IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 30, 2020, accepted August 8, 2020, date of publication August 18, 2020, date of current version August 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3017553

Securing Next Generation Multinodal Leadless Cardiac Pacemaker System: A Proof of Concept in a Single Animal

MUHAMMAD FAHEEM AWAN[1], RAFAEL CORDERO[2,3], KIMMO KANSANEN[1], (Senior Member, IEEE), AND DELPHINE FEUERSTEIN[3], (Senior Member, IEEE)

[1]Department of Electronic Systems, Norwegian University of Science and Technology, 7491 Trondheim, Norway
[2]Centre de Nanosciences et de Nanotechnologies, Université Paris-Sud, 91400 Paris, France
[3]Clinical Research, MicroPort CRM, 92140 Clamart, France

Corresponding author: Muhammad Faheem Awan (faheem.awan@ntnu.no)

This work was supported by the EU's H2020 MSCA: ITN grant for the Wireless In-Body Environment (WiBEC) Project under Grant 675353.

ABSTRACT As the next generation of implanted medical devices for cardiac rhythm management moves towards multi-nodal leadless systems that do without the limitations of transvenous leads, new security threats arise from the wireless communication between the systems' nodes. Key management and the key distribution problem used in traditional cryptographic methods are considered to be too computationally expensive for small implanted medical devices. Instead, inherent human biometrics could provide a reliable alternative. In this work, we tested the key generation process across different nodes of a mimicked dual-chamber leadless cardiac pacemaker system and a subcutaneous implantable relay (S-relay). The proposed key generation process utilizes the randomness available from inter beat intervals (IBIs). A pre-clinical in-vivo experiment was performed in one dog in order to validate the concept by implanting conventional bipolar cardiac pacemaker leads in the right atrium, the right ventricle and the subcutaneous space. Based on the available randomness and entropy of recorded IBIs, 3-bits were extracted per IBI by approximating a sequence of intervals with a normal distribution. This allowed for the generation of a 128-bit key string across the nodes with an average bit mismatch rate of about 3%. Parity check methods were used to reconciliate the keys across the multiple nodes of a multi-nodal leadless pacemaker and subcutaneous device system. The findings are encouraging and demonstrate that IBIs can be used to generate secure keys for data encryption across different nodes of a leadless pacemaker system and S-relay.

INDEX TERMS Physiological signals, security and privacy, multi-nodal leadless cardiac pacemaker, WBAN, physical layer security, key generation.

I. INTRODUCTION

Technological innovations in wireless body area networks (WBAN) have led to the development of many wireless wearable and implantable medical devices and systems. In the field of cardiac rhythm management, this was seen with the transformation of decades-old implantable medical devices such as cardiac pacemakers.

A. CLINICAL BACKGROUND

Pacemakers are implanted in patients presenting abnormal heart rhythms. There are over one million annual pacemaker implantations worldwide [1]. Traditionally, pacemakers and similar systems consist of a device casing or 'can' that is implanted subcutaneously in a pectoral pocket. This can is connected to transvenous wires or 'leads' that run down through veins and are fixed to the inner walls of the right atrium or right ventricle of the heart. Additionally a third lead can be introduced to the coronary sinus above the left ventricle for cardiac resynchronization therapy (CRT). Bipolar electrodes on the distal ends of these leads record cardiac electrophysiological signals known as electrograms (EGMs) and electrically stimulate the heart. The surface of the subcutaneous can, implanted in the pectoral pocket, also serves as a unipolar electrode.

The associate editor coordinating the review of this manuscript and approving it for publication was Lorenzo Mucchi.

Transvenous leads have been identified as the weakest element of the system – they may fracture, they may lead to infection, and their explantation is associated with a high risk of mortality [2]. Consequently, the next generation of pacemaker systems is becoming wireless, and doing without the transvenous leads that connect the various electrode nodes of the system together via the device's processor, in the can. Currently there is only one such leadless pacemaker that is commercially available: the single chamber Micra ™ (Medtronic) [3].

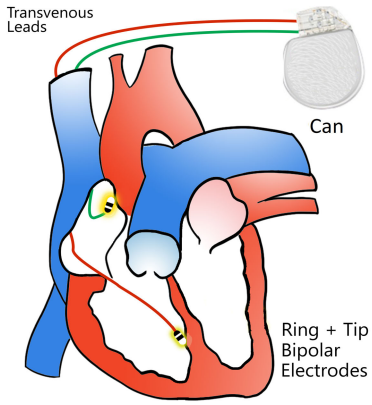
As multi-nodal pacemaker and similar systems become leadless, a wireless communication challenge arises between the various nodes of the systems. Depending on the exact cardiopathology being treated, there will be different embodiments of future leadless cardiac pacemaker (LCP) systems: from an autonomous single chamber leadless pacemaker like the Micra to a triple-chamber leadless CRT system.

