RSS-Based Secret Key Generation in Wireless In-body Networks

Muhammad Faheem Awan[1], Kimmo Kansanen[1], Sofia Perez-Simbor[2], Concepcion Garcia-Pardo[2], Sergio Castelló-Palacios[2] and Narcis Cardona[2]
[1]Department of Electronics, NTNU, Trondheim, Norway
[2]iTEAM, Universitat Politècnica de València, Spain
{faheem.awan}@ntnu.no

***Abstract*—Secure communication is considered as an integral part of next generation wireless implantable medical devices. In this work, we provide the symmetric cryptographic key generating approach by exploiting the randomness in received signal strength (RSS) for data encryption in an in-body network. The application of concern is the wireless modules for next generation leadless cardiac pacemaker with two units. For RSS based key generation method, both the units probe the wireless channel for RSS measurements within the coherence time and outputs the encryption key bits based on available randomness and quantization algorithm. To evaluate the available randomness in RSS measurements, the methodology of phantom experiments is adapted to emulate the cardiac cycle. It has been found that the measurements emulating the cardiac cycle can be approximated to follow the log-Normal distribution. Moreover, a high correlation of RSS measurements is observed across the pacemaker units to generate a symmetric key whereas the eavesdropper link is found to be highly de-correlated. Based on the available randomness, the quantization algorithm generates 2- bits per cardiac cycle and requires 64 cardiac cycles to generate a 128-bit binary key string with an average mismatch percentage of 1 % over 1000 key runs.**

***Index Terms*—Implanted Medical Devices; Wireless leadless cardiac pacemaker; WBAN, Security and Privacy, Physical layer security, RSS based Quantization**

I. Introduction

The technological advancements in wireless body area networks results in number of implantable and wearable medical devices. Among these devices the most notable are cardiac pacemaker and implanted cardiac defibrillators.

Pacemakers are implanted inside the human heart for treatment of cardiac arrhythmia's. There are about 0.7 million pacemaker implantation's worldwide [1]. Current versions of pacemakers contain subcutaneous implant (can) under the skin beneath the shoulder that is connected via wires through sub-clavian vein to the electrodes in right atrium and right ventricle. The next generation of these pacemakers is expected to be wireless between electrodes and subcutaneous implant. Fig. 1 shows the implementation of leadless cardiac pacemaker (LCP) in the right ventricle communicating with subcutaneous implant wirelessly [1]. The only available leadless pacemakers in the market are Medtronics Micra [2] and Nanostim-LCP, which are autonomous leadless pacemakers in right ventricle without subcutaneous implant.

The wireless nature of these leadless pacemakers is significant source of security risks and makes it more visible, facilitating eavesdropper to overhear the communication. Due to the sensitive nature of these pacemakers, it's essential to protect the communication between these pacemaker modules.

In [3], Halperin et al exploits the wireless vulnerabilities to extract the patients data from pacemaker by using off the shelf programmer and antennas. A complete review of security and privacy concerns related to implanted medical devices is provided in [4].

Several approaches are available in the literature to secure the wireless body area network (WBAN) communications, that includes techniques from traditional cryptographic algorithms to wireless physical layer security methods (PLS). This work focuses on physical layer security methods.

PLS methods exploit wireless channel to secure communication between legitimate parties. In [5], Zhang et al provides a comprehensive review on key generation techniques from wireless channels. The concept of key generation from wireless channels was first introduced by Maurer in [6]. The commonly used parameters for key generation are Received signal strength (RSS), Angle of Arrival (AoA), Channel transfer function (CTF) and Channel Impulse Response (CIR). In [7], a novel key generating architecture is provided for low power constrained devices. Similarly, in [8] [9], an RSS based secret key generation method is utilized for on-body WBAN nodes. In context of wireless in-body area networks, most of the literature is focussed on generating the secret key by using common bio-metric feature like ECG, EEG and EMG [10]–[12].

