2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)

A Novel Authentication Biometric for Pacemakers*

Kenedi Heather, Kunal K. Shah, Krishna K. Venkatasubramanian, Hang Cai
Worcester Polytechnic Institute
{kheather,kkshah,kven,hcai}@wpi.edu

Ken Hoyme, Michael Seeberger, Grace Wiechman
Boston Scientific Inc.
{Ken.Hoyme,Michael.Seeberger,Grace.Wiechman}@bsci.com

ABSTRACT

Pacemakers are devices used to regulate heart rate in individuals with abnormal heart rhythms. They are often paired with a programmer, which can receive data from and send commands to them. The goal of this work is to explore a new biometric-based authentication layer to pacemaker-programmer communication. In this paper we present our work on exploring the fusion of pacemaker electrogram and externally-measured cardiac rhythm (electrocardiogram, plethysmogram) as biometrics for authenticating a programmer to a pacemaker. In this preliminary work we use Right Ventricular Electrogram (RV EGM) signal from the pacemaker and Atrial Electrogram (Atrial EGM) as a proxy for the externally measured cardiac rhythm (particularly ECG) to show the feasibility of our approach, achieving an accuracy rate of ~92%.

CCS CONCEPTS

• **Security and privacy → Biometrics**;

KEYWORDS

Authentication, Pacemakers, Electrogram

ACM Reference Format:
Kenedi Heather, Kunal K. Shah, Krishna K. Venkatasubramanian, Hang Cai and Ken Hoyme, Michael Seeberger, Grace Wiechman. 2018. A Novel Authentication Biometric for Pacemakers. In *ACM/IEEE International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE '18), September 26–28, 2018, Washington, DC, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3278576.3278600

1 INTRO

Pacemakers are devices used to monitor and correct abnormalities in heart rhythm. The heart normally acts as its own natural pacemaker (i.e., it regulates itself), but in circumstances that cause an individual's heart to beat abnormally, a pacemaker may be required. The sensors in the pacemaker collect data from the heart by detecting electrical activity in the form of intra-cardiac electrogram (EGM) signals, which are then sent, through leads (or wires), to a computerized generator, or pulse generator. The pulse generator determines if a pacing pulse is needed to assist the heart in beating [9]. Pacemakers are typically inserted beneath the skin just below the collarbone, with leads and sensors going into the heart's right atrium and right ventricle [9]. Between 1993 and 2009, approximately 2.9 million pacemakers were implanted within individuals in the United States [1]. With such a large portion of the population relying on pacemakers, it is vital that these devices can only accessed with the patient's consent.

Pacemakers typically communicate wirelessly with nearby programmers, which are devices used to monitor and retrieve data recorded by pacemakers and send commands to them to change their operational mode [11]. Currently, many programmers come equipped with telemetry wands that can be placed close to a patientÕs skin to initiate communication with the pacemaker over an inductive link [11]. For Boston Scientific pacemakers, the inductive link also enables cryptographic key distribution between the pacemaker and the programmer. This establishes a secure and authenticated session between the pacemaker and the programmer. However, the inductive link adds cost to the manufacture of pacemakers and programmers. Therefore alternatives are required that enable secure and authentication communication between the pacemaker and the programmer, independent of the use of the inductive link.

In this paper, we focus on the authentication part of the problem and explore the use of a biometric-authentication between the pacemaker and a programmer. The overall aim to increase the authentication options available for pacemakers. The benefit of a biometric authentication scheme is that it uses the cardiac properties measured by the pacemaker, directly for authentication.In this regard, we develop a simple patient-specific authentication model (located at the patient's pacemaker device) that works by fusing synchronously measured intra-cardiac electrogram (EGM) data collected by the pacemaker deployed on a patient and externally measured cardiac signal collected from the same patient by the programmer. Before the programmer can be authenticated to send commands to the pacemaker, the programmer collects a cardiac signal snippet (e.g., electrocardiogram) and sends it over a secure channel to the pacemaker. The pacemaker then extracts characteristic properties of this received signal snippet in tandem with its own EGM signal to identify if the programmer is in the possession of a healthcare provide who is treating the patient on whom the pacemaker is deployed. If so, then subsequent commands from the programmer are accepted. Even though biometrics have been used for authentication in the past as in [4, 5, 7, 13, 14], they are all focused on using surface measured cardiac signals and hence cannot be used with pacemakers, which don't have access to such data. To the best of our knowledge, this is the first use of electrogram signals for biometrics in any form.

