Peris-Lopez, P., González-Manzano L., Camara C., de Fuentes, J.M. (2018). Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things . *Future Generation Computer Systems*, 81, pp. 67-77.

DOI: https://doi.org/10.1016/j.future.2017.11.037

Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things

Pedro Peris-Lopez [*], Lorena González-Manzano, Carmen Camara, José María de Fuentes

Computer Security Lab (COSEC), Carlos III University of Madrid, Spain

HIGHLIGHTS

- Security and privacy issues must be addressed in the Internet of Things (IoT).
- We have focused on the use of ElectroCardioGram (ECG) signals for Continuous Authentication (CA).
- We have explored different ECG-based CA techniques for three attacker settings.
- Our results exhibit promising accuracy figures, which support the use of ECG as identifier in the IoT.

ABSTRACT

Wearable devices enable retrieving data from their porting user, among other applications. When combining them with the Internet of Things (IoT) paradigm, a plethora of services can be devised. Thanks to IoT, several approaches have been proposed to apply user data, and particularly ElectroCardioGram (ECG) signals, for biometric authentication. One step further is achieving Continuous Authentication (CA), i.e., ensuring that the user remains the same during a certain period. The hardness of this task varies with the attacker characterization, that is, the amount of information about the attacker that is available to the authentication system. In this vein, we explore different ECG-based CA mechanisms for *known*, *blind-modelled* and *unknown* attacker settings. Our results show that, under certain configuration, 99.5 %of true positive rate can be achieved for a blind-modelled attacker, 93.5 % for a known set of attackers and 91.8 % for unknown ones.

Keywords:
Internet of Things
ElectroCardioGram
Continuous authentication
Attacker model

1. Introduction

Terms such as "wearable computing" and "body-area/body-sensor networks" have been much discussed since around 1995. They represent a wireless network of lightweight portable computers, sensors and actuators located in, on, and around the human body. This idea has traditionally been very well received in areas such as healthcare monitoring, where the possibility of instrumenting a patient with physiological sensors that provide information in almost real time, as well as implantable medical devices that can be remotely managed, is expected to be a significant breakthrough [1].

Internet-of-Things (IoT) devices allow the quick establishment and sharing of information through the Internet and it opens the door to new opportunities for medical devices with wireless connectivity as they facilitate data monitoring and management [2]. For this purpose, Pandey et al. have proposed a cloud-based architecture to remotely monitor and record patients data [3]. Beyond the pure medical usage, the emergence of the IoT paradigm enables using wearable devices for other purposes [4,5]. One of the fields that has received significant research attention is their application for authenticating the users — the so called *biometric authentication*. The term *biometrics* refers to the automatic identification of subjects using their physiological or behavioural patterns [6]. Accordingly, previous efforts have shown the effectiveness of body signals such as ElectroEncephaloGram (EEG) [7], ElectroCardioGram (ECG) [8] or PhotoPlethysmoGram (PPG) [9] signals for this purpose.

One interesting aspect of IoT-based biometric authentication is that smart devices can provide continuous streams of subject data. These data streams can be used for security purposes by analysing them in real-time. In fact, this feature enables taking authentication to the next level — instead of identifying the user at a given point in time, it is possible to perform this verification in a continuous fashion. This security mechanism is widely referred to as Continuous Authentication (CA).[2]

[*] Correspondence to: Avda. de la Universidad, 30 28911, Leganés, Madrid, Spain.
E-mail address: pperis@inf.uc3m.es (P. Peris-Lopez).

[2] Although "Continuous Identification" seems the natural extension of this term, we adopt CA in this paper for consistency with existing works.

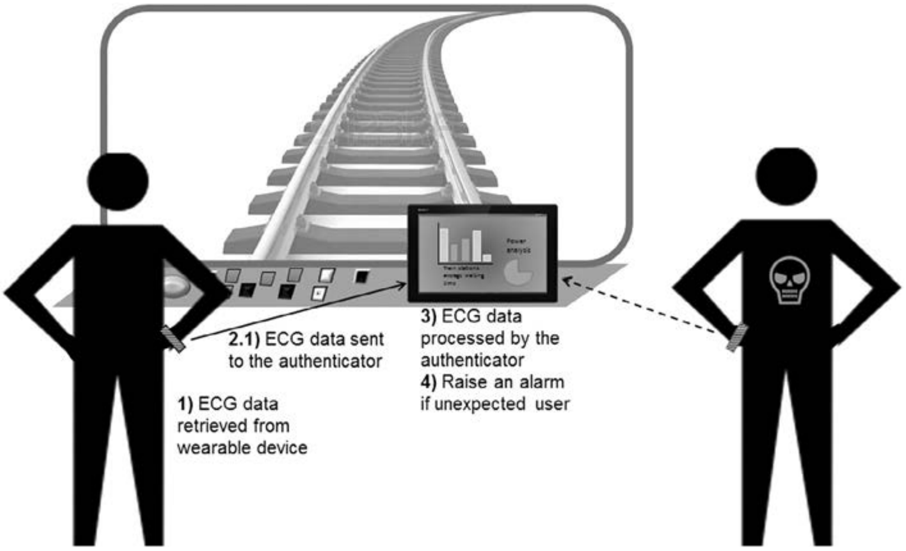
2.1) ECG data sent to the authenticator
3) ECG data processed by the authenticator
4) Raise an alarm if unexpected user
1) ECG data retrieved from wearable device

Fig. 1. Use case example.

Several motivating use cases can be found for CA. For example, consider a safety mechanism in trains that requires ensuring that the train driver has not been impersonated during the whole journey. In another context, a nuclear power plant may need that its supervisor is present and not replaced during a time slot. Both scenarios can be addressed through an IoT-based Biometric CA (IBCA), in which wearable devices monitor users (e.g., their ECG signals) and transmit their data to an authenticator, namely a mobile device with Internet connectivity, which raises an alarm if unexpected users are detected, see Fig. 1. It must be noted that this kind of authentication has been enabled by IoT capabilities, as it would be unfeasible otherwise. Several contributions have already tackled this issue — [10] and [11] are two good examples.

In order to achieve continuous authentication we need to consider the used biometric trait and how to determine if a given trait belongs to the authorized user. Concerning the former issue, ECG signals are a nice alternative for being hard to reproduce [12,13] specially in comparison with other approaches such as the use of fingerprints which can be copied [14] or even the use of authentication tokens like smartcards which can be misplaced, lost or stolen [15]. It is also worth noting that the electrocardiogram is one of the most used physiological signals for security issues [16]. With respect to determining if the trait belongs to the legitimate user, the hardness of this task varies with the attacker characterization, that is, the amount of information about the attacker that is available to the authentication system. According to the literature, there are three degrees of attacker, namely *known attacker*, i.e., it is one of the registered system users; *blind attacker*, i.e., partial knowledge exists about the attacker; *unknown attacker*, i.e., no hints are available about how the attacker behaves. Intuitively, the more knowledge the system has about the attacker, the easier is to tell both user and attacker apart. Going back to the train driver example, it is not the same to determine which driver is working (among those from the company) than detecting if a given driver has been impersonated by an unknown person. However, to the best of authors' knowledge, no previous work has analysed the effect of attacker characterization in this regard. To overcome this limitation, in this paper we propose three ECG-based continuous authentication mechanisms, one for each attacker type. For each one, we study how accurate, immediate and practical it is.

The remaining of this paper is organized as follows. Section 2 introduces used definitions, attacker models and requirements. Section 3 describes the proposal. Section 4 shows the system evaluation. Related work together with a comparison analysis is presented in Section 5. Finally, Section 6 concludes the work and points out future research directions.

2. Preliminaries

In this Section, main concepts are defined (Section 2.1). Afterwards, attacker models are introduced (Section 2.2) and the requirements to comply are presented (Section 2.3).

2.1. Definitions

Let $R_{\mathcal{U}_i}$ an entire ECG record of a user $\mathcal{U}_i$ (or an attacker $\mathcal{A}_i$). In order to prepare this set for our proposed mechanisms, three relevant groupings (or windows) have to be defined. First, the record is divided into chunks of W_C seconds. A vector F of features is extracted for each segment, as explained in Section 3.2.1.

