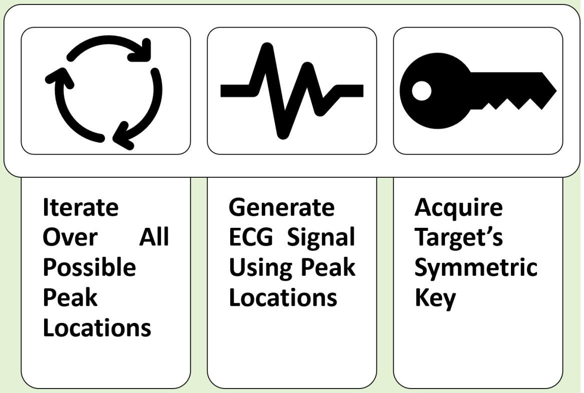
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2021.3079177, IEEE Sensors Journal

A New Attack Method Against ECG-based Key Generation and Agreement Schemes in Body Area Networks

Jack Hodgkiss, *Student Member, IEEE*, Soufiene Djahel, *Senior Member, IEEE*, and Zonghua Zhang, *Senior Member, IEEE*

***Abstract*— Body Area Networks (BAN) are wireless networks designed for deployment on or within the human body. These networks are primarily intended for application within the medical domain due to their capabilities for enabling wireless monitoring of physiological signals, and remote administration of medical devices. Due to their intended use case, securing these devices is paramount. In recent years, several key generation and agreement schemes that rely upon physiological signals of the wearer are developed. However, we have found that the application of Electrocardiogram (ECG) signals in this context may not be appropriate due to a potential vulnerability, wherein previously recorded ECG signals could be used against current and future key agreement attempts to compromise their security. This is a violation of temporal variance which is one of a few properties that make ECG signals suitable for use in key agreement schemes. By extracting the QRS complex from prior recordings and distributing them apart from one another we can construct synthetic signals that have a high level of coherence, and thus allow for the key to be intercepted. Based on the conducted experiments we have found that the proposed attack method yields a 0.7 coherence level regardless of how far away the adversary is from the target. This makes the success of such an attack extremely likely and is therefore a real threat to the security of these schemes.**


Iterate Over All Possible Peak Locations
Generate ECG Signal Using Peak Locations
Acquire Target's Symmetric Key

***Index Terms*— Body Area Networks, Body Sensor Networks, Authentication, Key Generation, Synthetic Signals**

I. Introduction

NOWADAYS, sensing technology [1] represents an essential source of data in many application domains, such as transportation and smart healthcare, as it offers the capability of real-time monitoring and reporting of various events and parameters. To account for the specific constraints of the tiny sensors used in this context and pave the way to novel sensor-based applications, innovative energy-efficient, lightweight and secure protocols are required. To that end, this paper focuses on the smart healthcare application domain and deeply analyses a key sensor technology used in it (i.e., body sensors or wearable sensors [2]), identifies a potential vulnerability in the way the authentication between sensors is performed, and proposes a novel attack method to exploit this vulnerability.

Body Area Network (BAN), also known as Body Sensor Network (BSN), is a wireless network composed of wireless sensor devices that can be worn or even implanted within the human body, this is only possible due their miniature size and low-power consumption. These devices may be used as sensors to collect information about the wearer, such as body temperature, glucose level or fall detection, in addition to their use as complex medical instruments such as a pacemaker. While these use cases are medical, standards like IEEE 802.15.6 [3] enable military and entertainment applications, but the primary focus remains in the medical domain. These devices will play a vital role in smart healthcare by enabling an improvement of the quality of care provided, a reduction in operating costs and number of deaths. According to [4], the global smart healthcare market size was US$ 141 billion in 2019 and is expected to grow at 14.5% through 2030, that is why significant research interest has been devoted to improving several aspects of BANs such as; power consumption, data dissemination and security.

Securing BAN miniature devices is essential to their successful wide adoption by the industry and the public. This is due to the significant risks associated with the disclosure of the wearer's private medical information or the potential for physical harms to be inflicted to the wearer. Moreover, security

Jack Hodgkiss and Soufiene Djahel are with the Department of Mathematics and Computing, Manchester Metropolitan University, All Saints Building, All Saints, Manchester M15 6BH Uk (e-mail:JACK.HODGKISS@stu.mmu.ac.uk, S.Djahel@mmu.ac.uk).

Zonghua Zhang is with Huawei France Research Center, Huawei Technologies France, Paris, France (e-mail: zonghua.zhang@huawei.com).

is also a legal requirement in many countries and markets such as the EU (General Data Protection Regulation (GDPR)) or USA (Health Insurance Portability and Accountability Act (HIPPA)). Therefore, a significant research portfolio has been established to secure BANs and major research activities are still in progress to achieve this aim.

To secure BAN against potential attacks, several techniques are proposed to facilitate security keys distribution between BANs sensors using Electrocardiogram (ECG) signals, such as the fuzzy commitment and the fuzzy vault approaches, where each of them presents unique performance limitations and design trade offs [5]. Physiological Signal Based Key Agreement (PSKA), Ordered Physiological Feature-based Key Agreement (OPFKA) and ECG Linear Prediction key Agreement (ELPA) [6]–[8] are examples of key generation and agreement schemes that exploit the unique capability of accessing physiological signals. Specifically, these schemes use ECG to derive a symmetric key to secure all future communications between compatible sensors. There exist also other methods for securing medical devices that capture ECG data such as [9] which uses random binary sequences derived from the interpulse interval between heartbeats. This work has been improved in [10] by enabling the scheme to variably select more or less bits if the data allows for it, significantly reducing execution times. Besides ECG, fingerprints were also used in [11] to secure implantable medical devices and reduce the resources consumption required in ECG based schemes.