We present a preliminary work to determine the feasibility of such an approach in this paper, using Right Ventricular Electrogram

*This work was done as part of an undergraduate capstone project.

CHASE '18, September 26–28, 2018, Washington, DC, USA

ACM ISBN 978-1-4503-5958-0/18/09…$15.00
https://doi.org/10.1145/3278576.3278600

(RV EGM) as the signal measured by the pacemaker and Atrial Electrogram (Atrial EGM) as proxy for the external cardiac signal to be recorded by the programmer. We show that with sample anonymized EGM data recorded from actual Boston Scientific-brand pacemakers, we are able to create a mock biometric-authentication system that operates with an accuracy of ~92%.

1.1 Problem Statement and Threat Model

The main aim of this work to is to ensure that the programmer sending commands to the pacemaker is authorized, that is it has patient's consent to do so. We address this by developing a new biometric authentication scheme for pacemakers based on using two electrogram signals RV EGM and Atrial EGM. The Atrial EGM is a proxy for an externally measured cardiac signal from the patient on whom the pacemaker is deployed. In this regard, the principal problem that we address in this paper is *to determine the potential of Atrial and Right Ventricle EGM as a biometric*. The **threat** to our approach comes from adversaries attempting to program a patient's pacemaker by using arbitrary EGM signals from other people to authenticate their programmer to the pacemaker. Further, we assume that adversaries: (1) do not have access to the biometric authentication model, (2) cannot pollute the model during the enrollment stage, and (3) do not have access to any form of cardiac signal from the patient's past or present. Further, we assume the communication between the programmer and the pacemaker is secure using any link-layer security solution.

2 AUTHENTICATION SCHEME

Our authentication approach is based on the premise that two signals characteristic of cardiac process collected from an individual, if collected concurrently, will exhibit unique patterns specific to the individual. The aim is to authenticate the programmer device to the pacemaker before the pacemaker accepts commands from the programmer. In our authentication approach, the programmer measures the patient's cardiac process and sends this *external cardiac signal* (e.g., electrocardiogram or plethysmogram) to the pacemaker over a secure channel. The pacemaker makes its own EGM measurement, synchronously with the programmer's measurement. In this regard our approach uses a novel biometric that is generated by the fusion of the two synchronously measured EGM and external cardiac signal and extracts several classes of features from them in tandem. These feature classes are then used to learn a patient-specific authentication model. This model essentially learns the relationship between the pacemaker-measured EGM and programmer measured cardiac signal for a given patient. This authentication model resides at the pacemaker and allows only those programmers that can measure the cardiac process from the same patient to query and control it. Such an authentication approach can be used to complement any additional authentication approach that may exist between the pacemaker and the programmer.

Our authentication approach consists of three phases: (1) *data collection*: obtaining the dataset used for authentication purposes, (2) *feature extraction*: extraction of feature points from processed data, (3) *enrollment and authentication*: construction and evaluation of patient-specific authentication models. We describe these phases below.