Let W_O be the user observation window, representing the minimal observation unit (in seconds) of the user at stake. Thus, W_O is formed by a set of the said chunks. For each W_O, the average value $(\overline{F})$ of its belonging vectors $\{F(i)\}_{i=1}^{W_o/W_c}$ is computed. Indeed, in continuous authentication applications, the identity of a user is checked each W_O seconds. For the sake of simplicity, in the following explanations and illustrations this average vector is called *ECG sample* and represented as $ECG^k_{\mathcal{U}_i}$ for the user $\mathcal{U}_i$ and the kth observation window.

The last window is the attacker one, of W_A seconds. It represents the amount of time that an impostor may remain in the system. In detail, it is formed by a grouping of observation windows (i.e., $N \times W_O$, where $N \geq 2$).

Regarding the system stakeholders, $\mathcal{U}$ represents the set of users $\mathcal{U}_i$ that are registered in the system, $\mathcal{U} = \{\mathcal{U}_1, \ldots \mathcal{U}_n\}$. For each user $\mathcal{U}_i$, a set of associated ECG samples exists, such that $ECG_{\mathcal{U}_i} = \{ECG^1_{\mathcal{U}_i}, \ldots, ECG^n_{\mathcal{U}_i}\}$ is the set of ECG samples for user $\mathcal{U}_i$.

Apart from registered users, a set $\mathcal{A}$ of attackers $\mathcal{A}_i$ exists, $\mathcal{A} = \{\mathcal{A}_1, \ldots \mathcal{A}_n\}$. As it happened with users, ECG samples are obtained from attackers, such that $ECG_{\mathcal{A}_i} = \{ECG^1_{\mathcal{A}_i}, \ldots, ECG^n_{\mathcal{A}_i}\}$ is the set of ECG samples for attacker $\mathcal{A}_i$.

Before moving into the production environment, each of our authentication mechanisms know one or more registered users. Thus, it is trained with a subset of $ECG_{\mathcal{U}_i}$ and $ECG_{\mathcal{A}_i}$ for every $\mathcal{U}_i$ known and $\mathcal{A}_i$ modelled, respectively. Such an observation is called *ECG user model*.

During the system operation only one user can be active, i.e., a cardiac signal from a legitimate user or an attacker is verified. The system is tested with unknown ECG samples. More precisely, in order to authenticate the user in a continuous way, the system will monitor the user in the interval $\{p, q\}$, thus acquiring $ECG_S^{(obs)} = \{ECG_S^p, \ldots, ECG_S^q\}$. The value of q is conditioned by the used time window, and the value of S depends on the assumed attacker model:

$$S \in \begin{cases} \mathcal{U}_i & \text{Unknown attacker} \\ \{\mathcal{U}_i, \mathcal{A}\} & \text{Blind-modelled attacker} \\ \{\mathcal{U}_i, \mathcal{A}_1 \ldots \mathcal{A}_N\} & \text{Known attacker} \end{cases}$$

$$q = \begin{cases} p & \text{for observed windows of } W_O \text{ secs.} \\ p + (\dfrac{W_A}{W_c} - 1) & \text{for attacker windows of } W_A \text{ secs.} \end{cases}$$

2.2. Attacker models

Our authentication system has to verify the identity of a user $\mathcal{U}_i$ leveraging on a $ECG_S^{(obs)}$ sample, thus avoiding impersonation attacks [17]. To achieve this goal, the system may or may not have knowledge about the attacker $\mathcal{A}$. In particular, based on common attacker models for authentication systems [18,19], three settings are considered:

- **Unknown attacker.** The system only knows $\mathcal{U}_i$, along with their associated ECG user model. The system has no knowledge about $\mathcal{A}_i$ or their respective $ECG_{\mathcal{A}_i}$ samples. In this sort of attacks, a third party attempts to impersonate any authorized user [20].
- **Known attacker.** Under this setting, the system knows $\mathcal{U}_i$ and $ECG_{\mathcal{U}_i}$ for all $\mathcal{U}_i$, as well as $ECG_{\mathcal{A}_i}$ for all $\mathcal{A}_i$. In this kind of attacks, the adversary represents an insider who tries to impersonate any other legitimate user [21].
- **Blind-modelled attacker.** As in the previous case, the system knows $\mathcal{U}_i$ and $ECG_{\mathcal{U}_i}$ for all $\mathcal{U}_i$. Furthermore, the system models $\mathcal{A}$ by a pool of samples (i.e., $\{ECG^1_{\mathcal{A}_1}, ECG^2_{\mathcal{A}_1} \ldots, ECG^1_{\mathcal{A}_N}, ECG^2_{\mathcal{A}_N} \ldots\}$) belonging to a set of possible attackers ($\{\mathcal{A}_i\}_{i=1}^N$). In this model, attackers are in between know and unknown attackers (e.g., in [22], Riva et al. named this sort of adversaries as“known non-owners”).

It must be noted that in this paper we leverage on data retrieved by wearable devices in order to achieve continuous authentication of the holder. However, note that these devices are subject to different threats. Liu and Sun categorize them into integrity, authenticity and privacy ones [23]. In the remainder, we leave this particular type of attacker out of the scope — our proposed strategies are intended to work under the assumption that these threats have already been countered.

2.3. Identifier requirements and feasibility criteria

Our CA mechanisms have to fulfil the commonly adopted identifier requirements [24]:

- **Universality.** In the same way cars have number plates to be identified, every subject should have an identifier which facilitates her/his identification.
- **Uniqueness.** Each subject should only have one identifier to be identified worldwide regardless the authentication procedure. Then, two subjects should have different identifiers.
- **Permanence.** Identifiers should authenticate the subject throughout her/his life and thus, it should not change, nor be changeable.
- **Collectability.** Identifiers could be used in innumerable occasions and times. Then, identifiers should be collectible in any occasion.
- **Acceptability.** Despite the variety of identifiers that could be developed and managed, the use of identifiers should be in line with contemporary social standards.

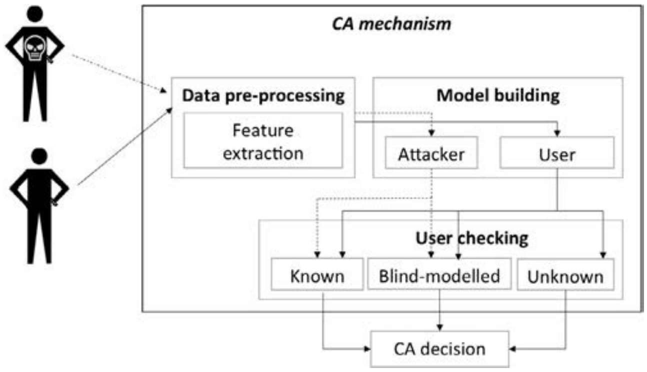

Fig. 2. Overview.

In line with the aforementioned requirements, the feasibility of the proposed mechanisms can be evaluated in terms of:

- **Accuracy.** The system has to authenticate the user against any third party with a high success rate. This implies achieving high True Positive (TPR) and True Negative (TNR) rates.
- **Easy start-up.** The system has to be ready to operate quickly. Thus, the amount of time needed to start operating (referred to as *training period*) has to be as small as possible.
- **Practicality.** The system needs to authenticate the user by retrieving her/his ECG values in a continuous way. Thus, the amount of time the user has to be observed for this purpose (and, thus, the attacker window) has to be as small as possible.

3. Proposal description

This section describes the proposal by firstly presenting an overview (Section 3.1). Then, it is introduced how data is preprocessed (Section 3.2). Afterwards, each of the proposed CA mechanisms are presented. For ease of presentation, we divide them into two groups, namely the one intended to work under the **unknown** attacker model (Section 3.3) and those to work under the characterized one, which covers both the **blind-modelled** and **known** attackers (Section 3.4).

3.1. Overview

The proposed approach presents three different CA mechanisms based on ECG data for different types of attackers (known, blind-modelled and unknown). An overview of all of them is presented in Fig. 2. The system is composed of three building blocks, called data pre-processing, model building and user checking.

At the beginning, ECG signal is collected to be subsequently preprocessed, which includes the extraction of features. This signal is collected from the legitimate user, and eventually from the attacker depending on the particular setting. Then, the model per user (and attacker, if it is the case) is built to be later used.

At the time users try to authenticate, the user checking is carried out. In case of using the known attacker mechanism, attackers and user models come into play, as well as in the case of blind-modelled attackers. However, just the user model is considered when working with the unknown attacker mechanism. Finally, the system outputs a decision on whether the legitimate user is authenticated or not.