In this work, we utilize an RSS based secret key generation approach in context of wireless in-body network. Our used case application is next generation of

[1]EU Horizon 2020 Project WiBEC

leadless cardiac pacemakers which contains one leadless pacemaker unit in the right ventricle and the other subcutaneously implanted (see Fig. 1). These units probe the wireless channel during the cardiac cycle to extract the RSS measurements from channel transfer function in Ultrawide (UWB) frequency band which are then approximated with log-normal distribution to extract the random bits. The quantizer generates 2- bits from a single cardiac cycle. Phantom experiments are adapted to emulate the single cardiac cycle. By phantom experiments, we approximate the heart movement by moving the antenna to different spatial positions. Similarly, the blood in- and out flow from a ventricle is mimicked with adding and removing the blood phantom respectively. As it is not possible to emulate the dynamic flow of blood, thus we can only approximate the two levels of blood in a cardiac cycle i.e. when the RV is completely-filled and empty. The approximation can be considered as a sensible choice because it provides the available extremes.

The rest of the paper is organized as follows. Section II provides system model and methodology followed by results in Section III. Section IV concludes the work along with our future directions.

II. System Model and Methodology

This section provides the system model and methodology used in our work. Fig. 1 shows the system model, where the leadless cardiac pacemaker (LCP) in right ventricle of human heart communicates with subcutaneous implant under the skin beneath the left shoulder. We name LCP as traditional Alice and subcutaneous implant as Bob, whereas Eve is outside the body in free space trying to eavesdrop the communication. The link between Alice-Bob and Alice-Eve is referred as AB- and AE-link respectively. Alice and Bob uses the UWB frequency band for wireless communication ranging between 3.1-5.1 GHz.

First, the heart dynamics during a single cardiac cycle is explained followed by the measurement setup to emulate the cardiac cycle.

A. Dynamics of Cardiac Cycle

A cardiac cycle is the number of events that take place during a single human heart beat. The beat starts with arterial contraction, that pumps the blood to the ventricles. In the next phase, the ventricles contract and pumps the blood. The right ventricle pumps the de-oxygenated blood to the lungs, whereas the left ventricle pumps the oxygenated blood to the body. After pumping the blood, the ventricles relaxes and again filled with the blood. During the entire cycle the right ventricle is first filled with blood and then emptied again. This contraction and relaxation of heart chambers during a cardiac cycle also causes the rotational back and forth displacement of a heart.

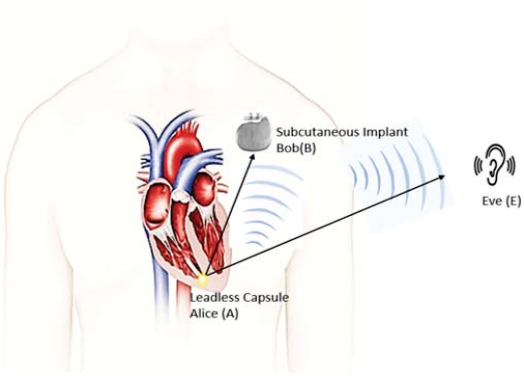

Fig. 1. Pacemaker Scenario with an Eavesdropper

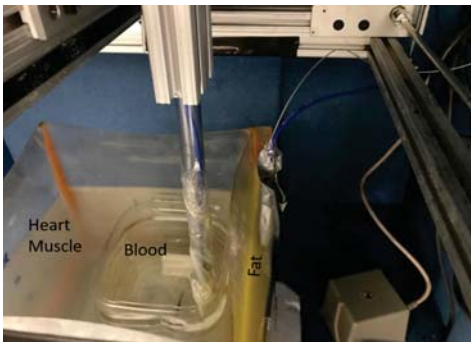

Fig. 2. Phantom containers, containing blood phantom, heart muscle and Fat

To emulate a cardiac cycle, phantoms are developed that mimics the dielectric properties of human tissues/organs. The radio transmission path for AB link involves heart muscle, blood and fat. Thus, we develop the phantom for heart muscle, blood and fat in UWB frequency band. These phantoms are then filled in containers used for experimentation. Fig. 2 shows the containers filled with their respective phantoms.

