by the *Programmer/reader*) physiological signal [19]. Thus, if the same key (or two ones with only a few different bits) is obtained, the proximity between both entities is assumed. In the context of cardiac IMDs, Inter-Pulse Intervals (IPIs) is the common

solution [20] within this category. Alternatively, to avoid the capture and processing of the physiological signal required in the solutions mentioned above, some authors propose a biometric solution [21]. Finally, it is worth mentioning that, as an alternative to distance bounding schemes, some authors have proposed the use of multichannel protocols [22]. However, there is no practical implementation for real scenarios. Alternatively, Choudary and Stajano proposed the use of noisy cryptography [23]. The main drawbacks of this approach are a high complexity to be supported on-board of constrained devices such as IMDs, and the possibility for an attacker with higher computing capabilities than those of legitimate entities to compromise the security of the system.

In our particular case, and although we provide the details below, we would like to highlight that our proposal and the other existing distance-bounding solution for IMDs are entirely different. Rasmussen *et al.* scheme is based on measuring delay time between sending a challenge and receiving the response [18]. In our proposal, we guarantee that the involved entities are within the NA whether a physiological signal (ECG signal in our experiments) recorded internally by the Prover (IMD) is close enough to an external signal gathered by the Verifier (*Programmer*). Besides, and in comparison with existing solutions that compare external and internal signals, in these solutions such as the ones based on IPI values [20] only some characteristics points of the physiological signals are employed while in our proposal we use the entire signals in the comparison.

B. Motivation and contribution

The motivation of this paper is twofold. On the one hand, IPI-based solutions are one of the most common approaches to assure the distance between a cardiac implant and a Programmer. Both devices need to extract some features from the cardiac activity of a subject. In particular, these solutions use only one fiducial point (i.e., R peaks in Electrocardiogram (ECG) or Photoplethysmograph (PPG) signals) that can be measured internally and externally by the implant and Programmer respectively. This kind of solutions assumes that an attacker cannot infer this feature from a distant place, which has been proven not to hold [24]. This fact allows a malicious party to access to the IMD from a remote location illegally.

On the other hand, it is commonly assumed that IMDs must support two operation modes: *normal* and *emergency* [3]. The normal operation mode is the usual one that operates while no anomaly related to the health of the patient is detected. In contrast, the emergency mode occurs when the user suffers from a serious medical problem (e.g., a heart attack, a hypoglycemic episode or an epileptic attack) that endangers her life. Thus, the access control mechanism added on-board of the IMD has to deal with both operation modes. In each mode, there is a trade-off between the level of security and speed of the authentication process. Note that in an emergency condition, we can relax the security requirements since keeping the patient at life (safety) is the principal goal. On the contrary, in the normal setting, we demand a higher security level since guaranteeing the security properties (e.g. confidentiality and authentication) of the system is the main goal.

To address these issues, we propose a novel distance bounding protocol (referred to as ACIMD[1]). ACIMD leverages the entire signal (i.e., several QRS complexes of an ECG record; note that a QRS complex represents the propagation of a stimulus through the ventricles), thus limiting the attacker capabilities for remote acquisition of the physiological signal. Particularly, ACIMD tests the proximity between the IMD and the *Programmer* by measuring the similarity between an internal and external physiological signal. Interestingly, ACIMD supports both normal and emergency operation modes, which is beneficial for its real-world use. ACIMD keeps computation and communication to a minimum to save battery power and facilitate implementation on the chip. Finally, it is worth noting that ACIMD has been tested with ECG signals of 199 users who were recorded during a 24-hour period.

Paper contributions: 1) We propose a novel access control (authentication and distance checking) scheme for implantable medical devices; 2) The proposal faces with normal and emergency conditions, and we have verified their security properties from a formal and informal point of view. 3) We have evaluated the performance of the scheme and also tested its accuracy (and adversary advantages) with a pubic dataset with long electrocardiogram records.

Paper organization: In Section II, ACIMD is described and the evaluation dataset and pre-processing techniques are introduced. Next, Section III focuses on results and their discussion. Finally, Section IV concludes the paper and points out future research lines.

II. Methods and Materials

ACIMD is a distance bounding mechanism. It implies that the involved entities can verify the identity of each other (i.e., mutual authentication between the *Programmer* and the IMD as described in Section II-A). Besides, the IMD can verify (distance checking) that the *Programmer* is in its Neighborhood Area (NA) –see Section II-B for details. We describe then in Section II-C how ACIMD deals with normal and emergency operation modes of IMDs.

Fig. 3 illustrates a typical authentication scenario to facilitate the understanding of the interactions between the main entities. The IMD records an internal signal and the *Programmer* externally reads the same signal through a wand. The proximity between both devices is verified using our distance checking scheme. If both signals present enough similarity, the *Programmer* is considered to be within the NA of the implant. In contrast, any adversary is supposed to be out of NA and thus could not successfully complete the authentication.

Regarding the threat model and similarly than in [7], we assume the well-known Dolev-Yao cryptographic model. Note that the model mentioned above is one the most common adversary models used to verify IoT proposals [26]. Conforming the model, the communication channel between the IMD and the *Programmer* is bidirectional and occurs via

[1]This protocol was first introduced in Carmen Camara's thesis [25].

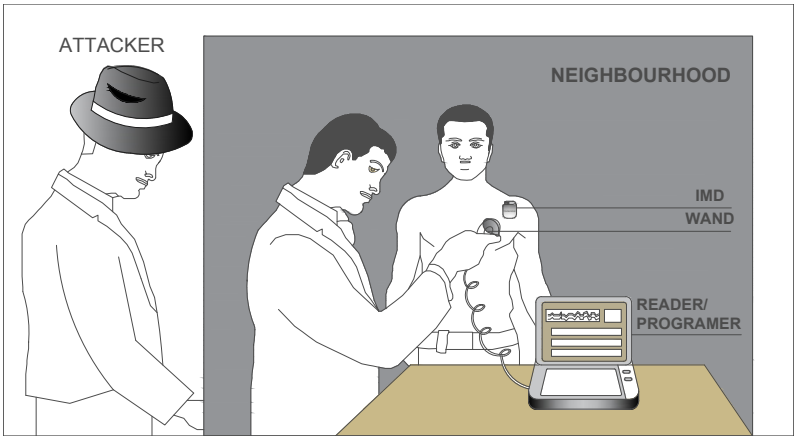

Fig. 3. A typical scenario: IMD, *Programmer* and Adversary

an insecure communication medium. It means that a passive attacker can eavesdrop communications, and an active one can also insert, delete or modify messages transmitted over the channel. Concerning physical manipulation, this sort of attacks is not considered in the Dolev-Yao model, which is reasonable in the context of IMDs as explained below. Firstly, the memory of the IMD is inaccessible since the implant is inside the body of the patient. Secondly, the attacker also cannot physically manipulate the *Programmers* since the hospital controls exhaustively this sort of devices, which are only available to authorise medical personnel.