3.2. Data pre-processing

Our system relies upon ECG values that are periodically obtained from the subject at stake. However, in order to perform authentication decisions, there are several steps to be carried out. Such a pre-processing algorithm is depicted in Fig. 3.

Before dealing with the ECG records, the first step is to filter out all noise (step 1, Fig. 3). For this purpose, firstly the DC component is eliminated. Then, the ECG signals are passed through a pass-band filter. Afterwards the ECG records are segmented into chunks without overlapping (step 2, Fig. 3) to continue with feature extraction.

3.2.1. Feature extraction

In order to extract features from the ECG signal, two main approaches have been proposed in literature, namely fiducial-based and non-fiducial methods. In the former, characteristic points, like amplitude or duration of the QRS complex are extracted [25,26]. Contrarily, non-fiducial methods compute some features, like auto-correlation or Fourier transform coefficients, applying spectral analysis techniques over the signal [27,28]. In this paper, we opt for this second approach. In particular, we obtain the features via the Walsh–Hadamard Transform (WT) [29] (step 3, Fig. 3). This transform is advisable to use for ECG signals, and biomedical signals in general terms, since it is efficient from the computing (matrix multiplication) and storage point of view (signal compression) [30,31].

WT consists on a projection of the signal onto a set of orthogonal and rectangular waveforms called Walsh functions. The forward and inverse WT of a data sequence $x(n)$ of length N, where $M = \log_2 N$, are given below:

$$X_w(k) = \sum_{n=0}^{N-1} x(n) \prod_{i=0}^{M-1} (-1)^{n_i k_{M-1-i}}, \qquad k = 0, 1, \ldots, N-1 \qquad (1)$$

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X_w(k) \prod_{i=0}^{M-1} (-1)^{n_i k_{M-1-i}}, \qquad n = 0, 1, \ldots, N-1. \quad (2)$$

Note that the WT of x can be interpreted as the matrix multiplication between the aforesaid data sequence and the Walsh matrix (H). That is, $X_w = Hx$.

Thus, a set of coefficients $X_w(k)$, where $k = 0, 1, \ldots, N-1$, are obtained for each chunk. After that, set a window of length W_O (for simplicity W_O is restricted to be a multiple of W_C seconds), an average value for each coefficient is computed for this observation window, (step 4 of Fig. 3):

$$F(k) = \frac{1}{W_O/W_C} \sum_{i=1}^{W_O/W_C} X_w^i(k), \qquad k = 0, 1, \ldots, N-1. \qquad (3)$$

Therefore, an average vector $\overline{F} = [\overline{F}(1)\ \overline{F}(2)\ \ldots \overline{F}(N-1)]$ (set of features of length $1 \times N$) is computed for each observed window of W_O seconds. As previously stated in Section 2.1, for the sake of clarity, this average vector is represented as ECG_S^k for $S \in \{\mathcal{U}_i, \mathcal{A}\}$ and the kth observation interval. The reasoning behind using an average value is motivated by the target application. Commonly ECG sensors sample the cardiac signal in a continuous way taking many samples per second, however, the term “continuous” in continuous authentication is less demanding.

3.3. ECG-based CA mechanism with unknown attacker

In this setting, the CA mechanism is intended to work in scenarios in which it is possible to monitorize a given user for a long time period and the knowledge beforehand about the attacker is zero. A realistic scenario is a smartphone authentication mechanism — the device can retrieve ECG values from its legitimate user, but it does not know anything about a potential impostor.

The system operation follows the architecture described in Fig. 2. Once data pre-processing has been presented (recall Section 3.2), we hereby describe how model building and user checking issues are carried out. The pseudo-code of both phases is displayed in Algorithm 1.

```
Data: $R_{\mathcal{U}_i}$, an entire ECG record of a user $\mathcal{U}_i$; $th$, threshold
      value; $trainSize$, percentage of samples used to train
      the system; $ECG_{\mathcal{U}_i}^{(obs)}$, pre-processed ECG signal
      observed from user $\mathcal{U}_i$ during a timeframe.
Result: ⊤ if the observed data corresponds to $\mathcal{U}_i$, ⊥
        otherwise
begin Model building phase
    TimeTotal = size($R_{\mathcal{U}_i}$);
    TimeModel = TimeTotal * trainSize ;
    UserModel = { $ECG_{\mathcal{U}_i}^1, \cdots, ECG_{\mathcal{U}_i}^{TimeModel}$ } ;
    Half1Model = { $ECG_{\mathcal{U}_i}^1, \cdots, ECG_{\mathcal{U}_i}^{TimeModel/2}$ } ;
    Half2Model = { $ECG_{\mathcal{U}_i}^{(TimeModel/2)+1}, \cdots, ECG_{\mathcal{U}_i}^{TimeModel}$ } ;
    RefDist = distanceCalc(Half1Model, Half2Model) ;
end
begin User checking phase
    ObsDist = distanceCalc(UserModel, $ECG_{\mathcal{U}_i}^{(obs)}$) ;
    if $ObsDist \in (RefDist - th , RefDist + th)$ then
        return ⊤ ;
    else
        return ⊥ ;
    end
end
```

Algorithm 1: ECG-based CA mechanism with unknown attacker

In the model building phase, features vectors obtained after data pre-processing are at stake, that is, *ECG user model* is created. In particular, this set is divided into two parts. With both subsets, a distance is computed. Such a distance (called *RefDist*) is taken as reference for further comparisons in the next phase. The rationale behind this is that ECG samples from each user may be distributed in such a way that the distance between them may serve to tell users apart.

In the user checking phase, the subject is observed for a period of W_A seconds. During this period, ECG signal is recorded, pre-processed and features are extracted (i.e., $ECG_{\mathcal{U}_i}^{(obs)}$). After this initial phase, the distance of this set to the ECG user model is computed (called *ObsDist*). The user is authenticated if Eq. (4) holds, in which *th* is a system variable that represents the tolerance of the authentication system against variations in the distance.

$$ObsDist \in (RefDist - th, RefDist + th). \qquad (4)$$

3.4. ECG-based CA mechanisms with characterized attacker

In the previous section no knowledge about the attacker is assumed. Nevertheless the attacker can be modelled using ECG datasets of users non-registered in the system. We have explored two approaches that restrict the attacker knowledge to a greater or lesser extent.

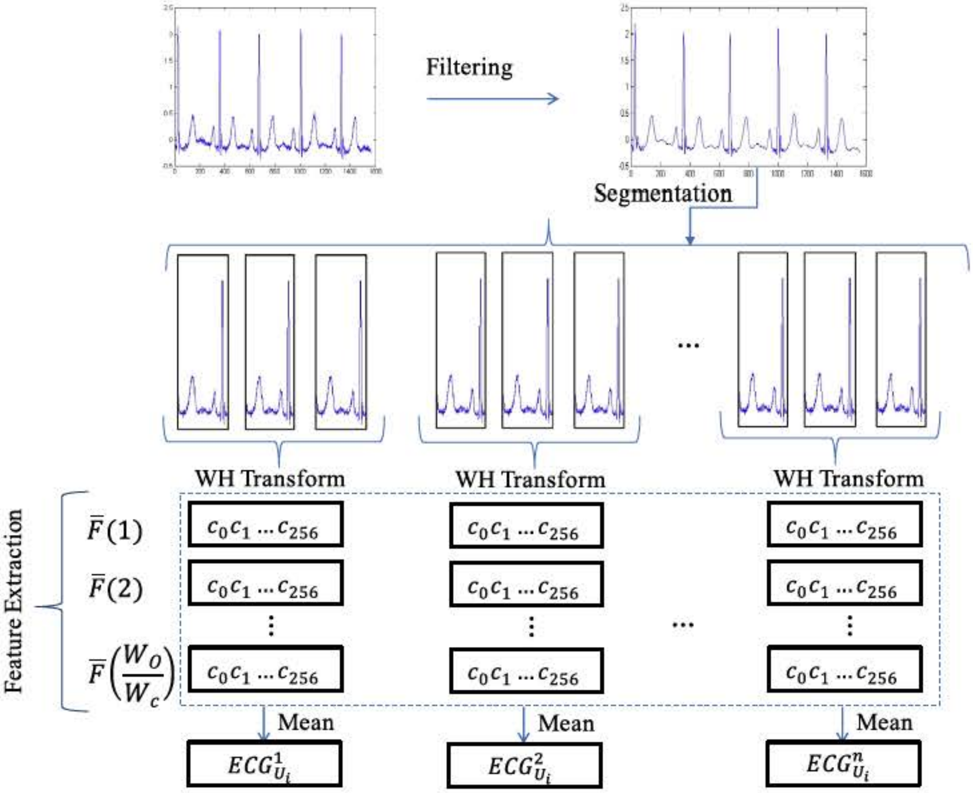

Fig. 3. Data pre-processing procedure.