B. Measurement Setup

The setup used for the channel measurements is shown in Fig. 3 [13], [14]. Our experimentation setup includes, phantom containers to hold the liquid phantoms, Anechoic chamber to avoid surrounding contributions, Vector Network Analyzer (VNA) to generate sounding signal in UWB frequency band, a magnetic tracker to track the distance between transmitter and receiver antenna at different spatial measurement positions, and the positioner, to move the antenna to different positions. The VNA is controlled via software on a designated laptop.

Once the equipment is in-place, the software on a laptop performs the initial calibration of coaxial cables and VNA. The temperature of a phantom is maintained at 24°C due to it's variation with temperature change. The phantom temperature at 24 °C mimics the dielectric

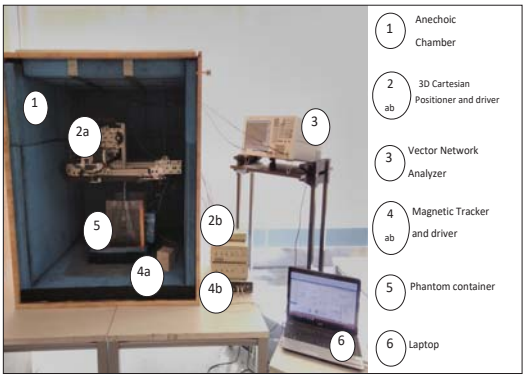

Fig. 3. Measurement Setup

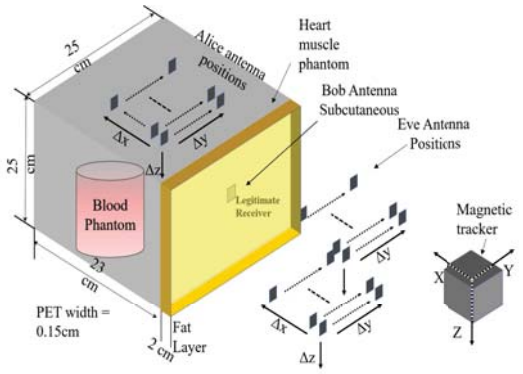

Fig. 4. Measurement Grid points

properties at body temperature of 37 °C.

C. Channel Measurements

In order to perform the channel measurements, we used three set of UWB antennas. Two monopole antennas with quasi-omnidirectional radiation pattern are used for Alice and Bob respectively. Third antenna with same radiation pattern is used to replicate an eavesdropper outside the body. The Alice transmits the sounding signal to Bob, and resultant transmission reflection coefficient (S_{21}) is evaluated. With in a coherence time, Bob transmits the sounding signal to Alice and the transmission reflection coefficient (S_{12}) is measured. These transmission coefficients are used to depict path loss from Alice to Bob and Bob to Alice which are then transformed to RSS measurements. The RSS measurements are later used to generate a symmetric secret key at both the ends.

To approximate the cardiac cycle, we place the container filled with heart muscle and fat inside the anechoic chamber. As mentioned earlier, it is not possible to emulate the dynamic pumping of blood in RV, thus by adding and removing the blood container, the RV filling and emptying is approximated. First, the Alice antenna attached with positioner is submerged into the blood

TABLE I
SETUP PARAMETERS

Frequency Band	UWB
Phantom	Heart muscle, blood & Fat
Frequency range	3.1-5.1 GHz
Resolution points	1601
Resolution Frequency	1.25 MHz
Intermediate Frequency	3 KHz
Snapshots per position	Ns = 5
Measurement parameters	S_{21} and S_{12}

phantom, whereas Bob antenna is mounted inside the fat layer. The setup parameters are listed in Table I. In order to emulate the physical displacement of heart during a cardiac cycle, we moved the Alice antenna in different grid points in three dimensional space with $\Delta x = \Delta y = \Delta z = 0.5\ cm$, having the maximum separation of 3 cm between spatial positions. This is because, we approximated that the cardiac displacement during a cycle is about 3 cm (back and forth). On each measuring point, the forward transmission coefficient (S_{21}) is first estimated, followed by backward transmission coefficient (S_{12}). Moreover at each measuring position, five snapshots are taken and averaged to avoid any errors.