A. Authentication

A key agreement scheme is applied so that both parties can be sure of each other's identity. Three main alternatives can be used. On the one hand, we can assume that a pre-established key is shared between both entities. This approach raises the risk of endangering future communications if the key gets compromised or leaked to an adversary. Alternatively, as suggested in [27], a fuzzy extractor can be employed for the key generation. Nevertheless, solutions based on fiducial points like R-peaks in ECG or PPG signals are not secure from adversaries who can infer that peaks from a long distance [24]. Interestingly, in 2007, Karimian et al. proposed a fuzzy approach for deriving keys from an ECG signal and using non-fiducial features [28]. Likewise, in [29] or [30], the above design is novelly combined with a PUF function to increase the security of the system. Unfortunately, the authors did not check the viability of the proposals mentioned above when we use internal (IMD) and external biosignals (*Programmer*) as is typical when we deal with implantable medical devices.

Driven by the limitations of the solutions mentioned above, we propose the use of a short-range and secure channel for the transmission of a session key. In particular, as suggested in [31] the use of photobiomodulation seems an interesting approach due to its resistance against eavesdroppers —it allows short-range communications and needs line-of-sight between the transmitter and the receiver. Photobiomodulation (or also known as Low-Level Light Therapy, LLLT) consists in the emission of light by a diode or laser in the spectral range of 600–1000 nm and at a low-power (<500 nW) [32].

Usually, session keys are used several times (e.g., suppose a hospitalised patient who has a pacemaker, her authentication key could be used during her entire hospital stay or be updated every day). Under this assumption, every time we need to renew the session key (including the first time) a key agreement protocol through the LLLT channel is executed before the distance checking and authentication verification. This sort of channel needs a line of sight between the participating entities. We can assume, therefore, implicit proximity between the Programmer and the IMD during this protocol phase – the presence of unauthorized device would be easily detected since the attacker would have to be in the neighbourhood area. Even if despite this we consider that an attacker has a high probability of overpassing this control, we can require that this process only occurs in a controlled environment (note that this is a widespread assumption for key distribution solutions).

Alternatively, in a very demanding scenario (from the security level point of view) in which session keys are used only once time, the exchange of the session key can be done once the distance verification has successfully passed. In this case, the order would be as follows, first verification of the distance, second (only if distance checking has success) exchange of the session key and finally, the authentication protocol.

In any case, let ID_R and ID_I be the identifiers of the *Programmer* and the IMD, $\{\cdot\}_{K_x}$ an encrypted token using the key K_x and "||" the concatenation operation, the exchange of messages for session key agreement (Steps 1-3) and the *Programmer* authentication (Steps 3-6) is as follows:

- **Step 1:** The *Programmer* sends a "Wake-up" message and its identifier ID_R to the IMD.
- **Step 2:** The IMD replies three values: a session key K_s, its identifier ID_I and finally the starting time t_s for recording the physiological signal. This means that the first recorded-window $ECG^{(i)}_{I/R}$ starts at that particular time.
- **Step 3:** During the signal acquisition phase, IMD and *Programmer* record ECG signals and compute δ and

β, respectively (see Section II-B and Equation 5 for details).

Step 4: IMD sends to *Programmer* a random number N_I.

Step 5: *Programmer* generates a nonce N_R and computes an authentication token. The authentication token is computed using K_s and four input values: the nonces $\{N_R, N_I\}$, identifier ID_R of the IMD, and finally β. Finally, *Programmer* sends m_1 message to IMD ($m_1 = \{N_R||N_I||ID_I||\beta\}_{K_s}$).

Step 6: The IMD checks the correctness of the authentication token. In detail, it confirms the addressee of the message by checking the received identifier ID_I and also verifies the validity of nonces $\{N_R, N_I\}$.

B. Distance checking

In ACIMD, we assess the proximity of the *Programmer* and the IMD by comparing the ECG signals recorded by each device. The extraction of the features used for comparison rests on the Walsh-Hadamard transform and its coefficients. For completeness, we give a brief introduction to the Walsh-Hadamard transform computation in Section II-B1. Afterwards, Section II-B2 describes ACIMD's distance checking mechanism.

1) Walsh-Hadamard Transform: The Discrete Walsh-Hadamard Transform (DWT) of a data sequence $x(n)$ of length N (i.e., $n = \{0, 1, ..., N-1\}$ and $M = log_2(N)$) is defined as below:

$$X_w(k) = \frac{1}{N} \sum_{n=0}^{N-1} x(n) \prod_{i=0}^{M-1} (-1)^{b_i(n) b_{M-1-i}(k)}, k = 0, 1, ..., N-1 \quad (1)$$

where $b_i(n)$ is the binary representation of n and being the subscript zero the least significant bit.

The above equation is equivalent to:

$$X_w(k) = \frac{1}{N} \sum_{n=0}^{N-1} x(n) (-1)^{\sum_{i=1}^{M-1} b_i(n) b_{M-1-i}(k)} \quad (2)$$

In fact, X_w can be calculated by the multiplication of the Wash Matrix ($N \times N$-matrix) with the sequence x ($1 \times N$-vector):

$$X_w = H_N \cdot x \quad (3)$$

The calculation of the Hadamard matrix can be computed recursively as described below:

$$H_{2^i} = \frac{1}{\sqrt{2}} \begin{bmatrix} H_{2^{i-1}} & H_{2^{i-1}} \\ H_{2^{i-1}} & -H_{2^{i-1}} \end{bmatrix} \quad (4)$$

where $H_1 = 1$ and $i = \{1, ...M = 2^N\}$.

A straight forward implementation of the Walsh-Hadamard transform has a computational complexity of $\mathcal{O}(n^2)$. In our experiments, we have used the fast Walsh–Hadamard transform [33]. The complexity reduces to $\mathcal{O}(n \log n)$, and it only requires the computation of additions and subtractions.

2) Mechanism description: The steps for distance checking in ACIMD are depicted in Fig. 4 and detailed as follows:

Step 1: Electrocardiogram signals are obtained from both the IMD (ECG_I) and the *Programmer* (ECG_R).

Step 2: The noise of the signals is eliminated and then ECG records are split into windows of L_w seconds as further described in detail in Section II-D. The i-th window of length L_w is represented by $ECG_I^{(i)}$ when it comes from the IMD (or $ECG_R^{(i)}$ for those from the *Programmer*).

Step 3: We perform the analysis of the ECG windows in a transformation domain. In detail, we use a Walsh-Hadamard transformation due to both its compression capabilities and its low computing requirements. The Hadamard coefficients of the i-th $ECG_{I/R}^{(i)}$ window are represented by $X^{ECG_{I/R}^{(i)}}$. The value of these coefficients has been quantized using a dynamic quantizer with 2^8 levels as in [34] to facilitate its analysis.

