Towards Fast and Robust Authentication Schemes in Body Area Networks

Jack Hodgkiss

PhD

2022

Towards Fast and Robust Authentication Schemes in Body Area Networks

Jack Hodgkiss

A thesis submitted in partial fulfilment of the requirements of
Manchester Metropolitan University for the degree of Doctor of Philosophy

Smart and Sustainable Cities (S2C) Lab
Department of Computing and Mathematics
Manchester Metropolitan University, United Kingdom

PhD

2022

Contents

List of Tables

List of Figures

Acronyms

AC Autocorrelation.

AP Access Point.

BAN Body Area Network.

BANZKP Body Area Network Zero Knowldege Proof.

BCH Bose–Chaudhuri–Hocquenghem.

BLE Bluetooth Low Energy.

BOM Bill of Materials.

CGM Continuous Glucose Monitor.

COTS Commercial Off-The-Shelf.

DCT Discrete Consine Transformation.

DDoS Distributed Denial of Service.

DoS Denial of Service.

DWPT Discrete Wavelet Packet Transform.

ECC Error Correction Code.

ECG Electrocardiogram.

EEG Electroencephalogram.

ELPA ECG Linear Prediction Key Agreement.

EMG Electromyography.

FAR False Acceptance Rate.

FFT Fast Fourier Transform.

FRR False Rejection Rate.

HMAC Hash-Based Message Authentication Code.

HRM Heart Rate Monitor.

iARC **I**nducing **A**rtificial **R**andomness in the **C**hannel.

IEEE Institute of Electrical and Electronics Engineers.

IJS Improved Jules and Sudan.

KDC Key Distribution Center.

LPC Linear Prediction Coding.

MAC Media Access Control.

MARS Mobile Assisted RSSI Secret Key Extraction.

MBPSKA Multi-biometric and Physiological Signal-Based Key Agreement.

MEMS Micro Electromechanical System.

MITM Man-In-The-Middle.

NIST National Institute of Standards and Technology.

OPFKA Ordered-Physiological-Feature-Based Key Agreement.

PKI Public Key Infrastructure.

PPG Photoplethysmogram.

PSKA Physiological-Signal-Based Key Agreement.

RAFV Rotational Assisted Fuzzy Vault.

RSI Repetitive Strain Injury.

RSSI Received Signal Strength Indicator.

SEAM Synthetic Electrocardiogram Attack Method.

SKA Simple Key Agreement.

SKE Secret Key Extraction.

TI Texas Instruments.

UWB Ultra-Wide Band.

ZKP Zero Knowledge Proof.

Abstract

The emergence of Body Area Networks (BANs) has paved the way for real-time sensing of human biometrics in addition to remote control of smart medical devices, which in turn is beginning to revolutionise the smart healthcare industry. However, due to their limited power and computational capabilities they are vulnerable to myriad of security attacks, thus securing BANs is paramount to their success and wider adoption in the medical and nonmedical domain. Achieving the desired security level for BANs while adhering to their strict constraints imposed by the limited resources available is an ongoing challenge. Solving such a challenge will be the focus of my thesis. In particular, my thesis will develop a novel, fast and robust authentication mechanisms amongst BAN devices while exploring new potential vulnerabilities that may threaten the existing approaches. To accomplish this goal the thesis provides a review of the state-of-the-art literature exploring authentication protocols that focus on biometrics, physical channel characters or other approaches, before proceeding to introduce three novel works. Firstly, identifying a concerning vulnerability within existing Electrocardiogram (ECG) based schemes, secondly, a solution to mitigate this exploit and finally a strategy which aims to reduce the time taken to complete the authentication process.

Publications List

Please note that the work conducted in this thesis has been either published or submitted and accepted prior to submission of this thesis. Whilst I share authorship of this papers with my Director of Studies and his colleague I can confirm that they did not provide any contribution beyond reviewing of manuscripts.

- J. Hodgkiss, S. Djahel and Z. Zhang, ”A New Attack Method Against ECG-Based Key Generation and Agreement Schemes in Body Area Networks,” in IEEE Sensors Journal, vol. 21, no. 15, pp. 17300-17307, 1 Aug.1, 2021, doi: 10.1109/JSEN.2021.3079177. Chapter 3
- J. Hodgkiss and S. Djahel, ”Securing Fuzzy Vault Enabled Authentication in Body Area Networks based Smart Healthcare,” in IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2020.2991387. Chapter 4
- J. Hodgkiss and S. Djahel, ”MARS - Towards Mobile Assisted RSSI Secret Key Extraction Strategy in WBANs” 2022 19th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2022 doi: 10.1109/CCNC49033.2022.9700605. Chapter 5

Acknowledgements

I would like to thank my parents, Sarah and Paul, and my brother, Harvey, for the support and patience they have provided over the past three years. It is they who pushed me to complete this thesis. Also, my friends, David and Joshua who were there throughout the entire process.

Secondly, I would like to thank my Director of Studies, Dr. Soufiene Djahel for selecting me for this PhD position and opportunities it has provided. In addition to the support for guidance they have offered over the years.

Finally, I would like to thank the Manchester Metropolitan University for the student scholarship that has funded me during my studies.

Chapter 1

Introduction

This thesis aims to answer the following research question; how can we meet the stringent requirements of BANs based e-healthcare systems, in terms of energy efficiency and latency, while maintaining the desirable level of security and privacy of patients' sensitive health data? To that effect, how can we efficiently combine physical channel properties with the patient's vital signs to provide robust and cost-effective authentication techniques?

BANs is a network composed of wireless sensors that are situated on or within the human body. By allowing for wireless sensor devices to operate on or within the human body new and innovative applications may be developed (e.g., advanced vital sign monitoring, media playback, and embedded key for access to secure areas). Institute of Electrical and Electronics Engineers (IEEE) 802.15.6 (IEEE, 2018) is an international specification for low power, short-range, and extremely reliable wireless communication within the surrounding area of the human body. The specification allows for the application of these sensors for use within the medical, entertainment, and military domains.

Focusing on the potential application of BAN within the medical domain these sensors promise to provide medical professionals unprecedented real-time access to the vital signs of their patients (e.g., heart rate, blood glucose levels, and body temperature). Devices present within a BAN are not limited to passively monitoring vital signs of the wearer, as they may take on a more proactive role, controlling medical devices such as a pacemaker, insulin pump, and heating pads. These devices and others can be controlled remotely by the assigned medical professionals, automated intelligent systems, other sensors present within the BAN. An example of this would be an insulin pump receiving commands from a Continuous Glucose Monitor (CGM) system, to make micro adjusts to the level of insulin being released into the wearer. The medical industry attracts significant investment from private and public sources, See Figure 1.1 for the healthcare expenditure of the G7 nations as a percentage of GDP.

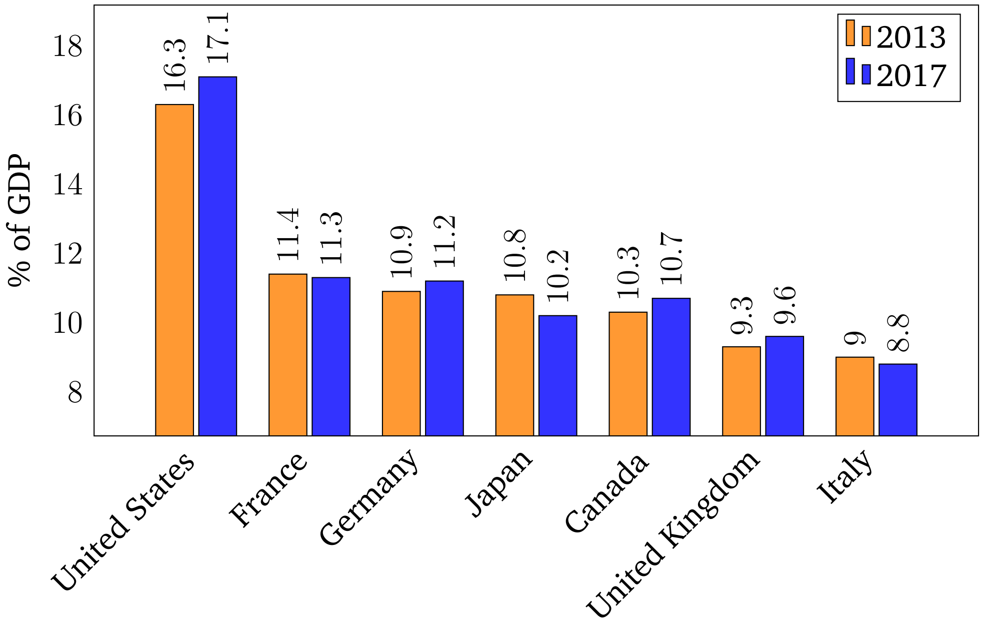


Figure 1.1: Healthcare expenditure of G7 countries as a percentage, from the Office of National Statistics

Due to the intended use cases of these devices, an appropriate security service must be implemented and made available to users to prevent unauthorised access and control of these devices. Several attacks may be carried out by an adversary who wishes to harm either the network or its users, an adversary may attempt the following; eavesdropping attack, impersonation attack, and data manipulation. In addition to these aforementioned attacks, the adversary may also aim to physically harm users of these devices which could be achieved if these sensors are improperly configured and are vulnerable to an attack that allows the adversary to remotely override the safety limits of a device such as an insulin pump. An example for instance could see users receive too little or too much insulin which can cause an insulin-induced coma or even death. It is clear due to the risks alone that securing these devices is paramount to the successful adoption of them by medical institutions (e.g, hospitals, clinics and research facilities) in addition to private individuals. Also, it is a legal requirement (Data Protection Act, 2018) for such devices and networks to be adequately secured due to the transmission of private medical data.

Unfortunately due to the miniature size of these devices, they are severely limited in what authentication protocols can be carried out. This is due to the device's limited processing power, memory, in addition to the low rate of power consumption that these devices must achieve. Therefore, new authentication processes must be developed to ensure that the devices are secure for deployment. However, this area of research is new and therefore limited, providing the opportunity for novel and groundbreaking research to be achieved. The IEEE 802.15.6 specification does attempt to propose a series of security mechanism designed to prevent the earlier mentioned attacks whilst conforming to the limited capabilities of these devices, however, these attempts have been shown to be inadequate with many weaknesses and vulnerabilities discovered (Toorani, 2015). Therefore, the primary objective of this work shall be to develop an authentication protocol that meets the stringent requirements of these devices.

There are a number of design factors that need to be considered when developing such authentication protocols. These are the following:

- **Speed:** any authentication protocol developed must be fast due to the environment that it shall be deployed within, where time wasted waiting for authentication to complete could risk harm to individuals and their life.
- **Robustness:** the designed protocol must be capable of successfully defending against adversaries attempting to compromise the authentication process. This is very important due to the critical nature of the data collected and equipment used.
- **Cost-Effectiveness:** due to the miniature size of these devices resources such as memory, computation and power are at a premium and therefore any scheme developed must balance the two previous design factors with the limited resources in mind.

To summarise, the main aim of this work is to design an authentication protocol that meets the specific constraints of these miniature sensors that control medical devices or report vital signs readings. This authentication protocol must be robust against security attacks that threaten the authentication and communication facilities of these devices. The attacks include; Man-In-The-Middle (MITM), replay attack, injection attack, forgery attack. The protocol must also ensure that it remains efficient in terms of computational complexity, energy consumption and memory usage, in order to meet the constrained resources of these devices. Moreover, the design of this protocol should include an original approach to combine the biometrics being collected by body sensors with the physical channel characteristics. It must be able to function with a high level of security while handling the fuzzy nature of biometrics, as various body measurements are not exact due to sensors resolution or noise distorting the reading.

The chapters of this thesis is structured as follows;

- **Chapter 2**: contains a review of literature related to communication standards related to BANs, common security threats and state-of-the-art contributions focusing on authentication schemes that utilise physiological signals or physical channel characteristics.
- **Chapter 3**: provides the first contribution originating from this body of work. It highlights and exposes a vulnerability present within authentication scheme whereby an adversary can use old ECG signals to break present and future keys generated from these schemes. Something previously deemed not possible.
- **Chapter 4**: proposes a method to mitigate the vulnerability identified within Chapter 3 by combining both the physiological signal of the wearer and the sensors physical channel characteristics which is a major goal of this thesis.
- **Chapter 5**: focuses on improving key generation times which plagues schemes in certain scenarios that are common body sensor networks
- **Chapter 6**: summarises the contributions made throughout this thesis before exploring where potential future work may exist.

Chapter 2

Literature Review

2.1 Introduction

As discussed in the previous chapter, the security facilities readily available to BANs, is limited by the constraints imposed due to the small form factor of the sensors that compose such a network. These restrictions put in jeopardy the privacy and safety of users in addition to the successful adoption of such important technology. Therefore, significant research has been conducted in recent years in order to overcome this open and ongoing challenge. Researchers have explored a number of different avenues when attempting to solve this issue, such as using physiological and wireless channel characteristics or relying on conventional cryptography.

The remainder of this chapter is split into the following sections; Section 2.2 will explore communication standards related to BANs, Section 2.3 will outline threats or attacks that could be launched by an adversary, Section 2.4 will investigate the state-of-the-art authentication schemes for BANs, and finally, Section 2.5 will conclude this chapter.

2.2 Communication Standards for Body Area Networks

At present, there are a number of international communication standards related to BANs and their purpose of real-time health monitoring. Communication standards guarantee interoperability between communication components that originate from different manufactures, provided that they conform to the same standard. This is possible due to communication standards which define and govern various aspects of a network, such as; physical layer, routing, and security requirements. Another important aspect of communication standards is ensuring that they abide by local law and communication regulators with regard to radio spectrum utilisation, power consumption and maximum radiation emitted, which is especially important when discussing BAN sensors as they have direct contact with human tissue and organs.

IEEE 802.15.6 (IEEE, 2018) is an international standard defined by IEEE and it outlines how short range, low powered, wireless communication may operate in close proximity to humans, either worn or implanted. This specification provides support for a date rate starting at 0.25 Mbps and up to 10 Mbps, which is ample amount of bandwidth for the intended purposes. The standard discusses also three levels of security that the network may provide. **Level 0**: unauthenticated and without encryption, **Level 1**: authentication without encryption, **Level 2**: authentication with encryption. In the IEEE standard there exists four protocols for generating a master key however, in (Toorani, 2015), the authors highlight that these four protocols are vulnerable to myriad of exploits and therefore is incapable of ensuring the desired level of authentication and security. This remains an active issue as it has not been addressed by the specification. In addition to IEEE 802.15.6 there also exists more general purpose communication standards that could be utilised within a body area network primarily due to their low power consumption. This includes; Bluetooth Low Energy (BLE) (*Bluetooth Core Specification*, 2021), Zigbee (*Zibgee Specification*, 2015) and Wi-Fi HaLow (IEEE, 2019). See Table 2.1 for a summary of these competing communication standards.

Name	Description
(*Bluetooth Core Specification*, 2021)	Bluetooth Low Energy is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range to IEEE 802.15.6
(*Zibgee Specification*, 2015)	Zigbee is based upon the IEEE 802.15.4 specification for the construction of small and low-powered personal area networks. As Zigbee has data rate of 250 kbit/s it is ideal medical data collection. Zigbee networks use 128-bit symmetric key for securing against intrusion.
(IEEE, 2019)	Wi-Fi HaLow, aka IEEE 802.11ah, utilises the 900MHz frequency band to provide Wi-Fi networks extended range whilst also offering low energy consumption. Can compete against BLE as it does offer significantly higher data throughput and range.
(IEEE, 2018)	IEEE 802.16.6 is an international standard on low-powered and short range wireless communication that may operate on or within the human body

Table 2.1: Communication standards

2.3 Security Threats Against Body Area Networks

In this section, we shall explore the myriad of attacks that threaten the security of a BAN, as it is important to be aware of what you are defending against when attempting to develop a security scheme. We shall investigate how these attacks operate, possible motives that an adversary may have for deploying such an attack in addition to the defences that can be deployed in order to mitigate or prevent an attack in the first place.

2.3.1 Attacks

The attacks that shall be explored in this section are the following; deauthentication, MITM, Distributed Denial of Service (DDoS), eavesdropping, offline and finally, acoustic attacks. See Table 2.2 for a summary of these attacks.

Deauthentication attack: this attack attempts to disrupt communication between a sensor and the Access Point (AP) it is currently connected to. It involves an adversary making an undesired request to deauthenticate its target from the AP, thus preventing further communications between these devices. This attack is possible as some communication standards found within the IEEE 802 Set, allow for deauthentication frames to be transmitted in an unauthenticated and unencrypted manner (Bellardo and Savage, 2003). This therefore, enables an adversary to easily spoof a deauthentication frame with the Media Access Control (MAC) address of the target, thus ejecting it from the network and preventing the flow of network traffic. It is feared that this same attack could be applied to BANs (Sethuraman et al., 2019).

MITM attack: this attack sees the adversary attempt to situate themselves between legitimate network users and infrastructure with the primary goal of being able to capture and manipulate all network traffic (Callegati et al., 2009). This would allow the adversary to prevent the wearer of medical devices being informed of concerning changes to their health in addition to stopping remote commands from ever being received (Sinha et al., 2017).

DDoS attack: this attack involves the adversary performing a Denial of Service (DoS) attack in a distributed manner. A DoS attack consists in the adversary overwhelming the network with so many requests so that the system becomes incapable of handling any further requests, legitimate or malicious. Whereas a DoS attack originates from a single source and can therefore be easily blocked, the same cannot be said for a DDoS (Salim et al., 2020). This is because, a DDoS has that attack originating from many devices that are enrolled within a botnet. Not only does this make it harder to mitigate, it also allows for a much stronger attack allowing for even larger targets being vulnerable. This attack could be levied against the internal network of a hospital or external services that they rely upon. In addition to this, the sensors could be targeted to be enrolled within a botnet so that they are not victims of DDoS attack, however unwittingly be part of the attack against a network.

Eavesdropping attack: this attack is a passive attack, as the adversary only observes network activity and makes no attempt to modify or manipulate such traffic. This is made possible by configuring their Commercial Off-The-Shelf (COTS) hardware to listen in promiscuous mode, which will instruct the radio receiver to decode all transmissions especially those not addressed to it (Anand et al., 2005). As this attack is carried out passively it is impossible to detect any eavesdropping being conducted by an adversary.

Offline attack: an offline attack is an attack that is carried by an adversary on their own machine rather than a network. The attack shall involve some form of data, which could be hashed passwords leaked from a database and the adversary can begin to try various combinations of passwords in order to derive the original password. As they are computing this on their own machine they do not have to fear of being detected nor rate limited as they will make no interaction with networked resources until after the offline attack has finished (Blocki et al., 2018).

Acoustic attack: finally this attack involves the use of ultrasonic and other sound frequencies in order to disrupt or manipulate the target sensor (Hamed and Khalek, 2019; Fu and Xu, 2018). These attacks work because of onboard sensors, such as a Micro Electromechanical System (MEMS) accelerometer found on fitness trackers, detect these ultrasonic frequencies and register them as valid input. Thus, misleading the wearer about the fitness activities (Trippel et al., 2017). Acoustic attacks can also be carried out against pacemakers, cardiac defibrillators, and insulin pumps (Sethuraman et al., 2019) which can cause significant harm if that is what the adversary intends.

2.3.2 Countermeasures

In order to defend against the aforementioned attacks, network administrators and users employ the following defences; authentication, encryption, firewall and Hash-Based Message Authentication Code (HMAC).

Authentication: is the process of validating the identity of a user or system and is achieved by some challenge requiring possession of some secret such as a password or key. Without authentication an adversary could effortlessly impersonate anyone or anything and therefore gain access to critical systems. Authentication can be categorised as follows;

- One-way authentication: allows for only one sensor to authenticate the other, typically a device that provides access to network resources such as a gateway or a server.

- Mutual authentication: allows for both parties to authenticate one another providing a higher level of trust between them.
- Anonymous authentication: allows for authentication without leaking the identity of the user.

Encryption: is the act of converting plaintext into ciphertext and thus securing it from being accessed by unwanted individuals. Encryption is useful for storing and transmitting data securely as you cannot ensure that nobody that is unauthorised, could acquire the data. Encryption is achieved with the use of mathematical techniques whereby data is secured with the use of key. This key can either be symmetric - one key for both encryption and decryption or asymmetric - one key for each of the processes.

Firewall: a firewall is a method available to network administrators to protect the network by limiting incoming and outgoing communication with well defined rules. This could range from something simple such as blocking all incoming communications or a rule to block access to specific ports from everything not local.

HMAC: is a cryptographic technique that allows for the recipient of a message to authenticate that the content has not been modified during transmission (Bellare et al., 1996). The process involves the sender using a hash algorithm to generate a hash of the intended message and a secret key that is already in the possession of the receiver. The sender will then transmit the message and the HMAC to the receiver who will then take the received message and combine it with the secret key and produce a hash which shall then be compared against the HMAC. If they match then the receiver shall know the message is authentic, however if it does not match then the receiver will know the message has been modified during transmission and can be discarded.

Attack	Motivation	Countermeasures
Deauthentication	Deny and disrupt network communications	Ensure the deauthentication frame is authenticated
MITM	Capture and manipulate network between users and services	Mutual authentication, encrypted communications and use of HMAC to validate message authenticity
DDoS	Deny and disrupt network communications	Detect attack traffic and respond by rerouting to handle across multiple systems, firewalls could be used to block troublesome traffic or could use DDoS protection services
Eavesdropping	Capture all network traffic	Cannot be prevented due the nature of wireless communication, however, it can be mitigated with the use of encryption to keep data private
Offline	Acquire information such as passwords or encryption keys	Ensure that no data is shared in plain-text in addition to refreshing keys regularly
Acoustic Attack	Manipulate and deceive sensor readings	Use enhanced hardware and software algorithms that can detect this type of manipulation

Table 2.2: Table summarising attacks, motivations and Countermeasures

2.4 Authentication Schemes for Body Area Networks

In this section we shall explore the related state of-the-art literature on developing authentication schemes for body area networks, which is an important first step to ensure that we are aware of what has and has not been attempted by other researchers. In this literature review we shall categorise the works into the following categories; physiological-based authentication schemes, wireless channel-based authentication schemes and cryptographic-based authentication schemes. Also see Table 2.3 for a summary of all literature exploring evaluation methods, strengths & weaknesses and other comparison metrics. The authentication schemes within review shall typically achieve authentication through the generation and exchange of a symmetric key, however, other approaches shall be explored.

2.4.1 Physiological-based authentication schemes

Physiological-based authentication schemes are schemes which utilise physiological signals in order to provide authentication mechanisms to the users and network (Rui and Yan, 2019). Physiological signals, are measurements that originate from various processes that the human body undertakes such as; O2 saturation, heart rate, body temperature and electrical activity of heart, muscles and brain. These physiological signals can be measured with the use of a pulse oximeter, Heart Rate Monitor (HRM), thermometer, ECG, Electromyography (EMG) and Electroencephalogram (EEG) respectively. Within the current literature, the most common physiological signal used within authentication schemes targeting BANs is the ECG signal, as it is meets three design criteria discussed in (Poon et al., 2006; Venkatasubramanian et al., 2008). These criteria are described as follows;

- **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.

See Figure 2.1 for an illustration of what an ECG signal looks like.

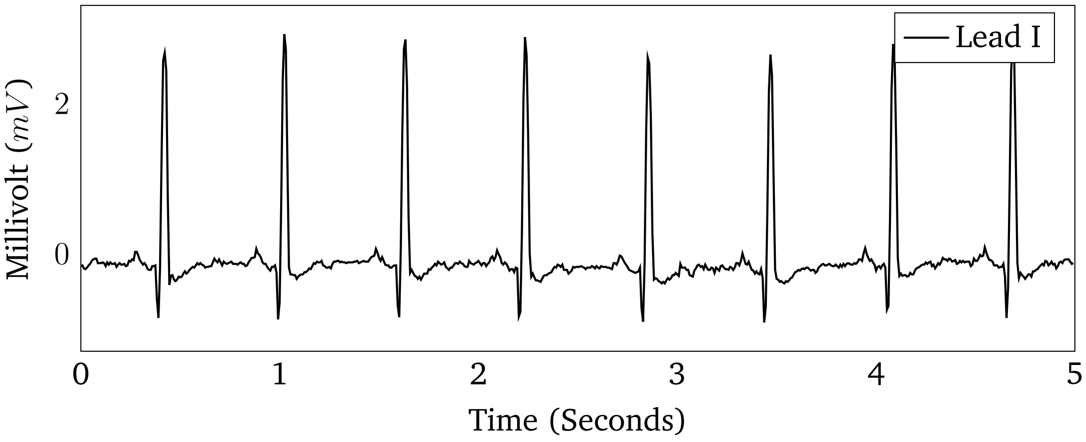


Figure 2.1: Five second ECG signal sampled at $128Hz$, obtained from NSRDB Dataset

In (Venkatasubramanian et al., 2010) the authors propose a scheme known as Physiological-Signal-Based Key Agreement (PSKA) which enables two separate ECG sensors to agree upon a symmetric key for the purpose of authentication and encryption, whilst not requiring any form of predeployment or prior knowledge. PSKA achieves this by concealing the key within a fuzzy vault, which is a cryptographic primitive introduced in (Juels and Sudan, 2002), that is capable of concealing a secret that can only be revealed if enough features are known. The fuzzy vault can achieve this in the following steps; **1)** set the coefficients of a polynomial to the secret, **2)** project a set of features onto the polynomial, **3)** conceal the polynomial by inserting chaff points, **4)** publish or share the vault, **5)** recover the polynomial by utilising a set of features identical or similar to the features originally projected onto the polynomial. PSKA uses this primitive as the mechanism for sharing the symmetric key with another sensor, the features used are extracted from the ECG or Photoplethysmogram (PPG) signal. The feature extraction process is simple, with a simple peak detection algorithm applied against the signal within the frequency domain, which can be acquired with a Fast Fourier Transform (FFT).

In the evaluation of PSKA the authors present a scheme that performs rather well, with key agreement times at around four seconds, with the majority of that being needed to sample enough data for feature extraction. However, one weakness of the scheme would be the large communication overhead required when sharing the vault with another sensor. This is due to the large number of chaff points that are required to conceal the secret as the strength of the fuzzy vault is tied directly to the number of chaff points. To alleviate this issue, the authors in (Hu et al., 2013) present a scheme based upon PSKA known as Ordered-Physiological-Feature-Based Key Agreement (OPFKA) which attempts to reduce the communication overhead associated with PSKA. OPFKA achieves this by requiring that features are recalled within the order that they were locked within the vault. By doing so the security of the vault increases which can then be traded for a reduced vault size without lowering the strength of the vault when compared to PSKA.

In (Zaghouani et al., 2015), the authors present a scheme known as ECG Linear Prediction Key Agreement (ELPA), which differs from the aforementioned schemes as it derives the symmetric key for the ECG signal itself. ELPA achieves this by using Linear Prediction Coding (LPC) which is typically used within audio processing. LPC when applied against the ECG signal produces a set of errors and set of coefficients. The errors are transformed into the key using a pulse train code and therefore are not transmitted to the receiver. Instead, the coefficients are sent as these will provide the receiver with the ability to arrive at the same set of errors once combined with their own reading of the ECG signal. ELPA greatly reduces the communication overhead incurred when compared to the previously mentioned schemes, as it does not rely upon transmitting a large vault.