Once the measurements with blood container are done, then it is removed safely to estimate the transmission coefficients for same measurement positions with out blood. Similar procedure is followed for Alice-Eve link measurement, in which, we fixed the Alice antenna inside the phantom and move the Eve antenna in different spatial positions. As we assumed that Eve is of passive nature, so it only measures the transmission coefficients from Alice to Eve. Fig. 4 shows the measurement positions for AB- and AE- link.

D. Received Signal Strength RSS

Received signal strength (RSS) for both forward and reverse link in terms of average coupling over N resolution points per spatial position can be expressed as;

$$RSS_{i_l} = P_t - 10 \times \log_{10}\left(\sum_{k=N} \frac{|H_k(f)|^2}{N}\right), \quad i\epsilon(S_{21}, S_{12}), \tag{1}$$

where, P_t is the transmitted power, l represents the spatial positions and $H_k(f)$ is the channel transfer function in frequency domain over N resolution points (sampling frequency of 1.25 MHz) and is expressed as;

$$H_k(f)_i = |S_i| e^{-j\angle S_i} \quad i\epsilon(S_{21}, S_{12}) \tag{2}$$

where $|S_i|$ and $\angle S_i$ are module and phase of the forward and backward transmission coefficients. Moreover, all the values below -90 dB are discarded, and are considered as noise. We consider the transmit power of

0 dBm, due to which path loss and RSS can be used interchangeably.

E. Secret Key Generation

To generate a secret key between Alice and Bob, they must exploit a common source of randomness in between them. In this work, we use the RSS measurements as a source of randomness.

1) RSS based key generation: In case of RSS based key generation, the legitimate nodes probe the channel with in coherence time (time during which the channel response is flat) to obtain the channel transfer function (CTF). After probing the channel, both communication parties extract RSS from CTF. Once the RSS is depicted, both the communication parties apply the quantization algorithm based on a single or multilevel thresholding to generate the output binary key string.

a) Channel Probing: As mentioned earlier, in this work we used the methodology of phantom experiments to approximately emulate the cardiac cycle. To mimic the heart movement we move the Alice antenna to different spatial locations and evaluate RSS for both Alice and Bob, with and without blood using (1). Fig. 5 shows all the RSS measurements evaluated during a single cardiac cycle in forward direction that is from Alice to Bob[2]. One can observe the random fluctuations around the mean. From statistical point of view, these fluctuations can be approximated as a normal distribution. Fig. 6 shows the histogram of the RSS measurement samples with an assumption of log-normal fitting. The log normal fitting parameters evaluated from the measurement samples are transformed into zero mean with standard deviation of 4.0423 dB, and can be expressed as $\mathcal{N}(0, 4.0423)$. In real case scenario (implanted pacemaker units), both Alice and Bob probes the channel for RSS measurements during the cardiac cycles for symmetric key generation. The randomness in RSS values is observed due to reflections from different human organs and tissues along with variation in inter-beat timings. In order to reduce the redundancy in generated bits, Alice and Bob do not sample consecutive cardiac cycles and follow an arbitrary selection of cardiac cycles for bits extraction.

b) Quantization Algorithm: This section shows the extraction of the random bits during a single cardiac cycle which can be provided by an entropy of a random source. Entropy of a normal distribution can be expressed as;

$$\mathbb{H} = 1.44 \times \frac{1}{2} \times \log(2\pi\sigma^2 e) \approx 2.71 \; bits, \qquad (3)$$

where σ is in linear scale. Equation (3) shows that during a single cardiac cycle, 2.713 random bits can be extracted. We model the quantization algorithm in such away that it extracts only 2 bits from RSS measurements