Each of ECG-based schemes takes advantage of several qualities that make the application of ECG suitable for key generation. One such quality is temporal variance – the knowledge of the wearer's past physiological signal will not provide the adversary with any advantage into discovering the keys being agreed upon at present or in the future. However, as this work will demonstrate, this is no longer the case as an adversary may use historical ECGs data to synthesize a new signal to compromise keys that have been agreed upon using the schemes. The method for producing synthetic ECGs signals is a novel approach involving the reconstitution of QRS complexes which are the major positive deflection on the ECGs produced by ventricular depolarization.

The remainder of this paper is organized as follows. Section II will review the most important key generation and agreement schemes that could be vulnerable to our proposed attack method. In Section III, we will present the threat model and the details of our proposed Synthetic Electrocardiogram Attack Method (SEAM). In Section IV, we will evaluate the success rate and practicality of SEAM. Finally, we conclude the paper and outline potential future work in Section V.

II. Overview on ECG-based Key generation and agreement schemes in BANs

Many key generation and agreement schemes have been developed in recent years, such as PSKA [6], OPFKA [7], ELPA [8] and Multi-Biometric and Physiological Signal-Based Key Agreement (MBPSKA) [12]. Each of these schemes provides the participating devices with the capability to derive a symmetric key from the shared physiological signal (i.e., ECG in this context). Although each of these schemes is distinguished by its feature extraction and key reconstruction stages, they all share a common weakness (i.e., they rely upon the ECG signal remaining a secret) that an adversary may target to compromise the secret key that has been agreed upon. In the following, we will briefly present the working principle of each of these schemes.

PSKA [6] is a key agreement scheme that uses a cryptographic primitive known as the fuzzy vault [13] to achieve symmetric key generation and agreement between compatible BAN devices. The fuzzy vault conceals a secret using some of the properties found within error-correction codes. Such a secret can only be retrieved if there is significant overlap between two sets of elements. Any secret hidden within a fuzzy vault shall be encoded within a polynomial as its coefficients. Elements from the first set, known as the locking set, shall be projected onto the polynomial which will be disguised by the presence of chaff points which are indistinguishable from the elements of the locking set. Any attempt to reveal the secret within the vault will require sufficient knowledge of the elements contained within the locking set, anyone with possession of enough elements may reconstruct the secret contained within. PSKA uses the fuzzy vault to transmit the symmetric key from the sender to receiver. To enable unlocking the vault by the receiver, both devices must have their own set of elements that overlap, that is why a physiological signal such as ECG is used. The authors of this scheme, therefore, propose an ECG feature extraction method which allows for two devices measuring ECG from the same body to agree upon a symmetric key securing all future communications. The results presented in this paper show that two ECG sensing BAN devices can generate and agree upon a key in a timely manner with little computation required when compared to Diffie-Helman.

MBPSKA [12] is another scheme that uses the fuzzy vault primitive and relies on multiple biometrics to improve the security of the key generation and agreement process. The usage of multiple biometrics, such as fingerprint or iris, increases the security level of MBPSKA as an adversary needs to compromise all biometrics and physiological signals used. However, there remains a concern about the feasibility of such a scheme as templates of the patient's biometric must be uploaded beforehand in a secure manner, which could prove costly both in terms of time and money. Finally, biometrics, such as fingerprints, do not vary over time unlike ECG signals. Therefore, once a user's fingerprint is known to an adversary it will forever be compromised, weakening schemes that may rely upon it in the process.

OPFKA [7] is another key generation and agreement scheme that uses a similar combination of the fuzzy vault and physiological signals as its foundation. However, OPFKA aims to generate a symmetric key with reduced communication overhead compared to other schemes like PSKA. This is because the vault used in both schemes is composed of thousands of two-dimensional points which consumes a significant amount of communication bandwidth. OPFKA remedies this issue by removing the order-invariance property of the fuzzy vault scheme. Order-invariance enables unlocking the vault using an unlocking set that has sufficient overlap with the locking set but the order in which the elements are recalled is not required for it to succeed. The authors of OPFKA determined that with an appropriate ECG feature extraction process the features that form both sets will occur in the same position, and thus do not require order-invariance to function. By dropping order-invariance OPFKA benefits from an increase in security because an adversary needs to identify points from the locking set in addition to the order in which they occur. This reduces the number of chaff points used to conceal the secret and in turn reduces the communication overhead incurred as the vault size has decreased overall.