Step 4: A set of N windows from the external and internal signals are used in the similarity checking module. The correlation coefficient has been the metric used for the comparison of the coefficients. The N parameter is set in order to optimize the performance of the system and to minimize the observation period of the signal, i.e., the time interval required for recording the internal and external signals. Mathematically,

$$S(\delta, \beta) = S\left(X^{ECG_I^{(i)}}, X^{ECG_R^{(i)}}\right) = \\ = corr\left(\begin{bmatrix} X^{ECG_I^{(i)}} \\ X^{ECG_I^{(i+1)}} \\ \cdots \\ X^{ECG_I^{(i+(N-1))}} \end{bmatrix}, \begin{bmatrix} X^{ECG_R^{(i)}} \\ X^{ECG_R^{(i+1)}} \\ \cdots \\ X^{ECG_R^{(i+(N-1))}} \end{bmatrix}\right) \quad (5)$$

where *corr* represents the correlation operation.

Step 5: A decision is taken based on the similarity of the signals. If both signals are considered *sufficiently close*, it means that the IMD and the *Programmer* are within the neighbourhood area. The proximity implies that the *Programmer* is able to record the ECG signal with all its fruitful components —the entire QRS complex is used. A threshold α is defined for this comparison, see Eq. 6.

$$\begin{cases} |S\left(X^{ECG_I^{(i)}}, X^{ECG_R^{(i)}}\right)| < \alpha & \text{Inside NA} \\ Otherwise & \text{Outside NA} \end{cases} \quad (6)$$

C. Normal and emergency modes of operation

ACIMD operates under normal and emergency scenarios. In a normal setting, the user keeps doing her daily routines and no restrictions of time and computation apply, apart from those intrinsic to IMDs. Thus the authentication procedure can be time-consuming to ensure the maximum level of security. On the contrary, in the emergency mode, keeping the IMD holder alive is the priority. The access to the implant should not be delayed by heavy security mechanisms. Thus, a lightweight

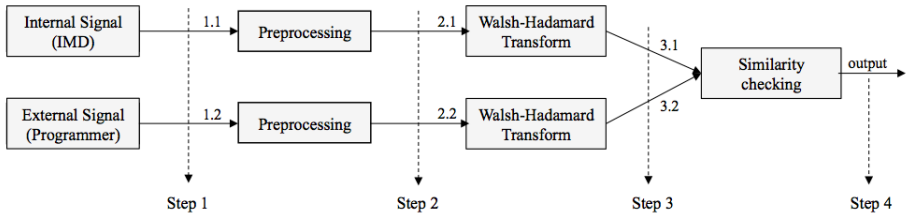

Fig. 4. Distance checking mechanism

authentication mechanism being less secure but faster can be considered.

In order to cope with these two scenarios, two modes of ACIMD are proposed.

1) ACIMD *in normal mode:* In this mode, ACIMD performs the key agreement steps for authentication (recall Section II-A). Moreover, distance checking procedure (recall Section II-B2) is also carried out. The scheme is depicted in Fig. 5.

The access control decision is based on the result of both procedures. In particular, after having the ECG signal of the holder and receiving message m_1 from the *Programmer*, the IMD computes its answer m_2 as follows:

$$\begin{cases} m_2 = \{N_I||N_R||h(\beta||1)\}_{K_s} & \text{If } \perp auth \text{ and } |S(\delta,\beta)| < \alpha \\ m_2 = \{N_I||N_R||h(\beta||0)\}_{K_s} & \text{If } \perp auth \text{ and } |S(\delta,\beta)| \geq \alpha \\ m_2 = random\_value & \text{Otherwise} \end{cases}$$

where h symbolizes a one-way hash function. This answer is sent to the *Programmer*, which verifies its correctness. In particular, if m_2 is valid with $h(\beta||1)$, it means that IMD and *Programmer* are (1) mutually authenticated and (2) within the NA of IMD. If it is not the case, but m_2 is valid with $h(\beta||0)$, this means that the mutual authentication is successful but the reader is out of NA. Otherwise, none of these conditions are fulfilled.

2) ACIMD in emergency mode: In emergency mode, we cannot assume that IMD and Programmer are under a controlled environment. For instance, this can be the case when the holder of the implant is in a foreign country or, for example, s/he is not in her/his corresponding referral hospital.

Therefore, in emergency mode, only distance checking (Section II-B2) is applied. In Fig. 6 we sketch this mode of operation. Essentially, *Programmer* sends the ECG signal in clear to the IMD. This entity then computes the similarity with its internal signal and takes a decision following Equations 5 and 6, respectively.

Note that the security requirements are relaxed since the primary requirement becomes the speed and success of the process in order to keep the holder of the implant alive. The proposed solution is a trade-off between safety of the IMD holder and security of the system.

D. Dataset and Pre-processing

ACIMD has been evaluated using physiological signals. Since cardiovascular diseases are the principal death cause around the world [35], implantable cardiac defibrillators and pacemakers are the most deployed IMDs. Motivated by this, we have used electrocardiogram (ECG) signals in our experimentation. In particular, cardiac signals from E-HOL-03-202-003 dataset (Telemetric and Holter ECG Warehouse of University of Rochester), are the ECG recordings used in our experiments [36]. In detail, this dataset was acquired using the SpaceLab-Burdick digital Holter recorder (SpaceLab-Burdick, Inc., Deerfield, WI) and a pseudo-orthogonal lead configuration with three electrodes $\{X, Y, Z\}$ was used. The results shown in this article correspond to the pair of leads $\{Y, Z\}$. Thus, the lead X is taken as ECG_I and Y is taken as ECG_R.

The rationale for using this dataset is four-fold. Firstly, as mentioned, cardiac implants are currently the most widespread IMD in the healthcare sector. Therefore, ECG records seem an interesting signal for our study. Secondly, the dataset has a high number of individuals – 199 out of 203 have been employed since 4 had an insufficient file size. Thirdly, the recordings were taken during a long period of 24 hours. Last but not least, we can assume that the population is homogeneous (without any bias) since no important cardiac problems were detected over the subjects under study.

Before any other processing, we need to clean the ECG signals. We follow the procedure described below, which is typically for ECG pre-processing. We start eliminating the DC component. After that, a filter is used, aiming to eradicate the respiration and the power-line source of noises. More precisely, we pass ECG signals over a pass-band filter with 0.67 Hz (lower-cut-off-frequency) and 0.45 Hz (upper-cut-off-frequency). The respiration noise is eliminated through the lower stop-band. The pass-band pursues to keep as much information as possible while the upper-stop band is related to the elimination of the power line noise. We follow the above-described process with all the signals of the dataset. Then, we use a Heart Rate Variability (HRV) analysis that could help us to detect errors in the process. As shown in Table I, we extract features in the time domain (statistics of RR-intervals) and the spectral domain (spectral power analysis). The obtained values are within the margins of the standard HRV values, taking as a reference, for instance, the retrospective analysis by Nunan et al. [37]. Therefore, it confirms the absence of errors in the cleaning process and the nonexistence of bias in the dataset used.

Once cleaned, ECG records are split into windows of $L_w = 2$ seconds. Since a healthy individual beats between 60 and 100 times per minute, it entails that each window contains 2 or 3 heartbeats. The usage of this window size is inspired on previous works in ECG identification with high accuracy rate [38].