The authors in (Reshan et al., 2019), propose a scheme known as Multi-biometric and Physiological Signal-Based Key Agreement (MBPSKA), that uses both physiological signals and biometrics to deliver a key agreement scheme with greater reliability and security. This is possible as the scheme uses both ECG and fingerprints from the patient to conceal the key during transmission between sensors. The use of the fingerprint enables MBPSKA to deliver a higher level of security by XORing the key with the minutiae or features of the fingerprint. In addition to this just like OPFKA (Hu et al., 2013), it uses order-invariance to further improve the security of the scheme allowing for a much smaller fuzzy vault to be transmitted thus reducing communication overhead when compared to PSKA (Venkatasubramanian et al., 2010). The authors of MBPSKA, demonstrate that it is more efficient to existing schemes whilst still delivering a high level of security with defence against various attacks. However, one concerning aspect of the scheme is the use of static biometrics such as fingerprints, which do not change, therefore posing a potential weak spot if an adversary ever managed to collect the fingerprint of their target.

In (Sammoud et al., 2020) the authors propose a key generation and establishment protocol for sensors measuring ECG. In their proposal they generate a symmetric key derived from the ECG signal available to sensors within the network. The scheme relies on error correction codes and morphing function in order to generate and agree upon the key. Unlike prior schemes it explores its capabilities in defending against various attacks such as; impersonation, eavesdropping and MITM. This has been proven with the use of informal and formal methods such as; AVISPA (Armando et al., 2005). Finally this scheme also manages to achieve this with reduced energy consumption, compared to other schemes.

2.4.2 Wireless Channel-based authentication schemes

Wireless channel-based authentication schemes are schemes that exploit characteristics found within the physical layer of wireless transceivers. Schemes categorised as such may utilise characteristics such as Received Signal Strength Indicator (RSSI). What benefits these schemes bring, as opposed to physiological-based authentication schemes, is that these characteristics can be found and accessed on all wireless transceivers. Whilst physiological-based authentication schemes fragment the network, as sensors can only perform key generation and agreement with similarly capable sensors, wireless channel-based authentication schemes do not have this issue and are therefore universal.

At the foundation of any wireless channel-based authentication scheme is the desire to observe the variations in the wireless channel between the sensors involved in the authentication process (Premnath et al., 2013). To achieve this, there is a need to transmit and receive network frames, extract features and then attempt to reconcile this information, as described in (Jana et al., 2009). The process for wireless channel-based authentication can be described generally as follows; a scheme typically involves two sensors that wish to generate and agree upon a symmetric key. At the start one of the sensors shall send transmission probes to the other. The receiver shall extract the RSSI values from each probe it receives. This process shall last only a short duration, around 100ms, as at the end the receiver shall quantize the measured RSSI values, converting them into discrete bits, see Equation 2.1. The role of sending and receiving of transmission probes must swap between sensors at a high frequency in order to ensure that not too much time has passed making reconciliation between the two sensors measurements impossible. Once this has been completed the sensors shall swap roles and will continue until enough bits have been extracted allowing for the generation of a key with a desired size. With enough bits, have been extracted, one of the sensors will generate and send Error Correction Codes (ECCs) to the other, allowing for the identification and repair of any errors or bit mismatch. Finally, once the errors have been repaired and confirmation that both sensors are in possession of the same symmetric key they can commence secure and authenticated communication.

$$f(n) = \begin{cases} 1 & \text{if } n > \mu + \alpha * \sigma \\ 0 & \text{if } n < \mu - \alpha * \sigma \end{cases} \tag{2.1}$$

Research surrounding wireless channel-based authentication has focused on improving the time taken to construct the symmetric key. Recent literature may focus on making the scheme quicker in general or attempt to tackle situations when the characteristics become stagnant and therefore suffer low bit generation. Situations that may cause this issue include when sensors are stationary which could be common for BAN sensors, as they are either worn or implanted within the same patient, therefore suffer from low bit generation.

In (Li, Wang, Daneshmand and Fang, 2017), the authors propose a technique for increasing the rate at which the key can be generated between two sensors, intended when the internode distance remains static, causing poor variation in channel characteristics. This technique requires the establishment of a cooperative virtual group between sensors that are already initialised and available to assist. When a sensor outside the group intends to communicate with a sensor or sensors the group will render aid, by synthesising RSSI to make up for low variation. This is possible as the two sensors attempting to generate a key are acquiring information from multiple sources, thus increasing the rate of bit extraction. The authors of this paper have since followed it up with (Li, Wang and Fang, 2017) where they look further at the improvements it provides in addition to testing its resistance against eavesdropping. One disadvantage of this approach would be the potential for collisions between packets, for which, the probability would increase as the size of the virtual group increases. This would in turn reduce the effectiveness of the scheme. No data has been provided to demonstrate what an ideal group size would be.

The authors of (Li and Wang, 2016) identify that an existing wireless channel scheme (Zhang et al., 2013) suffers from significant communication overhead. This communication overhead arises due to the need to correct errors or discrepancies between the two sensors' measurements of RSSI. To alleviate this issue they propose the use of either Improved Jules and Sudan (IJS) or Reed-Solomon Codes (Reed and Solomon, 1960). The motivation for this, is that too much energy is used by communicating check-bits between sensors, in addition, too much is being revealed enabling the adversary to launch an attack.

In (Revadigar et al., 2015) the authors propose a method known as **I**nducing **A**rtificial **R**andomness in the **C**hannel (iARC) for the purpose of increasing entropy and bit generation rate in situations where the channels are static such as no mobility. This therefore, increases security strength, whilst reducing the time taken to generate the key. The authors achieve this by using dual antennas and frequency diversity, in doing so, enabling a 128-bit key to be generated within 160ms. However, this comes at a cost, specifically the dual antennas increasing the Bill of Materials (BOM), in addition to space and power requirements. This requirement of dual antennas may also run into resistance with the lack of devices equipped with such an arrangement of hardware.

In more recent works such as; (Javali et al., 2021) the authors propose a method for generating symmetric keys by exploiting the wireless-channel characteristics between multiple sensors. However, their approach focuses on situations where one device is out of the range of another through the use of a relay node. This could be extremely beneficial for situations in healthcare where sensors are distributed over a large distance such as in paramedics attending the scene of a medical emergency, somewhere within a town or city. They also propose a multi-level quantization method which combined with relay node achieves extremely high results with regard to bit entropy without revealing anything to an eavesdropper. In (Kumar et al., 2021), the authors suggest that in certain scenarios the measurements are highly correlated, however, they are not similar and would benefit from preprocessing before quantization. Therefore, the authors propose to apply Discrete Wavelet Packet Transform (DWPT) against the wireless channel measurements. In their simulation results they were able to demonstrate an improvement over existing results whilst also capable of passing all the National Institute of Standards and Technology (NIST) randomness tests. The authors in (Gao et al., 2020), also propose an enhanced preprocessing phase to their RSSI key generation scheme, in order to make it lightweight and efficient. Their proposal involves the use of Discrete Consine Transformation (DCT) which helps removing the small differences between the measurements carried out between the two sensors. Once completed, the data is provided to an adaptive quantization function to further increase the rate at which bits are generated for the symmetric key. The authors demonstrate that their scheme is capable of generating strong keys at a quick rate due to their alternative preprocessing and quantization method.

2.4.3 Cryptographic-based authentication schemes

As mentioned earlier, cryptographic techniques can be quite demanding for such limited devices and therefore not always appropriate. However, some state-of-the-art literature attempts to reduce the demands imposed by such schemes, thus making it suitable for BANs.

In (ABI-CHAR et al., 2007), the authors propose the combined use of elliptic-curve cryptography, ElGamal signature scheme (Elgamal, 1985) and Simple Key Agreement (SKA) (Ryu et al., 2003), which enables authenticated key agreement between low-powered mobile devices. Since the scheme was designed with the needs of low-powered mobile devices, it is possible that this work could be adapted for BANs. The authors also demonstrate, that their scheme is capable of resisting against a slew of attacks, however, some researchers have raised concerns regarding the use of certain elliptic curves, as they can be weaker than others (Bernstein and Lange, 2013). Another issue with elliptic-curve cryptography found within (ABI-CHAR et al., 2007) is the reliance on Public Key Infrastructure (PKI) which can make the process harder to maintain. More recently, work such as; (Liu et al., 2014; Guo et al., 2015; Saeed et al., 2018), attempt to provide additional features such as anonymous authentication.

In (Khernane et al., 2016), the authors propose a method of securing BANs with the use of Zero Knowledge Proof (ZKP), known as Body Area Network Zero Knowldege Proof (BANZKP). The authors boast about their schemes significant reduction in time, memory and energy consumption when compared to other schemes such as; TinyZKP (Ma et al., 2014) and W-ECDSA (Wang et al., 2011). The authors in (Bu and Potop-Butucaru, 2018), have identified that a number of failings present within (Khernane et al., 2016) and propose BAN-GZKP. Firstly, (Khernane et al., 2016) is vulnerable to a number of attacks such as; DDoS and replay attack. The authors in (Bu and Potop-Butucaru, 2018), have proposed a number of additions to prevent and mitigate this. Also, (Bu and Potop-Butucaru, 2018), explores the impact the human body and its various postures, have on their scheme and identifies that their scheme does not suffer as much when compared to BANZKP. Finally, the authors in (Bu and Potop-Butucaru, 2018), demonstrate that BAN-GZKP is capable of achieving all of this without using more memory or energy when compared to BANZKP.

Table 2.3: Summary of authentication schemes

Name	**Category**	**Summary**	**Pros (+) & Cons (-)**	**Evaluation Method**
(Venkatasubram et al., 2010)	Physiological	Allows two BAN sensors to agree upon a symmetric key by concealing with the aid of physiological signals such as ECG or PPG	+ Fast + Low latency − Communication overhead − Fragments network	Simulation

Continued on next page

Table continued from previous page

Name	Category	Summary	Pros (+) & Cons (-)	Evaluation Method
(Hu et al., 2013)	Physiological	Improves (Venkatasubramanian et al., 2010) by removing order-invariance and thus increasing the level of security that can be provided with small vault sizes and reduced communication overhead	+ Reduced communication overhead − Communication overhead	Simulation
(Zaghouani et al., 2015)	Physiological	Enables two BAN sensors to generate a key from the features extracted from an ECG signal utilising LPC	+ Fast + Low latency + Reduced communication overhead − Fragments network	Simulation
(Reshan et al., 2019)	Physiological	Novel application of both physiological and biometric measurements to agree upon a key between BAN sensors	+ Reduced communication overhead + Provides higher level of security − Requires registration of fingerprint features across BAN sensors − Security depends on fingerprint remaining a secret	Simulation
(Sammoud et al., 2020)	Physiological	Permits BAN sensors within a network to generate and establish a key using ECG signals based on error correction codes and morphing function	+ Fast + Low power consumption − Fragments network	Simulation
(Li, Wang, Daneshmand and Fang, 2017)	Wireless Channel	Attempts to improve generating symmetric keys via RSSI, by increasing entropy with the aid of cooperative BAN sensors in a virtual group	+ Fast + Does not fragment network − Benefits only achieved after enough BAN sensors join the group − Too many BAN sensors can be detrimental	Test bed

Continued on next page

Table continued from previous page

Name	Category	Summary	Pros (+) & Cons (-)	Evaluation Method
(Li, Wang and Fang, 2017)	Wireless Channel	Improves upon (Li, Wang, Daneshmand and Fang, 2017) by providing resistance against eavesdropping	+ Protection against eavesdropping on the key being generated	Test bed
(Li and Wang, 2016)	Wireless Channel	Allows for the generation of a symmetric key without the need for significant communication overhead as seen in (Zhang et al., 2013), by providing alternative encoding and decoding schemes	+ Significant reduction of communication overhead − Suffers from low entropy with small internode distance	Test bed
(Zhang et al., 2013)	Wireless Channel	Enables key generation from channel information such as RSSI and uses Fuzzy Vault to reconcile key	+ Does not fragment network − Significant communication overhead	Test bed
(Revadigar et al., 2015)	Wireless Channel	Uses dual antennas and frequency diversity to increase entropy and lower key generation time for BAN sensors with no or little mobility	+ Extremely fast + Does not fragment network + Not limited by sensor mobility − Increases hardware requirements for already constrained devices	Test bed
(Javali et al., 2021)	Wireless Channel	Proposes a multi-level quantization function for generating symmetric keys from wireless channel characteristics, in addition to enabling key generation between a relay allowing for nodes out of range to authenticate	+ High entropy in bits generated + Protection against eavesdropper + Allows for authentication between nodes outside communication range	Test bed
(Kumar et al., 2021)	Wireless Channel	Suggest the use of DWPT when preprocessing wireless channel characteristics in order to improve similarity between BAN sensors	+ High entropy	Simulation
(Gao et al., 2020)	Wireless Channel	Scheme generates symmetric key between BAN sensors using RSSI measurements with enhanced preprocessing and quantization to generate stronger keys faster	+ Strong keys + Fast + Simple	Test bed

Continued on next page

Table continued from previous page

Name	Category	Summary	Pros (+) & Cons (-)	Evaluation Method
(ABI-CHAR et al., 2007)	Cryptographic	Enables authenticated and encrypted communication using elliptic curves	+ Quick & efficient − Requires PKI	Simulation
(Liu et al., 2014)	Cryptographic	Provides mechanisms for anonymous authentication	+ Anonymous authentication + Defence against various attacks − Utilises fixed network infrastructure − Places more work on the limited sensor than the more powerful network infrastructure	Simulation
(Guo et al., 2015)	Cryptographic	Four phase authentication scheme resistant against various attacks whilst remaining efficient	+ Efficient − Relies on network infrastructure	Simulation
(Saeed et al., 2018)	Cryptographic	Allows for remote anonymous authentication suitable for data exchange over Internet	+ Quick + Anonymous authentication − Requires network infrastructure	Simulation
(Khernane et al., 2016)	Cryptographic	Authentication for BANs sensors to mutually verify their identity with assistance of a ZKP	+ Efficient in terms of energy, memory and time − Vulnerable DDoS attacks	Simulation
(Bu and Potop-Butucaru, 2018)	Cryptographic	Improves work found in (Khernane et al., 2016), by identifying and defending against DDoS attacks	+ Efficient + Anonymous authentication	Simulation

2.5 Conclusion

In this chapter we have explored communication standards, threats faced by BANs and generic countermeasures that can be utilised in addition to a review on the state-of-the-art literature. In this review we have studied various contributions attempting to categorise them as either physiological-based, wireless channel-based or cryptographic-based authentication schemes. Doing so has enabled for easily identifying what and where the current research efforts are, and what is being neglected, which has informed the design and evaluation of the proposals to be explored in the remaining chapters of the thesis.

Chapter 3

Research Task A: Vulnerabilities of ECG-based key Agreement Schemes

3.1 Introduction

As discussed in Chapter 2, there are a number of state-of-the-art schemes that take advantage of physiological signals to provide authentication mechanisms via key generation and agreement. Schemes such as; PSKA, OPFKA and ELPA exploit the sensor's ability to measure a physiological signal known as ECG. The authors in (Venkatasubramanian et al., 2010) state that the use of ECG for key generation and agreement is suitable due to three properties which has been discussed in Chapter 2.4.1.

One property of interest is temporal variance, which refers to how the signal varies over time. This property is taken advantage of within the previously mentioned ECG key generation schemes as the authors claim that it is not possible for an adversary to use prior recorded ECG data (Venkatasubramanian et al., 2010; Zaghouani et al., 2015; Hu et al., 2013). However, in this chapter we will explore this claim and propose a novel attack method known as Synthetic Electrocardiogram Attack Method (SEAM) which enables, with a high-level of success, an adversary to compromise the key being generated between legitimate sensors.

The remainder of this chapter is split into the following sections; Section 3.2 will introduce the attack method known as SEAM, Section 3.3 will evaluate the proposed attack method against an existing scheme, and finally Section 3.5 will conclude the chapter.

3.2 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.

3.2.1 Overview of Electrocardiogram Signals

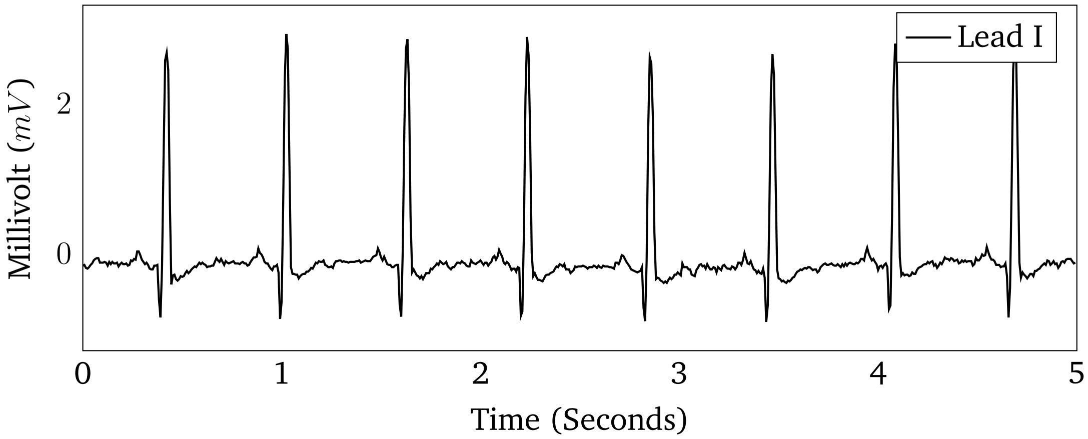


Figure 3.1: Annotated Five second ECG signal sampled at $128Hz$, obtained from NSRDB Dataset

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. 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 3.1 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 (Ashley and Niebauer, 2004).

As discussed in Chapter 2.4 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 (Venkatasubramanian et al., 2010). 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.

3.2.2 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 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 (Yaqoob et al., 2019), 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. An example of such vulnerabilities include weak encryption, lack of authentication, and unpatched and obsolete operating systems (Yaqoob et al., 2019). 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.

3.2.3 Synthetic Electrocardiogram Attack Method

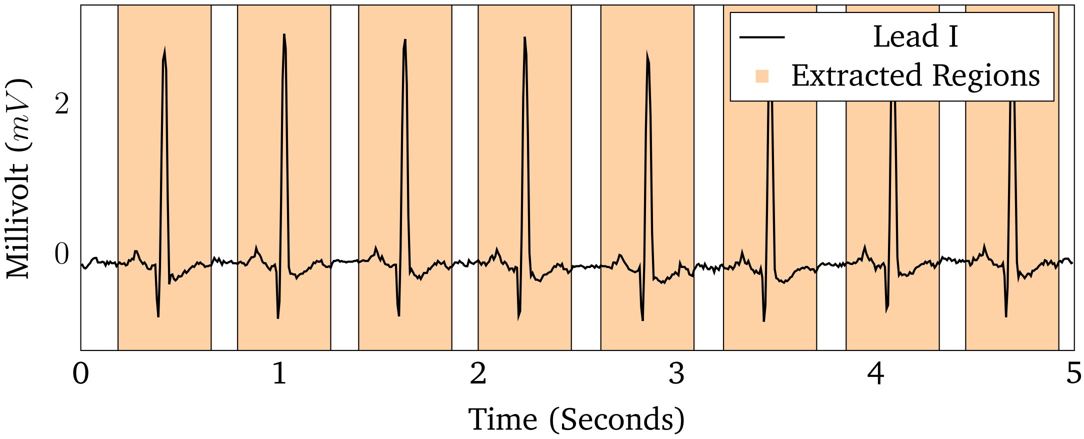


Figure 3.2: ECG signal with the extracted QRS regions highlighted

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 complex from the prior recorded signal data already obtained (stolen) by the adversary. 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 (Xu et al., 2020; Zhang et al., 2020; Jumahat et al., 2019), 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 3.2 demonstrates this process, the shaded region of each QRS complex is kept whilst the unshaded regions are discarded.

3. Split the extracted complexes into equally sized groups, this is done to make averaging and manipulating all complexes easier. 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 can apply a brute force method 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.

3.3 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.

3.3.1 Experimental Purpose

To evaluate the capabilities of the attack proposed within this chapter 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 BANs 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.

3.3.2 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 (Stoica and Moses, 2005) 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.

Datasets	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 and 12 Hours

Table 3.1: Evaluation parameters setting used in SEAM's experiments

3.3.3 Evaluation Settings

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 3.1. The experiments have been conducted to evaluate the effectiveness of SEAM and make use of the publicly available dataset known as Normal Sinus Rhythm Dataset (The Beth Israel Deaconess Medical Center, 1990) from the Physionet Project (Goldberger et al., 2000). This dataset contains 18 long-term ECG recordings in which no significant arrhythmias were identified, which if present would negatively impact the quality of recordings and the effectiveness of the schemes being targeted by SEAM. All 18 patients were used as we had no reason to omit certain records from the experiments in addition to remaining consistent with other published works. This dataset had been used by the authors in (Zaghouani et al., 2015; Venkatasubramanian et al., 2010) to evaluate the capabilities and performance of their respective key agreement schemes. Therefore, it is appropriate to use here when attempting to demonstrate vulnerabilities that may impact their schemes. Schemes such as (Zaghouani et al., 2015; Venkatasubramanian et al., 2010) consume five seconds of ECG signal data to successfully authenticate two sensors. With the dataset being used having a sample rate of 128Hz it would mean that fair representation of a target signal would have only 640 samples available in their ECG recording. Whereas the adversary could have access to a larger range of data such as 38400 samples or 300 seconds. The motivation behind SEAM is to demonstrate that not only are these ECG based key agreement schemes vulnerable to synthetic signals generated with recent stolen data in addition to more long term data with similar success. Over 30,000 experiments have been carried out whereby each experiment loads a target signal and provides the *adversary* with *stolen data* wherein SEAM can be applied to as described in Section 3.2. Within each experiment various delays are applied to what the adversary has in order to evaluate how effective the attack is with older signal data.

The experiments have been performed using COTS hardware, which is hardware readily available to everyone, as opposed to bespoke custom solutions (Khan et al., 2022). The hardware used in these experiments is a desktop machine with an AMD Ryzen 7 3700X 8/16 (Cores/Threads) @ 4.4 GHz which is reasonable to assume that any adversary would have easy access to as they are sold to the general consumer at relatively low cost.

3.3.4 Results Analysis

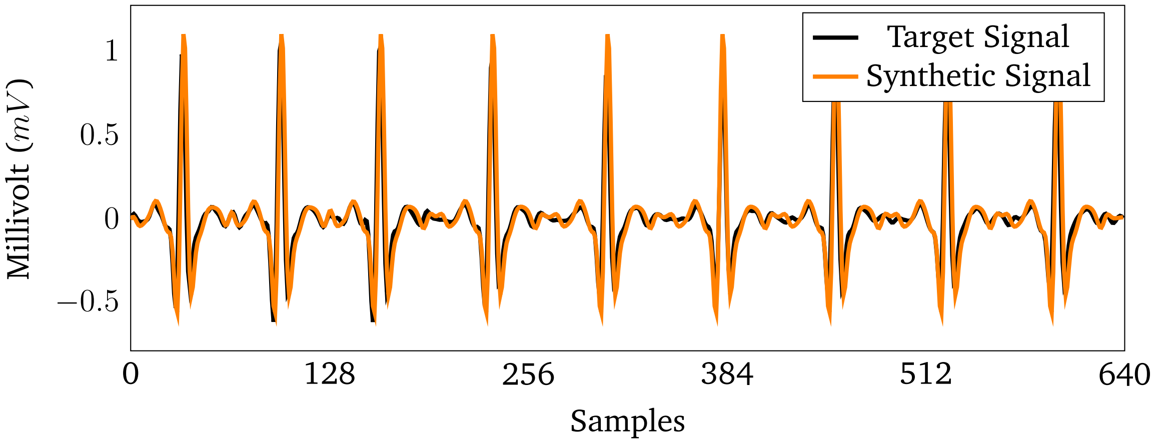


Figure 3.3: Comparison of the target and synthetic signal in the time domain

During our investigations, we were able to construct 100,000s 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 3.3. Whilst there is no 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 3.4 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, however they also share similar magnitude which means that the synthetic signal has the ability to exploit the fuzzy nature of the target key agreements schemes (Venkatasubramanian et al., 2010; Zaghouani et al., 2015). The fuzzy schemes which are forgiving of errors between legitimate parties due to slight discrepancies between recording originating from trustworthy sensors (Venkatasubramanian et al., 2010; Zaghouani et al., 2015).

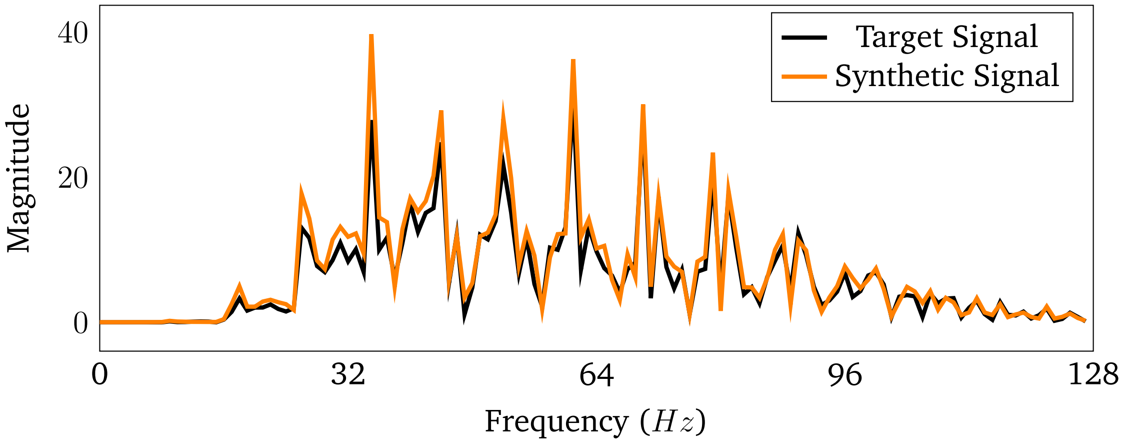


Figure 3.4: Comparison of the target and synthetic signal in the frequency domain

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 (Venkatasubramanian et al., 2010; Zaghouani et al., 2015). The coherence levels between delays also demonstrates 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 3.6 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 3.5 which statistically insignificant variation between the various delays and the average coherence obtained.