ELPA [8] is a key generation and agreement scheme that, unlike the above works, does not use the fuzzy vault primitive and instead uses Linear Prediction Coding (LPC). ELPA allows two BAN devices measuring ECG from the same person to agree upon the same symmetric key. It achieves this by using LPC which attempts to reproduce the same signal by identifying parameters for a linear model. Before LPC can be used features must be extracted from the source signal, however, unlike the previous schemes, ELPA uses Discrete Cosine Transformation (DCT) of the Autocorrelation (AC) of the signal. The coefficients gathered from the DCT are used by the sender within the linear prediction stage of this scheme. This stage will produce a set of errors and coefficients. The errors are converted by the sender to generate a 128-bit key using pulse-code train transformation. These errors are never transmitted, however, the LPC coefficients are sent to the receiver who will attempt to recover the errors via a key decoding and error correction process. This process requires that the receiver possesses both the source signal and the LPC coefficients. If successful, both the sender and receiver will have generated a symmetric key that can be used to secure all future communications. As ELPA only transmits a small number of coefficients the communication overhead is greatly reduced compared to schemes that use the fuzzy vault primitive.

III. Our Proposal

In this section we will present the threat model considered and the detailed working principle of our proposed attack method against ECG-based key generation and agreement schemes.

A. Overview of Electrocardiogram Signals

ECG is a physiological signal that is of interest to medical professionals as it enables them to diagnose serious health conditions such as arrhythmia, heart attack, or coronary heart disease [15]. These conditions may be identified by an ECG as it observes the electrical activity of the heart, this is achieved by placing sensors, on the surface of the skin, capable of measuring the few millivolts that the heart emits. Figure 1 shows a simplified diagram of an ECG signal in which a normal sinus rhythm is present. Whilst it is referred to as the QRS complex it should be understood that the complex will not always contain each wave. The Q wave represents depolarization of the interventricular septum, R wave reflects depolarization of the main mass of the ventricles and the S wave observation of the final depolarization of the ventricles as it setups for the next cycle [16].

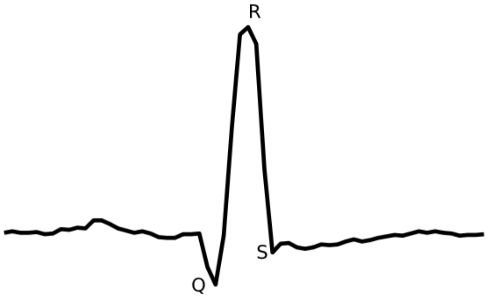


Fig. 1: Annotated ECG signal demonstrating the location of the components that make up the QRS complex (derived from [14])

As discussed in Section II there are several key generation and agreement schemes that are designed to take advantage of ECG for either deriving or concealing the key being agreed upon. These schemes are designed to be used by BAN sensors capable of measuring ECG. The application of physiological signals such as ECG in this manner has been deemed appropriate as they exhibit certain properties as highlighted in [6]. These properties are the following,

- **Temporal Variance**: knowledge of the wearer's past physiological signal will not provide the adversary with any advantage into discovering the keys being agreed upon at present or in the future.
- **Distinctiveness**: knowledge of one individual's physiological signal does not provide the adversary with any advantage in obtaining another's.
- **Length and randomness**: any key being agreed upon is random with adequate length to prevent attempts at brute-forcing.
- **Low latency**: the number of samples required is small.

Each of the above properties contributes to the success of any key generation and agreement scheme such as PSKA or ELPA. These schemes exploit features that are present within two separate readings of the same signal.

B. Threat Model

Before we introduce our method of attack we must first outline the capabilities of an adversary in order to understand what is required to carry out such an attack and the likelihood of its success. We assume that the adversary has access to Commercial-off-the-shelf (COTS) hardware, such as a modest powered laptop with wireless communication capabilities. With such a device the adversary will need to observe the key agreement taking place which can be achieved by configuring their device to listen in promiscuous mode. In this mode, the adversary can capture all network traffic including the pertinent and related key agreement data such as LPC coefficients and Bose–Chaudhuri–Hocquenghem (BCH) coding for ELPA. However, the adversary would need to also acquire prior ECG recordings of their target which could be accomplished by compromising the data storage location where the ECG data is being stored. The required skills and resources for the adversary to acquire the ECG data will depend on the security configuration and sophistication level of the storage solution used. As highlighted in [17], existing medical devices in the healthcare market are vulnerable to a myriad of security attacks due to the lack of built in sophisticated security mechanisms by their manufacturers. Example of such vulnerabilities include weak encryption, lack of authentication, and unpatched and obsolete operating systems [17]. Therefore, these vulnerabilities would enable the adversary to capture the necessary data to perform the aforementioned attack.

Once the adversary has acquired both the transmitted key agreement data and the prior ECG recordings, the attack can be mounted to compromise the key agreement scheme. This attack will be outlined in the next subsection.

C. Synthetic Electrocardiogram Attack Method (SEAM)

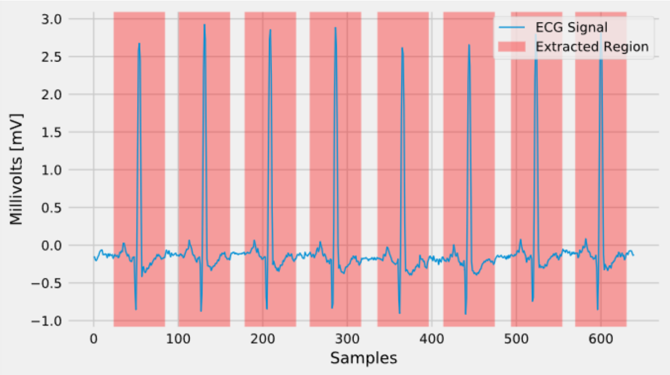


Fig. 2: 640 sample ECG plot with the highlighted regions demonstrating the segments that shall be extracted and utilized by SEAM

Based on the threat model analysis, we propose a SEAM, which is a new attack technique that could enable the adversary to intercept the symmetric keys being agreed upon in ECG based schemes.