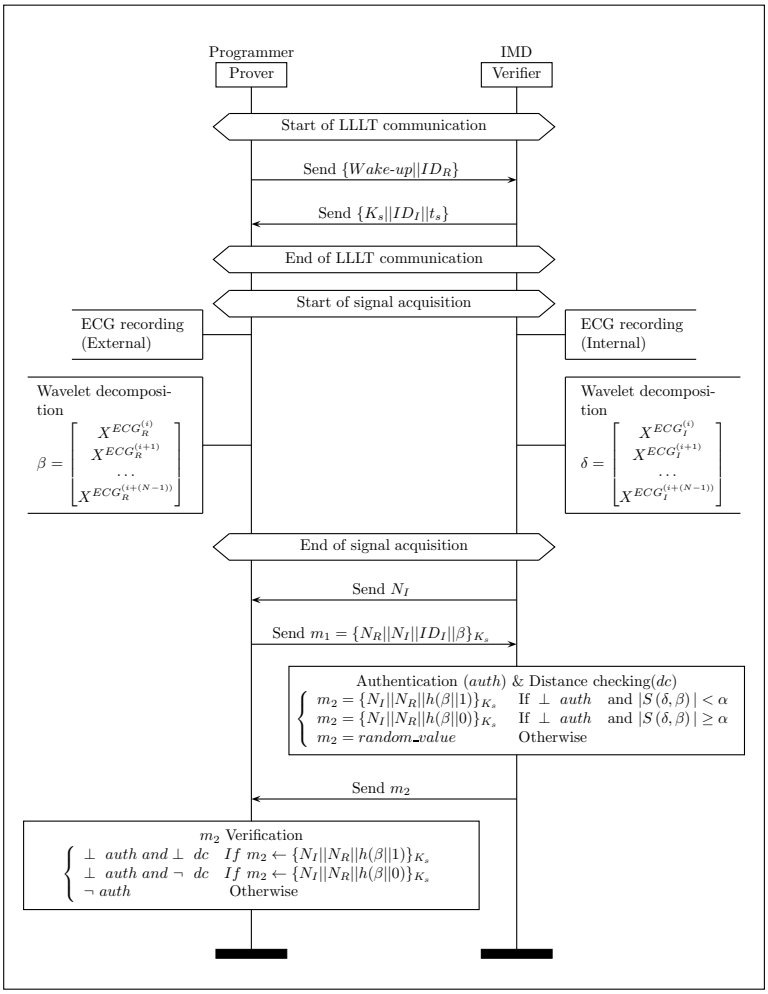

Fig. 5. ACIMD in normal mode

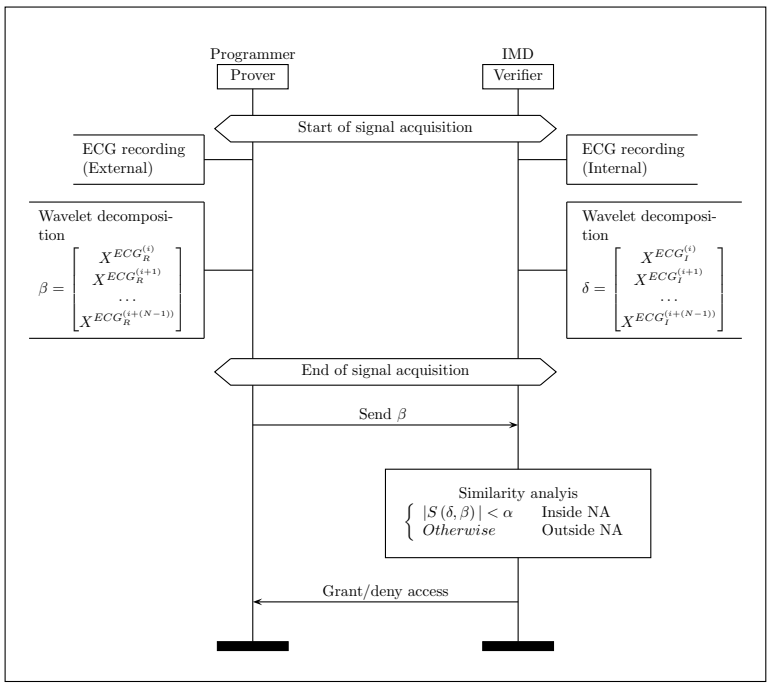

Fig. 6. ACIMD in emergency mode

HRV Measure	Mean	SD	CV (%)	Median	Range
mRR (ms)	881.98	60.97	6.91	859.27	817.35-1075
SDNN (ms)	44.53	15.90	35.71	40.06	16.96 - 89.95
rMSSD(ms)	45.12	24.61	54.54	40.06	12.65 - 136.84
LF (ms^2)	503.29	239.19	47.52	455.63	151.12 - 994.62
HF (ms^2)	539.52	534.49	99.07	339.85	34.11 - 2763.6
LF:HF	1.79	1.72	95.72	1.25	0.26 - 11.56

†Notation: SD (standard deviation); CV (coefficient of variation = (SD/mean x 100); mRR (mean of RR-intervals); SDNN (standard deviation of normal-to-normal RR-intervals); rMSSD (root mean square of successive differences between adjacent RR-intervals); LF (low-frequency spectral power); HF (high-frequency spectral power); LF:HF (ratio of low-frequency power to high-frequency power).

TABLE I
HRV ANALYSIS

III. RESULTS AND DISCUSSION

ACIMD has been assessed considering its three major capabilities – authentication, distance checking and its ability to operate in emergency scenarios. Each capability is evaluated and discussed separately.

A. Authentication

We have analysed the security of the authentication protocol from an informal and formal point of view. We focus both analyses in the normal operation mode since in the emergency mode there is only a comparison between the external and internal signal recorded (see Fig. 6). Concerning the first analysis, we have evaluated the main security properties demanded to an authentication protocol:

- **Confidentiality:** None of the confidential information (e.g., external/internal signals β and δ) is transmitted in clear on the radio channel because otherwise it could be captured by a passive adversary.
- **Anonymity:** Each of the entities involved in the protocol generates a random number which guarantees the anonymity (and freshness) of the m_1 and m_2 authentication tokens.
- **Integrity:** Regarding the messages passes over the channel, if the tokens m_1 and m_2 are correctly verified (the protocol ends successfully), it guarantees the integrity of the content of the messages. Besides, and concerning the memory of the devices, in the case of IMDs, this cannot be physically manipulated since the implant is within the body. The memory of the *Programmer* is also protected since this sort of devices are heavily supervised and are only accessible to authorised medical personnel.
- **Mutual Authentication:** The IMD authenticates the *Programmer* by verifying the message m_1. Similarly, the *Programmer* authenticates the IMD through the message m_2. Therefore, if the protocol concludes successfully, both entities are mutually authenticated.
- **Man-in-the-middle Attack Prevention:** This sort of attack is inviable since our proposal consists on a mutual authentication in which two nonces (n_1 and n_2) and an external/internal signals (β and δ), are used. Note that the random numbers and the captured signals are refreshed in each protocol execution.
- **Replay Attack Prevention:** Replay attacks are avoided for two main reasons. On the one hand, the generation of a random number of each of the intervening entities hinders this sort of attacks. On the other hand, these attacks are unlikely since the usefulness of an old ECG record (β^{old} or δ^{old}) in a new session is almost null (see Section III-B).
- **Forgery Resistance:** As the adversary can not physically manipulate the IMD, s/he can only eavesdrop the messages over the channel. However, this would be unsuccessful since the m_2 is protected with the session key ($\{\}_{K_s}$), and this message is only valid for the current session.
- **Denial-of-Service Attack:** As same as in any other scheme that uses the radio channel for communications, an adversary can block the proper functioning of the protocol by emitting a signal of high power and uninterruptedly. This threat is not particular of our proposal but represents an inherent limitation to the use of the radio channel.