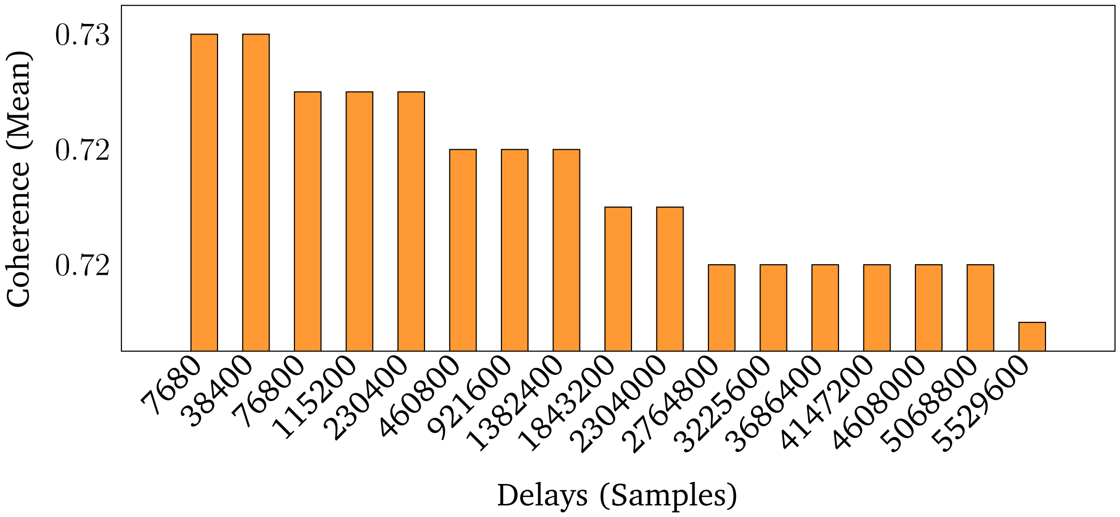
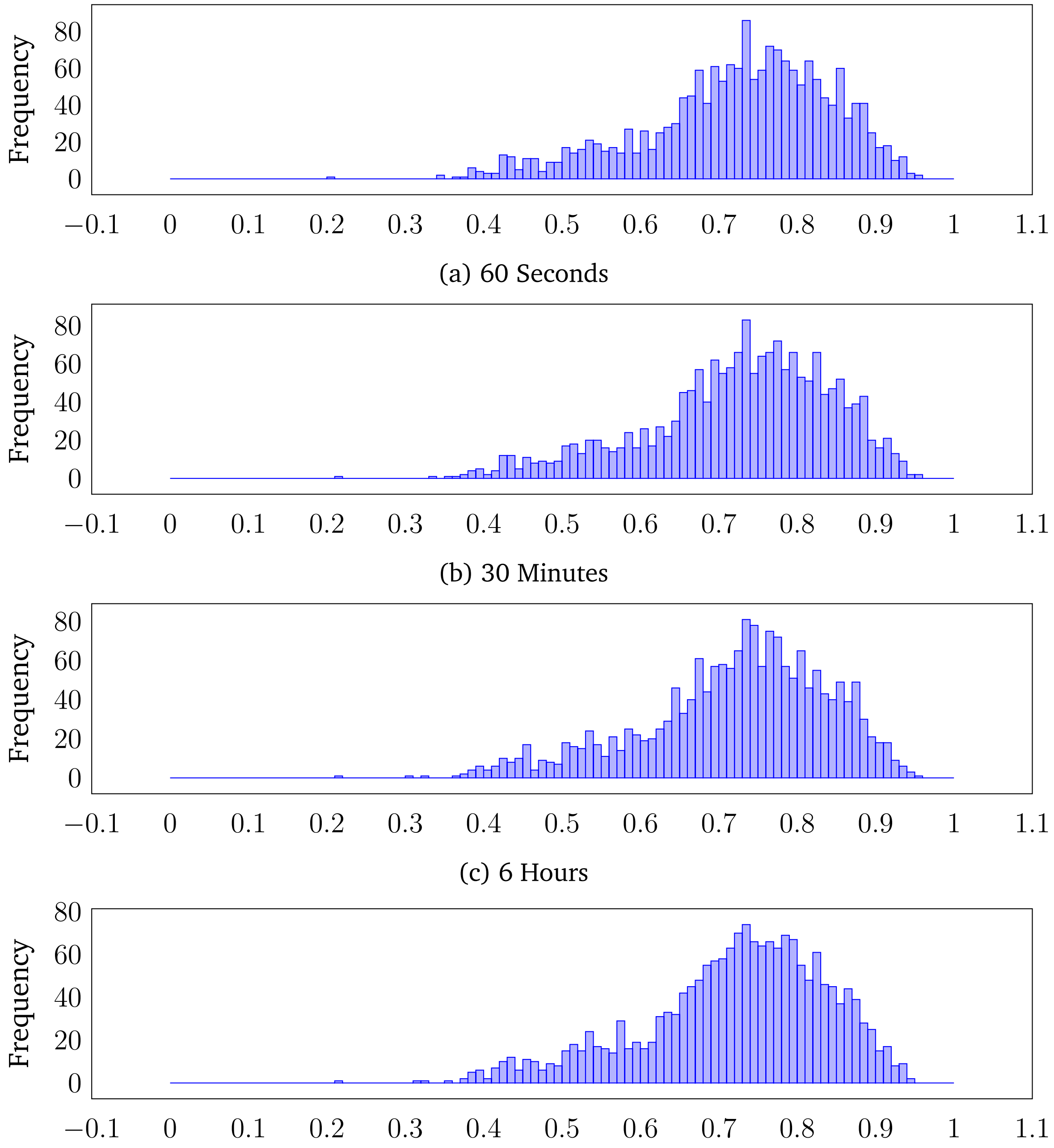


Figure 3.5: The impact of the delay on the achieved coherence level of synthetic signals

3.3.5 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 LPC applied against features obtained from the Autocorrelation (AC)/DCT method presented in (Wang et al., 2007). Our reimplementation of their scheme achieves similar performance results with regard to False Rejection Rate (FRR) and False Acceptance Rate (FAR) and therefore is suitable for applying our attack method against. 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



(a) 60 Seconds

(b) 30 Minutes

(c) 6 Hours

(d) 12 Hours

Figure 3.6: 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)

the correct key; otherwise, the adversary would simply try the next synthetic signal. 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 3.6) 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 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 3.7 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.

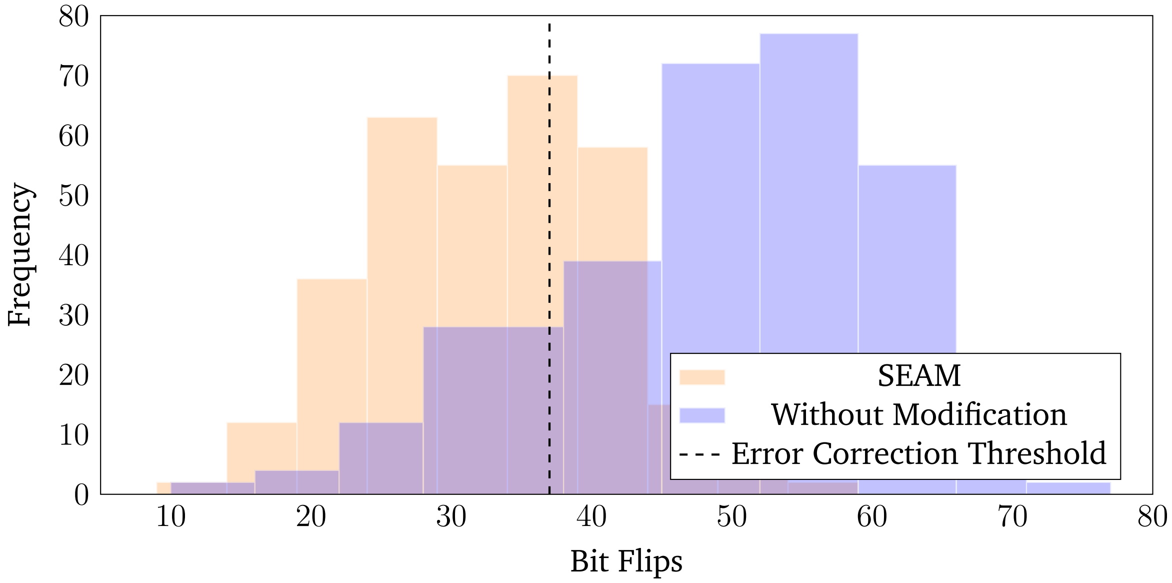


Figure 3.7: Impact of SEAM on increasing the success rate of attack attempts against ELPA

3.4 Limitations

The work presented in this chapter whilst introduces a concerning vulnerability related to ECG signal based key generation schemes such as (Zaghouani et al., 2015) has limitations that will need to be addressed in future work. Mainly the search space given in section 3.2 as s^r is prone to growing very quickly even with small inputs. This could minimise the impact of the attack method if the targeted schemes used data sampled at a higher rate or sampled for a longer period to obtain more QRS peaks. Another limitation would be that the effectiveness of the attack has not been evaluated with higher sample rate or high bit resolution data. This had not been investigated during the thesis as capturing the data first-hand with a reasonable number of individuals would have been difficult due to national lock down procedures during COVID-19.

3.5 Conclusion

This chapter 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.

Therefore, this raises serious concerns about the security implications of using physiological signals within the key generation phase in BAN, and immediate actions are needed to mitigate potential attacks. The next chapter shall propose and evaluate a method for preventing and minimising risk to schemes impacted by SEAM by including the use of RSSI, something all BAN sensors are capable of measuring.

Chapter 4

Research Task B: Securing ECG-based Key Agreement Schemes

4.1 Introduction

In the previous chapter we proposed a vulnerability targeting the temporal variance within physiological-based key generation and agreement schemes such as ELPA. With such a vulnerability uncovered it is important to identify ways to mitigate such an attack otherwise the affected schemes would be unsuitable for continued use.

Therefore, in this chapter we shall introduce a novel method known as Rotational Assisted Fuzzy Vault (RAFV) which is designed to mitigate the vulnerability discussed in the previous chapter. This proposal utilises the physiological signal that could be compromised in combination with wireless channel characteristics such as RSSI.

The remainder of this chapter is split into the following sections; Section 4.2 will introduce defence mechanism against situations where an adversary has possession of prior ECG, Section 4.3 will evaluate RAFV looking at the strength it provides in addition to the impact on execution time, and finally Section 4.5 will conclude the chapter.

4.2 Proposal

4.2.1 Fuzzy Vault Threat Model

Before we propose any solution to improve upon these works or something entirely independent of others, we must describe what we are defending against in terms of the capabilities of an adversary. As described earlier in this report, an adversary is someone who wishes to attack the network and its users, therefore we must ensure that any solution developed is one that can repel anticipated attacks.

Our assumptions about an adversary who would target a BAN are as follows; they would have access to much more powerful computers relative to the sensors they are targeting. Therefore, they would be able to leverage the computational power of laptops, desktops and high-end workstations in any of their attacks. This would provide an advantage to the adversary as they may attempt demanding computations to attack authentication services such as through brute force. An adversary will also be capable of listening in promiscuous mode which will allow observing passively any communications taking place within range of their wireless antenna. This will provide them with insight into how their target network is functioning and being able to recognise when new sensors are added and how cryptographic keys are being generated. Figure 4.1 illustrates an example of the sequence of events an adversary may follow when attempting to undermine a key agreement scheme such as PSKA.

Two pioneering solutions use the fuzzy vault or a similar construction known as PSKA (Venkatasubramanian et al., 2010) and OPFKA (Hu et al., 2013). These schemes enable key agreement between BAN nodes that are equipped with either ECG or PPG sensors, as these physiological signals are used to conceal the symmetric key to be agreed upon. While these schemes provide a novel way of agreeing upon a key accompanied by a high-security level, they do not account for the possibility of the physiological signals being captured remotely off the body, without knowledge or consent of the patient. This remote capture of physiological signals may allow an adversary to successfully impersonate a genuine body sensor and enable them to carry out further attacks within the BAN, such as data manipulation in which they send

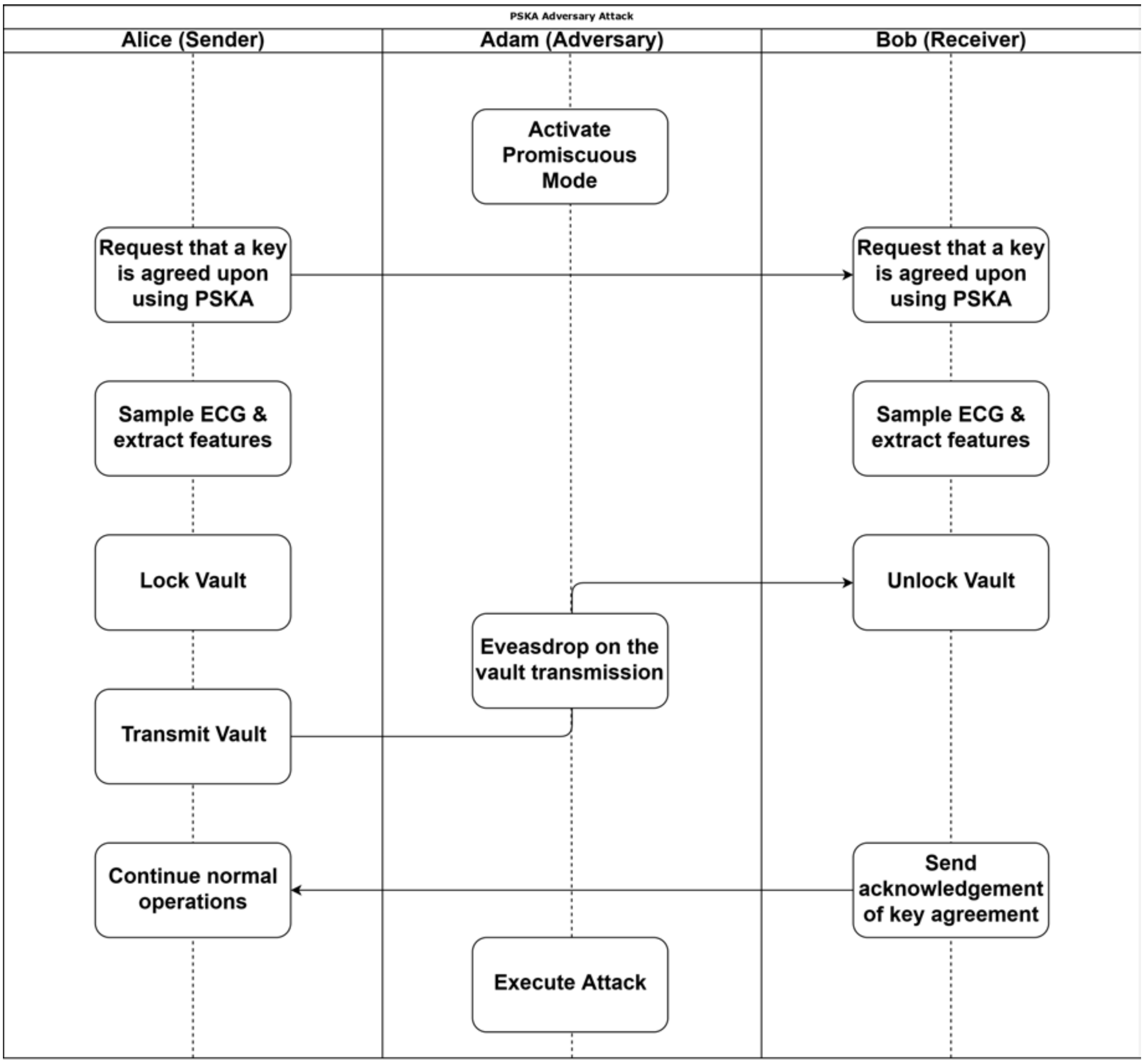

PSKA Adversary Attack
Alice (Sender)
Adam (Adversary)
Bob (Receiver)
Activate Promiscuous Mode
Request that a key is agreed upon using PSKA
Request that a key is agreed upon using PSKA
Sample ECG & extract features
Sample ECG & extract features
Lock Vault
Unlock Vault
Eveasdrop on the vault transmission
Transmit Vault
Continue normal operations
Send acknowledgement of key agreement
Execute Attack

Figure 4.1: Sequence of events an adversary might be engaging in when attacking schemes such as PSKA and OPFKA

fake readings that can mislead medical professionals and have serious consequences for the patient. In (Kim et al., 2019), the authors investigated the potential of using prediction filters, such as a Kalman filter, to unlock PSKA based fuzzy vaults using leaked physiological signals such as PPG. As stated in (Lee et al., 2018), the remote capture of PPG signals using Ultra-Wide Band (UWB) radars is possible, thanks to advancements in remote sensing technology. This presents a serious security risk for devices aiming to achieve authentication and key agreement using PSKA or similar schemes as the key could be unlocked by an adversary and neither the user nor the network administrator would be aware of the intrusion. In (Zhao et al., 2016), a concern is raised regarding the security of PSKA vaults with the advent of remote sensor technology and its potential to capture the necessary information to unlock a vault. This fear is reinforced with the use of electric potential probes that enable remote capturing of ECG and PPG (Harland et al., 2001; Mahdi and Faggion, 2011).

Due to this development in adversary capabilities, it is necessary to explore new ways of protecting the fuzzy vault construction and the schemes that rely upon it while minimising the incurred overhead. We, therefore, propose an original scheme named RAFV that builds upon the fuzzy vault scheme by leveraging channel side characteristics known as RSSI to obfuscate the locked vault. If an adversary is capable of collecting physiological signals originating from the target BAN sensors then they would be able to carry out impersonation attacks if the current iterations of PSKA, OPFKA and schemes similar in nature are used. This is because adversaries can utilize a remotely captured signal to unlock the vault and obtain the key concealed within it, compromising all future communication between the nodes targeted. However, RAFV will ensure that knowledge of the physiological signal alone does not provide access to the secret concealed within the vault. This is because any attempt to acquire the secret requires knowledge of how the vault has been obfuscated, which is not impacted by the leakage of locking elements to an adversary.

4.2.2 Rotational Assisted Fuzzy Vault: Overview

The objective of RAFV is to secure any authentication scheme that uses the fuzzy vault construction mechanism, wherein the elements used for locking and unlocking the vault are susceptible to leakage within a wireless network. RAFV can be seen as an extension to the fuzzy vault scheme and is situated within the post-locking and pre-unlocking phase of this scheme. RAFV shall transmit an obfuscated fuzzy vault from the sender to the receiver, any attempt by an adversary to unlock the intercepted vault would fail even if the adversary is aware of the full set of locking elements. This is because RAFV does not conceal the polynomial but rather ’corrupts’ it preventing successful unlocks until the vault has been ’repaired’. The vault shall be obfuscated by dividing it into quadrants and rotating the points within each quadrant around its centre.

RAFV relies on the ability to agree upon a sequence of bits in an out-of-band manner to ensure that an adversary cannot obtain this sequence. This sequence can be seen as a symmetric key that is used to lock and unlock the vault itself. To achieve this, RAFV makes use of RSSI which is a measurement of the power contained in the received signal. This measurement is only computed locally on the device and cannot be obtained by an adversary, which makes it ideal for attempting to harden the security of the fuzzy vault scheme. RSSI reconciliation is a process that enables the two BAN nodes to agree upon the key that shall be used to secure the vault. RSSI values between two wireless devices are prone to discrepancies and need to be corrected, therefore we model the errors as communication errors and use error correction codes, such as Reed-Solomon, to ensure that the sender and the receiver are in agreement (i.e., they measure the same value). This process has been used in many key generation and key agreement schemes, including the ones applied in BAN such as (Li and Wang, 2016; Li, Wang, Daneshmand and Fang, 2017; Ali et al., 2012).

RAFV locking phase consists of the following steps; 1) Measuring the RSSI value between the two BAN devices, 2) The sender generates Reed-Solomon coefficients and sends them to the receiver, 3) The receiver uses the received Reed Solomon coefficients to correct its ’copy’ of RSSI, if the receiver fails to correct the errors the process should be restarted from the first step, 4) The sender constructs the locked fuzzy vault, 5) Dividing the vault into several quadrants, 6) Assigning a rotation direction and order for each quadrant, 7) Executing the rotation. These steps are

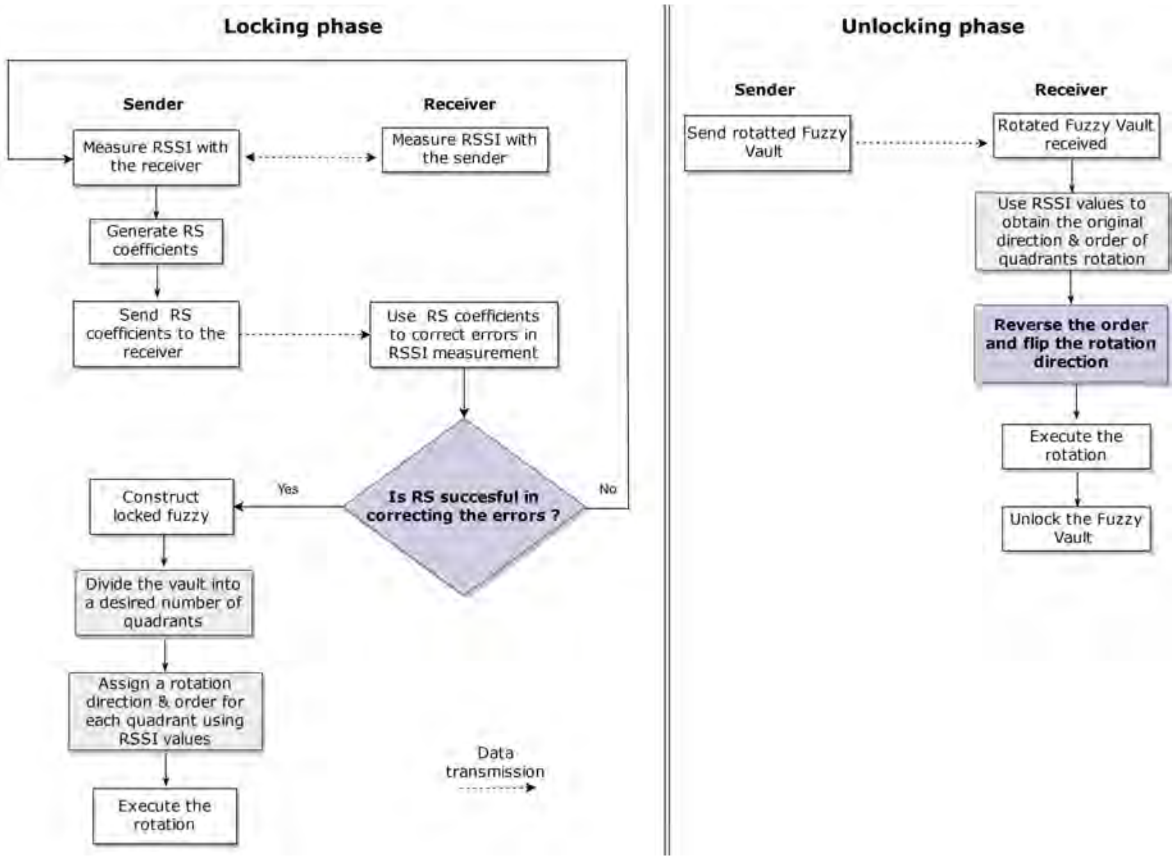

Locking phase
Sender
Receiver
Measure RSSI with the receiver
Measure RSSI with the sender
Generate RS coefficients
Send RS coefficients to the receiver
Use RS coefficients to correct errors in RSSI measurement
Is RS succesful in correcting the errors ?
Yes
No
Construct locked fuzzy
Divide the vault into a desired number of quadrants
Assign a rotation direction & order for each quadrant using RSSI values
Execute the rotation
Data transmission
Unlocking phase
Sender
Receiver
Send rotatted Fuzzy Vault
Rotated Fuzzy Vault received
Use RSSI values to obtain the original direction & order of quadrants rotation
Reverse the order and flip the rotation direction
Execute the rotation
Unlock the Fuzzy Vault

Figure 4.2: The fuzzy vault locking and unlocking process in RAFV

summarized in Fig. 4.2.

As for the unlocking phase, upon reception of the fuzzy vault from the sender BAN device the following actions are taken: 1) Generating the original direction and order of rotation for each quadrant using the agreed RSSI values, 2) Reversing the order and direction of rotation for each quadrant, 3) Executing the rotation, 4) And finally proceed with unlocking the fuzzy vault. These steps are depicted in Fig. 4.2.

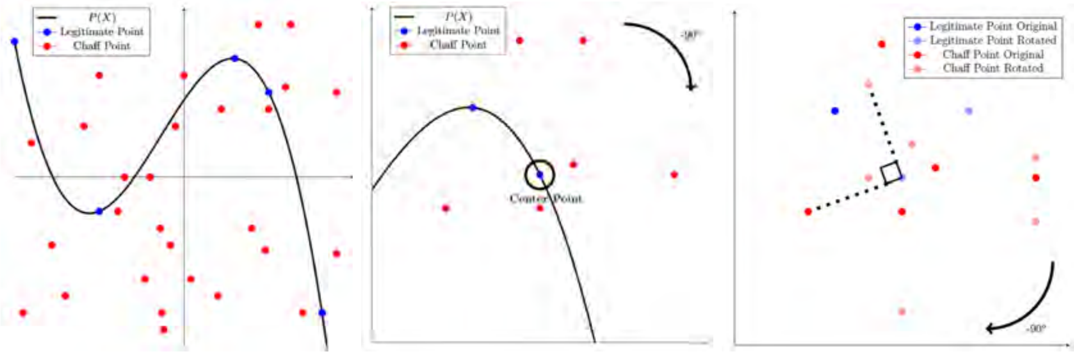
4.2.3 Vault division and quadrants rotation in RAFV

In the context of RAFV, a quadrant is used to split the vault into evenly spaced partitions. If a quadrant is selected all the points contained within its boundaries shall be rotated either clockwise or counterclockwise around the centre point of the quadrant. More quadrants can be created by dividing all of the quadrants in the current deepest layer into four smaller ones. In doing so each newly created quadrant (child) shall cover $\frac{1}{4}$ of the area of its parent. Quadrants can be represented using the quadtree data structure where the deeper layers contain more quadrants, however each quadrant represents a smaller area of the vault.

Once the vault has been divided into the desired number of quadrants the angle and order of rotation can be assigned. In RAFV, the angle of rotation is either 90° or -90°. This is because other angles, such as 45°, 135° or 215° will cause quadrants to overlap with one another making the reconstruction of the original locked fuzzy vault, by the receiver, impossible. The angle of rotation is obtained from the RSSI values that have been agreed upon before vault construction. The RSSI values are assigned to the deepest layer of quadrants within the vault. Starting from the bottom left and moving across and up, each quadrant will be assigned an RSSI value in the order they occur in the list. If there are more quadrants than RSSI values then the list will loop back to the start. As for quadrants in layers above, their values are determined by summing their children's RSSI values. Once each quadrant has been assigned a value it can then be converted into an angle by looking at the parity (odd or even) of the value. If the assigned value is odd then the quadrant shall be rotated -90° and if the value is even then the angle of rotation is 90°.

Regarding the order of rotation, this also is obtained via the same RSSI values as the angle of rotation. However, the difference consists in using the collection of RSSI values to seed a random number generator which will randomly choose which quadrant shall be rotated next. The order of rotation has a significant impact on the obscured vault as each rotation carried out will fundamentally change the result. An illustration of the rotation applied to the content of a vault is shown in Figure 4.3. The first sub-figure (Figure 4.3(a)) shows a fully constructed fuzzy vault divided into 5 quadrants where there is a set of legitimate points (highlighted in blue) on a polynomial and chaff points (highlighted in red) that are used to conceal the secret. The second sub-figure (Figure 4.3(b)) depicts a close up of the top-right quadrant of the vault where its centre point has been marked and a rotation direction has been assigned to it. The final sub-figure (Figure 4.3(c)) shows the same quadrant after -90° rotation has been applied, where the rotated legitimate and Chaff points are highlighted using the same colour as their corresponding original points but with increased transparency.