In the blind-modelled attacker, the attacker is modelled by a set of non-legitimated users. This could be the case of a car-sharing company with a great amount of drivers register in the system and with a huge amount of potential attackers who will attempt to drive for free. Mathematically,

$$\begin{cases} \{ECG^1_{\mathcal{U}_i}, ECG^2_{\mathcal{U}_i}, \dots\} \in \mathcal{U}_i \\ \{ECG^1_{\mathcal{A}_1}, ECG^2_{\mathcal{A}_1} \dots ECG^1_{\mathcal{A}_N}, ECG^2_{\mathcal{A}_N} \dots\} \in \mathcal{A}. \end{cases}$$

On the contrary, in the known attacker model, attackers ($\mathcal{A}_i$) are not grouped into a single class but each of them is categorized as a different attacker class ($\mathcal{A}_i$). Therefore, this can be seen as an identification problem in which all the users, legitimated and attackers, are registered in the system — this can be the scenario of a company in which all the users are registered, however, each of them does not have the same privileges. In case of a user attempting to scale privileges, s/he would be considered an attacker. Similarly as in the previous one, the model can be mathematically expressed as:

$$\begin{cases} \{ECG^1_{\mathcal{U}_i}, ECG^2_{\mathcal{U}_i}, \dots\} \in \mathcal{U}_i \\ \{ECG^1_{\mathcal{A}_1}, ECG^2_{\mathcal{A}_1}, \dots\} \in \mathcal{A}_1 \\ \dots \\ \{ECG^1_{\mathcal{A}_N}, ECG^2_{\mathcal{A}_N}, \dots\} \in \mathcal{A}_N. \end{cases}$$

The pseudocode of instance classification algorithm is shown in Algorithm 2. As it happened in the known attacker approach (Section 3.3), the process is divided into two steps as was illustrated in Fig. 2. In the training phase, using a subset of samples belonging to $ECG_{\mathcal{U}_i}$ and $ECG_{\mathcal{A}_i}$, the ECG user model is generated. In our particular case, the training is minimal and all the training samples are retained as part of the model. Then the model is tested with unseen observed samples $ECG^{(obs)}_S$. As it can be seen, the differences with the mechanism under the unknown attacker model reside in the way the model is built and in the adoption of a majority voting procedure among several labels for taking the authentication decision.

```
Data: $ECG$: matrix of ECG samples in which each row $ECG^k_S$,
      where $k = \{1, \cdots, m\}$, corresponds to an ECG frame of
      $W_O$ seconds ; $C$: vector of class labels, where each
      element $C^k \in S$ (being $S$ as defined in Section 2.1);
      $ECG^{(obs)}_S$: unseen ECG sample.
Result: class label for $ECG^{(obs)}_S$
begin
    for $k \leftarrow 1$ to $m$ do
        Compute distance $d(ECG^k_S, ECG^{(obs)}_S)$;
    end
    Compute set $I$ containing indices for the $K$ smallest
    distances $d(ECG^k_S, ECG^{(obs)}_S)$ ;
    return majority label for $\{C_i$ where $i \in I\}$
end
```

Algorithm 2: Classification algorithm for ECG-based CA with characterized attacker: Classify($ECG, C, ECG^{(obs)}_S$)

4. Evaluation

This Section discusses the satisfaction of the identifier-related requirements (Section 4.1). The evaluation of the system accuracy for each attacker setting is also described (Section 4.2). A discussion on the overall accuracy and workability of the proposed mechanisms is finally presented (Section 4.3).

4.1. Achievement of identifier-related requirements and feasibility criteria

ECG-based continuous authentication complies with the imposed identifier-related requirements since ECG signals can be

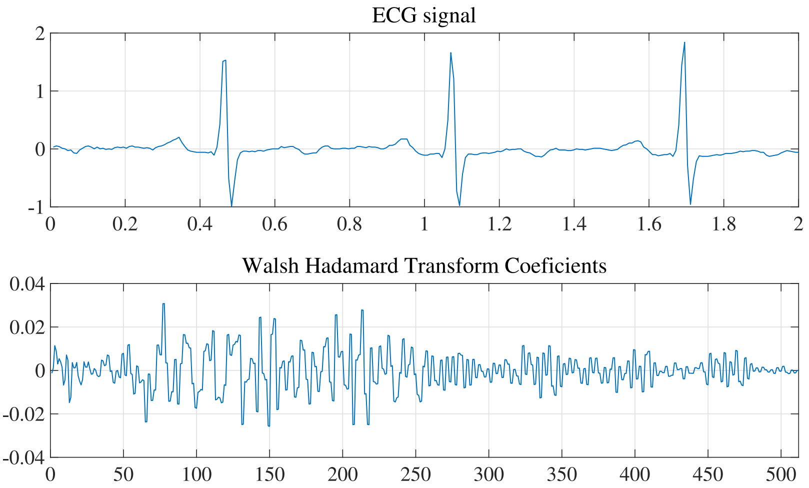

Fig. 4. ECG signal and Walsh–Hadamard spectrum.

retrieved for any individual (universality); are not changed if the person is healthy and there are not significant changes in her/his physical activity (permanence); can be retrieved at any time (collectability); and are available through wearable devices, which is a growing trend (acceptability). The discussion on uniqueness is deferred to Section 4.3, since it is related to the accuracy issues addressed in the next section.

4.2. Accuracy evaluation

After presenting the experimental settings (Section 4.2.1), the accuracy of proposed approaches per each attacker model is studied separately (Sections 4.2.2–4.2.4).

4.2.1. Experimental settings

The considered dataset comes from PhysioBank, and more precisely, MIT-BIH Normal Sinus Rhythm dataset has been used [32]. The reasoning of using this dataset is twofold. On the one hand, it includes long-term recordings (around 24 h) of subjects observed at Boston's Beth Israel Hospital. On the other hand, the subjects do not have significant arrhythmias — that is, the population is homogeneous without any bias between individuals. Ten of the whole set of individuals have been used for our experimentation.

ECG signals are passed through a pass-band filter to eliminate noise. Regarding this filter, the lower-cut off frequency is set to 0.67 Hz to avoid the noise due to the respiration and the upper-cut-off frequency is fixed to 45 Hz as a trade-off between eliminating the power-line noise and preserving as much information as possible of the original signal. Then, since an individual, without cardiac ailments, beats between 60 and 100 times per minute, the chunk length is fixed in 2 s (i.e., $W_C = 2$ s). Therefore, each chunk includes 2 or 3 heart beats. We have used this value inspired on the fact that a chunk length of several seconds is a common value used in ECG identification proposals [16].

For feature extraction, depicted in Fig. 4, we sketch 2 s of an ECG signal and its corresponding 512 initial coefficients of the WT. As it can be observed, lower frequency coefficients keep most of the signal information. In our experimentation only the lower 256 ($N = 256$) coefficients are used as a commitment to system efficiency and storage requirements.

Finally, note that for the case of unknown attacker, without loss of generality, we adopt Mahalanobis [33], although eventually any distance could be applied. By contrast, for a characterized attacker, for the classification of the instances we opt for non-parametric algorithms, since they do not make any assumption about the data distribution. In particular, we use a K-Nearest Neighbour (KNN) [34]. KNN is a lazy algorithm, meaning that it avoids to do generalizations with the training data, which is quite reasonable for the CA problem. KNN parameters have been tuned in order to maximize the TP rate and minimize FP rate. After conducting a battery of experiments, the number of neighbours (K) is fixed to 5 (an odd number is commonly used whether the number of classes is 2 to avoid ties in the majority voting [35]) and the euclidean distance [36,37] has been employed as distance metric.