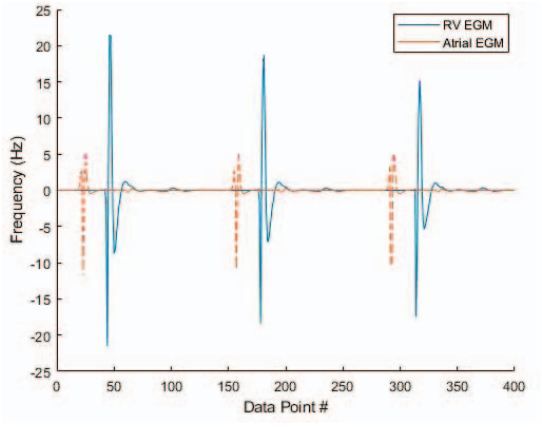


Figure 1: The Atrial and RV EGM episode from a patient

2.1 Data Collection

The first step in building our authentication model is to obtain several snippets of EGM measurements at the pacemaker and cardiac signal measurements measured at the the programmer, which can then be used to build the authentication model. However, we did not have access to a dataset containing synchronously measured EGM and external cardiac signal. We therefore utilized two streams of EGM measurements as the two signals. We used a dataset provided to us by Boston Scientific with Right Ventricular Electrogram (RV EGM) measurements, and Atrial Electrogram (Atrial EGM) measurements. For this work, we assume RV EGM as the EGM measured by the pacemaker and Atrial EGM as the external cardiac signal measurement performed at the programmer. This assumption of using Atrial EGM as the external cardiac signal is a strong assumption because such EGM measurements cannot be done outside the body as required by our approach. However, Atrial EGM data is very similar in temporal and morphological properties as externally measured electrocardiogram (ECG) and therefore forms a nice proxy for an externally measured cardiac signal. Figure 1 shows an example of Atrial and RV EGM measurements for a patient plotted in tandem, showing how data collected from the two waveforms. Figure 2 shows the similarity between the atrial EGM and ECG signals overall.

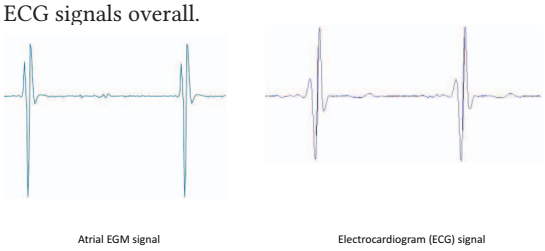


Figure 2: The temporal and morphological similarity between a typical Atrial EGM and ECG signals

2.2 Feature Extraction

In order to build an authentication model we need to extract features from the Atrial and RV EGM signals. In this work, the features are obtained from the fusion of synchronously measured Atrial and RV EGM signal snippets. In the feature extraction process, we first partition each episode of Atrial and RV EGMs into w time-unit

segments, or *windows*. The size of the window is independent of the episode length, but is usually kept as small as possible in order to keep the authentication process fast. We then extract a total of 36 features from each window, that is, each segment produces a 36-dimensional feature point. The features we extract from these windows fall into five categories: (1) matrix features, (2) time-domain features, (3) frequency-domain features, (4) beat-time-interval features, (5) waveform similarity features. We now describe the main idea behind each of these feature type below.

Matrix Features: These features capture the spatial interrelationship between synchronously measured RV EGM and Atrial EGM signals in a window. To generate the matrix features we first generate a portrait for the RV and Atrial EGM snippets. A portrait is defined as an n-dimensional representation of the relationship between several time-series in one multi-dimensional space [6]. The 2-dimensional portrait P is calculated as such: $f(t) = (rv(t), a(t))$, where $rv(t)$ and $a(t)$ are the normalized RV EGM and Atrial EGM windows respectively, and $1 \leq t \leq w$. Given the portrait, the matrix features describe the distribution of points in the portrait that capture the shape of the RV EGM signal with respect to the Atrial EGM signal. To obtain these features, we view the portrait under an $n \times n$ grid and count the number of points from the portrait that fall into each cell in the grid. This information is stored in an $n \times n$ matrix, C, where each element, $C(i, j)$, is the count of the number of points in that cell. We chose n = 500 for generating the matrix C. From this matrix we extract 3 features: (1) the square of the probability that a point falls into an element $C(i, j)$ of matrix C , (2) standard deviation of column averages of matrix C, and (3) quantified area under the curve formed by the column averages of matrix C.

Time-domain Features: Time-domain features describe the relationship between R-peaks (heart beat) in normalized RV EGM and Atrial EGM signals. There are two categories of time-domain features: individual time-domain features and tandem time-domain features. Individual time-domain features are extracted from RV EGM and Atrial EGM windows independently, whereas tandem time-domain features capture the interrelationship between RV EGM and Atrial EGM. For individual time-domain features we extract the following 6 features from both RV EGM and Atrial EGM windows (totaling 12 features): (i) number of peaks, (ii) average peak-to-peak distance, (iii) standard deviation of peak-to-peak distances, (iv) average peak height, (v) standard deviation of peak heights, (vi) distance between minimum and maximum peaks. Similarly, we calculate the following six tandem time-domain features: (i) ratio of number of R-peaks in RV EGM divided and number of R-peaks in Atrial EGM, (ii) ratio of RV EGM mean peak height and Atrial EGM mean peak height, (iii) ratio of standard deviation of RV EGM peaks and the standard deviation of Atrial EGM peaks. (iv) ratio of RV EGM peak-to-peak distance and the mean Atrial EGM peak-to-peak distance, (v) ratio of RV EGM standard deviation of peak-to-peak distance and the Atrial EGM standard deviation of peak-to-peak distance, (vi) ratio of distance between minimum and maximum peaks for RV EGM and the distance between minimum and maximum peaks for Atrial EGM. This results in a grand total of 18 time-domain features.