To be able to recover the locked fuzzy vault the receiver should know the number of layers present within the vault in addition to how many rotations have been carried



(a) Fully constructed fuzzy vault with 5 quadrants

(b) Overview of the top right quadrant of the vault before rotation

(c) Overview of the top right quadrant of the vault after rotation

Figure 4.3: Illustration of the rotation process in RAFV for both legitimate and Chaff points

out. This information must be communicated to the receiver, alongside the obfuscated locked vault, and be sent as plain text in a message appended to the fuzzy vault. This is because such information does not give the adversaries any advantage in their attempts to recover the vault. Once this information is obtained, the receiver can divide the vault the same way the sender did in addition to assigning the RSSI values and rotation order to each quadrant. The only difference, however, is that the receiver must swap 90° rotation with -90° and vice versa in addition to reversing the order of rotation.

4.2.4 Security Analysis of Rotational Assisted Fuzzy Vault

Two parameters can be used to calculate the size of the search space an adversary may face when attempting to directly brute force the rotation of the vault. These two parameters are the number of quadrants assigned a unique RSSI bit and the number of rotations carried out during the locking phase. The search space can be calculated using the following equation:

$$Search_{space} = 2^n \times r^n \tag{4.1}$$

Where n is the number of quadrants and r is the number of rotations. For example, a RAFV based vault that is locked using 85 quadrants and 32 rotations would yield $2^{85} \times 32^{85} = 3.15 \times 10^{153}$. However, whilst the search space is exponentially large it is ultimately limited by the size of the key agreed upon by the sender and receiver within the RSSI reconciliation because this key determines the rotation. Therefore, an appropriate sized key must be picked to ensure strong bit-security for the scheme to function. For example, a 128-bit key that has been agreed upon by the two BAN nodes will ensure sufficient protection against brute force attack as an adversary would, on average, have to search half of the key space, **e.g** 2^{127}, and use each key to generate its rotation pattern and attempt the unlocking process in full. As mentioned earlier in Section 4.2.2, RAFV will allocate the direction of rotation to the quadrants in the deepest layer and quadrants in the layers above will derive their direction from the sum of their children. For the 128-bit key to have a maximum effect there must be at least 128 quadrants in the deepest layer to ensure that this key is represented throughout the rotation pattern. It is therefore required that a vault must be at least four layers deep to ensure a minimum of 128 quadrants in the last layer. The number of quadrants in each layer can be determined using the following equation.

$$Quadrants_{number} = 4^{m-1} \tag{4.2}$$

Where m refers to the layer order. The layers are ordered starting from 1 until the deepest layer of the vault. To compute the total number of quadrants present within the entire vault we use the following the equation.

$$Quadrants_{total} = 4^{m-1} + 4^{m-2} + ... + 4 + 1 \tag{4.3}$$

Therefore, the fifth layer of a divided vault (i.e, the result of applying the division 4 times starting from the main layer) would contain 256 quadrants and the total number of quadrants in the entire vault would be 341. It is important to note that if an adversary had half of the rotation pattern used by the vault they would not be able to infer the other half. For example, if an adversary had managed to acquire the order of rotation used within a given iteration of the scheme they would not be able to determine what direction has been assigned to each quadrant within the vault.

Furthermore, two types of adversaries may attempt to compromise the security of the RAFV based key agreement. Adversary A is an adversary that is unaware of the locking elements used by the underlying fuzzy vault. This means that for every iteration of the rotated vault they would have to attempt to brute force the fuzzy vault unlocking process with no guarantee that they have the original vault. Adversary B, however, is aware of the elements used to lock the vault due to their ability to remotely capture the physiological signals being leaked by the wearer. Therefore, they will be able to process each vault much quicker because they will only be concerned with the points that overlap with the features they have illegitimately acquired, allowing them to discard chaff points. However, this does not give the adversary B any advantage to unlocking the vault as the knowledge of the locking elements does not provide any insight into how the vault has been rotated.

4.3 Evaluation

To evaluate the performance of RAFV we will compare it against the fuzzy vault scheme with regards to the required execution time. Such a comparison will enable an accurate assessment of the additional overhead induced by RAFV. Both schemes have been implemented in C++17 running on an Intel 8809G (3.10 GHz / 4.20 GHz) processor with a RAM of 2400 MHz C16. Whilst the performance of such a processor far exceeds the performance of wireless sensor devices used in the intended application area (i.e, Body Area Networks) this evaluation aims to provide a like-for-like comparison between the two schemes. Future work could, however, look at implementing both schemes on more appropriate hardware devices with the results being easily reproducible due the deterministic nature of the scheme provided the same inputs are used.

The evaluation scenario consists of running both schemes sequentially 100000 times to measure their performance for equally sized vaults. In addition to varying the vault size, from 100 to 5000, to assess its impact on the achieved execution time for both schemes, the quadrant layers (and consequently the total number of quadrants) and the number of applied rotations, relevant for RAFV only, are also varied to assess how they affect the execution time and the resulting search space. More specifically, we evaluated 3 and 4 quadrant layers with 5 different number of rotations: 16, 32,

	100 Points		1000 Points		2000 Points		5000 Points	
Execution Time (ms)	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**
Minimum	0.132	0.178	0.208	0.487	0.288	0.837	0.531	1.890
Maximum	0.760	0.791	1.043	1.367	1.594	1.267	2.424	4.725
Average	0.144	0.191	0.213	0.508	0.295	0.864	0.540	1.928
Standard Deviation	0.005	0.006	0.007	0.014	0.007	0.012	0.013	0.026
Delta	0.046		0.295		0.570		1.388	

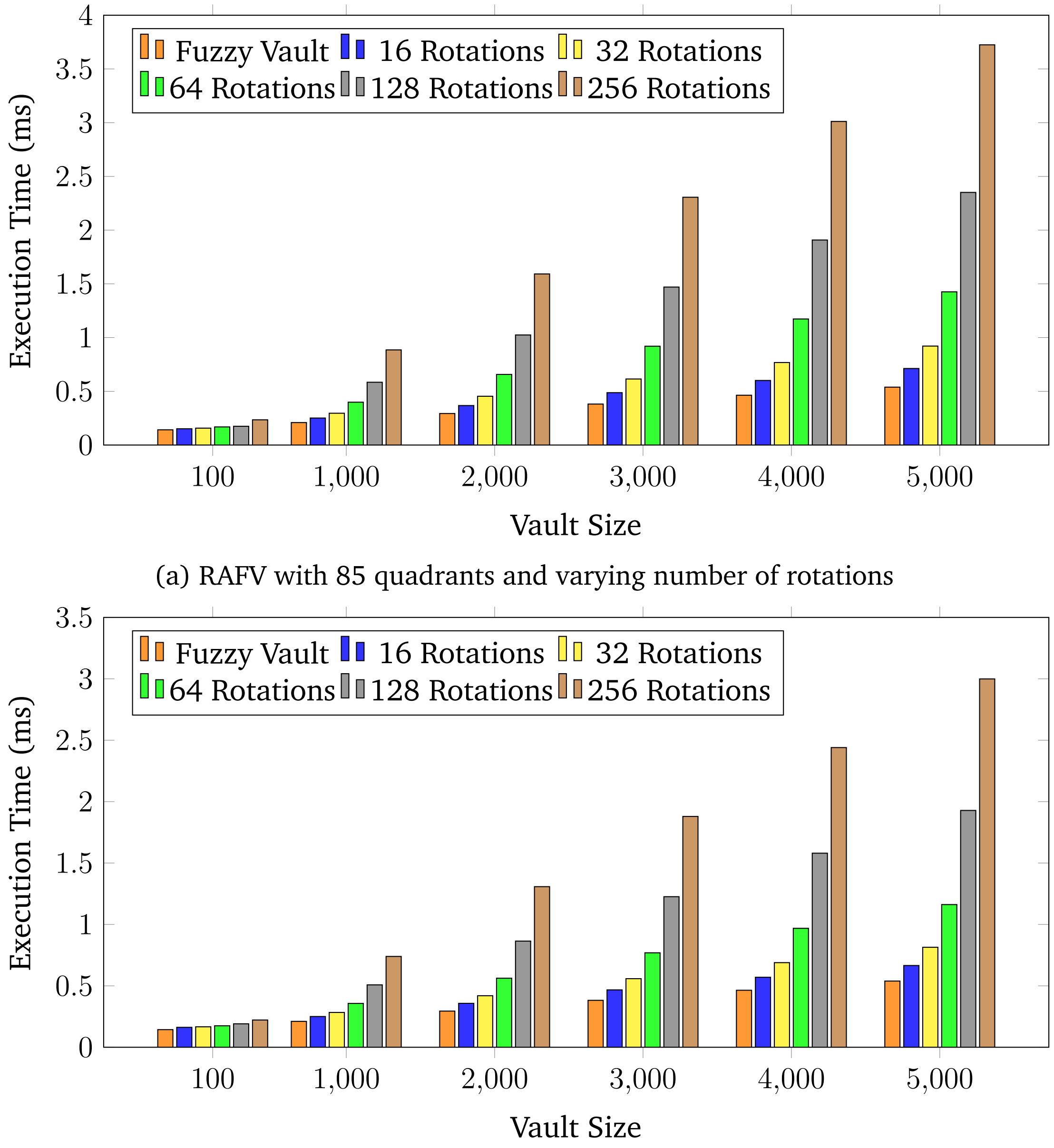
Table 4.1: Impact of the vault size on the achieved execution time: fuzzy vault scheme vs. RAFV (341 quadrants and 128 rotations)

64, 128 and 256.

Figure 4.4(a) shows the time taken to construct a RAFV over many parameters: various sizes, number of rotations in addition to the time taken to construct an identically sized fuzzy vault. This figure demonstrates that the execution time for either the fuzzy vault or RAFV scheme increases in line with the vault size. With regards to RAFV, its execution time increases further as more rotations are carried out, this is expected as more quadrants are being selected for rotation and, therefore, more points are being rotated. The biggest impact on the performance for RAFV is the number of rotations carried out, for example, a 5000 point vault rotated 16 times is 5.2 times quicker when compared with a vault rotated 256 times.

Figure 4.4(b) shows the construction time for RAFV with 341 quadrants present within the vault. This graph shows that a vault rotated 256 times produces similar results to a vault with 1000 fewer points but divided into 85 quadrants (see Figure 4.4(a), the case of a vault size equals to 4000). This is because the vault used for producing the results shown in Figure 4.4(b) has been divided once more, compared to the vault used in Figure 4.4(a), introducing an additional layer of smaller yet more abundant quadrants. These smaller quadrants are more likely to be selected for rotation as there is more of them, however, they each represent a smaller area of the vault, so if they are chosen fewer points will be rotated, which contributes to this performance uplift.

RAFV sees an increase in run time due to the extra operations it carries out on top of the underlying fuzzy vault scheme. However, this increase in execution time provides a fuzzy vault that is resilient against brute force attacks due to the rapid increase in



(a) RAFV with 85 quadrants and varying number of rotations

(b) RAFV with 341 quadrants and varying number of rotations

Figure 4.4: Time taken to construct a fuzzy vault and RAFV over various sized vaults

complexity, as shown in Fig. 4.5 which is a plot of the Equation 4.1. Fig. 4.5 plots the function shown in this equation with various values of r (i.e., the number rotations performed). This figure highlights that a small increase in the number of quadrant rotations leads to an exponential increase in the search space. This is designed to make brute force attack infeasible due to the required time to exhaust the search space.

However, this figure shows also the search space posed by the 128-bit key which is used to derive the rotation lock pattern. Whilst the search space generated using the key is many magnitudes smaller than even the smallest search space generated by the lowest number of rotations evaluated (i.e., 16), it is important to realize that RAFV is limited by this key. Although it may seem that there is no purpose for rotating beyond the limit imposed by the chosen key size, there may be advantages to picking many quadrants and quadrant rotations to prevent or hinder any attempt of unlocking the vault using smart analysis techniques or efficient search algorithms. Currently, there is no known efficient search algorithm, to the best of our knowledge, that the adversary may use to rotate the vault back to its original form, therefore the security of RAFV is defined by the size of the key used.

Table 4.1 shows the obtained execution time from the performed experiments for the fuzzy vault and RAFV schemes in terms of the measured minimum, maximum, average, standard deviation and delta (the difference between average execution times for both schemes) values under varying vault sizes. For RAFV, the vault has been divided into 341 quadrants with 128 rotations being applied. These results reveal that as the vault size increases the average execution time increases with the delta between the two schemes increases rapidly as well. However, even with RAFV being applied to a 5000 point vault it is only 1.388 ms slower than the fuzzy vault, which would not have any meaningful impact on the performance of the authentication scheme nor would the user be able to perceive such a small increase.

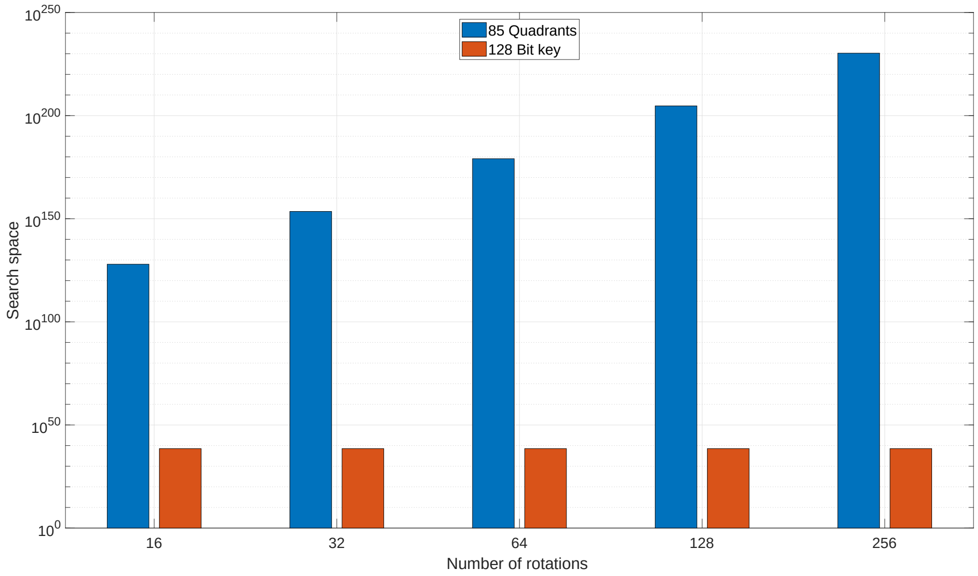


Figure 4.5: Evolution of search space size faced by an adversary when attempting to brute force the rotations of RAFV directly vs. the search space size generated by the 128-bit key

4.4 Limitations

The work presented in this chapter aimed to mitigate a vulnerability of ECG signal based key generation schemes discussed in the previous chapter. The main limitation of this work would be the limited analysis of how RAFV could be targeted by adversaries. It could be possible that an adversary inspects the rotated vault for weaknesses due to poor rotation stemming from the algorithm having inadequate entropy originating from the physical channel characteristics.

4.5 Conclusion

Due to the exceptional increase in adversaries' capabilities, the fuzzy vault construction scheme and all BAN authentication protocols that reply on it become vulnerable to a wide range of security threats. To counter such threats, we proposed RAFV to further enhance the security of any fuzzy vault based authentication scheme with minimum additional communication and computational overhead. RAFV extends the fuzzy vault scheme by leveraging channel side characteristics namely RSSI (Received Signal Strength Indicator) to obfuscate the locked vault by dividing it into many quadrants and rotating them following a given pattern. This obfuscation aims at preventing adversaries from using remotely captured BAN signals to unlock the vault and obtain the key concealed within it. RAFV has been evaluated against the fuzzy vault scheme and the obtained results have proven its effectiveness in enhancing the security level of the fuzzy vault scheme with a slight increase in the required computational overhead. Future work will look at what reduction can be achieved concerning the communication overhead as RAFV allows fewer chaff points to be present without sacrificing the achieved security level.

Chapter 5

Research Task C: Enabling Fast RSSI-based Secret Key Extraction Method

5.1 Introduction

In this final research task chapter, we shall explore how to improve wireless-channel based key generation schemes. This work is required as existing literature (Premnath et al., 2013) has highlighted how wireless-channel based key generation schemes experience prolonged key construction times, due to stationary devices leading to too little variation in the values extracted.

Therefore, this chapter shall explore how mandating that at least one of the devices involved is mobile and can therefore be moved in order to introduce variation in the values extracted. This chapter will also investigate various gestures that could be recommended to maximise performance whilst balancing them with costs associated with repetitive movements.

The remainder of this chapter is split into the following sections; Section 5.2 will introduce our strategy for improving wireless-channel based key generation schemes, Section 5.3 will evaluate the proposal looking at various evaluation metrics to identify high performing gestures, and finally Section 3.5 will conclude the chapter.

5.2 Strategy

As discussed in Chapter 2, RSSI Secret Key Extraction (SKE) can in certain scenarios suffer from prolonged construction times due to inadequate variation in the RSSI values, which negatively impacts entropy when quantized. The scenarios effected include when sensors are stationary, obstructed or experienced large amount of interference (Premnath et al., 2013). Chapter 2 also discusses existing approaches to solve this issue which can range from dual antenna design (Revadigar et al., 2015) or synthesising bits within a group (Li, Wang, Daneshmand and Fang, 2017). These solutions are unfortunately not appropriate to BANs as these sensors are constrained in terms of cost, form factor, power consumption and complexity. To remedy this we propose a new strategy, named Mobile Assisted RSSI Secret Key Extraction (MARS), that users may adhere to, enabling an increase in entropy which results in reduced construction times. This is important for the intended use case of BANs where time wasted generating keys could place the wearer's health at risk.

Mobile Assisted RSSI Secret Key Extraction (MARS) aims to increase the amount of entropy present within the quantized bits to achieve shorter construction times. This can especially be beneficial in emergency situations (e.g., road accidents and emergency department cases) where the time spent without functional body sensors should be significantly minimised. MARS can achieve this aim by stimulating the RSSI values which in turn will increase the entropy of the quantized bits. This is made possible because MARS requires that one of the sensors used is mobile, referring to the sensors ability to be picked up and moved such as a mobile phone. Due to such a requirement it is therefore possible to exploit the influence that movement can have on RSSI and generate stimulated values which when quantized shall have high levels of entropy. MARS focuses on the transmitting probes, quantized stage of an RSSI SKE as any improvement witnessed here will propagate down into the other stages of the SKE process.

MARS will prompt the user to perform a gesture during the probe transmission stages as this is when RSSI is being measured. The gesture to be recommended for the user to perform will be the one that improves upon the entropy of the quantized bits while remaining easy for the typical level motion a person is capable of. The gestures recommended could range from one of the following;

- Figure Eight
- Shaking (Light)
- Shaking (Heavy)
- Tilting
- Holding (Typical Use)
- Moving Towards & Away

Each of these gestures have been evaluated within Section 5.3.

5.3 Evaluation

In this section we will explore the effectiveness of MARS as outlined in the previous section. We will discuss the evaluation metrics, evaluation setup and analyse the obtained results.

5.3.1 Evaluation Purpose

In order to determine if the proposed strategy improves upon the status quo we have designed experiments that will inform us about any improvements within the quantization phase. We will also explore the acceleration forces exerted on the mobile device by the user. By investigating the impact of our proposed strategy on RSSI measurements and the quantization of such data we can accurately determine the improvements to the entire process. In addition, analysing motion sensor data will provide the necessary information to understand the trade-off involved with the different gestures.

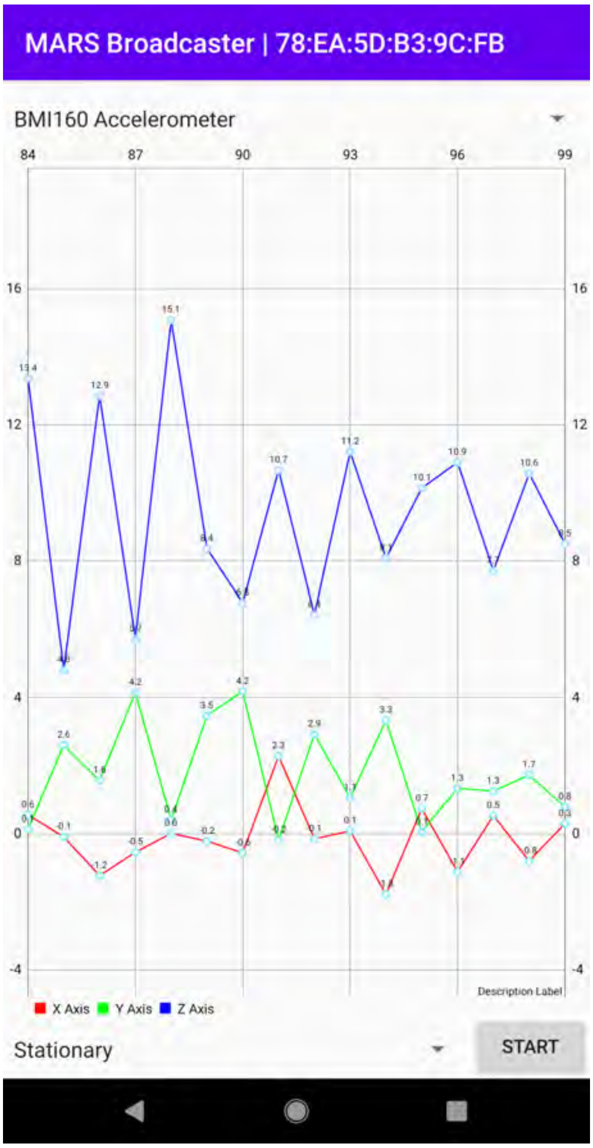
5.3.2 Evaluation Metrics

To evaluate the effectiveness of our proposed strategy we have opted to use the intermediate data from the quantization phase of the RSSI SKE. The data collected from this phase of the scheme provides insight into how non-stationary gestures perform against the stationary gesture in addition to their performance relative to one another. Insight from the quantization phase is provided by the number of bits quantized which will help determine which gestures reject the least number of RSSI readings, fewer rejections the better. Also extracted from the quantization phase of the RSSI readings is the entropy of quantized bits, which informs us on the randomness of the sequence of bits. High entropy will lead to an increase in the number of secret bits, therefore reducing the wait time. Quantization of the RSSI readings in these experiments will follow Equation 2.1. Besides the quantized output our evaluation will also attempt to understand the *cost* a gesture incurs as some gestures evaluated can be described as difficult to perform compared to others due to the required fast and wider motion to perform the gesture correctly. Therefore, by utilising the motion sensors built into the Smartphone we can evaluate each gesture's *cost* by calculating the magnitude of the motion data. By doing so we can determine which gesture has an appropriate trade-off in regard to performance and cost.

5.3.3 Evaluation Setup

In order to conduct the evaluation outlined above we need to setup an easily repeatable experiment on physical hardware as this is the easiest way to capture both RSSI and motion sensor readings. To achieve this, we used the Texas Instruments (TI) Launchpad CC26x2r1 as this is a development kit that includes support for various communication standards including BLE. This device was configured to broadcast a packet every 20 ms via BLE so that RSSI values could be measured. This device acted as a stationary device that would be worn by a user. As for the mobile device, a Google Pixel 3a Android Smartphone was used and was running a bespoke application, developed by us, capable of measuring RSSI from the packets the TI Launchpad was transmitting in addition to collecting motion sensor data from the onboard accelerometer.

Figure 5.1 is a screenshot of the Android application developed for these experiments. The screenshot shows a live plot of accelerometer data originating from the BMI160 Accelerometer, other sensors can also be viewed via the drop-down list. The RSSI data is being continuously collected from the device with MAC address listed at the top of the figure.



MARS Broadcaster | 78:EA:5D:B3:9C:FB

BMI160 Accelerometer

Stationary

Figure 5.1: Screenshot of the Android application used to collect both RSSI and motion sensor data

This setup allowed for the collection of RSSI data and motion sensor data in real-time. The mobile sensor was held by the participant and the stationary device was in a fixed location next to them. In this experiment we have explored the following gestures; figure-eight, shaking (light), shaking (heavy), tilting, holding (typical usage) and moving & towards and away. Each gesture was repeated 10 times by a single participant to ensure that the different gestures remain consistent.

5.3.4 Evaluation Results Analysis

Figure 5.2 shows the MAC values captured from a typical experiment performed with four gestures; *Stationary*, *Shaking (Heavy)*, *Figure Eight* and *Moving Towards & Away*. The figure demonstrates that *Stationary* has minimal variation between measurements, whereas other gestures such as *Shaking (Heavy)* have significant variation throughout. Not only do all non-stationary gestures have an important increase in the variance of the measured RSSI values they also exhibit an increase in range allowing for more unique values to occur as opposed to the same few values being repeated. This can have significant impact on the amount of data extracted during the quantization stage.

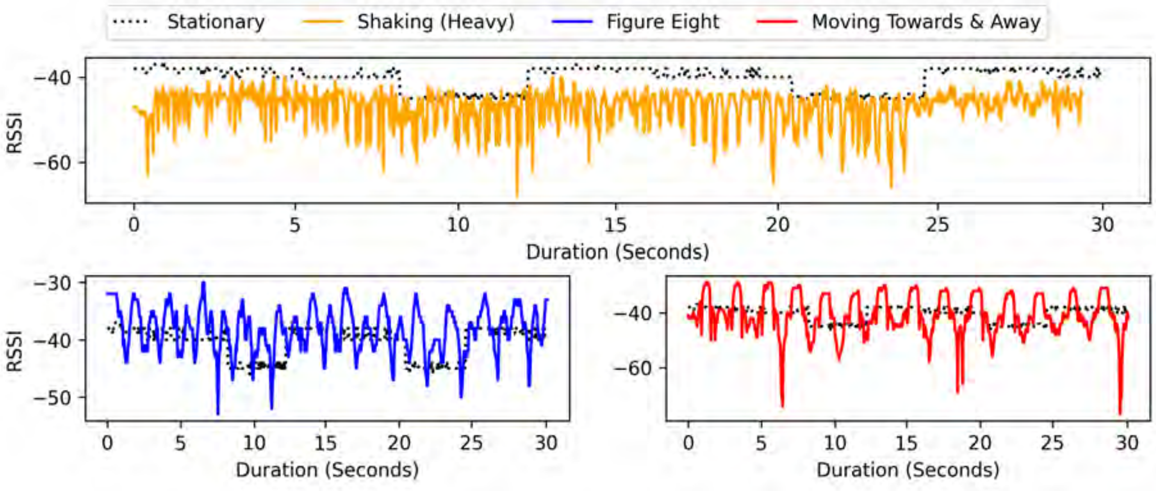


Figure 5.2: RSSI data captured from stationary and non-stationary gestures over a single 30 second experiment

Table 5.1 summarises what is evident across all gestures and repetitions of experiments with almost all gestures producing significant increases in metrics such as range, standard deviation and variance. This table includes also the average number of quantized bits from RSSI measurements captured during experiments, which can determine actual performance gains within the early stages of an RSSI SKE scheme following our strategy. *Moving Towards & Away* when compared to *Stationary* exhibits significant improvements with an increase of almost 200 quantized bits. *Figure Eight* also manages to increase the number of quantized bits generated however it did not perform similar to *Moving Towards & Away*. This could be due to the drop in metrics such as range, standard deviation and variance. This is also experienced with other gestures such as *Shaking (Light)* and *Tilting* which both make minor increases to average quantized bits when compared to a *Stationary* gesture.

