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.

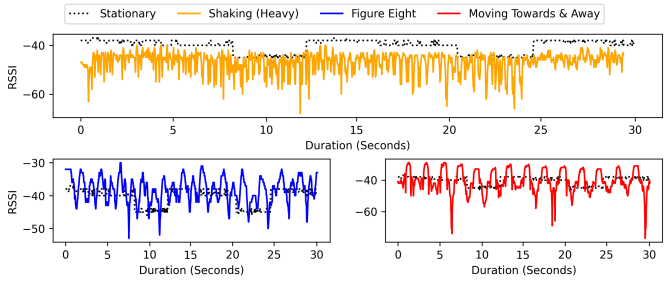

Fig. 1: RSSI data captured from stationary and non-stationary gestures over a single 30 second experiment

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.

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.

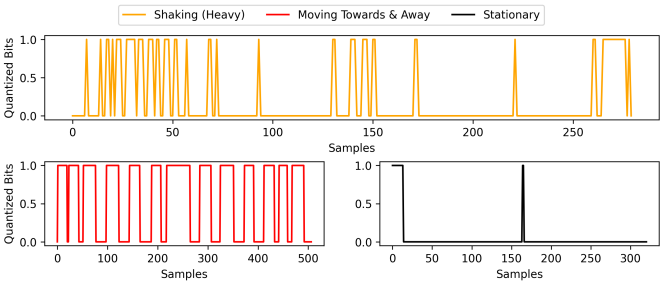

Fig. 2: Quantized bits extracted from collected RSSI data across multiple gestures

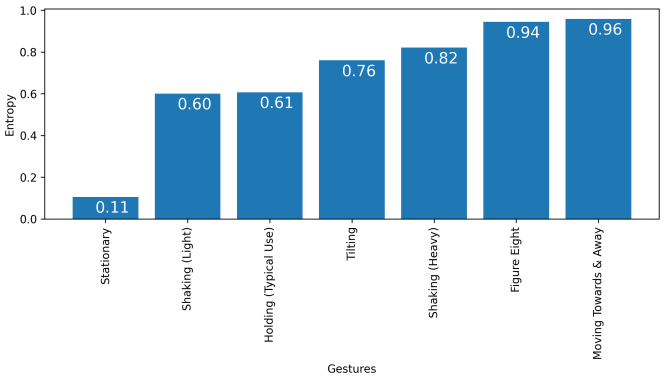

Fig. 3: Entropy of the quantized bits collected from the RSSI readings

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

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

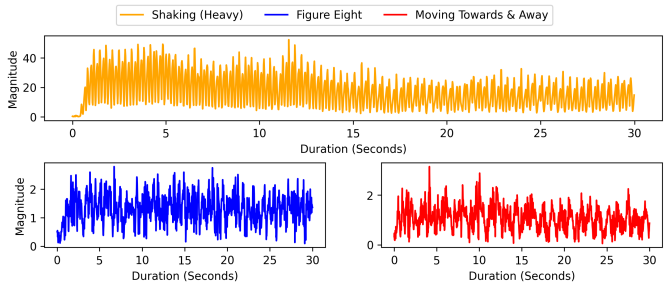

Fig. 4: Magnitude of linear acceleration during the experiments

	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.