The QRS complex is a segment of the signal that is expected to occur a number of times within the section used by the legitimate parties of a key agreement scheme. Therefore, SEAM operates by extracting the QRS complexes from the prior recorded signal data already obtained (stolen) by the adversary. This prior recorded signal data can be anywhere from a few seconds old or many hours. In Section IV, we explore the effectiveness of the scheme to at most 12 hours, beyond this limit we have no data to suggest if our method continues to perform as well as it does due to limited long term datasets available. This extraction allows for the construction of synthetic signals that can imitate valid or relevant signals used in a specific instance of a key agreement scheme. In addition, the adversary has to ascertain that the distance between peaks in the synthetic signal is equal to that of the target signal. Indeed, having the QRS complex only does not lead to a successful attack because the distance between each complex has significant impact on the synthetic signal's ability to imitate the target legitimate signal.

Specifically, SEAM can be broken up into a number of steps as described below,

1) Identify the location of all QRS complexes within the stolen signal data. This can be achieved by utilizing an automatic QRS detection method [18]–[20], however if the stolen signal data length is short then it could be achieved manually.
2) Extract the QRS complexes sample data ensuring that an equal amount from either side of the peak has been taken. This is done to ensure that only the QRS complexes are used when constructing the signal, the gaps between the complexes can be filled in with zeros. Figure 2 demonstrates this process.
3) Split the extracted complexes into equally sized groups. The number of groups should be equal to the number of complexes that are expected to occur within the target signal.
4) Reduce each group of complexes down into a single complex by averaging the population of each group. This is done to lower the number of complexes being used by the scheme. However, since we average the complexes we therefore maintain the common features found within each of the complex groups.
5) Construct the synthetic signal by placing a QRS complex at each of the peaks locations used within this instance of the attack. The construction requires nothing more than inserting the sample points of the QRS complex at the desired locations. The gaps between complexes can be zeroed.
6) Attempt to utilize the synthetic signal against the key agreement data, if no success then repeat Step 5 with new peak locations until success has been found or possible solutions are exhausted.

The steps described above detail how an adversary would extract the QRS complexes from the stolen data in their possession and use it to construct a synthetic signal. One thing omitted from this would be how to decide where the QRS complexes should be placed in relation to one another. As stated earlier, the distance between each complex determines the success of a given attack. Therefore, it is vital to have an efficient method for placing QRS complexes in order to provide the opportunity for a successful attack. Currently, we apply the brute force method [21] to construct a signal where the complexes and the distances between one another are fully explored. This method requires the construction of Cartesian product of a range of samples to search for the perfect placement of complexes. With such a set, the adversary could explore the placement of complexes in an iterative manner constructing new synthetic signals with each grouping of sample points. The search space (i.e., complexity) of this method can be expressed as s^r, where s is the range of samples to explore, and r is the number of peaks assumed to take place within the target signal. However, the range of samples to explore could increase due to the occurrence of more complexes and the fact that the target signal could be sampled at a higher rate. To overcome this, prior ECG data could be used again to inform the placement of complexes in the synthetic signal using some form of statistical analysis.

IV. Performance Evaluation

In this section we will evaluate the efficiency of our proposed attack method known as SEAM. This will cover what the evaluation's purpose is, the evaluation metrics and main settings used, and the analysis of the obtained results in addition to evaluating the effectiveness of SEAM against ELPA scheme.

A. Experimental Purpose

To evaluate the capabilities of the attack proposed within this paper we have designed an experiment that can measure the similarity level of the synthetic signal when compared against the target signal. The purpose of this is to understand if the proposed method can generate signals that can adequately impersonate a target signal in order to enable interception of the key being agreed upon between two BAN sensors. We also look at what impact an increase in the delay between the target and the stolen data has on the attack's success. The experiments designed provide information on whether the attack can succeed in addition to how frequently the attack can be expected to succeed. This is important in evaluating the efficiency of the attack and the potential of using it against real targets.

B. Evaluation Metrics

Algorithm 1 Evaluate the coherence between the target and synthetic signal

```
▷ Where $x$ is the target signal and $y$ is the synthetic signal
▷ Where $P$ is the power spectrum density
▷ Where $d$ is sample spacing and $n$ is signal length
▷ Where $Trapz()$ is the trapezium rule
function SIGNALCOHERENCE($x$, $y$)
    $a \leftarrow abs(Pxy)^2/(Pxx * Pyy)$
    $f \leftarrow [0, 1, ..., n/2 - 1, -n/2, ..., -1]/(d * n)$
    $n \leftarrow Scale(f, 0, 1)$
    $s \leftarrow n[1] - n[0]$
    return $Trapz(a, s)$
end function
```

In order to evaluate SEAM efficiency we have decided to use the signal coherence [22] between the target and synthetic signals as the main performance metric. This is a measurement that discloses the relationship between two signals in the frequency domain as it identifies correlation between the signals' frequency and phase. However, we must adapt the output of such a function in order to quantify how strong the correlation is overall. This can be achieved by calculating the area under the curve of the signal coherence output. This allows for the output to be reduced down into a single value between 0 and 1, where 1 indicates the highest level of coherence and the 0 indicates the lowest level. See Algorithm 1 for more details on how this measurement was implemented. In our experiments, we found that legitimate signals could expect to achieve a coherence level of greater than 0.7 on average.