Finally, *Holding (Typical Use)* and *Shaking (Heavy)* have demonstrably worse performance when compared to the *Stationary* gesture on the basis that they produce fewer quantized bits. However, in subsequent steps they may perform better than the *Stationary* gesture as the entropy of their quantization is higher and, therefore, they would experience fewer rejections requiring a smaller amount of quantized bits to proceed to the next phase. This is shown in Figure 5.3 where *Stationary* gesture contains large continuous blocks of the same bit value, whereas *Shaking (Heavy)* contains fewer bits which are not in large continuous blocks and therefore less likely to be rejected later within a scheme. This is also supported by the entropy calculated from the quantized bits presented in Figure 5.4. The entropy can be used to measure the predictability of the sequence of bits that has been quantized, the lower the value the easier it is to predict the sequence of quantized bits, whereas higher values imply it is harder to predict and therefore more resilient to security attacks.

	Minimum	**Mean**	**Maximum**	**Range**	**Standard Deviation**	**Variance**	**Average Quantized Bits**
Stationary	-46.00	-40.09	-36.67	9.33	2.89	8.38	312
Figure Eight	-52.67	-37.72	-30.33	22.33	3.63	13.19	423
Shaking (Light)	-68.67	-44.98	-39.33	29.33	4.26	19.31	321
Shaking (Heavy)	-73.33	-47.55	39.67	34.67	4.61	21.47	290
Tilting	-65.67	-45.99	-40.67	25.00	3.55	13.29	316
Holding (Typical Use)	-53.00	-46.24	-42.33	10.67	1.95	4.20	295
Moving Towards & Away	-74.33	-40.68	-27.67	46.67	7.57	57.46	509

Table 5.1: Statistics of RSSI values obtained during the MARS experiments

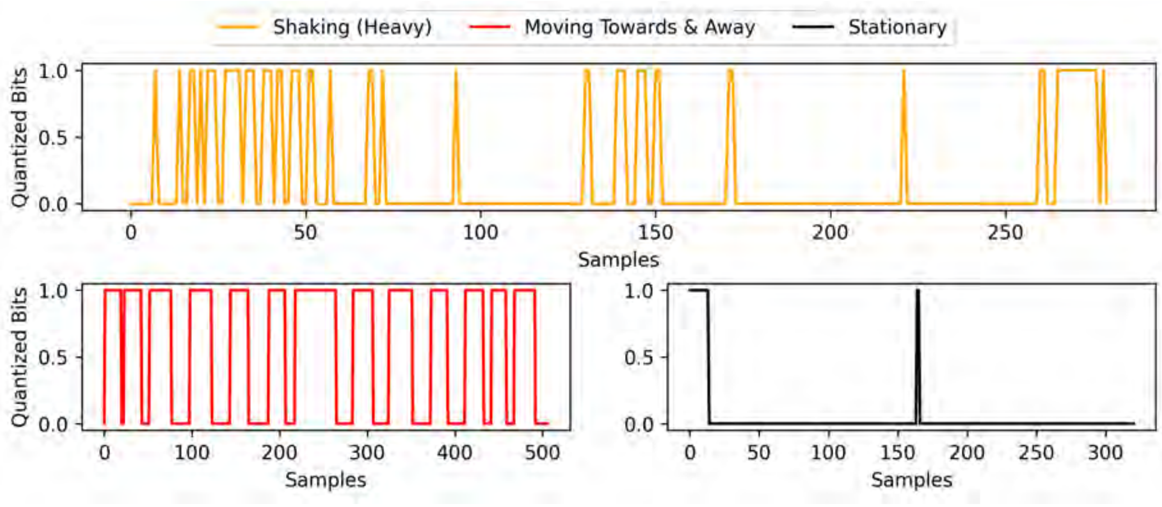


Figure 5.3: Quantized bits extracted from collected RSSI data across multiple gestures

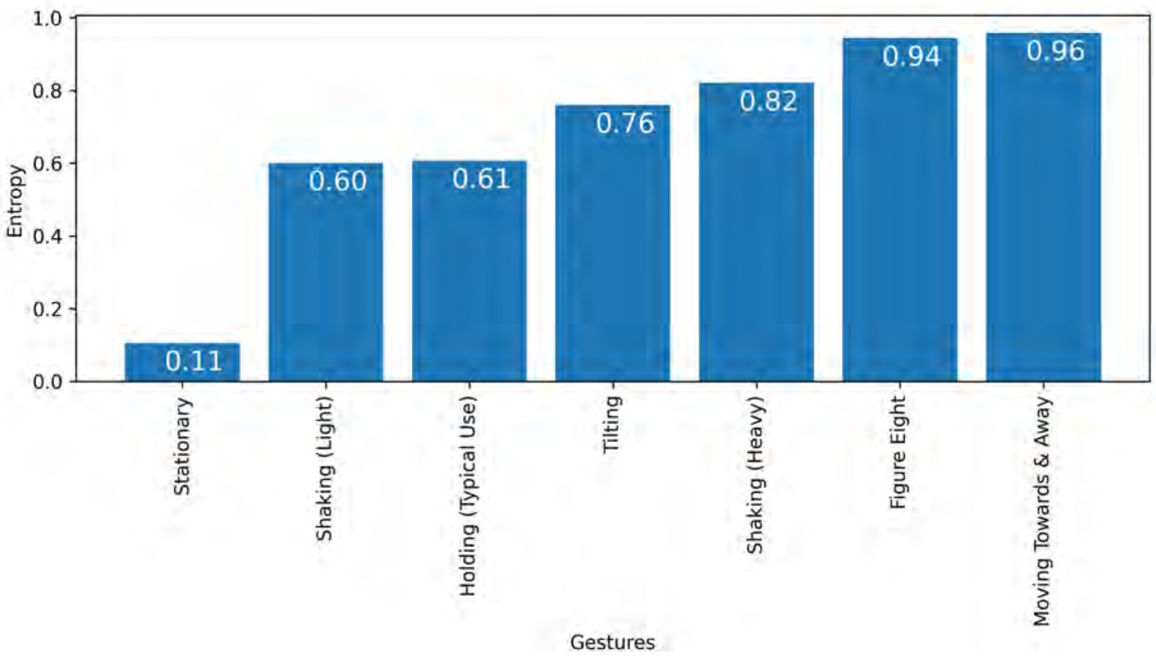


Figure 5.4: Entropy of the quantized bits collected from the RSSI readings

$$|v| = \sqrt{v_x^2 + v_y^2 + v_z^2} \tag{5.1}$$

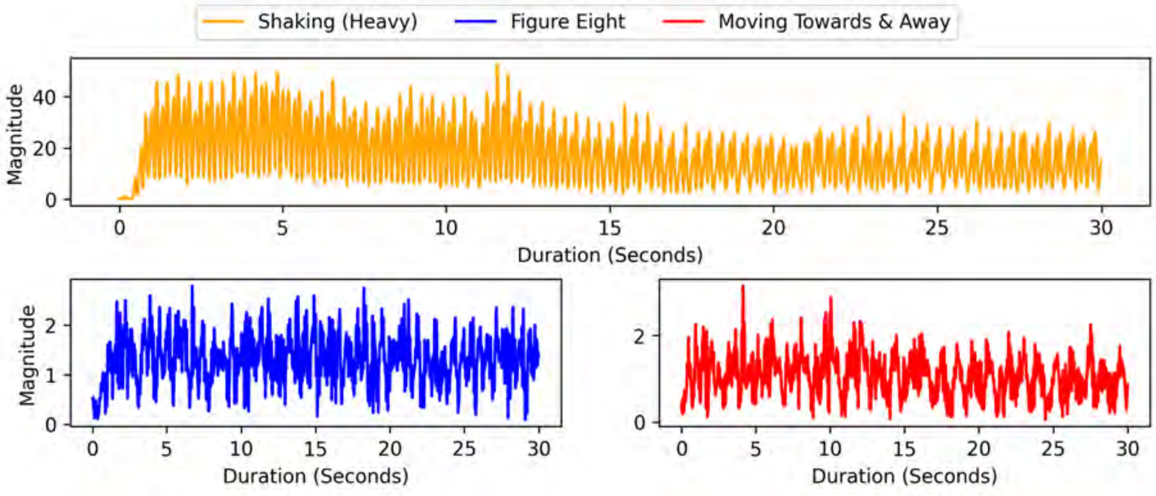


Figure 5.5: Magnitude of linear acceleration (ms^2) during the experiments

We must also analyse the associated *cost* of performing one of these gestures as we cannot simply recommend the gesture that yields the greatest uplift in quantization without considering its impact on users in terms of physical exertion. Using the linear acceleration sensor on board the Android Smartphone we can measure the acceleration experienced by the device without the impact of gravity. In addition, we will calculate the magnitude using Equation 5.1 to find out the total acceleration exerted on the device across the three axes x, y, and z where v refers to the current sampling of the linear acceleration data. Figure 5.5 shows the magnitude of linear acceleration across all axes. This figure demonstrates that *Shaking (Heavy)* has a significant amount of energy exerted by the user which can make performing this gesture harder for individuals with restricted motion. Moreover, this gesture may cause Repetitive Strain Injury (RSI) if performed on a regular and prolonged basis as stated in (Tegtmeier, 2018). Other gestures, such as *Figure Eight* and *Moving Towards & Away*, when compared to *Shaking (Heavy)* have a smaller magnitude, making them easier to perform by the user with a reduced risk to RSI.

Table 5.2 presents several key statistical metrics to enable understanding how demanding each gesture can be. In the case of *Shaking (Heavy)* and *Shaking (Light)* it is clear that they are both extreme outliers when compared to the other gestures evaluated. They are both demanding gestures to perform due to the constant back and forth motion whereas the other gestures have very limited and slow motion.

	Min	Mean	Max	Standard Deviation	Variance
Stationary	0.00	0.02	0.10	0.01	0.00
Figure Eight	0.07	1.32	3.06	0.50	0.25
Shaking (Light)	0.31	4.49	15.43	2.39	5.75
Shaking (Heavy)	0.21	19.19	54.47	10.50	110.47
Tilting	0.06	1.93	7.92	1.30	1.70
Holding (Typical Use)	0.02	0.42	3.13	0.35	0.12
Moving Towards & Away	0.06	1.05	2.56	0.45	0.21

Table 5.2: Statistics of motion sensor data obtained during the MARS experiments

5.4 Limitations

This chapter introduced a strategy for reducing the wait times experienced by BAN users when physical channel characteristics based key generation schemes are used. There are two limitations associated with this work, firstly the quality of data collected could be improved with additional or higher resolution sensors to provide better analysis of the gestures. Secondly, with there only being a single participant involved in the data collection it makes recommendation of a single gesture impossible as the sample size is too small to make a fair assessment of a gesture suitable for the average user.

5.5 Conclusion

We proposed a new strategy to shorten the secret key construction time in any RSSI SKE method. Our strategy requires that one of the two devices involved in the SKE process be mobile. It is thus the movement that dramatically improves the entropy of the quantization of measured RSSI values. This increase of entropy observed within the quantization stage of the SKE process will benefit subsequent stages and, therefore, allow for shorter wait times endured by the user when constructing the key. The performed experiments highlighted that all the evaluated gestures provide significant improvement to the entropy of the quantized bits compared to the stationary case. However, either moving towards & away or figure eight is an easy recommendation as they are both top performers in entropy and the number of quantized bits. Moreover, our experiments' results show that these gestures are some of the least demanding gestures performed by the user. In our future work, we will explore the RSSI SKE process in full enabling insight into the improvements experienced throughout as opposed to only the quantization phase. These future experiments will allow for the collection of any improvements to key construction time in addition to any impact the various gestures have on the quality of keys being produced.

Chapter 6

Conclusion and Future Work

In this chapter we shall summarise the contributions made in this thesis. We will begin in Section 6.1 with a discussion regarding the experiments performed throughout the thesis, looking at what they offer and how they are limited, due to various obstacles encountered. Following on from this discussion will be a short summary in Section 6.2 which aims to outline the impact and significance of the work conducted in this thesis. We will then follow this up with a discussion on potential solutions to maximise the proposed works' effectiveness. Finally, in Section 6.3 we will explore what work could be conducted in the future following on from this thesis.

6.1 Conclusion

For the duration of this thesis the work has focused on delivering the following; a fast and robust authentication scheme for BANs. Simply put the purpose of this thesis has been to develop an authentication scheme that is fast, this is due to the environment that it shall be deployed within, where time wasted waiting for authentication to complete could risk harm to individuals and their life. Whereas, robust refers to having the capability of defending against attacks by adversary who may desire to interfere with the authentication process. We also must ensure that the authentication process is performed with associated costs remaining low as miniature size of these devices resources such as memory, computation and power are at a premium and we cannot afford to design a scheme that meets the first two aims whilst ignoring the very constraints that make authentication for BANs difficult in the first place.

In Chapter 3 we explored if physiological-based schemes that rely upon physiological signals such as ECG are vulnerable to attacks involving prior recordings of ECG signals originating from the target. Therefore, in this chapter we developed a novel scheme for generating synthetic signals from prior recorded ECG signals and found that if the signal generated has peaks that are of equal distance between the peaks in the target signal, then key generation schemes such as ELPA are in fact vulnerable. This was the first contribution of this thesis, this discovery reveals that physiological-based key generated schemes are not as safe as the literature suggests and that steps must be taken to either secure these schemes from intrusion or look for alternative methods that do not rely upon physiological signals. The main limitation of the work in Chapter 3 would be the attack method can be categorised as a brute force method and therefore can present a challenge to potential adversaries reducing, the impact of the work.

In response to the attack method introduced in Chapter 3, the work in Chapter 4 has explored one such way to protect and ensure that existing physiological-based schemes are robust against this aforementioned attack. In Chapter 4, we present the second contribution of this thesis known as RAFV which focused on schemes that utilised the fuzzy vault and locked the key inside with the use of ECG such as PSKA or OPFKA. The proposed extension attempted to bridge the gap between physiological-based and wireless channel-based schemes. It achieved this by ensuring that the vault was obfuscated prior to transmission making it useless to anyone other than the intended recipient, such as the second ECG sensor. The inclusion of wireless channel-based approach allowed for a pattern or key to be agreed upon prior transmission via an out-of-band process. The extension or security patch was demonstrated to secure the vault and do so with little additional overhead regarding computation and time. However, the scheme has its faults such as the need to first generate a key using wireless-channel methods which does require additional time, however this could be performed at the same time as the sensor is sampling the physiological signal.

Finally, in Chapter 5 we see the work pivot away from physiological-based schemes in favour of wireless channel-based schemes. This is due to two reasons; firstly, wireless channel-based schemes appear to be secure from intrusion whereas in the prior chapters we explored the previously unknown weaknesses of physiological-based schemes. Secondly, wireless channel-based schemes are universal in the sense that they can be deployed and used on any wireless sensor within a BAN whereas the limitations of physiological based-schemes go a step further than simply being limited to worn or implanted sensors as the sensors must also carry the capability of measuring the physiological signal used within the selected key agreement method. Therefore, the work explore ways of attempting to mitigate a major weakness of wireless channel-based schemes and that is the low-key generation rate, which is due to the minimal variation in characteristics experienced when sensors are stationary. The contribution presented in this chapter therefore explored the impact of mandating the use of a mobile device that could aid with the establishment of symmetric keys. By requiring the mobile device is used we were able to take advantage of its mobility and could prompt the user to perform a gesture during the key generation process. Throughout the experiments we identified that performing simple gestures such as moving the mobile device towards and away from the sensor yielded extremely high entropy and would be ideal for ensuring wireless channel characteristics remain varied throughout. Unfortunately due to time constraints we were unable to explore the impact that this approach would have on disagreement between sensors and the quality of keys generated.

6.2 Impact and Significance of Thesis

This thesis has introduced and analysed three major contributions to the area of authentication within BANs. Firstly, we demonstrated SEAM, in Chapter 3, a security vulnerability within existing key generation and authentication schemes (Zaghouani et al., 2015; Venkatasubramanian et al., 2010) by utilising older ECG signals to compromise what should be a secure key. This has significant impact on the continued use of physiological signals such as ECG within the security domain, especially when dealing with BANs due to the potential risk to wearers' privacy and health. Secondly, we then introduced RAFV, in Chapter 4, a novel combination of physiological signals and physical channel characteristics to deliver authentication within BANs strengthening existing solutions and mitigating the risks imposed by SEAM. Finally, in Chapter 5 we explore a potential method for reducing the long wait times that can impact physical channel characteristic based schemes. This was done to meet the stringent requirements of BANs devices as laid out in Chapter 1 as existing approaches require additional hardware or costly computations making them inappropriate for BANs devices.

6.3 Future Work

In this thesis we proposed a number of contributions in attempting to develop an authentication scheme that met desired features whilst appreciating the constraints imposed by sensors found within a BAN. However, the work is not finished and future work and areas to explore need to be considered.

We will first look at the existing contributions and attempt to propose ways of improving them. Firstly, in Chapter 3 our attack method for compromising key physiological-based key generation schemes is classified as brute force. Which detracts from the strength of the contribution, therefore work could be carried out that would explore the solution space to better understand how many viable solutions exist. This should be considered as these physiological-based schemes are fuzzy in nature and can be quite forgiving of discrepancies found within the synthetic signal, meaning multiple synthetic signals could all be used to derive the key even though they are not perfect in replicating the target signal. In doing so we could demonstrate that our attack is therefore more likely and represents a credible threat. Secondly, in Chapter 4 we presented an extension to some existing schemes to protect against the previously mentioned attack. Whilst the proposal clearly demonstrates it is capable of defending against the attack and can do so with minimal additional overhead, the extension is limited to only fuzzy vault based schemes. Therefore, future work could explore the potential of applying physical channel characteristics to schemes such as ELPA whereby the BCH error correction codes could be XORed with the key generated from the wireless channel. Finally, in Chapter 5 we managed to present the improvements to entropy of generated bits provided one of the devices remains in motion. Unfortunately, we did not explore the impact that the approach would have on disagreement between sensors and the quality of keys generated and future work must explore this to ensure it is viable. In addition to this, we could explore which gestures are most favoured by people to better understand which gestures are more likely to be performed. This could be achieved by asking participants to perform the gestures and answer questions to reveal which gesture is more favoured.

Finally, due to various constraints that have impacted the thesis some work has never been conducted beyond the planning stages. Therefore, we would like to discuss these ideas as future work. Firstly, we could attempt to further improve the wireless channel schemes by manipulating the transceiver's power levels for transmitting and receiving of probes. This could have the effect of introducing variations within the wireless channel providing an improvement to key generation rate. This was not explored during the thesis as attempting to implement such an experiment would prove to be time consuming as it may require significant modification to firmware of the transceiver. Secondly, we had a proposal whereby multiple sensors attempt to generate a key via wireless channel approaches at the same time. This simultaneous approach could enable a collection of sensors to be initialised at the same time, therefore, reducing the wait experienced by medical professionals which is extremely important in time sensitive moments. However, during the design of such a proposal it was clear that it would be less than ideal to have multiple sensors attempting to generate the key at the same time as they would be pooling from the same source of randomness which would lead to either collisions or very similar keys which an adversary could take advantage of. Therefore, we would propose that any future work would limit the sensors access to the wireless channel and randomly select a subset of sensors, this way improvements to construction could be achieved without compromising the quality of the keys produced. Finally, we would also like to state that future work could explore the potential of using a mobile device as Key Distribution Center (KDC) in a large deployment of BAN sensors, which would facilitate the establishment of symmetric keys between sensors on body and off.

References

ABI-CHAR, P. E., MHAMED, A. and EL-HASSAN, B. (2007), A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications, *in* 'The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007)', pp. 235–240.

Ali, S. T. et al. (2012), Zero reconciliation secret key generation for body-worn health monitoring devices, *in* 'Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks', WISEC '12, ACM, New York, NY, USA, pp. 39–50.
URL: *http://doi.acm.org/10.1145/2185448.2185455*

Anand, M., Ives, Z. and Lee, I. (2005), Quantifying eavesdropping vulnerability in sensor networks, *in* 'Proceedings of the 2nd International Workshop on Data Management for Sensor Networks', DMSN '05, Association for Computing Machinery, New York, NY, USA, p. 3–9.
URL: *https://doi.org/10.1145/1080885.1080887*

Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., Drielsma, P. H., Heám, P. C., Kouchnarenko, O., Mantovani, J., Mödersheim, S., von Oheimb, D., Rusinowitch, M., Santiago, J., Turuani, M., Viganò, L. and Vigneron, L. (2005), The avispa tool for the automated validation of internet security protocols and applications, *in* K. Etessami and S. K. Rajamani, eds, 'Computer Aided Verification', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 281–285.

Ashley, E. A. and Niebauer, J. (2004), *Cardiology explained*, Remedica.

Bellardo, J. and Savage, S. (2003), 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions, *in* 'Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12', SSYM'03, USENIX Association, USA, p. 2.

Bellare, M., Canetti, R. and Krawczyk, H. (1996), Keying hash functions for message authentication, *in* N. Koblitz, ed., 'Advances in Cryptology — CRYPTO '96', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–15.

Bernstein, D. J. and Lange, T. (2013), Security dangers of the nist curves, *in* 'Invited talk, International State of the Art Cryptography Workshop, Athens, Greece'.

Blocki, J., Harsha, B. and Zhou, S. (2018), On the economics of offline password cracking, *in* '2018 IEEE Symposium on Security and Privacy (SP)', pp. 853–871.

Bluetooth Core Specification (2021), `https://www.bluetooth.com/specifications/specs/core-specification/`.

Bu, G. and Potop-Butucaru, M. (2018), 'Ban-gzkp: Optimal zero knowledge proof based scheme for wireless body area networks', *Ad Hoc Networks* **77**, 28–41.
URL: *https://www.sciencedirect.com/science/article/pii/S157087051830132X*

Callegati, F., Cerroni, W. and Ramilli, M. (2009), 'Man-in-the-middle attack to the https protocol', *IEEE Security Privacy* **7**(1), 78–81.

Elgamal, T. (1985), 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Transactions on Information Theory* **31**(4), 469–472.

Fu, K. and Xu, W. (2018), 'Risks of trusting the physics of sensors', *Commun. ACM* **61**(2), 20–23.
URL: *https://doi.org/10.1145/3176402*

Gao, X., Du, W., Liu, W., Wu, R. and Zhan, F. (2020), A lightweight and efficient physical layer key generation mechanism for manets, *in* '2020 IEEE 6th International Conference on Computer and Communications (ICCC)', pp. 1010–1015.

Goldberger, A. L. et al. (2000), 'PhysioBank, PhysioToolkit, and PhysioNet', *Circulation* **101**(23).
URL: *https://doi.org/10.1161/01.cir.101.23.e215*

Guo, D., Wen, Q., Li, W., Zhang, H. and Jin, Z. (2015), 'A novel authentication scheme using self-certified public keys for telecare medical information systems', *Journal of Medical Systems* **39**(6), 62.
URL: *https://doi.org/10.1007/s10916-015-0245-z*

Hamed, A. and Khalek, A. A. (2019), Acoustic attacks in the era of iot - a survey, *in* '2019 Amity International Conference on Artificial Intelligence (AICAI)', pp. 855–858.

Harland, C. J. et al. (2001), 'Electric potential probes - new directions in the remote sensing of the human body', *Measurement Science and Technology* **13**(2), 163–169.
URL: *https://doi.org/10.1088/0957-0233/F13/2/304*

Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X. and Chen, D. (2013), Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks, *in* '2013 Proceedings IEEE INFOCOM', pp. 2274–2282.

IEEE (2018), '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)* pp. 1–274.

IEEE (2019), 'Iso/iec/ieee international standard - information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 2: Sub 1 ghz license exempt operation', *ISO/IEC/IEEE 8802-11:2018/Amd.2:2019(E)* pp. 1–596.

Jana, S., Premnath, S. N., Clark, M., Kasera, S. K., Patwari, N. and Krishnamurthy, S. V. (2009), On the effectiveness of secret key extraction from wireless signal strength in real environments, *in* 'Proceedings of the 15th Annual International Conference on Mobile Computing and Networking', MobiCom '09, Association for Computing Machinery, New York, NY, USA, p. 321–332.
URL: *https://doi.org/10.1145/1614320.1614356*

Javali, C., Revadigar, G., Ding, M., Lin, Z. and Jha, S. (2021), *Cooperative Physical Layer Secret Key Generation by Virtual Link Estimation*, Springer International Publishing, Cham, pp. 99–128.
URL: *https://doi.org/10.1007/978-3-030-55366-1_5*

Juels, A. and Sudan, M. (2002), A fuzzy vault scheme, *in* ‘Proceedings IEEE International Symposium on Information Theory,’, pp. 408–.

Jumahat, S. et al. (2019), 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.
URL: *https://doi.org/10.1109/cspa.2019.8695982*

Khan, S. R., Mugisha, A. J., Tsiamis, A. and Mitra, S. (2022), ‘Commercial off-the-shelf components (cots) in realizing miniature implantable wireless medical devices: A review’, *Sensors* **22**(10).
URL: *https://www.mdpi.com/1424-8220/22/10/3635*

Khernane, N., Potop-Butucaru, M. and Chaudet, C. (2016), Banzkp: A secure authentication scheme using zero knowledge proof for wbans, *in* ‘2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)’, pp. 307–315.

Kim, J. et al. (2019), A study on the security vulnerabilities of fuzzy vault based on photoplethysmogram, *in* J. J. Park, V. Loia, K.-K. R. Choo and G. Yi, eds, ‘Advanced Multimedia and Ubiquitous Engineering’, Springer Singapore”, Singapore, pp. 359–365.

Kumar, M. S., Ramanathan, R., Jayakumar, M. and Yadav, D. K. (2021), ‘Physical layer secret key generation using discrete wavelet packet transform’, *Ad Hoc Networks* **118**, 102523.
URL: *https://www.sciencedirect.com/science/article/pii/S1570870521000767*

Lee, Y. et al. (2018), ‘A novel non-contact heart rate monitor using impulse-radio ultra-wideband (IR-UWB) radar technology’, *Scientific Reports* **8**(1).
URL: *https://doi.org/10.1038/s41598-018-31411-8*

Li, Z. and Wang, H. (2016), A key agreement method for wireless body area networks, *in* '2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)', pp. 690–695.

Li, Z., Wang, H., Daneshmand, M. and Fang, H. (2017), Secure and efficient key generation and agreement methods for wireless body area networks, *in* '2017 IEEE International Conference on Communications (ICC)', pp. 1–6.

Li, Z., Wang, H. and Fang, H. (2017), 'Group-based cooperation on symmetric key generation for wireless body area networks', *IEEE Internet of Things Journal* **4**(6), 1955–1963.

Liu, J., Zhang, Z., Chen, X. and Kwak, K. S. (2014), 'Certificateless remote anonymous authentication schemes for wirelessbody area networks', *IEEE Transactions on Parallel and Distributed Systems* **25**(2), 332–342.