The intracardiac pacemaker nodes could be wirelessly configured and programmed by using a subcutaneous relay node between the intracardiac leadless pacemaker nodes and an external programmer at a distance from the patient. One other possible configuration could consist of only multi-chamber leadless pacemaker nodes that communicate wirelessly with each other and with an external programmer directly without a relay. Fig. 1a shows the traditional (i.e. transvenous) dual chamber pacemaker system whereas one of the variant of next-generation leadless pacemaker systems with subcutaneous relay is shown in Fig. 1b.

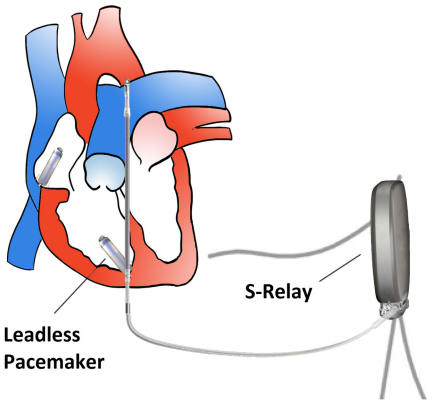
B. MOTIVATION AND SECURITY OF IMPLANTED DEVICES

The wireless nature of these multi-nodal leadless pacemaker systems acts as an important source of security risks, as patient physiological information and therapy-related commands are communicated wirelessly, making the communication more visible and thus facilitating eavesdropping and potential hacking [4], [5]. Due to the sensitive and often life-critical nature of these systems, it is essential to protect the communication between their various nodes. To illustrate this concern, Halperin *et al.* [6] performed software-based attacks on implanted cardioverter defibrillators (ICDs) using off-the-shelf programmer and directional antennas, demonstrating that patient safety and privacy can be compromised due to insecure wireless communication links.

Several approaches have been reported in the literature to secure WBAN communications and preserve confidentiality and integrity. These include techniques ranging from traditional cryptographic algorithms and keys, to wireless physical layer security methods (PLS). A survey on privacy and security issues related to implanted medical devices (IMD's) is provided in [7]. The cryptograhic algorithms utilizes cryptographic keys in order to encrypt and decrypt the information. Therefore, the keys should be kept secret by the manufacturers and require servers to manage and store them. The infrastructure based key management and distribution servers are difficult to implement in emerging paradigms like in-body wireless sensor networks. Another alternative



(a) Traditional dual chamber pacemaker system. The subcutaneous can is connected to the electrodes by transveneous leads



(b) Next generation multi-nodal leadless pacemaker system with S-relay

FIGURE 1. Comparison between traditional (a) and a variant (b) of the next generation pacemaker systems. S-relay is the subcutaneous relay.

could be using PLS methods. The idea of PLS was first introduced by Shannon in 1948 [8]. Number of methods and techniques have been developed since, utilizing the physical layer to provide information confidentiality including methods based on the spread spectrum [9], modulation techniques [10], [11], or methods that can be implemented using keyless or key-based security approaches. Keyless security involves pre-coding strategies to hide the communicated information from the eavesdropper (Eve) [12]–[15] and mostly depends on the performance metric of secrecy capacity [16]–[18]. The key-based approach involves the use of cryptographic keys which are not already stored but generated from a common information source among legitimate communication nodes. The common source could be the wireless channel or any third-party source. Using PLS methods for securing WBAN, one can exploit different characteristics of the wireless channel e.g. Angle of Arrival AoA, Phase, and Received Signal Strength RSS [19], [20]. Key generation using these characteristics relies on channel reciprocity.[1]

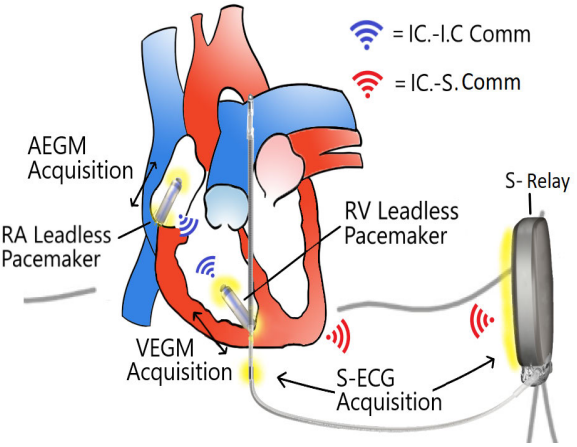
[1]the same channel response between transmitter to receiver and receiver to transmitter

An attractive and feasible key generation alternative for WBAN is using a third party common source such as the physiological signals of the patient. Although physiological signals such as the electrocardiogram (ECG), electromyogram, electroencephalogram, or blood pressure vary in morphology and amplitude depending on where they are recorded, but certain underlying physiological metrics, such as the heart rate, do not, irrespective of position where they are recorded. Further the acquisition of these physiological signals is performed via direct contact to the body, avoiding the risk of being eavesdropped by an external third-party.