C. Evaluation Settings

Dataset	MIT-BIH Normal Sinus Rhythm Dataset
Selected Records	All 18
Target (Samples)	640
Adversary (Samples)	38400
Delays	1, 5, 10, 15, and 30 Minutes [1, 12] Hours

TABLE I: Evaluation parameters setting used in SEAM's experiments

A number of evaluation parameters have been selected which have an impact on the results of any experiments carried out, these parameters have been summarized in Table I. Firstly, the experiments have been carried out on COTS hardware (i.e., a Desktop machine with CPU specifications: AMD Ryzen 7 3700X 8/16 (Cores/Threads) @ 4.4 GHz) that is reasonable to assume that any adversary would have easy access to. The experiments have used the ECG and annotations data from the Normal Sinus Rhythm Dataset [23] via the Physionet Project [24]. This dataset is composed of 18 long-term ECG recordings in which no significant arrhythmias were identified. All 18 patients ECG recordings were used in the experiments, with target data being selected at random. For the stolen data, it is selected based on the target's starting point minus the delay, which is the time between target and stolen data. This has been varied within the experiments looking at the effects of an increase in the distance (delay) between the target's starting point and adversary's end point of their ECG data. This has been varied from 60 seconds, 5 minutes, 10 minutes, 15 minutes, 30 minutes, 1 hour and every hour up-to and including 12 hours. Over 30,000 experiments have been carried out.

D. Results Analysis

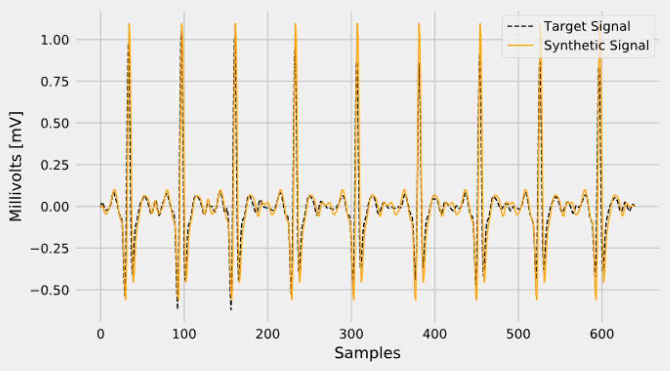


Fig. 3: Comparison of the target and synthetic signal in the time domain

During our investigations, we were able to construct a large number of synthetic signals made up of only prior recorded data and the current peak locations from the target. A significant number of the synthetic signals produced do well to mirror the target signal as evidenced in Figure 3. Whilst there is not perfect alignment between the two signals the synthetic does well to mirror the target to the extent that it does. This alignment translates over into the frequency domain which is where feature extraction takes place in a scheme such as PSKA. Figure 4 shows these similarities within the frequency domain, for example the zoomed inset shows high similarity due to their proximity between the peaks' location and magnitude. This figure demonstrates that not only do the peaks occur at the same frequency but they also share similar magnitude which means that the synthetic signal has the ability to deceive a fuzzy key agreement scheme.

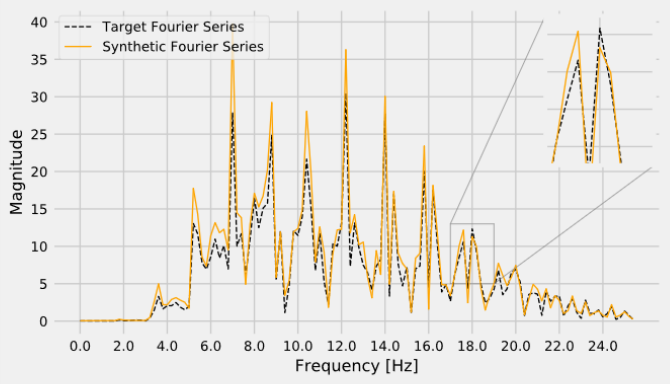


Fig. 4: Comparison of the target and synthetic signal in the frequency domain

Looking at the coherence values between the target and the synthetic signal it is clear that a majority of all signals produced a coherence of greater than 0.7, which is something that the intended parties of the key agreement schemes are capable of achieving. The coherence levels between delays also shows little to no change as the delays get larger. This implies that SEAM is capable of generating signals that achieve a high level of coherence without losing performance as the delay widens. Figure 6 shows two histograms providing a look at the distribution of coherence achieved within the experiments for a delay of 60 seconds and 12 hours. This distribution is found within all delays attempted within the experiments, which would mean that regardless of the distance (delay) between the target and adversary the key to success lies within the positioning of peaks and the structure of the QRS complexes used. This is further reinforced in Figure 5 which statistically insignificant variation between the various delays and the average coherence obtained.

E. Performance Against Existing Works

The focus of this evaluation so far has been on the coherence or similarities between the target and the synthetic signal within the frequency domain. Whilst the results demonstrate the potential of our attack method we recognize the need to apply this against existing works. To that end, we have implemented the key generation and agreement scheme known as ELPA which utilizes linear prediction coding applied against features obtained from the AC /DCT method presented in [25]. Our implementation of the scheme achieves similar performance results with regards to false rejection rate (FRR) and false acceptance rate (FAR) and therefore is suitable for applying our attack method against.