Ma, L., Ge, Y. and Zhu, Y. (2014), 'Tinyzkp: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks', *Wireless Personal Communications* **77**(2), 1077–1090.
URL: *https://doi.org/10.1007/s11277-013-1555-4*

Mahdi, A. E. and Faggion, L. (2011), 'Non-contact biopotential sensor for remote human detection', *Journal of Physics: Conference Series* **307**, 012056.

Poon, C., Zhang, Y.-T. and Bao, S.-D. (2006), 'A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health', *IEEE Communications Magazine* **44**(4), 73–81.

Premnath, S. N., Jana, S., Croft, J., Gowda, P. L., Clark, M., Kasera, S. K., Patwari, N. and Krishnamurthy, S. V. (2013), 'Secret key extraction from wireless signal strength in real environments', *IEEE Transactions on Mobile Computing* **12**(5), 917–930.

Reed, I. S. and Solomon, G. (1960), 'Polynomial codes over certain finite fields', *Journal of the Society for Industrial and Applied Mathematics* **8**(2), 300–304.
URL: *https://doi.org/10.1137/0108018*

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

Revadigar, G., Javali, C., Asghar, H. J., Rasmussen, K. B. and Jha, S. (2015), Mobility independent secret key generation for wearable health-care devices, *in* ‘Proceedings of the 10th EAI International Conference on Body Area Networks’, BodyNets ’15, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, p. 294–300.
URL: *https://doi.org/10.4108/eai.28-9-2015.2261446*

Rui, Z. and Yan, Z. (2019), ‘A survey on biometric authentication: Toward secure and privacy-preserving identification’, *IEEE Access* **7**, 5994–6009.

Ryu, E.-K., Kim, K.-W. and Yoo, K.-Y. (2003), A simple key agreement protocol, *in* ‘IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, 2003. Proceedings.’, pp. 128–131.

Saeed, M. E. S., Liu, Q.-Y., Tian, G., Gao, B. and Li, F. (2018), ‘Remote authentication schemes for wireless body area networks based on the internet of things’, *IEEE Internet of Things Journal* **5**(6), 4926–4944.

Salim, M. M., Rathore, S. and Park, J. H. (2020), ‘Distributed denial of service attacks and its defenses in iot: a survey’, *The Journal of Supercomputing* **76**(7), 5320–5363.
URL: *https://doi.org/10.1007/s11227-019-02945-z*

Sammoud, A., Chalouf, M. A., Hamdi, O., Montavont, N. and Bouallegue, A. (2020), ‘A new biometrics-based key establishment protocol in wban: energy efficiency and security robustness analysis’, *Computers & Security* **96**, 101838.
URL: *https://www.sciencedirect.com/science/article/pii/S0167404820301115*

Sethuraman, S. C., Vijayakumar, V. and Walczak, S. (2019), ‘Cyber attacks on healthcare devices using unmanned aerial vehicles’, *Journal of Medical Systems* **44**(1), 29.
URL: *https://doi.org/10.1007/s10916-019-1489-9*

Sinha, P., Jha, V. K., Rai, A. K. and Bhushan, B. (2017), Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of osi reference model: A survey, *in* ‘2017 International Conference on Signal Processing and Communication (ICSPC)’, pp. 288–293.

Stoica, P. and Moses, R. L. (2005), *Spectral analysis of signals*, Pearson Education.

Tegtmeier, P. (2018), ‘A scoping review on smart mobile devices and physical strain’, *Work* **59**, 273–283.
URL: *https://doi.org/10.3233/WOR-172678*

The Beth Israel Deaconess Medical Center, T. A. L. (1990), ‘The mit-bih normal sinus rhythm database’.
URL: *https://physionet.org/content/nsrdb/*

Toorani, M. (2015), On vulnerabilities of the security association in the ieee 802.15.6 standard, *in* ‘International conference on financial cryptography and data security’, Springer, pp. 245–260.

Trippel, T., Weisse, O., Xu, W., Honeyman, P. and Fu, K. (2017), Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks, *in* ‘2017 IEEE European Symposium on Security and Privacy (EuroS P)’, pp. 3–18.

Venkatasubramanian, K., Banerjee, A. and Gupta, S. (2008), Ekg-based key agreement in body sensor networks, *in* ‘IEEE INFOCOM Workshops 2008’, pp. 1–6.

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

Wang, H., Sheng, B., Tan, C. C. and Li, Q. (2011), ‘Public-key based access control in sensornet’, *Wirel. Netw.* **17**(5), 1217–1234.
URL: *https://doi.org/10.1007/s11276-011-0343-x*

Wang, Y. et al. (2007), ‘Analysis of human electrocardiogram for biometric recognition’, *EURASIP Journal on Advances in Signal Processing* **2008**(1).

Xu, J. et al. (2020), 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)', Vol. 1, pp. 1301–1305.

Yaqoob, T. et al. (2019), 'Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review', *IEEE Communications Surveys Tutorials* **21**(4), 3723–3768.

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

Zhang, Z., Wang, H., Vasilakos, A. V. and Fang, H. (2013), Channel information based cryptography and authentication in wireless body area networks, *in* 'Proceedings of the 8th International Conference on Body Area Networks', BodyNets '13, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, p. 132–135.
URL: *https://doi.org/10.4108/icst.bodynets.2013.253689*

Zhang, Z. et al. (2020), 'A kalman filtering based adaptive threshold algorithm for QRS complex detection', *Biomedical Signal Processing and Control* **58**, 101827.
URL: *https://doi.org/10.1016/j.bspc.2019.101827*

Zhao, H. et al. (2016), 'Physiological-signal-based key negotiation protocols for body sensor networks: A survey', *Simulation Modelling Practice and Theory* **65**, 32 – 44. Analyzing and Visual Programming Internet of Things.
URL: *http://www.sciencedirect.com/science/article/pii/S1569190X15001744*

Zibgee Specification (2015), `https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf`.

Appendix

```python
def location_of_last_beat(path: str) -> Union[int, None]:
    """
    Identify the location of the last normal beat within the specified
  ↪  patient record.
    :param path: :param path: relative path to the record to be loaded
  ↪ .
    :return: either None or the sample point at which the last normal
  ↪ beat occurred.
    """
    loc_and_sym: tuple = (*Annotations(path).locations_and_symbols,)
    for location, symbol in reversed(loc_and_sym):
        if symbol is Code.NORMAL:
            return int(location)
    return None
```

```python
def extract_compl(signal: np.ndarray, location_of_normal_beat: tuple,
  ↪ n_samples: int = 30) -> np.ndarray:
    """
    Extract a single QRS complex that can identified from the normal
  ↪ beat locations.
    :param signal: the signal data in which the QRS complex shall be
  ↪ extracted from.
    :param location_of_normal_beat: tuple containing the location of
  ↪ normal beats within the signal.
    :param n_samples: number of samples either side of the normal beat
  ↪  be extracted as a single complex.
    :return: a new ndarray of containing the samples that make up that
  ↪  complex.
    """
    start, end = location_of_normal_beat - n_samples,
  ↪ location_of_normal_beat + n_samples
    if start < 0 or end >= len(signal):
        return None
    identify_peak = lambda : np.argmax(signal[start:end])
    peak_location = start + identify_peak()
    start, end = peak_location - n_samples, peak_location + n_samples
    return signal[start:end]
```

```python
def extract_all_compls(signal: np.ndarray, location_of_normal_beats:
  ↪ tuple, n_samples: int = 30) -> np.ndarray:
    """
    Extract all of the QRS complexes within the provided signal.
    :param signal: the signal data in which the QRS complexes shall be
  ↪  extracted from.
    :param location_of_normal_beat: tuple containing the location of
  ↪ normal beats within the signal.
    :param n_samples: number of samples either side of the normal beat
  ↪  be extracted as a single complex.
```

```
    :return: a new ndarray of containing all of the QRS complexes.
    """
    compls = [extract_compl(signal, location, n_samples) for location in location_of_normal_beats]
    valid_compls = [*filter(lambda compl : compl is not None, compls)]
    return ([*filter(lambda compl : compl.size == 2 * n_samples, valid_compls)])
```

```
def construct_signal(segment: np.ndarray, peak_locations: tuple, signal_length: int = 640) -> np.ndarray:
    """
    Construct a signal using a QRS complex and a tuple of peak locations where the complexes shall be placed.
    :param segment: single QRS complex segment.
    :param peak_locations: tuple containing the location where peaks should be placed.
    :param signal_length: max size of the constructed signal.
    """
    signal = [None] * signal_length
    segment_size = len(segment)
    peak_offset = segment_size // 2
    for peak_location in peak_locations:
        start, end = peak_location - peak_offset, peak_location + peak_offset
        if start != abs(start):
            n_samples_discarded = abs(start)
            signal[:end] = segment[n_samples_discarded:]
        else:
            signal[start:end] = segment
    signal = [0 if sample is None else sample for sample in signal]
    return np.asarray(signal[:signal_length])
```

```
def cartesian_power_indices(n: int, n_symbols: int, order: int) -> tuple[int, ...]:
    result = [0] * order
    result[0], remainder = divmod(n, n_symbols ** (order - 1))
    for counter in range(order - 2, -1, -1):
        result[order - counter - 1], remainder = divmod(remainder, n_symbols ** counter)
    return result

def cartesian_power_index(cartesian_power: tuple[int, ...], symbols: tuple[int, ...]) -> int:
    result = 0
    order, n_symbols = len(cartesian_power), len(symbols)
    power_indices = [symbols.index(element) for element in cartesian_power]
    for counter in range(order - 1, -1, -1):
        result += power_indices[order - counter - 1] * n_symbols ** counter
    return result

def cartesian_power_n(n: int, symbols: tuple[int, ...], order: int) -> tuple[int, ...]:
    return (*(symbols[index] for index in cartesian_power_indices(n, len(symbols), order)),)

def cartesian_product(symbols: tuple[int, ...], order: int) -> Generator[tuple[int, ...], None, None]:
    for counter in range(len(symbols) ** order):
        yield cartesian_power_n(counter, symbols, order)
```

```
/**
```

```cpp
 * In order to conceal the polynomial chaff points must be added to the vault in order to prevent the adversary from
 * simply reconstructing the polynomial with the points contained within. This process works by excluding of locking
 * element points from being candidate chaff points. Then a sample is taken ensuring if a point is choosen it is only
 * chosen once. Then each candidate abscissa is combined with a random  ordinate that must not equal P(abcissa)
 */
void FuzzyVault::apply_chaff()
{
    std::vector<unsigned short> reserved_abscissas, permitted_abscissas(this->vault_width), selected_abscissas;
    for(auto coordinate : this->vault_data) { reserved_abscissas.push_back(coordinate.abscissa); }
    auto ordinate_distribution = std::uniform_int_distribution<unsigned short>(0, this->vault_height);
    auto generate_permitted_abscissas = [n = 0, &reserved_abscissas]() mutable
    {
        n++;
        auto find_result = std::find(reserved_abscissas.begin(), reserved_abscissas.end(), n);
        return find_result != std::end(reserved_abscissas) ? 0 : n;
    };
    std::generate(permitted_abscissas.begin(), permitted_abscissas.end(), generate_permitted_abscissas);
    std::sample(permitted_abscissas.begin(), permitted_abscissas.end(), std::back_inserter(selected_abscissas),
        this->vault_size, *this->mersenne_twister_engine);
    selected_abscissas.erase(std::remove(selected_abscissas.begin(), selected_abscissas.end(), 0), selected_abscissas.end());
    selected_abscissas.shrink_to_fit();
    for(auto abscissa : selected_abscissas)
    {
        unsigned short invalid_ordinate = this->vault_polynomial(abscissa) % this->vault_height;
        bool has_found_ordinate = false; unsigned long ordinate = 0;
        while(!has_found_ordinate)
        {
            ordinate = ordinate_distribution(*this->mersenne_twister_engine);
            has_found_ordinate = (ordinate != 0 && ordinate != invalid_ordinate) ? true : false;
        }
        this->vault_data.push_back(Coordinate(abscissa, ordinate));
        if(this->vault_data.size() >= this->vault_size) break;
    }
}
```

```cpp
/**
* The vault is ordered to ensure that the adversary can not simply use  the first n elements to reconstruct the
* polynomial. This is because they would be the locking elements that would allow for polynomial reconstruction.
* The vault is ordered by abscissa smallest to largest. Ordinates are not compared as there should only be one point
* at most for each abscissa within the vault.
*/
void FuzzyVault::order_vault()
{
    std::sort(this->vault_data.begin(), this->vault_data.end(), [](Coordinate left, Coordinate right) {
        return left.abscissa < right.abscissa;
    });
}
```

```
void Quadrant::divide()
{
    if(this->level < this->max_level)
    {
        unsigned short quadrant_width = this->width / 2;
        unsigned short quadrant_height = this->height / 2;
        for(auto counter = 0; counter < 4; counter++)
        {
            unsigned short row = counter / 2;
            unsigned short column = counter % 2;
            unsigned short quadrant_abscissa = this->abscissa + column * quadrant_width;
            unsigned short quadrant_ordinate = this->ordinate + row * quadrant_height;
            auto child_quadrant = std::make_shared<Quadrant>( quadrant_abscissa, quadrant_ordinate, quadrant_width,
                quadrant_height, this->level + 1, this->max_level, this->vault_data, this->tree_map);
            if(counter == 0)
                this->south_west = child_quadrant;
            else if(counter == 1)
                this->south_east = child_quadrant;
            else if(counter == 2)
                this->north_west = child_quadrant;
            else
                this->north_east = child_quadrant;
        }
    }
}
```

```
std::vector<int> Quadrant::get_occupants()
{
    auto result = std::vector<int>();
    auto is_in_boundaries = [&] (Coordinate& coordinate) -> bool
    {
        auto coordinate_abscissa = coordinate.abscissa; auto coordinate_ordinate = coordinate.ordinate;
        if(this->abscissa < coordinate_abscissa && this->abscissa + this->width > coordinate_abscissa
        && this->ordinate  < coordinate_ordinate && this->ordinate + this->height > coordinate_ordinate)
            return true;
        else
            return false;
    };
    auto vault_iterator = this->vault_data.begin();
    while(vault_iterator != this->vault_data.end())
    {
        vault_iterator = std::find_if(vault_iterator, this->vault_data.end(), is_in_boundaries);
        if(vault_iterator != this->vault_data.end())
        {
            result.push_back(std::distance(this->vault_data.begin(), vault_iterator));
            vault_iterator++;
        }
    }
    return result;
}
```

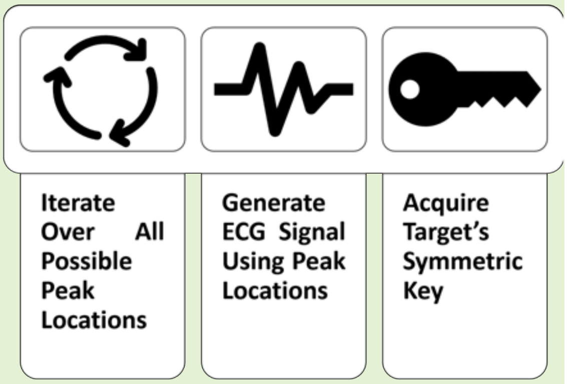
```
void RotationalVault::rotate_vault(QuadTree quad_tree, std::vector<std::pair<int, bool>> rotation_pattern)
{
    for(auto pair : rotation_pattern)
    {
        auto point_indices = quad_tree.get_occupants(pair.first);
        auto center = quad_tree.get_center(pair.first);
        for(auto index : point_indices)
        {
            this->rotate_point(index, pair.second, center);
        }
    }
}
```

```
void RotationalVault::rotate_point(int index, bool clockwise_direction, Coordinate center)
{
    auto original_abscissa = this->vault_data[index].abscissa;
    auto original_ordinate = this->vault_data[index].ordinate;
    if(clockwise_direction)
    {
        this->vault_data[index].abscissa = original_ordinate - center.ordinate + center.abscissa;
        this->vault_data[index].ordinate = -1 * (original_abscissa - center.abscissa) + center.ordinate;
    }
    else
    {
        this->vault_data[index].abscissa = -1 * (original_ordinate - center.ordinate) + center.abscissa;
        this->vault_data[index].ordinate = 1 * (original_abscissa - center.abscissa) + center.ordinate;
    }
}
```

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].

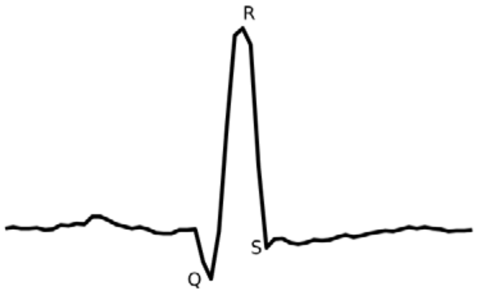


Fig. 1: Annotated ECG signal demonstrating the location of the components that make up the QRS complex (derived from [14])

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)

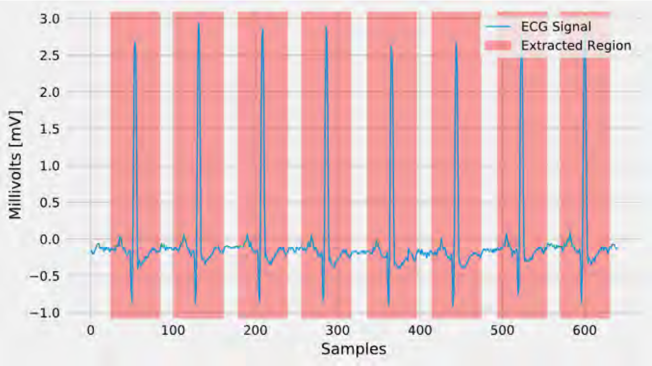


Fig. 2: 640 sample ECG plot with the highlighted regions demonstrating the segments that shall be extracted and utilized by SEAM

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

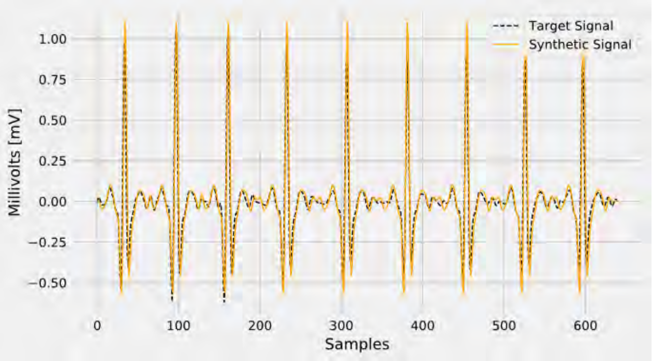


Fig. 3: Comparison of the target and synthetic signal in the time domain

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.

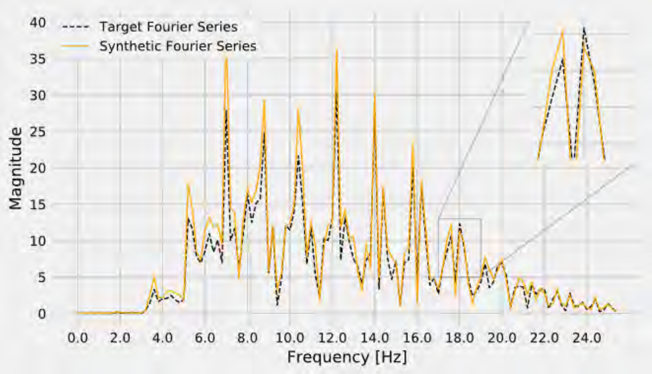


Fig. 4: Comparison of the target and synthetic signal in the frequency domain

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.

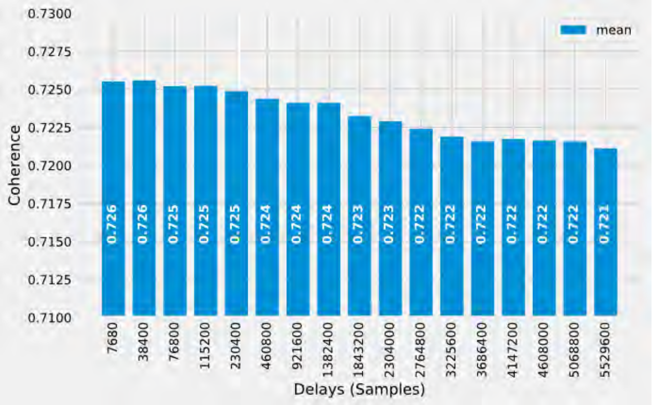
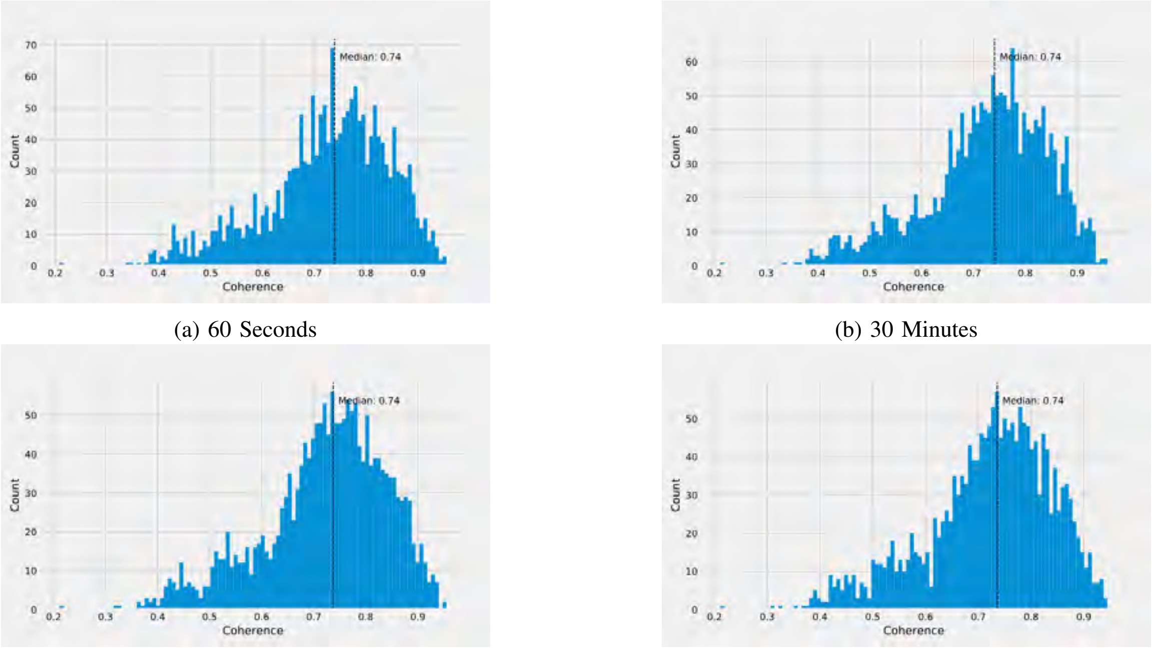


Fig. 5: The impact of the delay on the achieved coherence level of synthetic signals

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)

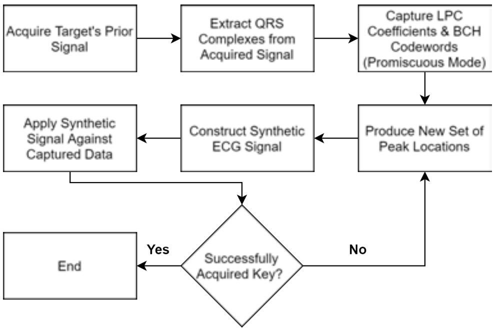

Acquire Target's Prior Signal
Extract QRS Complexes from Acquired Signal
Capture LPC Coefficients & BCH Codewords (Promiscuous Mode)
Apply Synthetic Signal Against Captured Data
Construct Synthetic ECG Signal
Produce New Set of Peak Locations
End
Yes
Successfully Acquired Key?
No

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.

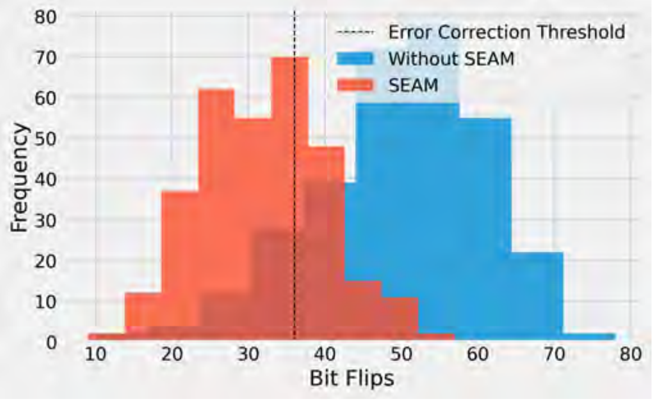


Fig. 8: Impact of SEAM on increasing the success rate of attack attempts against ELPA

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.

Securing Fuzzy Vault Enabled Authentication in Body Area Networks based Smart Healthcare

Jack Hodgkiss and Soufiene Djahel
Department of Computing and Mathematics, Manchester Metropolitan University, UK

Abstract—**The emergence of Body Area Networks (BANs) has paved the way for real-time sensing of human biometrics in addition to remote control of smart wireless medical devices, which in turn are beginning to revolutionize the smart healthcare industry. However, due to their limited power and computational capabilities they are vulnerable to a myriad of security attacks. To secure BAN sensors against these threats processor-intensive cryptographic techniques need to be avoided as they are not suitable in this context. This paper focuses on authentication service for BAN sensors and proposes an original scheme named "RAFV: Rotational Assisted Fuzzy Vaults" to harden the security of any authentication solution using the fuzzy vault construction approach. The evaluation results have shown that RAFV can successfully conceal the secret of the vault even if the locking elements are known to the adversary. Also, RAFV may improve upon communication overhead by enabling a reduction in the size of the vault without compromising its security. It has achieved all of this while remaining competitive with regards to additional computational overhead.**

I. Introduction

Body Area Networks (BANs) are expected to play a major role in enabling "smart healthcare", which is the inclusion of technology to help sense, evaluate and react to the environment and patients to deliver high-quality care. BAN sensors are a type of network devices small enough to be worn on or implanted within the human body [1]. These devices enable continuous patient vital sign monitoring in addition to remote control of medical devices such as insulin pump, pacemaker, or continuous glucose monitoring. Due to their nature (i.e., limited power resources, memory usage and computational capabilities) and the environment, they operate within, securing these devices along with their network is crucial to the success and wide adoption of this technology.

Authentication is a crucial process in safeguarding BANs and their operations such as the transmission of patients' health data or receiving commands. Many lightweight authentication schemes have been proposed over the years to ensure the required security level for BAN sensors while meeting their stringent constraints [2]. Authentication enables BAN sensors or devices to prove their identity for verification by completing an authentication process or challenge. Without any form of authentication, BAN sensors are vulnerable to various security attacks that may be carried out by a motivated adversary. In [3], the authors outline the security requirements for BANs based smart healthcare and highlight the unique challenges that need to be overcome to develop robust biometrics based authentication schemes for BAN. Moreover, using fingerprints as an authentication mechanism to unlock mobile devices for payment authorization purpose was investigated in [4]. This study raised some concerns about fingerprint-based authentication and potentially other biometrics, such as ECG, due to their associated vulnerabilities. Issues discussed include how fingerprints may be captured, how users cannot easily avoid leaving their fingerprint behind and how once an adversary compromises it, the revocation is impossible. A review of the developed authentication protocols for deployment within implanted medical devices (IMDs) was presented in [5]. This paper outlines the security challenges and functionality requirements for authentication schemes targeting IMDs that can be classified as either proximity-based, biometric-based or a combination of the two.