Frequency-Domain Features: Frequency-domain features capture properties of RV EGM and Atrial EGM time-series in their frequency-domain representations. Similar to time-domain features, frequency-domain features are broken up into two categories: individual frequency-domain features and tandem frequency-domain features. The features are the same as the time-domain features expect they are computed on the fast Fourier transform (FFT) of the RV and Atrial EGMs. There are a total of 18 frequency-domain features as well.

Beat-Time Interval Features: These features focus on the relationship between peak locations in RV EGM and Atrial EGM. This first involves calculating the forward distance and backward distance between RV and Atrial EGM windows. Forward distance is defined as the distance between an RV peak, and the closest Atrial peak that follows it. Backward distance is defined as the distance between an RV peak, and the closest Atrial peak that precedes it. After obtaining separate arrays containing all forward distances and all backward distances in a window, we extract the following six features: the average, standard deviation, root-mean-square of the forward distances, followed by the average, standard deviation, root-mean-square of the backward distances.

Waveform Similarity Features: We compute a single waveform similarity feature that determines the distance between the RV EGM and Atrial EGM in a window. To obtain a scalar value that is characteristic of distance between two waveforms, we use a technique called Dynamic Time Warping (DTW). This technique takes two waveforms as input (in this case, RV EGM and Atrial EGM windows), and "stretches" the waveforms in such a way that it minimizes the Euclidean distances between corresponding points in the signals. The output of the function is equal to the sum of the Euclidean distances between each point.

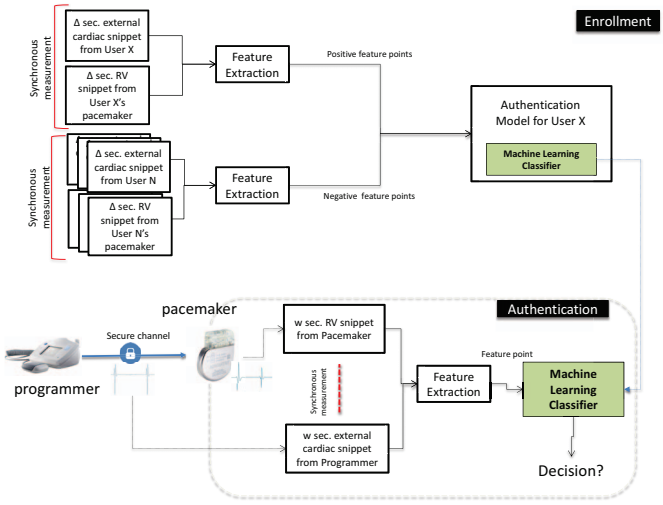


Figure 3: Overview of the approach for authenticating a programmer to a pacemaker using the fusion of an externally measured cardiac signal at the programmer and the RV electrogram measured at the pacemaker as a biometric. In this work we use the Atrial electrogram as a proxy for the external cardiac signal.

2.3 Enrollment and Authentication

The goal of *enrollment stage* is to build a patient-specific model that captures the characteristics of the Atrial and RV EGM signals measured from them in tandem. We use a supervised-learning classifier to construct (train) the patient-specific model.

The feature vectors we used during our enrollment stage were 36-dimensional values extracted from w time-units of synchronously measured Atrial and RV EGM signals. We generate a total of $F_p = \Delta/w$ number of feature points per patient. Here, Δ represents the amount of data required for enrollment of the patient-specific model, and p is the index of the patient. Our classifier requires as input two classes of feature vectors referred to as positive and negative class points. Each w window therefore generates a positive or negative class feature point for the model. The positive class points capture the situations where the Atrial and RV EGMs originate from the patient whose model is being trained, while the negative class points capture the situations where the Atrial and RV EGM signals originate from other patients in our dataset. Hence to train a model for patient 1, we have F_1 positive class feature points obtained from patient 1, and $\sum_{p=2}^{n} F_p$ negative points, where n is the total number of patients in the dataset.