4.2.2. Unknown attacker model

In the harder settings (unknown attacker model) only a user $\mathcal{U}_i$ is known and observed along different time slots (windows of attack), from 30 min ($W_A = 18 \cdot 10^2$ s) to 200 min ($W_A = 12 \cdot 10^3$ s). Once ECG signals are processed, considering 35% of data as training set, the best results are achieved for observed ECG windows of 1 min (i.e., $W_O = 60$ s) and *th* 1, thus the study presented herein considers this setting. True Positive (TPR) and True Negative (TNR) rates for different W_A are presented in Fig. 5. The maximization of TPR and TNR is the main goal, that is when both parameters cross each other. In this context, the best W_A is between 70–75 min, such that TPR is 90.63% and 91.85% and TNR is 92.08% and 91.94% respectively. One important benefit of this approach is that, though it would be desirable the reduction of W_A, no previous information about other users is required.

4.2.3. Blind-modelled attacker model

In the blind attacker model the user $\mathcal{U}_i$ is known and the unknown attacker $\mathcal{A}$ is modelled by a set of possible non-legitimated users, nine users in the conducted experiments (recall that the used dataset is composed of 10 users, Section 4.2.1). For each individual, we have carried out the KNN classification with two classes, namely the target individual class $\mathcal{U}_i$ and the adversary class $\mathcal{A}$, as described in Section 3.4.

Table 1 shows the results for each subject. It can be seen that all of them are quite similar to each other. An overall value has been computed, resulting a 99.5% of TPR and a 94.1% of TNR. Furthermore, the ROC Area is 0.993, which is a value very close to the optimal (ROC= 1.0), and thus the accuracy of the classifier can be categorized as excellent.

Additionally, we have tested how much the algorithm can be tight in terms of reducing the size of the training dataset. As shown in Table 2, the percentage of data used for training can be reduced drastically without a significant performance deterioration. In particular if the training set is drastically reduced from 60% to 20% or

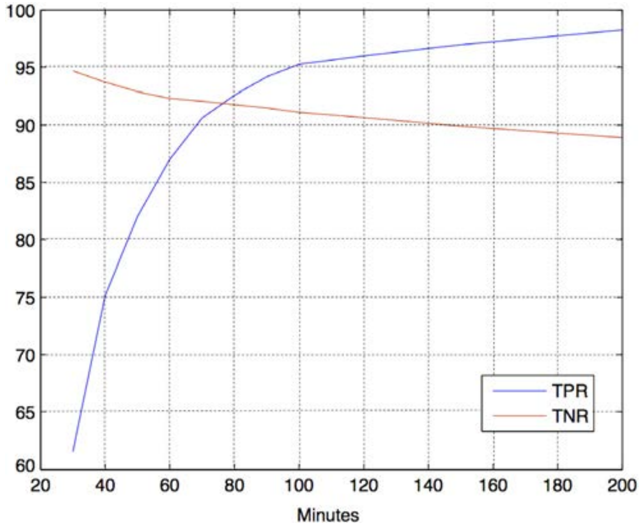

Fig. 5. Results for different windows of attack in the known attacker setting.

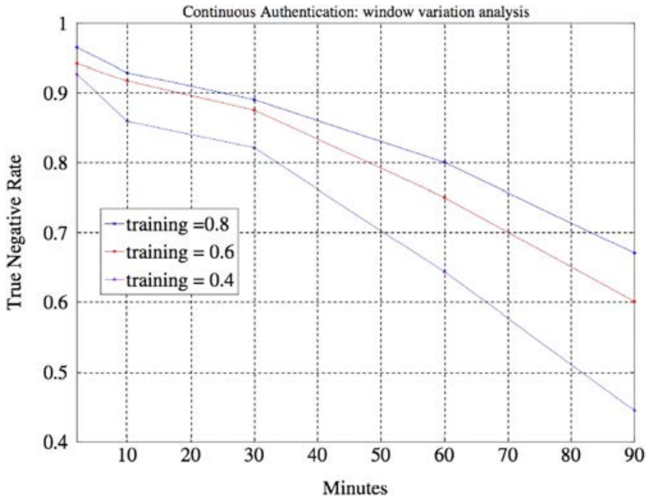

Fig. 6. Blind-modelled attacker model: Results for different ECG observed windows.

Table 1
ECG-based continuous authentication: blind-modelled attacker model.

Subject 1		Subject 2	
TP Rate	99.2%	TP Rate	99.6%
TN Rate	99.2%	TN Rate	88.3%
ROC Area	0.996	ROC Area	0.9860
Subject 3		Subject 4	
TP Rate	99.6%	TP Rate	100%
TN Rate	94.2%	TN Rate	92.9%
ROC Area	0.992	ROC Area	0.987
Subject 5		Subject 6	
TP Rate	100%	TP Rate	100%
TN Rate	92.1%	TN Rate	93.73%
ROC Area	0.991	ROC Area	0.996
Subject 7		Subject 8	
TP Rate	100%	TP Rate	98.8%
TN Rate	93.3%	TN Rate	94.2%
ROC Area	0.991	ROC Area	0.996
Subject 9		Subject 10	
TP Rate	99.2%	TP Rate	98.8%
TN Rate	96.7%	TN Rate	96.2%
ROC Area	0.999	ROC Area	0.997
Overall			
TP Rate	99.5%		
TN Rate	94.1%		
ROC Area	0.993		

Table 2
Blind-modelled attacker model: training size analysis.

% of training	Minutes for training	TP Rate	TN Rate
1	14	87.7%	62.1%
2	28	100%	66.9%
4	56	100%	75.3%
8	112	100%	84.3%
10	140	99.7%	86.0%
20	280	100%	92.4%
40	560	99.8%	93.9%
60	840	99.6%	97.3%

10% , the TPR remains almost constant and the TNR gets worse in only a 5% or 12%.

In all the above experiments the ECG observation time window is set to 1 min ($W_O = 60$ s). The system performs well using this window length and this value has been tuned through experimentation. For completeness, we have tested the CA system when the ECG observed time frame is varied — it would be equivalent to the window of attack W_A studied in Fig. 5. The TPR almost remains constant and close to the optimal 100% value for all the windows length — only a slight degradation is observed when W_O is bigger than the 60 min threshold. In Fig. 6 the TNR is displayed. If the lower allowed threshold for the TNR is set to 90% the observation window can be increased up to 25, 18 and 5 min for a training set of 80%, 60% and 40% respectively — the TPR is 100% for these three points.

4.2.4. *Known attacker model*

Finally we have assessed the authentication mechanism in which both the legitimate user $\mathcal{U}_i$ and a set of possible attackers $\{\mathcal{A}_i\}_{i=1}^N$ (e.g., legitimate system users with less access privileges) are registered. Similarly as in the blind attacker model, we have tested a KNN classification but instead of 2 classes, the user $\mathcal{U}_i$ and nine possible attackers ($\{\mathcal{A}_1 \ldots \mathcal{A}_9\}$) are the existing ones. The results shown in Table 3 clear point outs the excellent performance of the system. TPR and TNR are 93.5% and 99.3% respectively. Additionally, the ROC Area (0.99) is almost the optimal value and, once again, the classifier can be categorized as excellent.

4.3. *Discussion on uniqueness and workability*

According to the results shown in the previous section, the accuracy of the studied approaches for all the proposed attacker settings is satisfactory, thus also addressing the requirement of uniqueness. This is because an identifier derived from the ECG signal in this case is proven to be different and unique per subject, though with some limitations depending on the attacker setting.

With respect to feasibility of the proposed mechanisms, apart from the already discussed accuracy, the remaining ones are practicality and easy set-up. Regarding the first one, when the unknown attacker model is at stake, the window of attack has to be high (70 min) to achieve successful results. By contrast, the remaining models are not limited by this feature. In this sense, the unknown attacker setting is the least practical, but it may be the only option if no assumptions can be made about the attacker. With respect to the set-up easiness, the unknown attacker approach is the best choice since the training set needed is 35%, quite smaller in comparison with the characterized attacker model in which 80% of data is required to achieve competitive results. Note that 60% and 80% are common values for classification problems in the training phase [35,38].

Table 3
ECG-based continuous authentication: known attacker model.