[2]A similar figure can be represented for backward direction, which due to space constraint is not provided

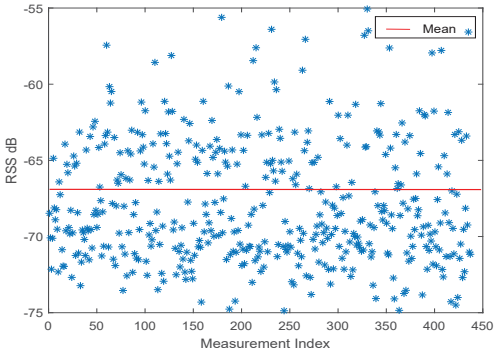

Fig. 5. RSS variations across mean for all the measurement positions during a single cardiac cycle

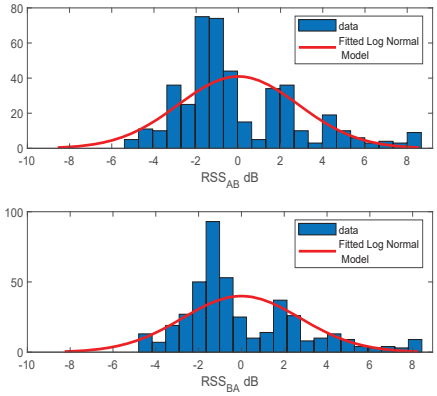

Fig. 6. Histogram of zero mean RSS values for S_{21} and S_{12} for all measurement positions during a cardiac cycle

in a single cardiac cycle. It is based on an assumption that the RSS follows the log normal distribution. Thus, with given (μ, σ) for log normal distribution, we divide the probability density function into four regions, in such a way that cumulative probability density of each region is $\frac{1}{4}$. Table II lists regions with corresponding values of μ and σ. All the regions are then mapped into 2-bit gray code.

The quantization algorithm, samples 2-bits of gray code from each cardiac cycle by taking a single sample from different measurement points. Thus, in total 64 beats or cardiac cycles are required in order to generate 128-bits of binary key string. Moreover, we also assume that both the Alice and Bob are perfectly synchronized and samples a common RSS value during the cardiac cycle with in a coherence time. Also, they decide some arbitrary pattern of selecting cardiac cycles to be used for bit extractions, instead of using the consecutive cycles. This is to add the inter-beat randomness because of its variations, which depends on individual health, age and gender. The resultant inter-beat variations are also reflected in RSS measurements.

TABLE II
LOG NORMAL DISTRIBUTION WITH CORRESPONDING REGIONS

S.No	Regions
1	($-\infty$ — μ -0.675σ)
2	(μ - 0.675σ — μ)
3	(μ — μ + 0.675σ)
4	(μ+0.675σ — ∞)

III. RESULTS

This section focuses on the 128-bit binary key string obtained from quantization algorithm and how well, the key matches at both ends (Alice and Bob) and how much it de-correlates from eavesdropper. In order to generate symmetric key at Alice and Bob, high correlation between channel measurements is required. Thus, first we provide the correlation between Alice and Bob measurements followed by de-correlation of AE link from AB link. Then, a key -mismatch and -generation rates are provided.

A. Correlation between A-B nodes

In statistics, correlation defines the mutual relation ship between two random variables. Based on principle of radio channel reciprocity, if forward and backward transmission coefficients are measured within a coherence time then there exits strong correlation between forward and reverse channel measurements. The widely used pearsen correlation cofficient that shows the linear dependence between two random variables (RSS_{AB} and RSS_{BA}) can be expressed by considering X = RSS_{AB} and Y = RSS_{BA} as;

$$\rho(X,Y) = \frac{1}{l-1}\sum_{i=1}^{l}\left(\frac{\overline{X_i - \mu_x}}{\sigma_x}\right)\left(\frac{Y_i - \mu_y}{\sigma_y}\right), \quad (4)$$

where, *l* is the total measurement positions. Fig. 7 shows the pearsen- correlation between RSS measurements in both directions between Alice and Bob. All the measurements (AB and BA) lies in a straight line at an angle of 45°, showing the high correlation between them. The pearsen-correlation coefficient extracted from (4) for AB-BA link is 0.9963.