In the *authentication stage*, the trained patient-specific model will decide whether to authenticate a programmer or not based on newly received w time-unit snippet of the externally measured cardiac signal (in our case the Atrial EGM signal, which is used as proxy) from it (i.e., programmer). The pacemaker then collects w time-unit of locally measured RV EGM signal from the patient, and then extracts the 36-dimensional feature from the Atrial and RV EGMs in tadem. We feed this feature point into the patient-specific model. The model then outputs a positive or negative label for this feature point. If the feature point is labeled as positive, then the programmer is considered as a legitimate patient and will be authenticated. Figure 3 shows the overview of the enrollment and authentication process.

3 EXPERIMENTAL SETUP

In this section, we illustrate how we select the three most important parameters of our system: (1) Δ, the amount of data used during enrollment of the patient-specific model, (2) w, which determines the speed with which we can make our authentication decision, and (3) the classifier of choice for our authentication model. We begin with a discussion our dataset, followed by performance metrics for identifying how well we are performing for various parameter choices. Finally, we discuss the parameter selection itself.

3.1 Dataset

Our dataset had the following key characteristics. (1) It contained RV and Atrial EGM from 67 patients. (2) For each patient we had about 50, 30-second episodes of RV and Atrial EGM measurements. (3) All measurements were obtained at a sampling rate of 200Hz. (4) We had an equal number of synchronously measured Atrial and RV EGM episodes per patient which we confirmed using the timestamps associated with the episodes. (5) Each set of synchronously measured RV and Atrial EGM episodes per patient were recorded at disparate intervals over the span of a year, and that each patient had data recorded at different intervals.

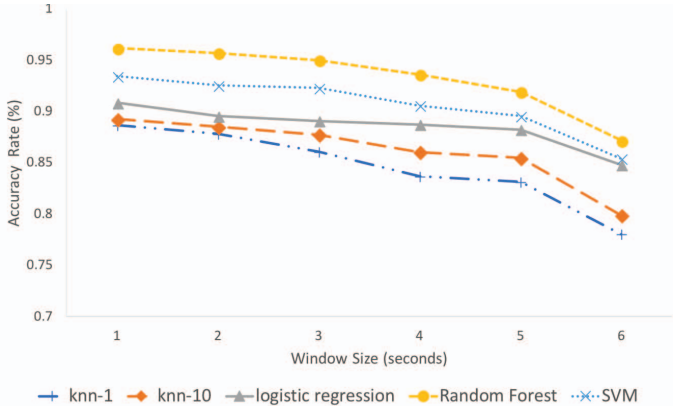


Figure 4: Average cross-validation accuracy rate for different ML algorithms, using different window sizes. Note the y-axis does not begin at the origin.

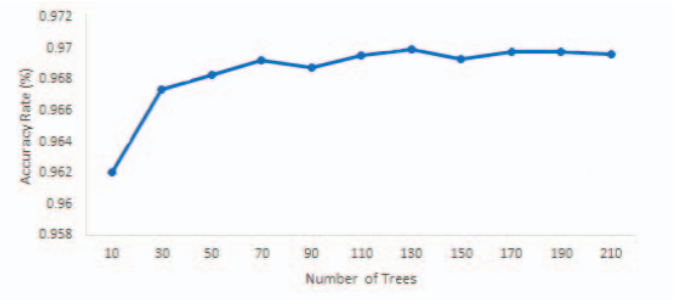


Figure 5: 10-fold cross-validation accuracy rate for a random forest classifier with a 2 second window size and varying numbers of trees