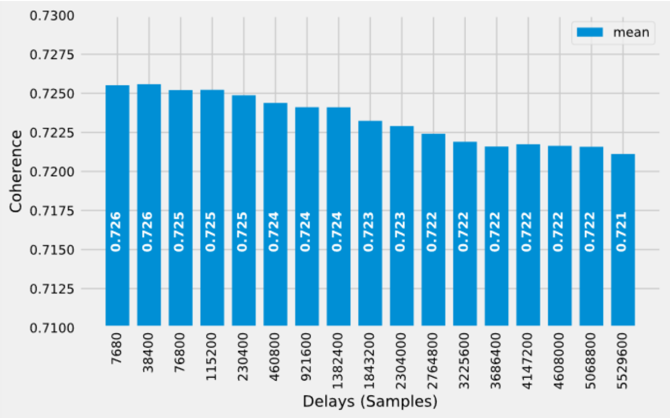
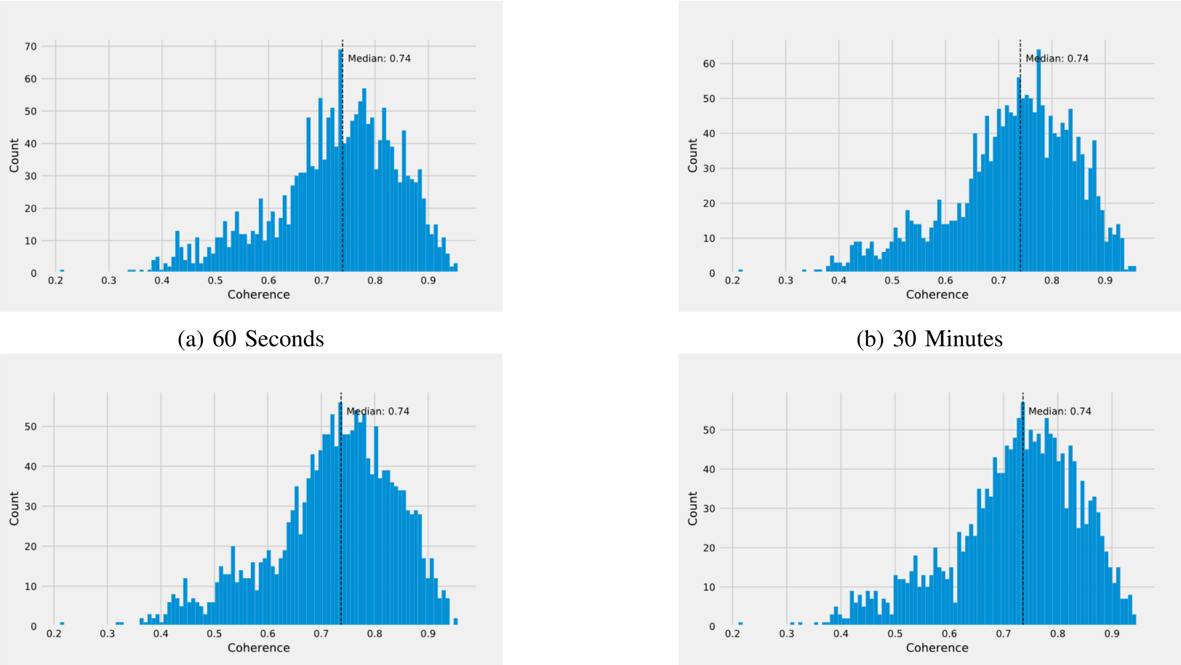


Fig. 5: The impact of the delay on the achieved coherence level of synthetic signals

When SEAM is applied by an adversary against a scheme, such as ELPA, such an adversary needs first to obtain the prediction coefficients and error correction codes which are transmitted by Alice during the agreement phase of ELPA. This can be achieved with relative ease by the adversary as they would configure the on board WiFi to listen in promiscuous mode, enabling the capture of all packets including those not addressed to it. This will then allow the adversary to perform an offline brute force attack until they acquire the key. The offline attack will use SEAM to produce synthetic signals which can be tried until they either identify the key agreed upon by Alice and Bob or they exhaust the solution space. The outcome of this attack will be communicated to the adversary by the error correction process; if it succeeds then the error correction will return the correct key; otherwise, the adversary would simply try the next synthetic signal. The steps involved in this attack scenario are summarized in Figure 7.

In our experiment we used all patients found within the MIT-BIH Normal Sinus Rhythm dataset, however we only looked at a delay of one minute as the previous experiments (see Figure 6) demonstrate little to no variation within the coherence between delays. Therefore, it is safe to assume that the performance obtained with a one minute delay can be experienced with larger delays.