Once we have revised the security properties of the authentication protocol, we have formally verified its correctness. As previously mentioned in Section II, we have assumed the Dolev-Yao threat model as same as in ProVerif [39] and in predecessors works [7], [40]. Drive by this, ProVerif is the tool used for the automatic verification of the protocol. It supports standard cryptographic primitives, including hash functions and symmetric encryption, which are the primitives employed in our scheme.

Before defining the protocol, we have to establish which are our premises. That is, we set the assumptions about the channel, session/secret keys, functions, etc. Particular, we summarise our assumptions in Fig. 7. For instance, "free c: channel" symbolises that c is a public channel, and "free x: bitstring [private]" represents that the bit-string x is unknown to the attacker. We urge to non-familiar readers with ProVerif to consult the reference manual [39]. The next step, and taking into account the protocol description (see Fig. 5), is to define the processes related with each of the involved entities (IMD and *Programmer*) in the protocol. We sketch these processes in Figure 8. Finally, we verify the proposed scheme using ProVerif. We can observe in the results of Figure 9 that all the events are "true". The adversary can thus not compromise the session key (K_s), and the *Programmer* and the IMD are successfully authenticated. In summary, we formally proof that ACIMD authentication protocol is secure. Besides, as mentioned, the proposed scheme conforms to the standard

```
(*-Scheme channels-*)
free c: channel.
type tag.
type entity.
type nonce.
type key.
(*-Scheme key-*)
free ks: key [private].
(*-Scheme constants-*)
const beta: tag [data].
const Idi: bitstring [private].
const B1: bitstring.
(*-Scheme functions-*)
fun h(bitstring): bitstring.
fun con(bitstring,bitstring):bitstring.
fun encrypt(bitstring,key): bitstring.
reduc forall x: bitstring, y: key;
decrypt(encrypt(x,y),y) = x.
(* 2 entity names IMD and Programmer *)
free IMD, Programmer: entity.
table keys(entity, key).
(*-Queries-*)
query attacker(ks).
query m2:bitstring; inj-event(AuthIMD(m2))
==> inj-event(BeginIMD(m2)).
query m1:bitstring; inj-event(AuthProgrammer(m1))
==> inj-event(BeginProgrammer(m1)).
(*-Events-*)
event BeginIMD(bitstring).
event AuthIMD(bitstring).
event BeginProgrammer(bitstring).
event AuthProgrammer(bitstring).
```

Fig. 7. Premises in ProVerif for the authentication process in ACIMD

```
let Verifier=
new Ni:bitstring;
out(c,Ni);
in(c,Vm1:bitstring);
let m1=Vm1 in
get keys(=IMD, ks) in
new VNr:bitstring;
new VNi:bitstring;
new VIdi:bitstring;
new Vbeta:bitstring;
let (=VNr, =VNi, =VIdi, =Vbeta) =
decrypt(Vm1, ks) in
if VNi=Ni && VIdi=Idi then
event AuthProgrammer(m1);
let m2=encrypt((Ni, VNr, h(con(Vbeta,B1))),
ks)in
event BeginIMD(m2);
out(c, m2).
```

```
let Prover=
in(c,PNi:bitstring);
new Nr:bitstring;
get keys(=Programmer, ks) in
let m1=encrypt((Nr, PNi, Idi, beta), ks)in
event BeginProgrammer(m1);
out(c,m1);
in(c,Pm2:bitstring);
new PNi2:bitstring;
new PNr:bitstring;
new Phbeta:bitstring;
let (=PNi2, =PNr,  =Phbeta) = decrypt(Pm2,
ks) in
let m2=Pm2 in
if PNi2=PNi && PNr=Nr then
event AuthIMD(m2).
```

Fig. 8. Processes in Proverif for the authentication process in ACIMD

ISO/IEC 9798-2 [41]. Regarding the security level offered, assuming the use of a secure cryptographic primitive and L the length of session key K_s, the security of the protocol is upper bounded $\frac{1}{2^{2 \cdot L}}$ (cf. Section II-A). Under the assumptions regarding the security of LLLT communications [31], which is used to transmit the session key, the above upper bound holds.

Finally, we have assessed the performance of our proposal, and we can use several metrics for this purpose. On the one hand, we consider critical the number of messages exchanged between the IMD and the *Programmer*. On the other hand, the computation cost, in terms of consuming time and energy consumption on the side of the IMD, which is the most critical element, is very relevant. We compare our proposal with the other [18] exiting distance bounding protocol and custom-designed for implantable medical devices. Concerning authentication protocols, we take as a reference [2] since this is one of the most recent works tailored-made for implantable cardiac defibrillators. Besides, we add to this comparative [42] since it is an exciting proposal for IMDs in which the authors provide details for both normal and emergency conditions.

Regarding the cryptography primitives and the consumed resources, we use the values shown in [8] and [43] as reference. In particular, a Hash Function (HF) takes 0.0032 seconds and consumes 0.0051 mJ. A symmetric cypher (SC –encryption or decryption) requires 0.0056 seconds and 0.009 mJ of energy. A Modular Exponentiation (ME) takes 0.0192 seconds and demands 0.58 mJ of energy. Finally, a Bilinear Pairing (BP) requires 0.197 seconds and 1.34 mJ. In our proposal, a Similarity (S) operation is computed, and its cost in comparison with a cryptographic function is meaningful in terms of consuming time and similar for the used energy. In particular, we have implemented the similarity (distance checking) function in an Artix-7 C7A35T FPGA, and it takes 0.1398 ms seconds and consumes 0.0163 mJ (operating frequency set to 100 MHz and assuming 25^o celsius of temperature).