B. Correlation between A-E nodes

Eavesdropper RSS measurements needs to be highly de-correlated for a reliable symmetric key generation at Alice and Bob. Fig. 8 shows the correlation between AB and AE links. It is evident that the RSS measurements are scattered over an entire space showing highly de-correlated AE channel from AB channel. The pearsen-correlation coefficient extracted from (4) for AB-AE link is 0.404. The Eve measurements are taken with in a close distance of 10-27 cm from Alice. The correlation will further reduce with Eve movement away from Alice.

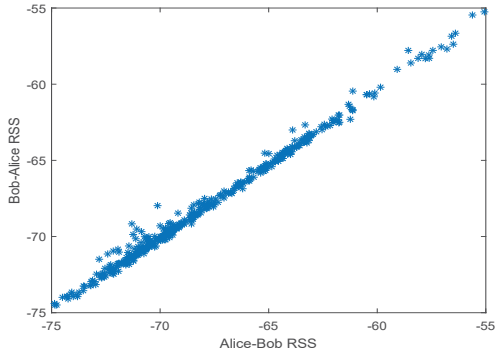

Fig. 7. Correlation between Alice-Bob and Bob-Alice RSS measurements

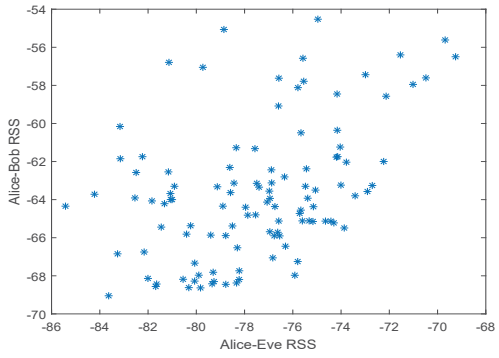

Fig. 8. Correlation between Alice-Bob and Alice-Eve RSS measurements

C. Key Mismatch rate/Bit Mismatch rate (BMR)

To determine the BMR between Alice and Bob, first we generate 128- bit binary key string from 64 cardiac cycles. Once the 128-bit symmetric binary key string is generated at both ends, the hamming distance is evaluated, which shows the number of bits that vary between the key at Alice and Bob. In order to test the bit strings generated, we make in total 1000 runs. Thus 1000, 128-bit keys are generated between Alice and Bob. Each key pair (K_{A_i} and K_{B_i}) is then evaluated for key mismatch rate, where K_{A_i} and K_{B_i} are the keys at Alice and Bob for a run *i*. Fig. 9 shows the hamming distance between the key at Alice and the key at Bob for 1000 generated keys. The empty spaces in Fig.9, shows the key mismatch rate of zero, which means that both Alice and Bob perfectly generate a common symmetric key from RSS measurements. On average for all 1000 runs, the key mismatch percentage is found to be a very low with a percentage value of approximately 1 %.

D. Key Generation Rate (KGR)

The quantization algorithm generates 2-bit gray code from a single cardiac cycle. If we consider the normal human heart rate of 64 bpm, then for consecutive 64

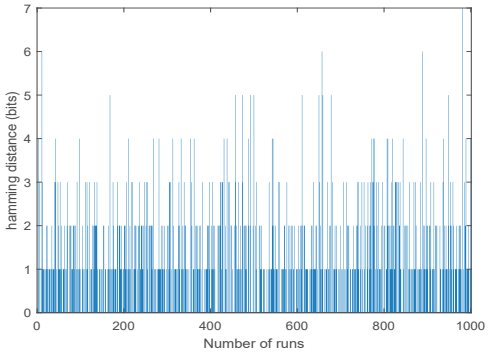

Fig. 9. Hamming distance between K_A and K_B for 1000-runs

beats, it will take 60 seconds for quantization algorithm to generate 128-bits.