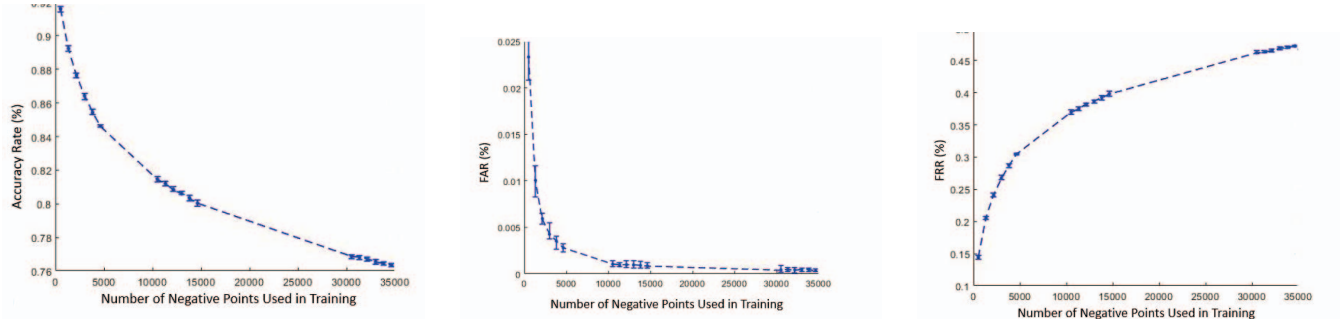
3.2 Metrics

We used the following metrics to evaluate the efficacy of our authentication scheme: false accept rate (FAR), false reject rate (FRR), and the accuracy rate. False accept rate (FAR) is defined as the ratio of negative class feature points being tested by a model that are misclassified as positive class feature points. False reject rate (FRR) is defined as the ratio of positive feature class points being tested by a model that are misclassified as negative class feature points. The accuracy rate is simply the ratio of correctly predicted feature points to total number of points tested by a model.

3.3 Parameter Selection

Our dataset consisted of ~50 Atrial and RV EGM episodes per patient. We chose the first 35 episodes to be used for training (i.e., Δ), leaving ~15 episodes for evaluation. The choice of 35 was arbitrary, we wanted to ensure that each patient-specific model was trained with the same number of episodes, and we had sufficient episodes remaining for each patient to use as testing sets.

Rather than testing for w and the classifier independently, we evaluated several different machine learning algorithms, for a range of window sizes each. We used 10-fold cross-validation and accuracy rate, FAR, and FRR as the primary metrics to determine which combination to use. Figure 5 illustrates the accuracy rate for various



(a) Accuracy Rate (b) False Accept Rate (c) False Reject Rate

Figure 6: Aggregate accuracy, false accept rate, and false reject rate for models with various degrees of class imbalance during enrollment.

w values for the following machine learning classifiers: random forest (with 10 trees), Support Vector Machine (SVM), logistic regression, k-nearest neighbors with 1 neighbor, k-nearest neighbors with 10 neighbors. Note that these classifiers were chosen based on their simplicity, as ultimately our classifier would reside in the pacemaker device, which is severely resource constrained. We used various values of w, which were factors of 30 to ensure that we could evenly partition each episode of 30 seconds without having left-over data. Figure 4 shows the average cross-validation accuracy rate for the 5 listed machine learning algorithms, and 7 different window sizes (starting from 1 second and ending at 30 seconds). The results show that the random forest classifier has the highest accuracy rate for every window size, and peaks at a window size of $w = 2$ seconds (accuracy rate = 96.1%).

After selecting the random forest algorithm with $w = 2$ seconds as our optimal parameters, we proceeded to fine tune the random forest classifier. We hypothesized that increasing the number of random forest decision trees would increase accuracy rate and reduce error. We decided to test training random forest classifiers with the same data, using different number of trees. We did not exceed 210 trees, as the accuracy rate started to stabilize by this point. Figure 5 shows accuracy rate for each classifier with $w = 2$s. Accuracy rate was highest for random forest with 130 trees, at 96.9%. Therefore we chose random forest with 130 trees as our classifier.

4 RESULTS

In this section, we present the results measuring the efficacy of our authentication approach. Our goal here is to compute the authentication accuracy, false accept rate and false reject rate aggregated over the 67 patient-specific models that we created. The quality of the results obtained depend upon the way the models are trained. As seen in Section 2 we have unbalanced enrollment data with an order of magnitude more negative class feature points than positive ones.