Table II summarises the performance comparative analysis. Our proposal outperforms predecessors schemes. In comparison with the Rasmussen et al. distance bounding protocol [18], it is remarkable how in our scheme the power consumption is 30 times lower in the worst case (normal operation mode). Marin et al. [2] is a novel proposal that considers both normal and emergency operation modes. Unfortunately, the bilinear paring used for the key agreement is very demanding in terms of resources (time and energy) which renders the proposal unfeasible principally in an emergency condition. Even assuming the cost of time as an acceptable value, the power consumption is very steep, which would drain the battery life of the IMD very quickly. Regarding [42], we can observe that the protocol is more demanding (time and power) in the emergency mode than in the normal mode. This result doesn't make sense since in an emergency (e.g., heart attack condition) we need to act as fast as we can as occurs in our proposal in which the access is almost instantaneous (less than a quarter of a millisecond).

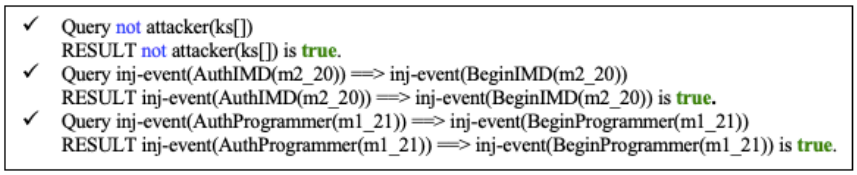

Fig. 9. ProVerif results for the authentication process in ACIMD

Protocol	Operation mode	N. of messages	Computation cost (time)	Computation cost (energy)
[18]	Not specified	6	2 HF+ME = 0.03872 sec.	1.1651 mJ
[2]	Normal & Emergency	7	1 BP+ 1 SE = 0.2026 sec.	1.3490 mJ
[42]	Normal	3	7HF+ 1 SC = 0.028 sec.	0.0447 mJ
	Emergency	5	12 HF + 1 SC = 0.044 sec.	0.0792 mJ
Our Proposal (ACIMD)	Normal	3	2 SC + 1 S = 0.0113 sec.	0.0343 mJ
	Emergency	2	1 S = 0.000138 sec.	0.0163 mJ

TABLE II
PERFORMANCE ANALYSIS: AUTHENTICATION PROTOCOL

B. Distance checking

Considering an IMD and a *Programmer* being in its neighbourhood area, we evaluate the accuracy of our system by computing the percentage of ECG signals recorded by each device that succeed the distance checking (Section II-B). In addition, we evaluate the success rate of three considered adversary strategies:

Definition 3.1 (Replay attack): We define as $\mathcal{A}_R$ the advantage of an adversary to overpass the system by using signals of a previous session of the same subject. Mathematically,

$$p(\mathcal{A}_R) = p(|S(X^{ECG_I^{(i)}}, X^{ECG_I^{(j)}})| < \alpha) \qquad \text{where } i < j \quad (7)$$

Definition 3.2 (Impersonation Attack): We define as $\mathcal{A}_I$ the advantage of an adversary to overpass the system by using a signal captured from another subject than the holder of the IMD performing the authentication. There is no correspondence between the internal signal (I) recorded by the IMD and the external signal (R') played by the attacker. The comparison is performed between the internal signal of a subject and the external signal of a different subject. It can be expressed as:

$$p(\mathcal{A}_I) = p(|S(X^{ECG_I^{(i)}}, X^{ECG_{R'}^{(i)}})| < \alpha) \quad \text{where } I \not\Rightarrow R' \quad (8)$$

Definition 3.3 (Random guessing): We define as $\mathcal{A}_G$ the advantage of an adversary to overpass the system by random guessing. Mathematically,

$$p(\mathcal{A}_G) = p(|S(random, X^{ECG_I^{(i)}})| < \alpha) \quad (9)$$

Table III summarizes the accuracy (**Acc. (%)**) of ACIMD for a normal authentication between two authorized devices according to different α values. Also, the success rate of an attack considering the three adversary advantages is provided. Four rows corresponding to four considered *configurations* are highlighted in the table. The design goals (e.g., maximum accuracy or minimum advantage for the attacker) conditions the choice of a particular configuration.

Configuration-A is the one with the highest accuracy (92.92%), but the adversary chances are relatively high (27.7% in the worst-case scenario). Fortunately, configuration-B offers a similar accuracy (89.41%) while the success probability for the adversary reduces by almost 40% (10.6%). Configuration-C represents the case in which the accuracy drops slightly but still over 85% (86.67%), and the adversary chances are considerably low (4.39%). The degeneration of configuration-3 is configuration-4 with a negligible probability of success for the adversary (1.7%) and a success rate for legitimate users of 83.88%. From a practical perspective, Configuration-C (or D) seems to be the most appropriate under a normal situation since it offers an acceptable accuracy (in both cases over 85%) while mitigating the three adversary advantages (in the worst circumstance around 10% of success probability). Under these settings, the penalty for the distance checking mechanism is that it might be executed several times in case the distance verification fails, and the legitimate reader is, in reality, within the neighbourhood area.

It is worth noting that the strategy to use signals of previous sessions or physiological signals from other users achieve a similar success rate. Note that this result is very favourable for our proposal because unlike what may occur in other ECG-based authentication proposals such as [44] or [45], the knowledge of the victim's previous ECG signals is not helpful in future sessions. Furthermore, the success rate of an attacker using a random guessing (and replay attack) approach is very low and decreases rapidly to zero when the parameter α increases.

C. Emergency mode

Considering that our authentication scheme must apply to emergency situations, the access to the implant must be guaranteed and as fast as possible in such scenarios. To ensure the access to the implant, the parameter α may be set to 0.05 (configuration-A) or a lower value in order to increase the success rate of authentication (>92.92%).

One key-point in an emergency condition is the duration of the signal monitoring. We experimentally tuned this parameter and selected an optimal value of 6 s. (considering $N = 3$ and $L_w = 2$ s.). We need to add the time consumed for computing the similarity operation (i.e., three Walsh-Hadamard transforms and the correlation operation) to these 6 seconds mentioned above for the total calculation. As shown in Table II, this operation only takes less than two hundreds milliseconds which is almost negligible compared to the ECG signal