Fuzzy vaults are one such scheme that is being used to facilitate a key agreement between communicating BAN nodes to achieve a robust authentication. Fuzzy vault [6] is a cryptographic construction that allows a user to conceal a secret value (e.g., message, password or cryptographic key) by locking it using elements obtained from a publicly known universe. Any attempt to unlock the vault and uncover the secret contained within it requires significant overlap between the set of elements used to lock the vault and the set being used to attempt unlocking it. The order in which these elements are used when unlocking the vault has no impact on success due to the fuzzy vault's possessing order invariance. These two properties make unlocking a fuzzy vault possible without a perfect or near-perfect recall of the elements used to lock the secret. This may appear as a security vulnerability, however, the fuzzy vault scheme is more suitable for environments where shared knowledge of the elements used to lock the vault originates from a source that is incapable of 100% successful capture. An appropriate example of such a source is "fingerprint minutiae" [7] where the positioning of the finger, the moisture present and any movement can have a significant impact on the sensor's ability to extract identifying markers. Even successive readings of the same finger by the same device can vary to such an extent that they would appear to be from separate users.

II. Fuzzy vault overview

The fuzzy vault scheme was first introduced in [6] to conceal a secret (S) using a set of elements A known at the time of vault construction. Once locked, the vault can only be unlocked using another set of elements B that has significant overlap with the set A. The fuzzy vault can be constructed in such a way to allow unlocking through the use of either error correction codes or polynomial interpolation. For the sake of simplicity, we will be using polynomial interpolation, specifically Lagrangian Interpolation. The vault is constructed as follows: 1) Generate an n^{th} order univariate polynomial P over the indeterminate x whose coefficients are an encoding of the secret S, 2) Evaluate $P(X)$ using the elements of the set A creating a new set $R = \{A_{\text{i}}, P(A_{\text{i}})\}$, 3) Randomly generate a set of chaff points C which do not share the same x with any point within R or any other chaff point, also no chaff point may imitate a legitimate point $C = \{(C_{\text{x}}, C_{\text{y}}) | C_{\text{x}} \notin A,\ C_{\text{y}} \neq P(x)\}$, 4) Combine the sets R and C together then order the resulting set in ascending order. Any attempt to reconstruct the polynomial, and by extension the secret S, will require knowledge of $n+1$ features (elements) present within the set A. The fuzzy vault construction steps are shown in Fig. 1.

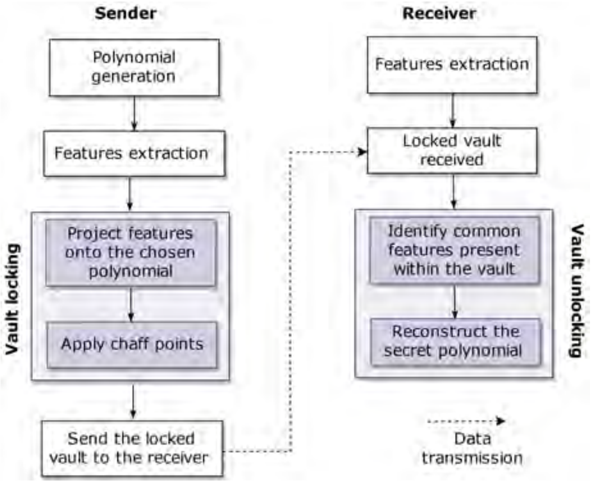

Sender
Receiver
Polynomial generation
Features extraction
Project features onto the chosen polynomial
Apply chaff points
Vault locking
Send the locked vault to the receiver
Features extraction
Locked vault received
Identify common features present within the vault
Reconstruct the secret polynomial
Vault unlocking
Data transmission

Figure 1: The main steps of the fuzzy vault construction process

An illustrative use case of the fuzzy vault scheme would be the following; $Alice$ wishes to exchange her contact details (i.e., phone/mobile number or email address) on travel forums with individuals who share the same interest with regards to international travel. Since $Alice$ does not want everyone to have access to her contact information she may distribute them using a fuzzy vault, by concealing within the vault her contact information as a secret to be recovered. Only those who have similar travel interests may successfully recover $Alice$'s contact information. $Alice$ will start by encoding her contact information within the coefficients of a polynomial $P(X)$ which has a degree that determines the error tolerance of the vault. The smaller the degree the fewer overlapping features are required for a successful unlock, whereas the higher the degree the more overlapping features are needed. $Alice$ will then construct a set of elements A which represents travel locations (i.e., features) around the world; $A = \{Manchester, Berlin, LosAngeles, ...\}$. These features will be mapped onto $P(X)$ followed by the generation of chaff points which must not fall upon the polynomial. The vault is then shuffled to ensure that the legitimate features are concealed amongst the chaff points. This vault can then be exchanged with other individuals with an interest in travelling. For example, Bob may attempt to unlock the vault using his features contained in the set $B = \{Berlin, LosAngeles, NewYork...\}$ and will achieve this as long as $|A \bigcap B| > 1+n$, where n is the degree of the polynomial. Any other user who does not meet this requirement will be unable to acquire Alice's contact information.

III. Fuzzy vault Security Vulnerability

Two pioneer solutions use the fuzzy vault or a similar construction known as PSKA (Physiological Secure Key Agreement) [8] and OPFKA (Ordered-Physiological-Feature-based Key Agreement) [9]. These schemes enable key agreement between BAN nodes that are equipped with either ECG (electrocardiogram) or PPG (photoplethysmogram) sensors, as these physiological signals are used to conceal the symmetric key to be agreed upon. While these schemes provide a novel way of agreeing upon a key accompanied with a high-security level, they do not account for the possibility of the physiological signals being captured remotely off the body, without knowledge or consent of the patient. This remote capture of physiological signals may allow an adversary to successfully impersonate a genuine body sensor and enable them to carry out further attacks within the BAN, such as data manipulation in which they send fake readings that can mislead medical professionals and have serious consequences for the patient. In [10], the authors investigated the potential of using prediction filters, such as a Kalman filter, to unlock PSKA based fuzzy vaults using leaked physiological signals such as PPG. As stated in [11], the remote capture of PPG signals using UWB (Ultra-Wide Band) radars is possible, thanks to advancements in remote sensing technology. This presents a serious security risk for devices aiming to achieve authentication and key agreement using PSKA or similar schemes as the key could be unlocked by an adversary and neither the user nor the network administrator would be aware of the intrusion. In [12], a concern is raised regarding the security of PSKA vaults with the advent of remote sensor technology and its potential to capture the necessary information to unlock a vault. This fear is reinforced with the use of electric potential probes that enable remote capturing of ECG and PPG [13], [14].

Due to this development in adversary capabilities, it is necessary to explore new ways of protecting the fuzzy vault construction and the schemes that rely upon it while minimising the incurred overhead. We, therefore, propose an original scheme named RAFV (Rotation Assisted Fuzzy Vault) that builds upon the fuzzy vault scheme by leveraging channel side characteristics known as RSSI (Received Signal Strength Indicator) to obfuscate the locked vault. If an adversary is capable of collecting physiological signals originating from the target BAN sensors then they would be able to carry out impersonation attacks if the current iterations of PSKA, OPFKA and schemes similar in nature are used. This is because adversaries can utilize a remotely captured signal to unlock the vault and obtain the key concealed within it, compromising all future communication between the nodes targeted. However, RAFV will ensure that knowledge of the physiological signal alone does not provide access to the secret concealed within the vault. This is because any attempt to acquire the secret requires knowledge of how the vault has been obfuscated, which is not impacted by the leakage of locking elements to an adversary.

IV. Our Proposal

In this section, we will present the main idea of our original scheme named RAFV, describe its locking and unlocking process and discuss its robustness against brute force attacks that may target the constructed vault.

A. RAFV: an overview

The objective of RAFV is to secure any authentication scheme that uses the fuzzy vault construction mechanism, wherein the elements used for locking and unlocking the vault are susceptible to leakage within a wireless network. RAFV can be seen as an extension to the fuzzy vault scheme and is situated within the post-locking and pre-unlocking phase of this scheme (See shaded areas in Fig. 1). RAFV shall transmit an obfuscated fuzzy vault from the sender to the receiver, any attempt by an adversary to unlock the intercepted vault would fail even if the adversary is aware of the full set of locking elements. This is because RAFV does not conceal the polynomial but rather 'corrupts' it preventing successful unlocks until the vault has been 'repaired'. The vault shall be obfuscated by dividing it into quadrants and rotating the points within each quadrant around its centre.

RAFV relies on the ability to agree upon a sequence of bits in an out-of-band manner to ensure that an adversary cannot obtain this sequence. This sequence can be seen as a symmetric key that is used to lock and unlock the vault itself. To achieve this, RAFV makes use of RSSI (received signal strength indicator) which is a measurement of the power contained in the received signal. This measurement is only computed locally on the device and cannot be obtained by an adversary, which makes it ideal for attempting to harden the security of the fuzzy vault scheme. RSSI reconciliation is a process that enables the two BAN nodes to agree upon the key that shall be used to secure the vault. RSSI values between two wireless devices are prone to discrepancies and need to be corrected, therefore we model the errors as communication errors and use error correction codes, such as Reed-Solomon (RS), to ensure that the sender and the receiver are in agreement (i.e., they measure the same value). This process has been used in many key generation and key agreement schemes, including the ones applied in BAN such as [15]–[17].

B. Locking and unlocking process in RAFV

RAFV locking phase consists of the following steps: 1) Measuring the RSSI value between the two BAN devices, 2) The sender generates RS coefficients and sends them to the receiver, 3) The receiver uses the received RS coefficients to correct its 'copy' of RSSI, if the receiver fails to correct the errors the process should be restarted from the first step, 4) The sender constructs the locked fuzzy vault, 5) Dividing the vault into several quadrants, 6) Assigning a rotation direction and order for each quadrant, 7) Executing the rotation. These steps are summarized in Fig. 2.

As for the unlocking phase, upon reception of the fuzzy vault from the sender BAN device the following actions are taken: 1) Generating the original direction and order of rotation for each quadrant using the agreed RSSI values, 2) Reversing the order and direction of rotation for each quadrant, 3) Executing the rotation, 4) And finally proceed with unlocking the fuzzy vault. These steps are depicted in Fig. 2.

C. Vault division and quadrants rotation in RAFV

In the context of RAFV, a quadrant is used to split the vault into evenly spaced partitions. If a quadrant is selected all the points contained within its boundaries shall be rotated either clockwise or counterclockwise around the center point of the quadrant. More quadrants can be created by dividing all of the quadrants in the current deepest layer into four smaller ones. In doing so each newly created quadrant (child) shall cover $\frac{1}{4}$ of the area of its parent. Quadrants can be represented using the quadtree data structure where the deeper layers contain more quadrants, however each quadrant represents a smaller area of the vault.

Once the vault has been divided into the desired number of quadrants the angle and order of rotation can be assigned. In RAFV, the angle of rotation is either 90° or -90°. This is because other angles, such as 45°, 135° or 215° will cause quadrants to overlap with one another making the reconstruction of the original locked fuzzy vault, by the receiver, impossible. The angle of rotation is obtained from the RSSI values that have been agreed upon before vault construction. The RSSI values are assigned to the deepest layer of quadrants within the vault. Starting from the bottom left and moving across and up, each quadrant will be assigned an RSSI value in the order they occur in the list. If there are more quadrants than RSSI values then the list will loop back to the start. As for quadrants in layers above, their values are determined by summing their children's RSSI values. Once each quadrant has been assigned a value it can then be converted into an angle by looking at the parity (odd or even) of the value. If the assigned value is odd then the

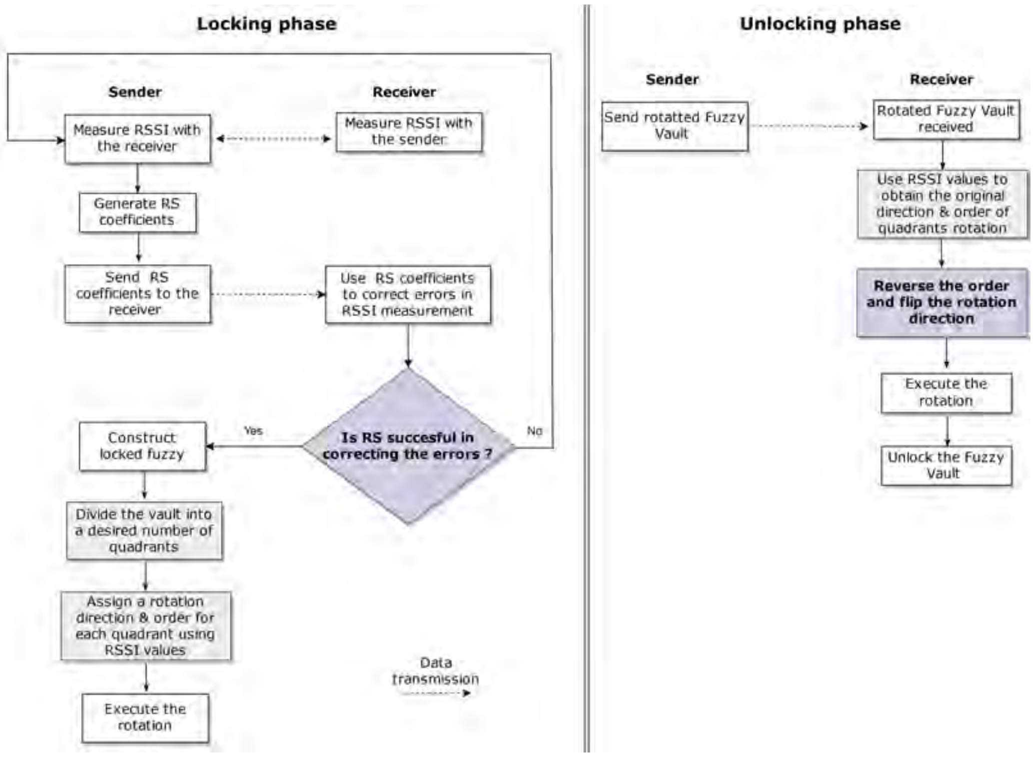

Locking phase
Sender
Receiver
Measure RSSI with the receiver
Measure RSSI with the sender
Generate RS coefficients
Send RS coefficients to the receiver
Use RS coefficients to correct errors in RSSI measurement
Is RS succesful in correcting the errors ?
Yes
No
Construct locked fuzzy
Divide the vault into a desired number of quadrants
Assign a rotation direction & order for each quadrant using RSSI values
Execute the rotation
Data transmission
Unlocking phase
Sender
Receiver
Send rotatted Fuzzy Vault
Rotated Fuzzy Vault received
Use RSSI values to obtain the original direction & order of quadrants rotation
Reverse the order and flip the rotation direction
Execute the rotation
Unlock the Fuzzy Vault

Figure 2: The fuzzy vault locking and unlocking process in RAFV

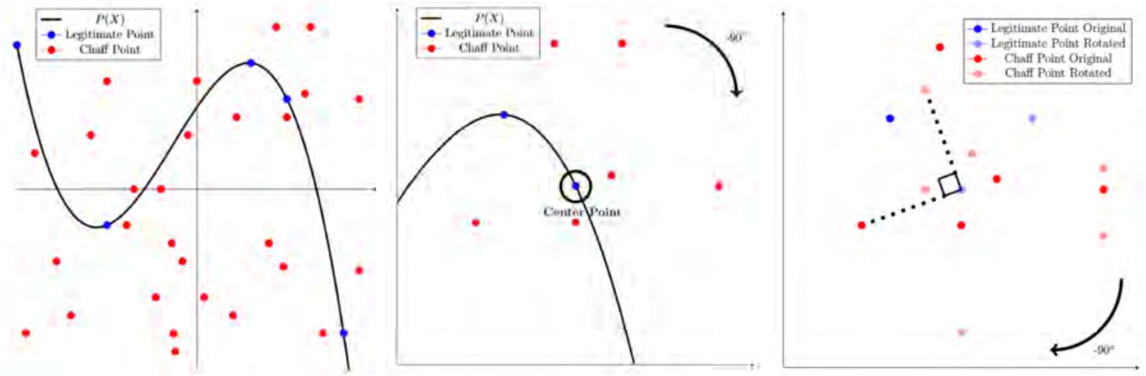
quadrant shall be rotated -90° and if the value is even then the angle of rotation is 90°.

Regarding the order of rotation, this also is obtained via the same RSSI values as the angle of rotation. However, the difference consists in using the collection of RSSI values to seed a random number generator which will randomly choose which quadrant shall be rotated next. The order of rotation has a significant impact on the obscured vault as each rotation carried out will fundamentally change the result. An illustration of the rotation applied to the content of a vault is shown in Fig. 3. The first sub-figure (Fig. 3(a)) shows a fully constructed fuzzy vault divided into 5 quadrants where there is a set of legitimate points (highlighted in blue) on a polynomial and chaff points (highlighted in red) that are used to conceal the secret. The second sub-figure (Fig. 3(b)) depicts a close up of the top-right quadrant of the vault where its center point has been marked and a rotation direction has been assigned to it. The final sub-figure (Fig. 3(c)) shows the same quadrant after -90° rotation has been applied, where the rotated legitimate and Chaff points are highlighted using the same colour as their corresponding original points but with increased transparency.

To be able to recover the locked fuzzy vault the receiver should know the number of layers present within the vault in addition to how many rotations have been carried out. This information must be communicated to the receiver, alongside the obfuscated locked vault, and be sent as plain text in a message appended to the fuzzy vault. This is because such information does not give the adversaries any advantage in their attempts to recover the vault. Once this information is obtained, the receiver can divide the vault the same way the sender did in addition to assigning the RSSI values and rotation order to each quadrant. The only difference, however, is that the receiver must swap 90° rotation with -90° and vice versa in addition to reversing the order of rotation.

D. Security analysis of RAFV

Two parameters can be used to calculate the size of the search space an adversary may face when



(a) Fully constructed fuzzy vault with 5 quadrants

(b) Overview of the top right quadrant of the vault before rotation

(c) Overview of the top right quadrant of the vault after rotation

Figure 3: Illustration of the rotation process in RAFV for both legitimate and Chaff points

attempting to directly brute force the rotation of the vault. These two parameters are the number of quadrants assigned a unique RSSI bit and the number of rotations carried out during the locking phase. The search space can be calculated using the following equation:

$$Search_{space} = 2^n \times r^n \tag{1}$$

where n is the number of quadrants and r is the number of rotations. For example, a RAFV based vault that is locked using 85 quadrants and 32 rotations would yield $2^{85} \times 32^{85} = 3.15 \times 10^{153}$. However, whilst the search space is exponentially large it is ultimately limited by the size of the key agreed upon by the sender and receiver within the RSSI reconciliation because this key determines the rotation. Therefore, an appropriate sized key must be picked to ensure strong bit-security for the scheme to function. For example, a 128-bit key that has been agreed upon by the two BAN nodes will ensure sufficient protection against brute force attack as an adversary would, on average, have to search half of the key space, **e.g** 2^{127}, and use each key to generate its rotation pattern and attempt the unlocking process in full. As mentioned earlier in Section IV-A, RAFV will allocate the direction of rotation to the quadrants in the deepest layer and quadrants in the layers above will derive their direction from the sum of their children. For the 128-bit key to have a maximum effect there must be at least 128 quadrants in the deepest layer to ensure that this key is represented throughout the rotation pattern. It is therefore required that a vault must be at least four layers deep to ensure a minimum of 128 quadrants in the last layer. The number of quadrants in each layer can be determined using the following equation.

$$Quadrants_{number} = 4^{m-1} \tag{2}$$

Where m refers to the layer order. The layers are ordered starting from 1 until the deepest layer of the vault. To compute the total number of quadrants present within the entire vault we use the following the equation.

$$Quadrants_{total} = 4^{m-1} + 4^{m-2} + ... + 4 + 1 \tag{3}$$

Therefore, the fifth layer of a divided vault (i.e, the result of applying the division 4 times starting from the main layer) would contain 256 quadrants and the total number of quadrants in the entire vault would be 341. It is important to note that if an adversary had half of the rotation pattern used by the vault they would not be able to infer the other half. For example, if an adversary had managed to acquire the order of rotation used within a given iteration of the scheme they would not be able to determine what direction has been assigned to each quadrant within the vault.

Furthermore, two types of adversaries may attempt to compromise the security of the RAFV based key agreement. Adversary A is an adversary that is unaware of any of the locking elements used by the underlying fuzzy vault. This means that for every iteration of the rotated vault they would have to attempt to brute force the fuzzy vault unlocking process with no guarantee that they have the original vault. Adversary B, however, is aware of the elements used to lock the vault due to their ability to remotely capture the physiological signals being leaked by the wearer. Therefore, they will be able to process each vault much quicker because they will only be concerned with the points that overlap with the features they have illegitimately acquired, allowing them to discard chaff points. However, this does not give the adversary B any advantage to unlocking the vault as the knowledge of the locking elements does not provide any insight into how the vault has been rotated.

V. Performance Evaluation

To evaluate the performance of RAFV we will compare it against the fuzzy vault scheme with regards to the required execution time. Such a comparison will enable an accurate assessment of the additional overhead induced by RAFV. Both schemes have been implemented in C++17 running on an Intel 8809G (3.10 GHz / 4.20 GHz) processor with a RAM of 2400 Mhz C16. Whilst the performance of such a processor far exceeds the performance of wireless sensor devices used in the intended application area (i.e, Body Area Networks) this evaluation aims to provide a like-for-like comparison between the two schemes. Future work could, however, look at implementing both schemes on more appropriate hardware devices.

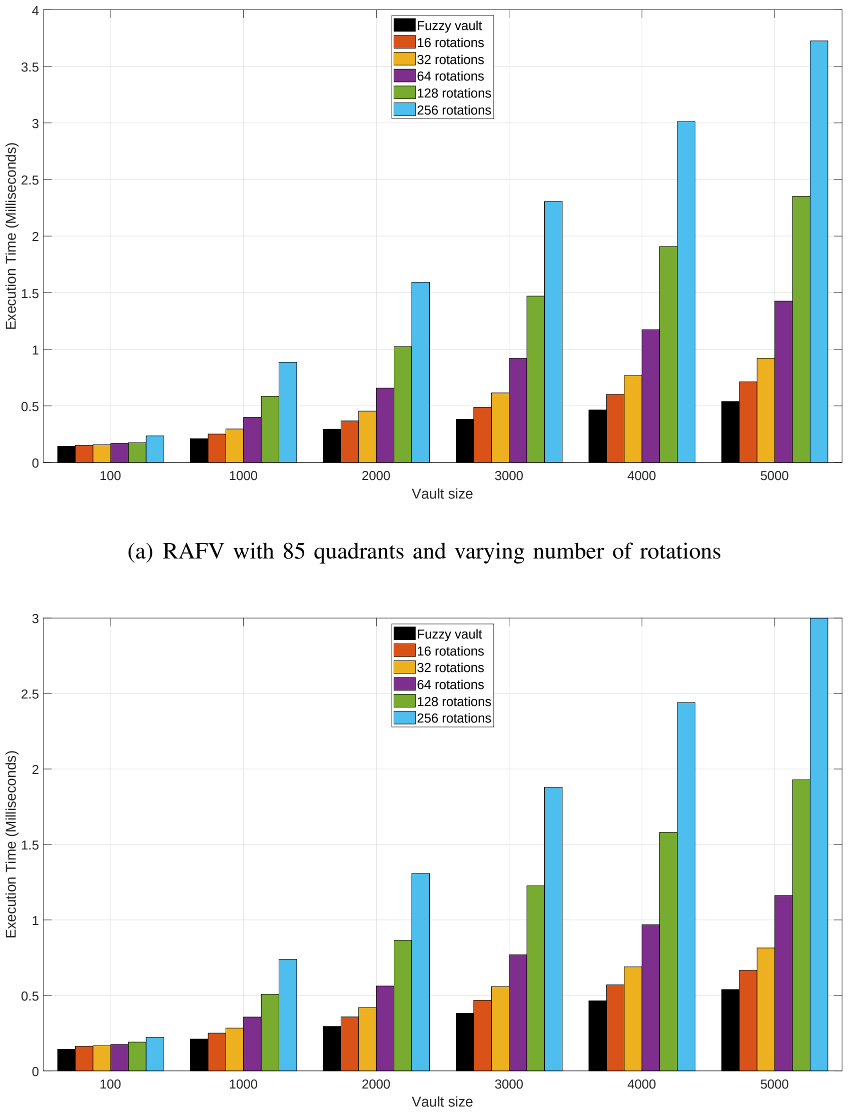
The evaluation scenario consists of running both schemes sequentially 100000 times to measure their performance for equally sized vaults. In addition to varying the vault size, from 100 to 5000, to assess its impact on the achieved execution time for both schemes, the quadrant layers (and consequently the total number of quadrants) and the number of applied rotations, relevant for RAFV only, are also varied to assess how they affect the execution time and the resulting search space. More specifically, we evaluated 3 and 4 quadrant layers with 5 different number of rotations: 16, 32, 64, 128 and 256.

Fig. 4(a) shows the time taken to construct a RAFV over many parameters: various sizes, number of rotations in addition to the time taken to construct an identically sized fuzzy vault. This figure demonstrates that the execution time for either the fuzzy vault or RAFV scheme increases in line with the vault size. With regards to RAFV, its execution time increases further as more rotations are carried out, this is expected as more quadrants are being selected for rotation and, therefore, more points are being rotated. The biggest impact on the performance for RAFV is the number of rotations carried out, for example, a 5000 point vault rotated 16 times is 5.2 times quicker when compared with a vault rotated 256 times.

Fig. 4(b) shows the construction time for RAFV with 341 quadrants present within the vault. This graph shows that a vault rotated 256 times produces similar results to a vault with 1000 fewer points but divided into 85 quadrants (see Fig. 4(a), the case of a vault size equals to 4000). This is because the vault used for producing the results shown in Fig. 4(b) has been divided once more, compared to the vault used in Fig. 4(a), introducing an additional layer of smaller yet more abundant quadrants. These smaller quadrants are more likely to be selected for rotation as there is more of them, however, they each represent a smaller area of the vault, so if they are chosen fewer points will be rotated, which contributes to these performance uplift.

RAFV sees an increase in run time due to the extra operations it carries out on top of the underlying fuzzy vault scheme. However, this increase in execution time provides a fuzzy vault that is resilient against brute force attacks due to the rapid increase in complexity, as shown in Fig. 5 which is a plot of the Equation 1. Fig. 5 plots the function shown in this equation with various values of r (i.e., the number rotations performed). This figure highlights that a small increase in the number of quadrant rotations leads to an exponential increase in the search space. This is designed to make brute force attack infeasible due to the required time to exhaust the search space.