There are more negative class feature points than positive class feature points during the enrollment phase. This creates a huge imbalance in the two classes of feature points used to train the model, which if left unchecked can lead to trivial models that learn to label all test data as belonging to the majority class. To overcome this problem we undersample the negative class feature points to create a balance between both the positive and negative class feature points. We start the enrollment phase of each patient-specific model with the same amount of positive and negative feature points: $(30/w) * \Delta$ where $\Delta = 35$ episodes, and $w = 2$ seconds. The results of our analysis is shown in Figure 6, displaying average accuracy rate, FAR, and FRR. It can be seen that the accuracy rate decreases as the number of negative feature points used in enrollment increases, which is accompanied by an increase in the FRR as well. Further, we performed 10 trials for each patient with different random samples of negative feature points in order to evaluate the spread of the various metrics. This shows that as the class imbalance increases the positive class becomes underrepresented, and hence misclassified more often. The bars represent the spread of the values based on 10 trials. Overall, we see that the value of the various metrics remain stable (have low variance) over the 10 trials. Since the performance of the balanced model with 525 positive and negative class feature points works the best, we use this model for the rest of the results.

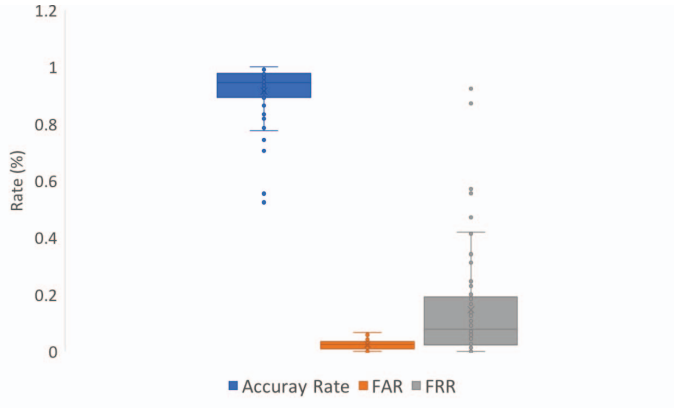


Figure 7: Box plot for Accuracy, FAR, FRR for the best model

Figure 7 provides a box plot for accuracy, FAR, and FRR for our balanced model with 525 points for both positive and negative classes. Overall, the median accuracy, FAR and FRR are 95%, 2.3% and 7.6%. There are 7 patients whose accuracy rate was below 80%, and 2 patients whose accuracy rate was below 60%. These outliers cause a drop in overall accuracy rate, and can be attributed to the enrollment data and testing data for these patients having

largely different characteristics. There are two potential causes for this: (1) the heart rhythm for the patient changed, or (2) an error in the pacemaker device led to a change in EGM recordings for the patient. Assuming it is not the latter, we can deal with patients whose physiology has changed since the time of training by retraining the model.

One way of determining when to retrain the models would be to see if accuracy drops as time between the model enrollment and testing increases. If it does, then we can find a threshold and re-train the model when the accuracy drops below this value. In this regard, we randomly sampled episodes from each patient over the span of a year and calculated the accuracy of these test feature points vis-a-vis the duration of the episode from the time the patient's model was trained. In our dataset, the spread of the testing set varied greatly from patient to patient, some patients' data spanning 20-30 days, and other patients' data spanning 150-200 days. Figure 8 shows testing spread (measured in days) plotted against classifier accuracy rate for each of 67 patients in our dataset. Upon analysis, we see that there is no correlation between classifier accuracy rate and the spread measured in days since training (Pearson coefficient R-value is: -0.2735, and the p-value is: 0.025126). This shows us that our model's authentication success depends purely on the immediate physiological state of the patient and how similar it is to the patient's physiological state during enrollment. Finding ways to deal with this problem to keep the authentication accuracy high over time is an open question.