α	Acc. (%)	$\mathcal{A}_R(\%)$	$\mathcal{A}_I(\%)$	$\mathcal{A}_G(\%)$	
0.050	92.924 [91.383, 94.466]$_{CI95\%}$	27.014 [25.934, 28.094]$_{CI95\%}$	27.769 [27.265, 28.273]$_{CI95\%}$	7.4249 [7.3212, 7.5285]$_{CI95\%}$	**Config.-A**
0.055	92.216 [90.536, 93.897]$_{CI95\%}$	22.461 [21.485, 23.438]$_{CI95\%}$	23.255 [22.765, 23.746]$_{CI95\%}$	4.8468 [4.7646, 4.9289]$_{CI95\%}$	
0.060	91.516 [89.704, 93.328]$_{CI95\%}$	19.564 [18.639, 20.489]$_{CI95\%}$	19.328 [18.854, 19.802]$_{CI95\%}$	3.1814 [3.1164, 3.2464]$_{CI95\%}$	
0.065	90.799 [88.857, 92.741]$_{CI95\%}$	15.154 [14.093, 16.215]$_{CI95\%}$	15.971 [15.527,16.415]$_{CI95\%}$	2.0035 [1.9492, 2.0577]$_{CI95\%}$	
0.070	90.102 [88.033, 92.171]$_{CI95\%}$	12.731 [11.700, 13.763]$_{CI95\%}$	13.053 [12.637, 13.468]$_{CI95\%}$	1.2543 [1.2079, 1.3007]$_{CI95\%}$	
0.075	89.410 [87.217, 91.603]$_{CI95\%}$	10.054 [9.1701, 10.938]$_{CI95\%}$	10.651 [10.267, 11.035]$_{CI95\%}$	0.69832 [0.66536, 0.73129]$_{CI95\%}$	**Config.-B**
0.080	88.742 [86.432, 91.051]$_{CI95\%}$	8.1366 [7.1870, 9.0861]$_{CI95\%}$	8.5637 [8.2128, 8.9145]$_{CI95\%}$	0.42031 [0.39529, 0.44533]$_{CI95\%}$	
0.085	88.058 [85.635, 90.480]$_{CI95\%}$	6.3889 [5.6614, 7.1164]$_{CI95\%}$	6.8933 [6.5744, 7.2122]$_{CI95\%}$	0.24234 [0.22270, 0.26197]$_{CI95\%}$	
0.090	87.335 [84.793, 89.877]$_{CI95\%}$	5.4552 [4.9822, 5.9283]$_{CI95\%}$	5.4955 [5.2093, 5.7816]$_{CI95\%}$	0.12951 [0.11607, 0.14295]$_{CI95\%}$	
0.095	86.672 [84.025, 89.319]$_{CI95\%}$	4.1937 [3.5112, 4.8762]$_{CI95\%}$	4.3916 [4.1388, 4.6443]$_{CI95\%}$	0.06281 [0.05317, 0.07245]$_{CI95\%}$	**Config.-C**
0.100	85.957 [83.202, 88.712]$_{CI95\%}$	3.8503 [3.3356, 4.3650]$_{CI95\%}$	3.4590 [3.2342, 3.6839]$_{CI95\%}$	0.03800 [0.02982, 0.04617]$_{CI95\%}$	
0.105	85.258 [82.402, 88.115]$_{CI95\%}$	2.3341 [1.9698, 2.6984]$_{CI95\%}$	2.7122 [2.5134, 2.9111]$_{CI95\%}$	0.02094 [0.01503, 0.02684]$_{CI95\%}$	
0.110	84.599 [81.649, 87.548]$_{CI95\%}$	2.2840 [1.9621, 2.6058]$_{CI95\%}$	2.1407 [1.9655, 2.3159]$_{CI95\%}$	0.00814 [0.00465, 0.01164]$_{CI95\%}$	
0.115	83.879 [80.831, 86.928]$_{CI95\%}$	1.3079 [1.0123, 1.6035]$_{CI95\%}$	1.7022 [1.5442, 1.8601]$_{CI95\%}$	0.00620 [0.00326, 0.00914]$_{CI95\%}$	**Config.-D**

TABLE III
ACIMD PERFORMANCE: ACCURACY AND ADVERSARY ADVANTAGES ($N = 3$ AND $L_w = 2$ S.)

recording. Therefore, ACIMD only requires a few seconds ($N \times L$ s.) in the emergency mode, which is reasonable to check proximity between the involved entities and to deal with the critical condition of an individual.

IV. CONCLUSIONS

There is an agreed consensus about the benefits of incorporating telemetry into the new generation of IMDs. In particular, it improves the patients' quality of life, facilitates remote management by the medical personnel and reduces costs. Unfortunately, many commercial IMDs still lack security protection mechanisms. Among the security requirements, controlling which devices can read from or send commands to the IMDs is paramount. For this purpose, in this paper, an access control protocol called ACIMD has been introduced. ACIMD implements a distance bounding mechanism based on physiological signals, particularly electrocardiograms in our experiments. In detail, our proposed scheme allows verifying the proximity between an IMD and a *Programmer* (distance checking) and also each entity can verify the identity of the other involved party and be sure of her/his presence during the protocol execution (mutual authentication). We want to highlight that we have verified the security of the proposed protocol from both a formal and informal point of view. Besides, we have evaluated the feasibility of the proposal with an ECG dataset with 199 subjects.

ACIMD outperforms previous approaches for various reasons. First, it considers the whole ECG signal, which is challenging to acquire remotely. Secondly, it is more efficient than their predecessors regarding the number of exchanged messages and the computation cost (time and energy). Finally, it can operate in the normal and emergency operation modes typical for IMDs.

As future work, we consider that there is room for proposing new methods that assess the similarity between the external and internal vital signals (distance checking phase).

ACKNOWLEDGEMENT

This work was supported by Leonardo Grant for Researchers and Cultural Creators, BBVA Foundation (P2019-CARDIOSEC) and by the Comunidad de Madrid (Spain) under the project CYNAMON (P2018/TCS-4566), co-financed by European Structural Funds (ESF and FEDER).

Data used for this research was provided by the Telemetric and Holter ECG Warehouse (THEW) of University of Rochester, NY.

REFERENCES

[1] C. Camara, P. Peris-Lopez, and J. E. Tapiador. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics*, 55:272 – 289, 2015.

[2] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel. On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. In *Proceedings of the 32nd Annual Conference on Computer Security Applications, ACSAC'16*, pages 226–236. ACM, 2016.

[3] L. Pycroft and T. Z. Aziz. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices*, 15(6):403–406, 2018. PMID: 29860880.

[4] Food and Drug Administration. FDA warns patients, providers about cybersecurity concerns with certain medtronic implantable cardiac devices. https://www.fda.gov/NewsEvents/Newsroom/FDAInBrief/ucm623191.htm, 2018.

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

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

[7] 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 Journal of Biomedical and Health Informatics*, 22(4):1299–1309, 2018.

[8] V. Odelu N. Kumar S. Kumari M. K. Khan A. V. Vasilakos S. Challa, K. Das. An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Computers & Electrical Engineering*, 69:534 – 554, 2018.

[9] X. Hei and X. Du. *The Resource Depletion Attack and Defense Scheme*, pages 9–18. Springer New York, 2013.

[10] L. Wu, X. Du, M. Guizani, and A. Mohamed. Access control schemes for implantable medical devices: A survey. *IEEE Internet of Things Journal*, 4(5):1272–1283, 2017.

[11] K. Heather, K. Shah, K. K. Venkatasubramanian, K. Hoyme, M. Seeberger, and G. Wiechman. A novel authentication biometric for pacemakers. In *IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pages 81–87, 2018.

[12] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implantable medical devices. *SIGCOMM Comput. Commun. Rev.*, 41(4):2–13, 2011.

[13] G. Avoine et al. Security of distance-bounding: A survey. *ACM Comput. Surv.*, 51(5):94:1–94:33, 2018.

[14] S. Brands and D. Chaum. *Distance-Bounding Protocols*, pages 344–359. Springer Berlin Heidelberg, 1994.