Accuracy – Weighted Average	
TP Rate	93.5%
TN Rate	99.3%
ROC Area	0.99

	$\mathcal{U}$	$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$	$\mathcal{A}_4$	$\mathcal{A}_5$	$\mathcal{A}_6$	$\mathcal{A}_7$	$\mathcal{A}_8$	$\mathcal{A}_9$
$\mathcal{U}$	271	0	9	0	1	0	0	1	0	1
$\mathcal{A}_1$	0	243	3	10	0	1	19	1	6	0
$\mathcal{A}_2$	0	9	262	4	2	0	0	0	6	0
$\mathcal{A}_3$	0	3	12	249	10	0	0	0	9	0
$\mathcal{A}_4$	2	0	11	1	269	0	0	0	0	0
$\mathcal{A}_5$	1	3	2	1	0	274	0	2	0	0
$\mathcal{A}_6$	0	8	0	0	0	1	271	2	1	0
$\mathcal{A}_7$	0	0	0	2	0	8	0	273	0	0
$\mathcal{A}_8$	0	8	7	3	0	0	0	0	264	1
$\mathcal{A}_9$	2	3	0	2	2	0	0	3	0	271

5. Related work

Biometrics has been extensively used for authentication purposes. For instance, the hand shape is used for this purpose [39]. The study of voice, face and gesture for authentication purposes in mobile devices is also a research line [40]. Another novel example is the use of the accelerometer sensor and touchscreen in smart devices [41]. Biometric signals are also used for authenticating users, i.e., PPG signal [42], EEG signal [7] or ECG signal [28,43–45]. Combination of different biometric features are also applied, such as ECG, Galvanic Skin Response (GSR) and airflow signals [46].

In addition, biometrics has also been widely used for continuous authentication, also by means of assorted features. For instance, Niinuma et al. [47] use the facial skin and colour clothes to authenticate users. In the context of mobile devices facial [48,49] and touch screen recognition [50–52] have been applied. Signal processing has also been used in this field, particularly PPG and ECG signals. Although some proposals work with PPG [53,54], here we focus on those related to ECG signals since electrocardiograms are a richer signal from the information point of views — PPG signals only provide beats and average heart rate. Indeed, ECG signals have the advantage of being robust against the application of falsified credentials [12]. In detail, P, Q, R, S and T waves characterize the ECG waveform, the amplitude of P wave remains constant throughout the life and amplitude of the remaining waves changes on small scale [13].

In the literature we can find how ECG signals have been significantly used for individuals' continuous authentication. In [26], the QRS complex, the most stable component of ECG signal, is applied in the continuous authentication process. Experiments aim to analyse the permanence and stability of the biometric features extracted from the QRS complex in ECG signals on a time period of a day. Guennoun et al. [55] present the use of several features of the ECG signal to perform continuous authentication. Mahalanobis distance is calculated between a heartbeat and a previously stored one such that results depend on a threshold when the process is repeated for 35 heartbeats. The negative side is that this model is not explained in detail and the experimentation is quite limited — ECG signals are short (15 min per user) and each experiment lasts for 30 s. In [56] Autocorrelation/Linear Discriminant Analysis (AC/LDA) algorithm is applied for the design of the biometric features extracted from the ECG signal. In the experiments a set of 10 users starts doing different activities during 5 min to be authenticated every 5 s. A different approach is proposed in [57,58], in which the ECG signal is converted into strings to be later classified. Again, the experimental part is limited in both proposals –data of 10 and 19 subject is recorded along 10 min. Interestingly, Derawi et al. [59] creates an ECG sensor to collect ECG data to later apply cycle detection of the pulse/heart rate of users. Though the number of subjects involved in the evaluation is higher regarding other works, just data during 5 sessions of 1 min is recorded. New ECG feature extraction techniques are proposed in [60,61]. However, while 112 subjects take part in the evaluation of [60], just 30 subjects along 30 s in [61]. Pasero et al. [62] use neural networks to classify ECG and discriminate between users of a given system and attackers — 40 subjects take part in the experiments and they get the maximum possible success rate. By contrast, support vector machines are applied in [63,64] for ECG data classification. In both works a small set of data is part of the experimental setting. However, [63] claims to get an almost perfect recognition rate. A quite different approach presents [65], it combines the use of ECG and PCG signal for cardiac recognition using decision fusion but, again, evaluation data is quite reduced.

5.1. Comparison analysis

In this section, we compare a variety of security approaches related to authentication with ECG signals. In addition, the most representative ECG-based works for continuous authentication are also studied herein. More precisely, the following features are studied per approach:

Table 4
Comparison analysis.

Approach	Accuracy	Fiducial features (F)/non-fiducial (NF)	Authentication (A)/Continuous Authentication (CA)	Number of subjects	Size of observations per subject	Type of attacker
Our Proposal	TPR 90.63–91.85% TNR 92.08–91.94%	NF	CA	185	24 h	Unknown
	TPR 99.5% TNR 94.1%	NF	CA	10	24 h	Blind-Modelled
	TPR 93.5% TNR 99.3%	NF	CA	10	24 h	Known
[58]	TPR 99.6% TNR 99.6%	NF	CA	19	10 min	Known
[26]	TPR 85%–95% TNR 85%–95%	F	CA	185	24 h	Known
[55]	TNR 84%	F	CA	15	15 min	Unknown
[56]	TPR 99.63% TNR 67%	F	CA	10	–	Known
[43]	TPR 83% TNR 83%	–	A	81	3 min	Known
[45]	TPR 70%–71% TNR 67%–70%	F	A	10	2 min	Unknown
[60]	TPR 100%* TNR 99.72%*	F	A	112	40 min	Known
[59]	TPR 97.5% TNR 96.7%	F	A	30	5 min	Known
[61]	TPR 98%–99%	F	A	18	Few secs. (12 QRS samples)	Known
[28]	TPR 95.5–98.8%* TNR 93.8–98.4%*	NF	A	52	4 min	Known
[44]	TPR 94.8% TNR 98.1%	NF	A	28	30 s	Known
[62]	TPR 95% TNR 90%	NF	A	40	3 min	Known
[63]	TPR 90%	NF	A	5	5 min	Known
[64]	TPR 87.28%*	NF	A	17	4 min	Known
[65]	TPR 95% TNR 96.5%	NF	A	21	3 min	Known

Legend: (–) No specified.
* When multiple experiments are carried out the best results are presented.

- **Accuracy** is studied in regard to TPR and TNR. These metrics are common performance values for biometrics and also are the metrics applied in our experiments.
- **Fiducial (F)/ Non-fiducial features (NF)** are the two general existing approaches for feature extraction. We distinguish between approaches that use characteristics points of the ECG signal in the time domain (e.g., amplitude difference between S and T peaks or time intervals between two consecutive R peaks) and solutions that extract features in a frequency domain (e.g., Fourier or Hadamard domain).
- **Authentication (A)/ Continuous authentication (CA)** are the applied techniques, while the former refers to the identification of a user at a particular time, the latter refers to the authentication of a subject along a period of time. That is, in CA the user credentials are checked at regular time intervals and the distance between intervals is conditioned by the intended application.
- **Number of subjects** and **Size of observations per subject** involved in their evaluation. These variables show the overall size of their experiments. Furthermore, the larger the value of these variables is, a greater confidence on the results and extracted conclusions, can be guaranteed.
- **Type of attacker** corresponds to the assumption of having a known, a blind-modelled or an unknown attacker. These are the three attacker settings considered in our experiments.

The proposed comparison is depicted in Table 4 — a total of fifteen representative works have been studied. For the sake of this paper, one key remark is that the vast majority of works (87%) assume a known attacker setting, whereas the remaining ones (13%) deal with the unknown attacker. Nevertheless, to the best of the authors knowledge, there is no paper working under the blind-modelled setting. This latter setting is very interesting in a business scenario in which a wide amalgam of legitimate users with different access privileges coexist.

With respect to the achieved accuracy, our results (i.e., $TPR =$ 90.63–91.85% and $TNR =$ 92.08–91.94%) notably outperform existing ones when the attacker is unknown. In the known attacker setting and considering the CA problem, our proposal (i.e., $TPR =$ 93.5% and $TNR = 99.3\%$) surpasses the fiducial based approaches and offers similar results with respect to the non-fiducial based solutions. Continuing with the known attacker setting, our results are similar to previous authentication proposals (e.g., [59] or [44]), regardless of the features used. Lastly, it is worth noting that the blind-modelled setting cannot be compared with previous works since this attacker model has not been formerly considered.

In relation to the features extraction, the situation is balanced between fiducial and non-fiducial based approaches when the authentication problem is tackle. Nevertheless, the use of fiducial features is the dominant (75%) existing approach in CA solutions, although it renders worst results. As in [58], our approach doest not extracts features in the time domain (non-fiducial based approach). In particular, our proposal exploits the benefits of working in the Hadamard domain as explained in Section 3.