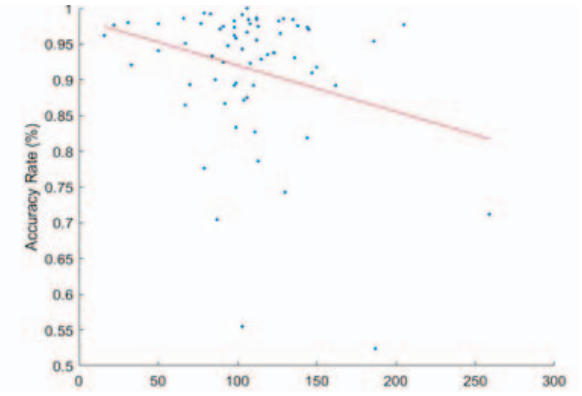


Figure 8: Accuracy Rate vs. Time since enrollment

5 RELATED WORK

Authentication in the domain of low capability devices (such as IoT devices) has been explored before [2, 3]. However, it is not clear if they can be used directly for extremely low capability, safety-critical devices such as pacemakers. Previous research specifically on pacemakers has focused on their unauthorized programming with rogue programmers, or external devices, bypassing the need for authentication [11]. Since then work has been done to augment existing pacemaker features that prevent them from being programmed in an unauthorized manner. For instance, in [10], the authors discovered a way to create a little external device that would jam the insecure communication to and from an implanted device and then overlay a new secure wireless communication mechanism. Other approaches have been proposed that authenticate the programmer using traditional biometrics such a fingerprint and iris scans for authentication, especially during emergencies [12]. All these approaches have been designed with existing pacemakers in mind and need extra devices and scanners to work. A usability analysis of solutions that use such additional devices for security found that users did not like carrying these additional devices [8]. Consequently, we take a different route, one that fundamentally augments the pacemaker functionality by addition a new layer of authentication without using any additional device and is therefore geared toward the next generation of pacemakers.

6 CONCLUSIONS

The purpose of our work was to determine the feasibility of using a fusion of cardiac signals as a biometric for an authentication scheme between the pacemaker and its programmer. In this regard, our authentication approach deploys a patient-specific classifier-based authentication model onto a pacemaker that fuses its own EGM signal with a synchronously measured external cardiac signal at the programmer. We showed that the fusion of right ventricular (RV) EGM and atrial EGM (as proxy for the externally measured cardiac signal) can produce an effective authentication scheme that achieves an accuracy rate of ∼92%. In the future, we plan to perform this work by (1) collecting actual external cardiac measurement instead of using one of the EGMs as proxies, (2) making the threat model less restrictive by allowing adversaries access to the user's historic cardiac data, (3) adding our own link security solution to the authentication process, and (4) evaluating the energy consumption of protocols thus developed.

REFERENCES

[1] 2012. Trends in Permanent Pacemaker Implantation in the United States From 1993 to 2009: Increasing Complexity of Patients and Procedures. *Journal of the American College of Cardiology* 60, 16 (2012), 1540 – 1545.
[2] 2018. On security challenges and open issues in Internet of Things. *Future Generation Computer Systems* 83 (2018), 326 – 337.
[3] 2018. A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity. *Future Generation Computer Systems* 82 (2018), 342 – 348.
[4] Shu-Di Bao, C.C.Y. Poon, Yuan-Ting Zhang, and Lian-Feng Shen. 2008. Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network. *Information Technology in Biomedicine, IEEE Transactions on* 12, 6 (nov. 2008), 772 –779.
[5] Shu-Di Bao, Y. T. Zhang, and Lian-Feng Shen. 2005. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In *27th IEEE Conference on Engineering in Medicine and Biology*. 2455–2458.
[6] H. Cai and K. K. Venkatasubramanian. 2016. Detecting Signal Injection Attack-Based Morphological Alterations of ECG Measurements. In *2016 International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 127–135.
[7] S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta. 2003. BioSec: A Biometric-based approach for securing communication in wireless networks of biosensors implanted in the human body. In *International Conference on Parallel Processing Workshops*. 432–439.
[8] Tamara Denning, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno, and William H. Maisel. 2010. Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. 917–926.
[9] Dario DiFrancesco. 1993. Pacemaker mechanisms in cardiac tissue. *Annual review of physiology* 55, 1 (1993), 455–472.
[10] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. 2011. They Can Hear Your Heartbeats: Non-invasive Security for Implantable Medical Devices. *SIGCOMM Comput. Commun. Rev.* 41, 4 (Aug. 2011), 2–13. https://doi.org/10.1145/2043164.2018438
[11] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. 2008. Pacemakers and Implantable Cardiac

Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*. 129–142.

[12] X. Hei and X. Du. 2011. Biometric-based two-level secure access control for Implantable Medical Devices during emergencies. In *2011 Proceedings IEEE INFOCOM*. 346–350.

[13] Krishna K. Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S. Gupta. 2010. PSKA: Usable and secure key agreement scheme for body area networks. *Trans. Info. Tech. Biomed.* 14, 1 (Jan. 2010), 60–68.

[14] Krishna K. Venkatasubramanian and Sandeep K. S. Gupta. 2010. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Trans. Sen. Netw.* 6, 4, Article 31 (July 2010), 36 pages.