To evaluate the performance of SEAM when applied against ELPA we need a metric that can inform not only on the success of these synthetic signals but also their quality. We decided to use the number of bit flips that occurs when attempting to repair the key within the error correction phase of ELPA, which can also be viewed as the ”hamming distance” between the key the target has generated versus the key the adversary has produced. A number of errors are expected to occur even in legitimate attempts due the discrepancies between sensors and their observation of the signal; however, a balance must be struck between tolerating the errors and enabling false acceptance of attempts made by an adversary. Therefore, the authors of ELPA have decided upon requiring that the number of errors should be below a reasonable threshold as defined in their paper being 36. Based on this threshold, when attempting to use stolen signals, without any prior modification applied to



(a) 60 Seconds

(b) 30 Minutes

(c) 6 Hours

(d) 12 Hours

Fig. 6: Variation of the coherence count achieved under varying sampling delays. Demonstrates little to no change between the two extremes (i.e., 60 seconds and 12 hours)

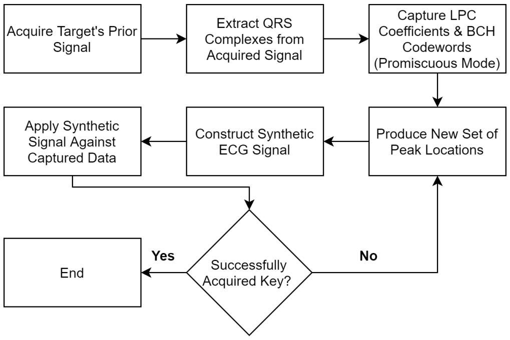

Acquire Target's Prior Signal
Extract QRS Complexes from Acquired Signal
Capture LPC Coefficients & BCH Codewords (Promiscuous Mode)
Produce New Set of Peak Locations
Construct Synthetic ECG Signal
Apply Synthetic Signal Against Captured Data
Successfully Acquired Key?
No
Yes
End

Fig. 7: Attack scenario demonstrating the approach an adversary may take to compromise a scheme such as ELPA

them, as input within ELPA the number of attempts below 36 is 12.74% only, however when applying SEAM to those same signals the number of attempts below 36 increases significantly to reach 71.97%. This is substantial improvement that places schemes, such as ELPA and alike, at risk of compromise by an adversary.

The histogram plotted on Figure 8 shows the number of bit flips that occur when the adversary attempts to compromise the key agreement scheme during the experiment. Therefore, it is capable of demonstrating the significant improvement that SEAM makes when compared to using past signals without any modification. We can see that almost three-quarters of SEAM attempts are below the error correction threshold, implying that these attempts would successfully agree upon the key that the target has generated. As for the attempts above the threshold, most of them are very close with only a few errors away from passing unlike the vast majority that fail without SEAM. Modifications to SEAM could be made in future which may enable the 25% that fail to succeed further exposing this vulnerability with ECG based key agreement schemes.

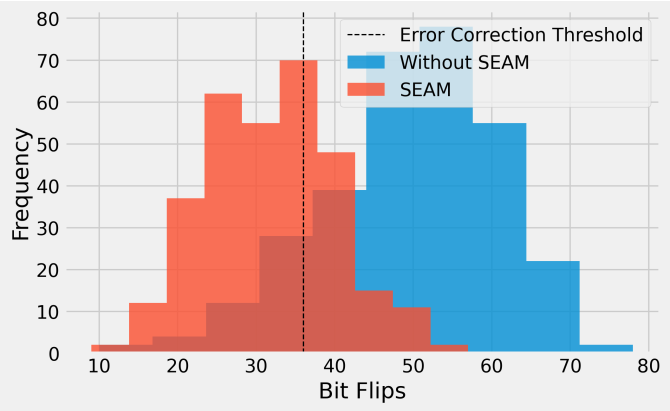


Fig. 8: Impact of SEAM on increasing the success rate of attack attempts against ELPA

V. Conclusion

This paper presented a novel attack technique, named SEAM, that takes advantage of a newly identified vulnerability in ECG based key generation and agreement schemes. SEAM relies on the use of prior recordings of ECG data, in combination with the perfect placement of peaks, to construct synthetic signals that imitate valid signals used in the key agreement process. The performance evaluation results highlighted that these synthetics can achieve a high level of coherence with the target signal, which translates into high probability of success (72 %) in compromising key agreement schemes, if the adversary could place the peaks in the correct locations. This, therefore, raises serious concerns about the security implications of using physiological signals within the key generation phase in BANs, and immediate actions are needed to mitigate potential attacks. In our future work, we will explore alternative methods, to a brute force approach, for peaks placement in order to reduce the cost of producing synthetic signals.

REFERENCES

[1] S. Ziegler, R. C. Woodward, H. H. Iu, and L. J. Borle. Current sensing techniques: A review. *IEEE Sensors Journal*, 9(4):354–376, 2009.

[2] A. Nag, S. C. Mukhopadhyay, and J. Kosel. Wearable flexible sensors: A review. *IEEE Sensors Journal*, 17(13):3949–3960, 2017.

[3] Iso/iec/ieee international standard - information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 15-6: Wireless body area network. *ISO/IEC/IEEE 8802-15-6:2017(E)*, pages 1–274, 2018.

[4] insightSLICE. Smart healthcare market - global market share, trends, analysis and forecasts, 2020 - 2030, July 2020.

[5] G. Zheng, R. Shankaran, W. Yang, C. Valli, L. Qiao, M. A. Orgun, and S. C. Mukhopadhyay. A critical analysis of ecg-based key distribution for securing wearable and implantable medical devices. *IEEE Sensors Journal*, 19(3):1186–1198, 2019.

[6] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta. Pska: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 14(1):60–68, 2010.