However, this figure shows also the search space posed by the 128-bit key which is used to derive the rotation lock pattern. Whilst the search space



(a) RAFV with 85 quadrants and varying number of rotations

(b) RAFV with 341 quadrants and varying number of rotations

Figure 4: Time taken to construct a fuzzy vault and RAFV over various sized vaults

generated using the key is many magnitudes smaller than even the smallest search space generated by the lowest number of rotations evaluated (i.e., 16), it is important to realize that RAFV is limited by this key. Although it may seem that there is no purpose for rotating beyond the limit imposed by the chosen key size, there may be advantages to picking a large number of quadrants and quadrant rotations to prevent or hinder any attempt of unlocking the vault using smart analysis techniques or efficient search algorithms. Currently, there is no known efficient search algorithm, to the best of our knowledge, that the adversary may use to rotate the vault back to its original form, therefore the security of RAFV is defined by the size of the key used.

Table I shows the obtained execution time from the performed experiments for the fuzzy vault and RAFV schemes in terms of the measured minimum, maximum, average, standard deviation and delta (the difference between average execution times for

Table I: Impact of the vault size on the achieved execution time: fuzzy vault scheme vs. RAFV (341 quadrants and 128 rotations)

	100 Points		**1000 Points**		**2000 Points**		**5000 Points**	
Execution Time (ms)	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**
Minimum	0.132	0.178	0.208	0.487	0.288	0.837	0.531	1.890
Max	0.760	0.791	1.043	1.367	1.594	1.267	2.424	4.725
Average	0.144	0.191	0.213	0.508	0.295	0.864	0.540	1.928
Standard Deviation	0.005	0.006	0.007	0.014	0.007	0.012	0.013	0.026
Delta	0.046		0.295		0.570		1.388	

both schemes) values under varying vault sizes. For RAFV, the vault has been divided into 341 quadrants with 128 rotations being applied. These results reveal that as the vault size increases the average execution time increases with the delta between the two schemes increases rapidly as well. However, even with RAFV being applied to 5000 point vault it is only 1.388 ms slower than the fuzzy vault, which would not have any meaningful impact on the performance of the authentication scheme nor would the user be able to perceive such a small increase.

VI. Conclusion

Due to the exceptional increase in adversaries' capabilities, the fuzzy vault construction scheme and all BAN authentication protocols that reply on it become vulnerable to a wide range of security threats. To counter such threats, we proposed "RAFV: Rotational Assisted Fuzzy Vaults" to further enhance the security of any fuzzy vault based authentication scheme with minimum additional communication and computational overhead. RAFV extends the fuzzy vault scheme by leveraging channel side characteristics namely RSSI (Received Signal Strength Indicator) to obfuscate the locked vault by dividing it into many quadrants and rotating them following a given pattern. This obfuscation aims at preventing adversaries from using remotely captured BAN signals to unlock the vault and obtain the key concealed within it. RAFV has been evaluated against the fuzzy vault scheme and the obtained results have proven its effectiveness in enhancing the security level of the fuzzy vault scheme with a slight increase in the required computational overhead. Future work will look at what reduction can be achieved concerning the communication overhead as RAFV allows fewer chaff points to be present without sacrificing the achieved security level.

Acknowledgement

The authors are very grateful to Prof. Rene Doursat for the advice provided, for the fruitful discussions during the meetings held as part of this work and for reviewing an early draft of this paper.

References

[1] S. Movassaghi et ali. Wireless body area networks: A survey. *IEEE Communications Surveys Tutorials*, 16(3):1658–1686, 2014.

[2] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1):51–58, February 2010.

[3] S. Pirbhulal et al. Medical information security for wearable body sensor networks in smart healthcare. *IEEE Consumer Electronics Magazine*, 8(5):37–41, 2019.

[4] G. Paul and J. Irvine. Ieds on the road to fingerprint authentication: Biometrics have vulnerabilities that pins and passwords don't. *IEEE Consumer Electronics Magazine*, 5(2):79–86, 2016.

[5] S. Challa et al. Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions. *IEEE Consumer Electronics Magazine*, 7(1):57–65, 2018.

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

[7] U. Uludag et al. Fuzzy vault for fingerprints. In *Lecture Notes in Computer Science*, pages 310–319. Springer Berlin Heidelberg, 2005.

[8] K. K. Venkatasubramanian et al. PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 14(1):60–68, Jan 2010.

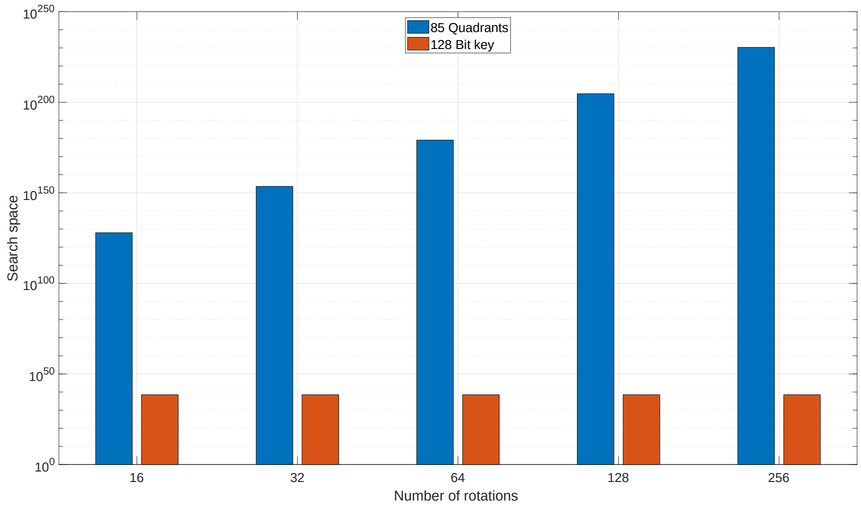


Figure 5: Evolution of search space size faced by an adversary when attempting to brute force the rotations of RAFV directly vs. the search space size generated by the 128 bit key

[9] C. Hu et al. OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In *2013 Proceedings IEEE INFOCOM*, pages 2274–2282, April 2013.

[10] Juyoung Kim, Kwantae Cho, and Sang Uk Shin. A study on the security vulnerabilities of fuzzy vault based on photoplethysmogram. In James J. Park, Vincenzo Loia, Kim-Kwang Raymond Choo, and Gangman Yi, editors, *Advanced Multimedia and Ubiquitous Engineering*, pages 359–365, Singapore, 2019. Springer Singapore.

[11] Y. Lee et al. A novel non-contact heart rate monitor using impulse-radio ultra-wideband (IR-UWB) radar technology. *Scientific Reports*, 8(1), aug 2018.

[12] H. Zhao et al. Physiological-signal-based key negotiation protocols for body sensor networks: A survey. *Simulation Modelling Practice and Theory*, 65:32 – 44, 2016. Analyzing and Visual Programming Internet of Things.

[13] C J Harland, T D Clark, and R J Prance. Electric potential probes - new directions in the remote sensing of the human body. *Measurement Science and Technology*, 13(2):163–169, dec 2001.

[14] A E Mahdi and L Faggion. Non-contact biopotential sensor for remote human detection. *Journal of Physics: Conference Series*, 307:012056, aug 2011.

[15] Zhouzhou Li and H. Wang. A key agreement method for wireless body area networks. In *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 690–695, April 2016.

[16] Z. Li et al. Secure and efficient key generation and agreement methods for wireless body area networks. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2017.

[17] S.T. Ali et al. Zero reconciliation secret key generation for body-worn health monitoring devices. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WISEC ’12, pages 39–50, New York, NY, USA, 2012. ACM.

Jack Hodgkiss received a Bachelor in Computer Science Degree from Manchester Metropolitan University in 2018. He now works towards a PhD focusing on authentication within body area networks. Contact him at jack.hodgkiss@stu.mmu.ac.uk.

Soufiene Djahel (M’11–SM’16) is a Senior Lecturer at the department of Computing and Mathematics, Manchester Metropolitan University, U.K.. His main research interests include Security and QoS issues in wireless networks, Intelligent Transportation Systems, and e-health. He has published more than 50 papers in top tier peer reviewed conferences and journals. Contact him at s.djahel@mmu.ac.uk.

MARS - Towards Mobile Assisted RSSI Secret Key Extraction Strategy in WBANs

Jack Hodgkiss and Soufiene Djahel
Department of Computing and Mathematics, Manchester Metropolitan University, UK
{jack.hodgkiss@stu.mmu.ac.uk, s.djahel@mmu.ac.uk}

***Abstract*—The emergence of wireless body area networks (WBANs) has paved the way for real-time sensing of human biometrics in addition to remote control of smart medical devices, which in turn is revolutionising the smart healthcare industry. However, the limited power and computational capabilities of WBAN sensors make them vulnerable to a myriad of security attacks, thus securing them is paramount to their success and wider adoption. Received signal strength indicator (RSSI) secure key extraction (SKE) methods are used for securing WBAN sensors. However, such methods may suffer from stagnant RSSI values, significantly increasing the secret keys construction time. To remedy this, we propose a new method that involves one of the two sensors being mobile and thus can be picked up and moved around. This results in the stimulation of RSSI values which in turn improves the quality of the generated keys and thus shortening the execution times of the SKE process. The evaluation results highlighted the effectiveness of our method.**

***Index Terms*—WBANs, RSSI, Secret Key Extraction**

I. Introduction

In recent years there has been significant progress in developing tiny wireless sensors capable of sensing events and enacting change within their deployment environment. The medical domain is among the most popular environments where such sensor technology is deployed (e.g., worn or implanted within the patient body) and used by medical professionals in hospitals to monitor the patients' health and control specialised medical instruments. Example of such sensors used in hospitals can range from ECG (Electrocardiogram), CGM (Continuous Glucose Monitor) or a pacemaker. Some of these sensors may also be purchased and used by home users who desire to monitor their current wellness and fitness.

These sensors are only capable of wireless communication and must form a WBAN (Wireless Body Area Network) which is a specialised network type for deployment on or within the human body. As these sensors engage in wireless communication this does open up the potential for intrusions by unauthorised adversaries who can eavesdrop on the information being transmitted throughout the network. This can put at risk not only the wearer's privacy, which must be maintained at all times as it is a requirement by law [1], but also their health as sensors, such as a pacemaker, could be tampered with in order to turn them off or operate outside safe limits. Unfortunately, any attempt to secure these sensors must overcome the stringent constraints that accompany sensors of such a miniature size. This is because to conform with the operating regulations and specifications these sensors must have a small form factor limiting the overall size of the components used such as the microprocessor and battery. This poses a significant challenge to researchers as conventional methods of authentication are not appropriate due to their demanding requirements.

Therefore, a significant work has been undertaken to secure such networks while satisfying the requirements of WBAN sensors. This has been achieved through novel and inventive ways to take advantage of what is available to sensors. For example, WBANs have unique access to vital signs, such as ECG, and therefore they can use them for the purpose of key generation and authentication [2], [3]. However, these methods fragment the network as only sensors capable of sensing the ECG signal can benefit from this feature and be involved in the authentication process. In addition, recent works, such as [4], have highlighted potential exploits and vulnerabilities that target PPG (Photoplethysmogram) based authentication schemes. Therefore, alternative methods should be used, such as RSSI (Received Signal Strength Indicator) Secret Key Extraction (SKE), due to the fact that all wireless sensors are capable of measuring such a metric. Despite of its advantage over the use of ECG, RSSI SKE based schemes have a serious weakness related to the key construction time which can be of the order of several minutes, making it not viable for use within emergency settings as every second counts. This paper will therefore introduce a novel strategy to complement RSSI SKE based authentication schemes by increasing the rate at which the keys are generated, thus reducing the wait time before these sensors can operate securely. This strategy is known as MARS (Movement Assisted RSSI SKE Strategy) and will be the focus of the rest of this paper.

II. Mobile Assisted RSSI SKE Strategy

RSSI SKE consists in four separate stages summarized as follows [5]. (1) *Transmitting Probes*: the two sensors involved transmit and receive probes or messages which can be used to measure RSSI from the point-of-view of one another. (2) *Quantization*: it could be lossy or lossless, in this stage both sensors reduce the measured values into a binary sequence. (3) *Reconciliation*: attempts are made to correct the discrepancies that exist due to the irregularities in measurements originating from wireless channel and temporal variations. (4) *Privacy Amplification*: steps are taken to ensure that quantization and reconciliation may not enable an eavesdropper to identify the agreed upon key due to low entropy or a leakage.

As discussed earlier, RSSI SKE can in certain scenarios suffer from prolonged construction times due to inadequate variation in the RSSI values, which impacts the entropy when quantized [5]. This can be experienced in situations where the sensors involved in the secret key extraction process remain stationary, which leads to low variation of RSSI values. This can have a serious negative impact on the satisfaction and security levels provided to end users, including significantly prolonged construction times, which refers to the time taken to generate and agree upon the key. To alleviate this issue, in the past, several contributions have been proposed, focusing on areas such as increasing the secret key strength and reducing the construction time. Strength and construction time can be at odds with one another as improvements to one come at the cost of another. However, recent works have proposed various modifications and improvements to individual stages of RSSI SKE that do not require this trade off. For example, [6] has improved the reconciliation stage by utilising Reed-Solomon error correction codes. The authors of [7] have used a virtual group to synthesis RSSI between more than two sensors, enabling the extraction of a greater number of bits due to the additional sources provided by the virtual group. In [8], the authors presented a multilevel quantization function in which the levels are determined based on the Nakagami-m channel model which allows for the optimal level selection.

Our proposal differs from the above works as it does not propose any changes to the stages, such as the application of Reed-Solomon error correction codes [6]. Whilst Smartphones may be equipped with multiple sensors there currently does not exist any functionality to hop between antennas as required by [9]. Rather, it is a strategy that can be used to speed up the process of generating and agreeing on a symmetric key between wireless sensors that are constrained by both the available hardware and software functionalities.

MARS aims to increase the amount of entropy present within the quantized bits to achieve shorter construction times. This can especially be beneficial in emergency situations (e.g., road accidents and emergency department cases) where the time spent without functional body sensors should be significantly minimised. MARS can achieve this aim by stimulating the RSSI values which in turn will increase the entropy of the quantized bits. This is made possible because MARS requires that one of the sensors used is mobile, referring to the sensors ability to be picked up and moved such as a mobile phone. Due to such a requirement it is therefore possible to exploit the influence that movement can have on RSSI and generate stimulated values which when quantized shall have high levels of entropy. MARS focuses on the transmitting probes, quantized stage of an RSSI SKE as any improvement witnessed here will propagate down into the other stages of the SKE process. MARS will prompt the user, such as a nurse or a doctor, to perform a gesture during the transmitting probes stages as this is when RSSI is being measured. The gesture to be recommended for the user to perform will be the one that improves upon the entropy of the quantized bits while remaining easy for the typical level motion a person is capable of. The gesture recommended could range from one of the following; (i) Figure Eight, (ii) Shaking (Light), (iii) Shaking (Heavy), (iv) Tilting, (v) Holding (Typical Use), and (vi) Moving Towards & Away. Each of these gestures has been evaluated within Section III.

III. Performance Evaluation

To determine if MARS improves upon the status quo we have designed experiments that will highlight any improvements within the quantization phase. We will also explore the acceleration forces exerted on the mobile device by the user. By investigating the impact of MARS on RSSI measurements and the quantization of such data we can accurately determine the improvements to the entire process. Moreover, analysing motion sensor data will provide the necessary information to understand the trade off involved with the different gestures.

A. Evaluation Metrics

To evaluate the effectiveness of MARS we have opted to use the intermediate data from the quantization phase of the RSSI SKE. The data collected from this phase of the scheme provides insight into how non-stationary gestures perform against the stationary gesture in addition to their performance relative to one another. Insight from the quantization phase is provided by the number of bits quantized which will help determine which gestures reject the least number of RSSI readings, fewer rejections the better. The entropy of quantized bits is also extracted from the quantization phase of the RSSI readings, as it highlights the randomness of the sequence of bits. High entropy leads to an increase in the number of secret bits, therefore reducing the wait time. Besides the quantized output our evaluation will also attempt to understand the *cost* a gesture incurs as some gestures evaluated can be described as difficult to perform compared to others due to the required fast and wider motion to perform the gesture correctly. Therefore, by utilising the motion sensors built into the Smartphone we can evaluate each gesture's *cost* by calculating the magnitude of the motion data. By doing so we can determine which gesture has an appropriate trade-off with regards to performance and cost.

B. Evaluation Setup

In order to conduct the evaluation outlined above we need to setup an easily repeatable experiment on physical hardware as this is the easiest way to capture both RSSI and motion sensor readings. To achieve this, we used the Texas Instruments (TI) Launchpad CC26x2r1 as this is a development kit that includes support for various communication standards including Bluetooth Low Energy (BLE). This device was configured to broadcast a packet every 20 ms via BLE so that RSSI values could be measured. This device acted as a stationary device that would be worn by a user. As for the mobile device, a Google Pixel 3a Android Smartphone was used and was running a bespoke application, developed by us, capable of measuring RSSI from the packets the TI Launchpad was transmitting in addition to collecting motion sensor data from the onboard accelerometer.

This setup enabled the collection of RSSI data and motion sensor data that have been used within the evaluation of MARS. For this experiment we have explored the following gestures; figure-eight, shaking (light), shaking (heavy), tilting, holding (typical usage) and moving towards & away. Each gesture was repeated 10 times to ensure that our results are reproducible. Every attempt has been made to ensure each gesture is performed in similar manner between repetitions.

C. Evaluation Results Analysis

Figure 1 shows the RSSI values captured from a typical experiment performed with four gestures; *Stationary*, *Shaking (Heavy)*, *Figure Eight* and *Moving Towards & Away*. The figure demonstrates that *Stationary* has minimal variation between measurements, whereas other gestures such as *Shaking (Heavy)* have significant variation throughout. Not only do all non-stationary gestures have an important increase in the variance of the measured RSSI values they also exhibit an increase in range allowing for more unique values to occur as opposed to the same few values being repeated. This can have significant impact on the amount of data extracted during the quantization stage.

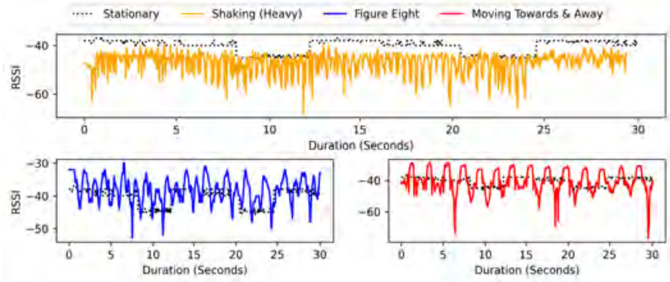


Fig. 1: RSSI data captured from stationary and non-stationary gestures over a single 30 second experiment

Table I summarises what is evident across all gestures and repetitions of experiments with almost all gestures producing significant increases in metrics such as range, standard deviation and variance. This table includes also the average number of quantized bits from RSSI measurements captured during experiments, which can determine actual performance gains within the early stages of an RSSI reconciliation scheme following our strategy. *Moving Towards & Away* when compared to *Stationary* exhibits significant improvements with an increase of almost 200 quantized bits. *Figure Eight* also manages to increase the number of quantized bits generated however it did not perform similar to *Moving Towards & Away*. This could be due to the drop in metrics such as range, standard deviation and variance. This is also experienced with other gestures such as *Shaking (Light)* and *Tilting* which both make minor increases to average quantized bits when compared to a *Stationary* gesture.

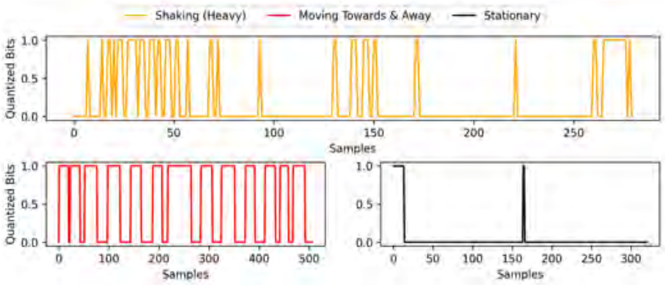


Fig. 2: Quantized bits extracted from collected RSSI data across multiple gestures

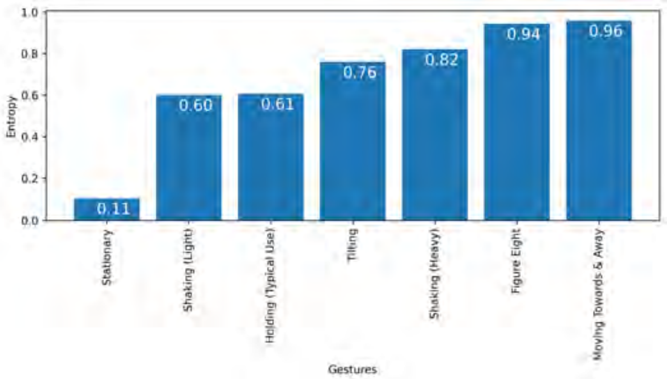


Fig. 3: Entropy of the quantized bits collected from the RSSI readings

Finally, *Holding (Typical Use)* and *Shaking (Heavy)* have demonstrably worse performance when compared to the *Stationary* gesture on the basis that they produce fewer quantized bits. However, in subsequent steps they may perform better than the *Stationary* gesture as the entropy of their quantization is higher and, therefore, they would experience fewer rejections requiring a smaller amount of quantized bits to proceed to the next phase. This is shown in Figure 2 where *Stationary* gesture contains large continuous blocks of the same bit value, whereas *Shaking (Heavy)* contains fewer bits which are not in large continuous blocks and therefore less likely to be rejected later within a scheme. This is also supported by the entropy calculated from the quantized bits presented in Figure 3. The entropy can be used to measure the predictability of the sequence of bits that has been quantized, the lower the value the easier it is to predict the sequence of quantized bits, whereas higher values imply it is harder to predict and therefore more resilient to security attacks.

$$|v| = \sqrt{v_x^2 + v_y^2 + v_z^2} \tag{1}$$

We must also analyse the associated *cost* of performing one of these gestures as we cannot simply recommend the gesture that yields the greatest uplift in quantization without considering its impact on users in terms of physical exertion. Using the linear acceleration sensor on board the Android Smartphone we can measure the acceleration experienced by the device without the impact of gravity. In addition, we will calculate the magnitude using Equation 1 to find out the total

	Min	Mean	Max	Range	Standard Deviation	Variance	Average Quantized Bits
Stationary	-46.00	-40.09	-36.67	9.33	2.89	8.38	312
Figure Eight	-52.67	-37.72	-30.33	22.33	3.63	13.19	423
Shaking (Light)	-68.67	-44.98	-39.33	29.33	4.26	19.31	321
Shaking (Heavy)	-74.33	-47.55	-39.67	34.67	4.61	21.47	290
Tilting	-65.67	-45.99	-40.67	25.00	3.55	13.29	316
Holding (Typical Use)	-53.00	-46.24	-42.33	10.67	1.95	4.20	295
Moving Towards & Away	-74.33	-40.68	-27.67	46.67	7.57	57.46	**509**

TABLE I: Statistics of RSSI values obtained during the MARS experiments

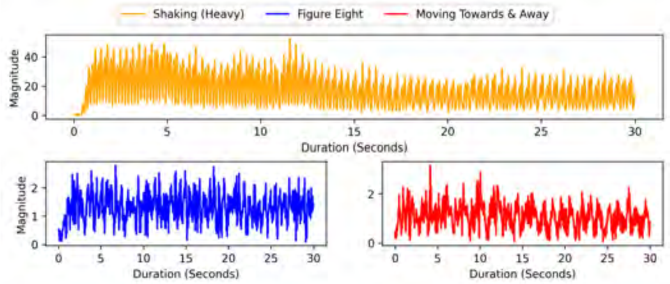


Fig. 4: Magnitude of linear acceleration during the experiments

	Min	Mean	Max	Standard Deviation	Variance
Stationary	0.00	0.02	0.10	0.01	0.00
Figure Eight	0.07	1.32	3.06	0.50	0.25
Shaking (Light)	0.31	4.49	15.43	2.39	5.75
Shaking (Heavy)	0.21	19.19	54.47	10.50	**110.47**
Tilting	0.06	1.93	7.92	1.30	1.70
Holding (Typical Use)	0.02	0.42	3.13	0.35	0.12
Moving Towards & Away	0.06	1.05	2.56	0.45	0.21

TABLE II: Statistics of motion sensor data obtained during the MARS experiments

acceleration exerted on the device across the three axes x, y, and z where v refers to the current sampling of the linear acceleration data. Figure 4 shows the magnitude of linear acceleration across all axes. This figure demonstrates that *Shaking (Heavy)* has a significant amount of energy exerted by the user which can make performing this gesture harder for individuals with restricted motion. Moreover, this gesture may cause repetitive strain injuries (RSI) if performed on a regular and prolonged basis as stated in [10]. Other gestures, such as *Figure Eight* and *Moving Towards & Away*, when compared to *Shaking (Heavy)* have a smaller magnitude, making them easier to perform by the user with a reduced risk to RSI.

Table II presents several key statistical metrics to enable understanding how demanding each gesture can be. In the case of *Shaking (Heavy)* and *Shaking (Light)* it is clear that they are both extreme outliers when compared to the other gestures evaluated. They are both demanding gestures to perform due to the constant back and forth motion whereas the other gestures have very limited and slow motion.

IV. Conclusion

We proposed a new strategy to shorten the secret key construction time in any RSSI secret key extraction (SKE) method. Our strategy requires that one of the two devices involved in the SKE process be mobile. It is thus the movement that dramatically improves the entropy of the quantization of measured RSSI values. This increase of entropy observed within the quantization stage of the SKE process will benefit subsequent stages and, therefore, allow for shorter wait times endured by the user when constructing the key. The performed experiments highlighted that all the evaluated gestures provide significant improvement to the entropy of the quantized bits compared to the stationary case. However, either moving towards & away or figure eight is an easy recommendation as they are both top performers in entropy and the number of quantized bits. Moreover, our experiments' results show that these gestures are some of the least demanding gestures performed by the user. In our future work, we will explore the RSSI SKE process in full enabling insight into the improvements experienced throughout as opposed to only the quantization phase.

References

[1] Data protection act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted, 2018.

[2] K. K. et al. Pska: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 14(1):60–68, 2010.

[3] E. K. Zaghouani et al. 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.

[4] Juyoung Kim et al. A study on the security vulnerabilities of fuzzy vault based on photoplethysmogram. In *Advanced Multimedia and Ubiquitous Engineering*, pages 359–365, Singapore, 2019. Springer Singapore.

[5] S. N. Premnath et al. Secret key extraction from wireless signal strength in real environments. *IEEE Transactions on Mobile Computing*, 12(5):917–930, 2013.

[6] M. Fernando et al. Reed solomon codes for the reconciliation of wireless phy layer based secret keys. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pages 1–6, 2017.

[7] Z. Li et al. Secure and efficient key generation and agreement methods for wireless body area networks. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6, 2017.

[8] M. Adil et al. On quantization for secret key generation from wireless channel samples. *IEEE Access*, 9:21653–21668, 2021.

[9] G. Revadigar et al. Mobility independent secret key generation for wearable health-care devices. *EAI Endorsed Transactions on Security and Safety*, 3, 01 2015.

[10] Patricia Tegtmeier. A scoping review on smart mobile devices and physical strain. *Work*, 59:273–283, 2018.