One key differentiating factor between our proposal and previous works is the size of the dataset. This size can be computed by multiplying the overall number of subjects by the time period during which a subject is observed. Accordingly, our dataset is on average 30 times larger than the ones used in previous works. We would like to highly note that in our experiments, 24 h of continuous ECG data is used for each individual. This ECG record length is only used in another proposal [26], but results are slightly worse in comparison with ours.

6. Conclusions

The use of wearable devices to extract biosignals that can be shared leveraging the Internet of Things (IoT) opens up the door to promising security applications. In this paper, we have focused on the use of ElectroCardioGram (ECG) signals for Continuous Authentication (CA). Such application is possible thanks to IoT, enabling an authenticator to process ECG data. However, a proper design of an IoT-enabled CA mechanism needs to take the attacker into account. Thus, the key difference with existing works is that we present three different mechanisms for known, unknown and blind attacker settings. In this way, we study the effect of attacker characterization. Our results exhibit promising accuracy figures, which support the use of ECG data as an identifier. Moreover, balanced practicability and reasonable easiness for the set-up are achieved in the three settings.

Future work will have three main directions. First, the use of variable ECG records (e.g., data recorded during physical activities) will be considered. Second, the use of another vital signals (e.g., EEG or GSR) will also be explored in the context of CA. Finally, the adoption of mobile-edge or fog computing schemes in this context will be assessed, taking into consideration the underlying security and privacy requirements.

Acknowledgements

Funding: This work was supported by the MINECO grant TIN2013-46469-R (SPINY: Security and Privacy in the Internet of You); by the CAM grant S2013/ICE-3095 (CIBER-DINE: Cybersecurity, Data, and Risks), and by the MINECO grant TIN2016-79095-C2-2-R (SMOG-DEV — Security mechanisms for fog computing: advanced security for devices). L. González and J. M. de Fuentes were also supported by the Programa de Ayudas para la Movilidad of Carlos III University of Madrid, Spain (MPP2017/MI-MA).

Authors would also like to thank the anonymous reviewers for their comments.

References

[1] S. Ullah, P. Khan, N. Ullah, S. Saleem, H. Higgins, K.S. Kwak, A review of wireless body area networks for medical applications, Int. J. Commun. Netw. Syst. Sci. 2 (8) (2009) 797–803.
[2] Cognizant, The internet of things: An excellent prognosis for medical device makers, Cognizant 20–20 Insights.
[3] S. Pandey, W. Voorsluys, S. Niu, A. Khandoker, R. Buyya, An autonomic cloud environment for hosting ECG data analysis services, Future Gener. Comput. Syst. 28 (1) (2012) 147–154.
[4] P. Hu, H. Ning, T. Qiu, Y. Xu, X. Luo, A.K. Sangaiah, A unified face identification and resolution scheme using cloud computing in internet of things, Future Gener. Comput. Syst. (2017).
[5] S. Kumari, X. Li, F. Wu, A. K.D., K.K.R. Choo, J. Shen, Design of a provably secure biometrics-based multi-cloud-server authentication scheme, Future Gener. Comput. Syst. 68 (2017) 320–330.
[6] A. Jain, R. Bolle, S. Pankanti, Biometrics: Personal Identification in Networked Society, Vol. 479, Springer Science & Business Media, 2006.
[7] A. Mukherjee, G. Dey, M. Dey, N. Dey, Web-based intelligent EEG signal authentication and tamper detection system for secure telemonitoring, in: Brain-Computer Interfaces, Springer, 2015, pp. 295–312.
[8] C. Camara, P. Peris-Lopez, J.E. Tapiador, Human identification using compressed ECG signals, J. Med. Syst. 39 (11) (2015) 148.
[9] N. Karimian, M. Tehranipoor, D. Forte, Non-fiducial ppg-based authentication for healthcare application, in: IEEE EMBS International Conference on Biomedical Health Informatics (BHI), 2017, pp. 429–432.
[10] A. Riera, S. Dunne, I. Cester, G. Ruffini, Starfast: a wireless wearable EEG/ECG biometric system based on the enobio sensor, in: International Workshop on Wearable Micro and Nanosystems for Personalised Health, 2008.
[11] S. Led, J. Fernández, L. Serrano, Design of a wearable device for ECG continuous monitoring using wireless technology, in: 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 2, IEEE, 2004, pp. 3318–3321.
[12] P. Sasikala, R. Wahidabanu, Robust R peak and QRS detection in electrocardiogram using wavelet transform, Int. J. Adv. Comput. Sci. Appl. 1 (6) (2010) 48–53.
[13] Y.N. Singh, S.K. Singh, Evaluation of electrocardiogram for biometric authentication, J. Inf. Secur. 3 (1) (2012) 39–48.
[14] Y. Zhang, P. Xia, J. Luo, Z. Ling, B. Liu, X. Fu, Fingerprint attack against touch-enabled devices, in: Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, ACM, 2012, pp. 57–68.
[15] R. Amin, N. Kumar, G. Biswas, R. Iqbal, V. Chang, A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment, Future Gener. Comput. Syst.
[16] I. Odinaka, L. Po-Hsiang, A.D. Kaplan, J.A. O'Sullivan, E.J. Sirevaag, J.W. Rohrbaugh, ECG biometric recognition: A comparative analysis, IEEE Trans. Inf. Forensics Secur. 7 (6) (2012) 1812–1824.
[17] P. Gope, T. Hwang, Bsn-care: A secure iot-based modern healthcare system using body sensor network, IEEE Sens. J. 16 (5) (2016) 1368–1376.
[18] A. Moini, A.M. Madni, Leveraging biometrics for user authentication in online learning: a systems perspective, IEEE Syst. J. 3 (4) (2009) 469–476.
[19] H. Xu, Y. Zhou, M.R. Lyu, Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones, in: Symposium On Usable Privacy and Security, SOUPS, Vol. 14, 2014, pp. 187–198.
[20] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, D. Song, On the feasibility of side- channel attacks with brain- computer interfaces, in: Proceedings of the 21st USENIX Conference on Security Symposium, USENIX Association, 2012.
[21] H.G. Kayacik, M. Just, L. Baillie, D. Aspinall, N. Micallef, Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. arXiv preprint arXiv:1410.7743.
[22] O. Riva, C. Qin, K. Strauss, D. Lymberopoulos, Progressive authentication: Deciding when to authenticate on mobile phones, in: USENIX Security Symposium, 2012. pp. 301–316.
[23] J. Liu, W. Sun, Smart attacks against intelligent wearables in people-centric internet of things, IEEE Commun. Mag. 54 (12) (2016) 44–49.
[24] R. Clarke, Human identification in information systems: Management challenges and public policy issues, Inf. Technol. People 7 (4) (1994) 6–37.
[25] Y. Gahi, M. Lamrani, A. Zoglat, M. Guennoun, B. Kapralos, K. El-Khatib, Biometric identification system based on electrocardiogram data, in: Int. Conference on New Technologies, Mobility and Security (NTMS), 2008, pp. 1–5.
[26] R.D. Labati, R. Sassi, F. Scotti, ECG biometric recognition: Permanence analysis of QRS signals for 24 hours continuous authentication, in: IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2013, pp. 31–36.
[27] F. Agrafioti, D. Hatzinakos, ECG based recognition using second order statistics, in: 6th Annual Conference on Communication Networks and Services Research (CNSR), 2008, pp. 82–87.
[28] M. Hejazi, S. Al-Haddad, Y.P. Singh, S.J. Hashim, A.F.A. Aziz, ECG biometric authentication based on non-fiducial approach using kernel methods, Digit. Signal Process. 52 (2016) 72–86.
[29] T. Beer, Walsh transforms, Amer. J. Phys. 49 (5) (1981) 466–472.
[30] W.S. Kuklinski, Fast walsh transform data-compression algorithm: E.C.G. applications, Med. Biol. Eng. Comput. 21 (4) (1983) 465–472. http://dx.doi.org/10.1007/BF02442635.
[31] D. Venugopal, S. Mohan, S. Raja, An efficient block based lossless compression of medical images, optik, Int. J. Light Electron Opt. 127 (2) (2016) 754–758. http://dx.doi.org/10.1016/j.ijleo.2015.10.154.
[32] A.L. Goldberger, L.A.N. Amaral, L. Glass, J.M. Hausdorff, P.C. Ivanov, R.G. Mark, J.E. Mietus, G.B. Moody, C.-K. Peng, H.E. Stanley, PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals, Circulation 101 (23) (2000) e215–e220.
[33] R.D. Maesschalck, D. Jouan-Rimbaud, D. Massart, The mahalanobis distance, Chemometr. Intell. Lab. Syst. 50 (1) (2000) 1–18. http://dx.doi.org/10.1016/S0169-7439(99)00047-7.
[34] L. Jiang, Z. Cai, D. Wang, H. Zhang, Bayesian citation-knn with distance weighting, Int. J. Mach. Learn. Cybern. 5 (2) (2014) 193–199.
[35] R.O. Duda, P.E. Hart, D.G. Stork, Pattern Classification, second ed., Wiley-Interscience, 2000.