IV. Conclusions & Future work

This work focuses on securing the communication between leadless cardiac pacemaker (Alice) implanted in right ventricle of human heart and subcutaneous implant (Bob) implanted beneath the skin under the shoulder. In this work, we exploit the channel randomness between Alice and Bob to generate a reliable 128-bit binary key string. The key is generated by using the in-body randomness observed in received signal strength (RSS). We adopted the methodology of phantom experiments to approximate the real-application scenario of a cardiac pacemaker during a single cardiac cycle. This involves the development of different phantoms for heart muscle, blood and fat that mimics the dielectric properties of respective organs. The measurements are performed in UWB frequency band to determine the RSS values across different spatial positions with- and without blood. The resultant RSS values are then modeled with log-Normal fitting in order to obtain different quantization regions. Afterwards, the quantization algorithm generates 2-bits of gray code from each cardiac cycle, ultimately requiring 64 beats to generate 128-bits binary key string. The average key mismatch rate between communication parties is found to be about 1 % after 1000 runs of key generation.

Our future work involves the key re-conciliation method in order to bring the key mismatch to approximately 0%. We are also planning to perform an in-vivo experiments to test the algorithm in real scenario.

V. Acknowledgments

"This work was supported by the EU's H2020 MSCA:ITN grant for the Wireles In-Body Environment (WiBEC) project with grant no: 675353".

References

[1] H. G. Mond and A. Proclemer, "The 11th world survey of cardiac pacing and implantable cardioverter-defibrillators: calendar year 2009–a world society of arrhythmia's project," *Pacing and clinical electrophysiology*, vol. 34, no. 8, pp. 1013–1027, 2011.

[2] "Medtronic micra leadless pacemaker," https://www.medtronic.com/us-en/patients/treatments-therapies/pacemakers/our/micra.html, accessed: 20-11-2018.

[3] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. IEEE, 2008, pp. 129–142.

[4] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of biomedical informatics*, vol. 55, pp. 272–289, 2015.

[5] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE transactions on information theory*, vol. 39, no. 3, pp. 733–742, 1993.

[7] C. T. Zenger, M.-J. Chur, J.-F. Posielek, C. Paar, and G. Wunder, "A novel key generating architecture for wireless low-resource devices," in *Secure Internet of Things (SIoT), 2014 International Workshop on*. IEEE, 2014, pp. 26–34.

[8] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2763–2776, 2014.

[9] P. Van Torre, T. Castel, and H. Rogier, "Encrypted body-to-body wireless sensor node employing channel-state-based key generation," in *Antennas and Propagation (EuCAP), 2016 10th European Conference on*. IEEE, 2016, pp. 1–5.

[10] C. C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[11] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ecg)," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 6, pp. 1400–1411, 2017.

[12] C. Camara, P. Peris-Lopez, H. Martín, M. Aldalaien *et al.*, "Ecg-rng: A random number generator based on ecg signals and suitable for securing wireless sensor networks," *Sensors*, vol. 18, no. 9, p. 2747, 2018.

[13] M. F. Awan, S. Perez-Simbor, C. Garcia-Pardo, K. Kansanen, P. Bose, S. Castelló-Palacios, and N. Cardona, "Experimental phantom-based evaluation of physical layer security for future leadless cardiac pacemaker," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2018, pp. 333–339.

[14] M. Awan, S. Perez-Simbor, C. Garcia-Pardo, K. Kansanen, and N. Cardona, "Experimental phantom-based security analysis for next-generation leadless cardiac pacemakers," *Sensors*, vol. 18, no. 12, p. 4327, 2018.