[7] Chunqiang Hu, Xiuzhen Cheng, Fan Zhang, Dengyuan Wu, Xiaofeng Liao, and Dechang Chen. Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. pages 2274–2282, 05 2013.

[8] E. K. Zaghouani, A. Jemai, A. Benzina, and R. Attia. Elpa: A new key agreement scheme based on linear prediction of ecg features for wban. In *2015 23rd European Signal Processing Conference (EUSIPCO)*, pages 81–85, 2015.

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

[10] Wanqing Wu, Sandeep Pirbhulal, and Guanglin Li. Adaptive computing-based biometric security for intelligent medical applications. *Neural Computing and Applications*, 32(15):11055–11064, November 2018.

[11] G. Zheng, W. Yang, C. Valli, L. Qiao, R. Shankaran, M. A. Orgun, and S. C. Mukhopadhyay. Finger-to-heart (f2h): Authentication for wireless implantable medical devices. *IEEE Journal of Biomedical and Health Informatics*, 23(4):1546–1557, 2019.

[12] M. A. Reshan, H. Liu, C. Hu, and J. Yu. Mbpska: Multi-biometric and physiological signal-based key agreement for body area networks. *IEEE Access*, 7:78484–78502, 2019.

[13] A. Juels and M. Sudan. A fuzzy vault scheme. In *Proceedings IEEE International Symposium on Information Theory,*, pages 408–, 2002.

[14] S. Pal. Ecg monitoring: Present status and future trend. *Encyclopedia of Biomedical Engineering*, pages 363–379, 2019.

[15] S. Serge Barold. Willem Einthoven and the birth of clinical electrocardiography a hundred years ago. *Cardiac Electrophysiology Review*, 7(1):99–104, 2003.

[16] Euan A Ashley and Josef Niebauer. *Cardiology explained*. Remedica, 2004.

[17] T. Yaqoob, H. Abbas, and M. Atiquzzaman. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. *IEEE Communications Surveys Tutorials*, 21(4):3723–3768, 2019.

[18] J. Xu, T. Gao, Y. Wang, and S. Zhou. A robust qrs detection method based on adaptive thresholding and particle swarm optimization. In *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, volume 1, pages 1301–1305, 2020.

[19] Zhong Zhang, Qi Yu, Qihui Zhang, Ning Ning, and Jing Li. A kalman filtering based adaptive threshold algorithm for QRS complex detection. *Biomedical Signal Processing and Control*, 58:101827, April 2020.

[20] Shaliza Jumahat, Gan Kok Beng, Norbahiah Misran, Mohammad Tariqul Islam, and Nurhafizah Mahri. Automatic QRS onset detection of ECG signal using secant line slope formula. In *2019 IEEE 15th International Colloquium on Signal Processing & Its Applications (CSPA)*. IEEE, March 2019.

[21] Marijn J. H. Heule and Oliver Kullmann. The science of brute force. *Commun. ACM*, 60(8):70–79, July 2017.

[22] Petre Stoica and Randolph L Moses. *Spectral analysis of signals*. Pearson Education, 2005.

[23] The Arrhythmia Laboratory The Beth Israel Deaconess Medical Center. The mit-bih normal sinus rhythm database, 1990.

[24] Ary L. Goldberger, Luis A. N. Amaral, Leon Glass, Jeffrey M. Hausdorff, Plamen Ch. Ivanov, Roger G. Mark, Joseph E. Mietus, George B. Moody, Chung-Kang Peng, and H. Eugene Stanley. Physiobank, physiotoolkit, and physionet. *Circulation*, 101(23):e215–e220, 2000.

[25] Yongjin Wang, Foteini Agrafioti, Dimitrios Hatzinakos, and Konstantinos N. Plataniotis. Analysis of human electrocardiogram for biometric recognition. *EURASIP Journal on Advances in Signal Processing*, 2008(1), 2007.

Jack Hodgkiss received the bachelor's degree in computer science from Manchester Metropolitan University, Manchester, U.K., in 2018. He is currently working toward the Ph.D. degree focusing on authentication within body area networks.

Soufiene Djahel (SM'16) received the M.Sc. degree in computer science from the University of Bejaia, Algeria, in 2007, and the Ph.D. degree in computer science from Lille 1 University of Science and Technology, France, in 2010. He has been a Senior Lecturer with the department of Computing and Mathematics, Manchester Metropolitan University, U.K., since 2015. His main research interests include Security and QoS issues in wireless networks, Intelligent Transportation Systems (ITS), and e-health. He has published more than 60 peer reviewed conference and journal papers in the reputable IEEE Core/Flagship conferences and journals in wireless networks and ITS research domain.

Zonghua Zhang (SM'18) received the Ph.D. degree in information science from JAIST, Japan, and the HDR Diploma degree in computer science from UPMC, France. He is currently with IMT Lille Douai, Institut Mines-Télécom. He used to work as a full-time Researcher with NICT, Japan, INRIA, France, and the University of Waterloo, Canada. He has contributed over a dozen national and international collaborative research projects dedicated to Cybersecurity. His research topics cover anomaly detection, network forensics, trust and reputation management, as well as security protocols. The current target scenarios include software-defined networking, network functions virtualization, and cyberphysical systems, such as e-healthcare and intelligent transportation systems. He serves as the Editorial Board Member of Computer and Security, Security and Communication Networks, and the International Journal of Network Security.