[36] P.-E. Danielsson, Euclidean distance mapping, Comput. Graph. Image process. 14 (3) (1980) 227–248.

[37] M.J. Greenacre, J. Blasius (Eds.), Multiple Correspondence Analysis and Related Methods, in: Statistics in the Social and Behavioral Sciences Series, Chapman & Hall/CRC, 2006.

[38] I.H. Witten, E. Frank, M.A. Hall, Data Mining: Practical Machine Learning Tools and Techniques, third ed., Morgan Kaufmann Publishers Inc., 2011.

[39] A. Gangopadhyay, O. Chatterjee, A. Chatterjee, Hand shape based biometric authentication system using radon transform and collaborative representation based classification, in: Second International Conference on Image Information Processing, IEEE, 2013, pp. 635–639.

[40] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, S. Ben-David, Biometric authentication on a mobile device: a study of user effort, error and task disruption, in: 28th Annual Computer Security Applications Conference, ACM, 2012, pp. 159–168.

[41] D.-H. Shih, C.-M. Lu, M.-H. Shih, A flick biometric authentication mechanism on mobile devices, in: International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS), IEEE, 2015, pp. 31–33.

[42] A. Lee, Y. Kim, Photoplethysmography as a form of biometric authentication, in: SENSORS, IEEE, 2015, pp. 1–2.

[43] N. Akhter, H. Gite, G. Rabbani, K. Kale, Heart rate variability for biometric authentication using time-domain features, in: International Symposium on Security in Computing and Communication, Springer, 2015, pp. 168–175.

[44] S.J. Kang, S.Y. Lee, H.I. Cho, H. Park, ECG authentication system design based on signal analysis in mobile and wearable devices, IEEE Signal Process. Lett. 23 (6) (2016) 805–808.

[45] J.S. Arteaga-Falconi, H. Al Osman, A. El Saddik, ECG authentication for mobile devices, IEEE Trans. Instrum. Meas. 65 (3) (2016) 591–600.

[46] C. Camara, P. Peris-Lopez, J.E. Tapiador, G. Suarez-Tangil, Non-invasive multimodal human identification system combining ECG, GSR, and airflow biosignals, J. Med. Biol. Eng. 35 (6) (2015) 735–748.

[47] K. Niinuma, U. Park, A.K. Jain, Soft biometric traits for continuous user authentication, IEEE Trans. Inf. Forensics Secur. 5 (4) (2010) 771–780.

[48] U. Mahbub, V.M. Patel, D. Chandra, B. Barbello, R. Chellappa, Partial face detection for continuous authentication. arXiv preprint arXiv:1603.09364.

[49] D. Crouse, H. Han, D. Chandra, B. Barbello, A.K. Jain, Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data, in: International Conference on Biometrics, IEEE, 2015, pp. 135–142.

[50] M. Frank, R. Biedert, E. Ma, I. Martinovic, D. Song, Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication, IEEE Trans. Inf. Forensics Secur. 8 (1) (2013) 136–148.

[51] H. Gascon, S. Uellenbeck, C. Wolf, K. Rieck, Continuous authentication on mobile devices by analysis of typing motion behavior, in: Sicherheit, Citeseer, 2014, pp. 1–12.

[52] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, N. Nguyen, Continuous mobile authentication using touchscreen gestures, in: Conference on Technologies for Homeland Security, IEEE, 2012, pp. 451–456.

[53] A. Bonissi, R.D. Labati, L. Perico, R. Sassi, F. Scotti, L. Sparagino, A preliminary study on continuous authentication methods for photoplethysmographic biometrics, in: Workshop on Biometric Measurements and Systems for Security and Medical Applications, 2013, pp. 28–33.

[54] J. da Silv Dias, I. Traore, V.G. Ferreira, J. David, Exploratory use of PPG signal in continuous authentication, in: Brazilian Symposium on Information and Computational Systems Security, pp. 1–14.

[55] M. Guennoun, N. Abbad, J. Talom, S.M.M. Rahman, K. El-Khatib, Continuous authentication by electrocardiogram data, in: Toronto International Conference on Science and Technology for Humanity, IEEE, 2009, pp. 40–42.

[56] R. Matta, J.K. Lau, F. Agrafioti, D. Hatzinakos, Real-time continuous identification system using ECG signals, in: 24th Canadian Conference on Electrical and Computer Engineering, IEEE, 2011, pp. 001313–001316.

[57] D.P. Coutinho, A.L. Fred, M.A. Figueiredo, ECG-based continuous authentication system using adaptive string matching, in: BIOSIGNALS, SciTePress, 2011, pp. 354–359.

[58] F. Babiloni, A.L.N. Fred, J. Filipe, H. Gamboa (Eds.), ECG-based Continuous Authentication System using Adaptive String Matching, SciTePress, 2011.

[59] M. Derawi, Wireless Chest-Based ECG Biometrics, Springer, Berlin, Heidelberg, 2015.

[60] S.I. Safie, J.J. Soraghan, L. Petropoulakis, Electrocardiogram (ECG) biometric authentication using Pulse Active Ratio (PAR), IEEE Trans. Inf. Forensics Secur. 6 (4) (2011) 1315–1322.

[61] K.A. Sidek, V. Mai, I. Khalil, Data mining in mobile ECG based biometric identification, J. Netw. Comput. Appl. 44 (2014) 83–91.

[62] E. E Pasero, C.F. Balzanelli, Intruder recognition using ECG signal, in: International Joint Conference on Neural Networks (IJCNN), 2015, pp. 1–8.

[63] C. Ye, B.V.K.V. Kumar, M.T. Coimbra, Human identification based on ECG signals from wearable health monitoring devices, in: 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, ISABEL'11, ACM, 2011, pp. 25:1–25:5.

[64] H.P. Da Silva, A. Fred, A. Lourenço, A.K. Jain, Finger ECG signal for user authentication: Usability and performance, in: Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE, 2013, pp. 1–8.

[65] S.Z. Fatemian, F. Agrafioti, D. Hatzinakos, Heartid: Cardiac biometric recognition, in: Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2010, pp. 1–5.

Pedro Peris-Lopez is Visiting Lecturer at the Department of Computer Science, Universidad Carlos III de Madrid, Spain. He holds a M.Sc. in Telecommunications Engineering and Ph.D. in Computer Science by Universidad Carlos III de Madrid. His research interests are in the field of security and e-health (biosignals and IMDs), hardware security and security for smart devices. In these fields, he has published a great number of papers in specialized journals and conference proceedings. For additional information see: http://www.lightweightcryptography.com/.

Lorena González-Manzano is assistant professor working in the Computer Security Lab at the University Carlos III of Madrid, Spain. She is Computer Scientist Engineer and Ph.D. in Computer Science by the University Carlos III of Madrid. Her Ph.D. focuses on security and privacy in social networks. She is currently focused on Internet of Things and cloud computing security, as well as, on cybersecurity. Indeed, she has published several papers in national and international conferences and journals and she is also involved in national R+D projects.

Carmen Camara is Ph.D. student working in the Computer Security Lab at the University Carlos III of Madrid, Spain. She holds a M.Sc. in Computer Science and Technology, with specialization in Artificial Intelligence (Carlos III University of Madrid) and a M.Sc. in Biomedical Engineering (Technical University of Madrid). Her research interests are in the fields of applied cryptography and biometrics. Currently, she is focused on designing secure solutions for implantable medical devices.

José María de Fuentes is visiting lecturer in the Computer Science and Engineering Department at University Carlos III of Madrid, Spain. He is Computer Scientist Engineer and Ph.D in Computer Science by the University Carlos III of Madrid. His main research interests are cybersecurity 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.