[15] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the fiat-shamir passport protocol. In *Advances in Cryptology - CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 1987.

[16] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment*. Springer, 1st edition, 2010.

[17] K. Fishkin and S. Roy. Enhancing rfid privacy via antenna energy analysis., 2003.

[18] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pages 410–419. ACM, 2009.

[19] S. Pirbhulal, H. Zhang, W. Wu, S. C. Mukhopadhyay, and Y. Zhang. Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Transactions on Biomedical Engineering*, 65(12):2751–2759, 2018.

[20] A. Levi D. K. Altop and V. Tuzcu. Deriving cryptographic keys from physiological signals. *Pervasive and Mobile Computing*, 39:65 – 79, 2017.

[21] G. Zheng, W. Yang, C. Valli, L. Qiao, R. Shankaran, M. A. Orgun, and S. C. Mukhopadhyay. Finger-to-heart (F2H): Authentication for wireless implantable medical devices. *IEEE Journal of Biomedical and Health Informatics*, pages 1–1, 2018.

[22] F. Stajano, F.-L. Wong, and B. Christianson. Multichannel protocols to prevent relay attacks. In *Financial Cryptography and Data Security*, pages 4–19. Springer Berlin Heidelberg, 2010.

[23] O. Choudary and F. Stajano. Make noise and whisper: A solution to relay attacks. In *Security Protocols XIX*, pages 271–283. Springer Berlin Heidelberg, 2011.

[24] A. Calleja, P. Peris-Lopez, and J. E. Tapiador. *Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-Based Protocols*, pages 36–51. Springer International Publishing, 2015.

[25] C. Camara. *Cybersecurity in implantable medical devices*. PhD thesis, Carlos III University of Madrid, 2018.

[26] Q. Do, B. Martini, and K.-K. R. Choo. The role of the adversary model in applied security research. *Computers & Security*, 81:156 – 181, 2019.

[27] C. Huth, D. Becker, J. G. Merchan, P Duplys, and T. Güneysu. Securing systems with indispensable entropy: Lwe-based lossless computational fuzzy extractor for the internet of things. *IEEE Access*, 5:11909–11926, 2017.

[28] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte. Highly reliable key generation from electrocardiogram (ecg). *IEEE Transactions on Biomedical Engineering*, 64(6):1400–1411, 2017.

[29] N. Karimian, Z. Guo, F. Tehranipoor, D. L. Woodard, M. Tehranipoor, and D. Forte. Secure and reliable biometric access control for resource-constrained systems and iot. *CoRR*, abs/1803.09710, 2018.

[30] F. Tehranipoor, N. Karimian, P. A. Wortman, and J. A. Chandy. Low-cost authentication paradigm for consumer electronics within the internet of wearable fitness tracking applications. In *IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–6, 2018.

[31] A. Juels and D.V. Bailey. Access control for implanted medical devices, 2013.

[32] A. Mandel and M. Hamblin. A renaissance in low-level laser (light) therapy – lllt. *Photonics & Lasers in Medicine*, 1(4):231 – 234, 2012.

[33] B. J. Fino and R. Algazi. Unified matrix treatment of the fast walsh-hadamard transform. *IEEE Transactions on Computers*, C-25(11):1142–1146, 1976.

[34] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-heart (h2h): authentication for implanted medical devices. In *ACM Conference on Computer and Communications Security*, pages 1099–1112. ACM, 2013.

[35] H. Alzubaidi K. Mc Namara and J. K. Jackson. Cardiovascular disease as a leading cause of death: how are pharmacists getting involved? *Integrated pharmacy research & practice*, 8:1–11, 2019.

[36] J.-P. Couderc. The telemetric and holter {ECG} warehouse (thew): The first three years of development and research. *Journal of Electrocardiology*, 45(6):677 – 683, 2012.

[37] D. Nunan, G. R. H. Sandercock, and D. A. Brodie. A quantitative systematic review of normal values for short-term heart rate variability in healthy adults. *Pacing and Clinical Electrophysiology*, 33(11):1407–17, 2010.

[38] C. Camara, P. Peris-Lopez, L. Gonzalez-Manzano, and J. Tapiador. Real-time electrocardiogram streams for continuous authentication. *Applied Soft Computing*, 68:784 – 794, 2018.

[39] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre. Proverif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial. 2018.

[40] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. R. Choo, and Y. Park. Design of secure and lightweight authentication protocol for wearable devices environment. *IEEE Journal of Biomedical and Health Informatics*, 22(4):1310–1322, 2018.

[41] C. Boyd and A. Mathuria. *Protocols Using Shared Key Cryptography*, pages 73–106. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[42] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga. Securing implantable cardiac medical devices: Use of radio frequency energy harvesting. In *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*, TrustED '13, pages 35–42. ACM, 2013.

[43] T. Unterluggauer and E. Wenger. Efficient pairings and ecc for embedded systems. In *Proceedings of the 16th International Workshop on Cryptographic Hardware and Embedded Systems — CHES'14 - Volume 8731*, page 298–315. Springer-Verlag, 2014.

[44] S. Eberz, N. Paoletti, M. Roeschlin, A. Patané, M. Kwiatkowska, and I. Martinovic. Broken hearted: How to attack ECG biometrics. In *24th Annual Network and Distributed System Security Symposium, NDSS*, 2017.

[45] N. Karimian, D. L. Woodard, and D. Forte. On the vulnerability of ecg verification to online presentation attacks. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 143–151, 2017.

Carmen Camara is Assistant Professor in the Computer Security Lab. at Carlos III University of Madrid, Spain. She holds a PhD. in Computer Science and a PhD in Biomedical Engineering. Her research interests are in the fields of Cybersecurity in e-Health, Bioengineering and Data Science.

Pedro Peris-Lopez is Associate Professor at the Department of Computer Science, Carlos III University of Madrid, Spain. He holds an M.Sc. in Telecommunications Engineering (2004) and PhD. in Computer Science (2008) by Carlos III University of Madrid. His research interests are in the field of cybersecurity and e-health, digital forensics and hardware security. In these fields, he has published a large number of articles in specialized journals (55) and conference proceedings (45). His works have more than 4000 citations, and his h-index is 29. For additional information see: https://www.lightweightcryptography.com/.

Jose Maria de Fuentes is Associate professor in the Computer Science and Engineering Department at Carlos III University of Madrid, Spain. He is Computer Scientist Engineer and Ph.D. in Computer Science by Carlos III University of Madrid. His main research interests are digital evidences management, non-repudiation in vehicular environments, as well as security and privacy in the internet of things and ad-hoc networks. He has published several articles in international conferences and journals. He is participating in several national R+D projects.

Samuel Marchal is a post-doctoral researcher in the secure systems research group at Aalto University. He received the M.Sc. degree in computer science in 2011 from TELECOM Nancy, France. He received the Ph.D. degree in 2015 jointly from the University of Luxembourg and the University of Lorraine, France. He conducted his doctoral research at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) in Luxembourg. His interests lie in system security, network security and machine learning.