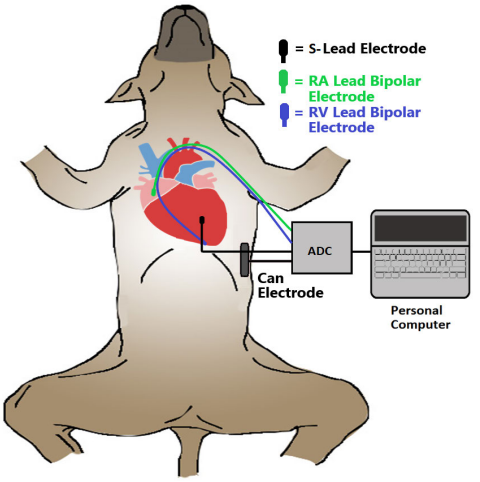
Monrose *et al.* [21], proposed the first biometric-based key generation method. These techniques were based on behavioral biometrics and are provided in [22], [23]. Biometric traits for key-generation can be divided into external and internal. The external traits refer to those that remain the same throughout the subjects life and include the iris, fingerprints, hand geometry, DNA and facial morphology [24]–[26]. The main drawback of external biometrics is that they can be easily forged (e.g we leave our fingerprints on all the objects we interact with on a daily basis). Conversely, internal biometrics are those that vary with time and typically represent internal physiological phenomena. They are therefore more resilient in this respect. These internal biometrics include the ECG, the photoplethysmogram (PPG), and the electroencephalogram (EEG) [27]. The use of inter-beat-intervals (IBIs) for key generation was proposed in [28] where PPG and ECG were utilized to extract IBIs. The IBI is the time elapsed between contiguous heart cycles and varies with time depending on different physiological factors. Other similar works are also available in the literature utilizing heart rate as a random source to generate the cryptographic keys [28]–[33].

In this work an IBI-based 128-bit group secret key generation method is tested by utilizing synchronous intracardiac EGM (local depolarization) and subcutaneous ECG (S-ECG) signals. The proof of concept was provided by performing an acute in-vivo experiment on a single dog.

The rest of the paper is organized as follows. Section II describes the Materials and Methods. Section III delivers the Results. Discussions and Conclusion are provided in section IV and V respectively.



(a) Dual-chamber leadless pacemaker system with S-relay. IC-IC is intracardia-intracardiac communication, IC.-S. is intracardiac to subcutaneous communications



(b) Dual-chamber leadless pacemaker system with S-relay using transvenous pacemaker leads and inactive 'can' in a dog. ADC is an analog to digital converter.

FIGURE 2: System Model

FIGURE 2. System model.

II. MATERIALS AND METHODS

A dual-chamber pacemaker with a subcutaneous relay was chosen as the potential future embodiment of a multi-nodal leadless pacemaker system. Such an embodiment is illustrated in Fig. 2a, and consists of two leadless pacemakers (one in the right atrium, and the other in the right ventricle), and a subcutaneous relay (S-relay). The S-relay in turn consists of a subcutaneous lead connected to a subcutaneous can which runs parallel to the sternum, on its left side. The subcutaneous can lies on the axillary midline, at the height of the fifth intercostal space. This particular embodiment of a multi-nodal leadless pacemaker system with an S-relay was chosen because it features both an intracardiac-intracardiac communication channel, and a intracardiac-subcutaneous communication channel.

A. EXPERIMENTAL PROTOCOL

A pilot experimental protocol was performed on one dog (golden retriever, male, 32 kg, 3.5-years) at the Institut Mutualiste Montsouris de Recherche, in Paris, France. All the ethical European guidelines and regulations for animal handling in laboratory were met and fulfilled. The experimental procedure was not performed specifically for this study, but rather for multiple other purposes, among which some were previously reported in [34].

The animal was put under general anesthesia, intubated and ventilated at a fixed rate of 12 breaths per minute. To mimic the leadless dual-chamber pacemaker with an

S-relay embodiment, two commercially available bipolar intracardiac pacing leads were implanted in the heart from a subclavian venous access (see Fig. 2b). One of these was fixed in the right atrium, and the other in the apex of the right ventricle. The sensing dipoles used in the leadless pacemaker are very similar to those used in bipolar transvenous pacemaker leads. Both consist of a ring and tip electrode separated by 10-20 mm, across which electrophysiological signals are recorded and the heart is paced. The EGM of the right atrial pacemaker lead was referred to as the AEGM, and the EGM of the right ventricle pacemaker lead was referred to as the VEGM. Each ring and tip electrode pair of the pacemaker leads made up a single node of the multi-nodal system.

The S-relay can was mimicked using an inactive casing that housed electronics unrelated to the present study. The surface of this can served as an electrode. The can was implanted by performing a cut along the anterior axillary line and manually creating a pocket in the subcutaneous space. The can was then inserted into this pocket, which was sutured close. The S-relay lead was mimicked by implanting a conventional (i.e. transvenous) pacemaker lead in the subcutaneous space, parallel and 5 mm to the left of the sternum using a pacemaker lead tunneling tool. The subcutaneous node consisted of the dipole created between the electrode on the tip of the subcutaneously-implanted pacemaker lead, and the surface of the can. This dipole recorded a subcutaneous ECG (S-ECG).

A median-plane X-ray as shown in Fig. 3 describes the implanted intracardiac and subcutaneous leads, the can, as well as several other sensors that are not relevant to this work.

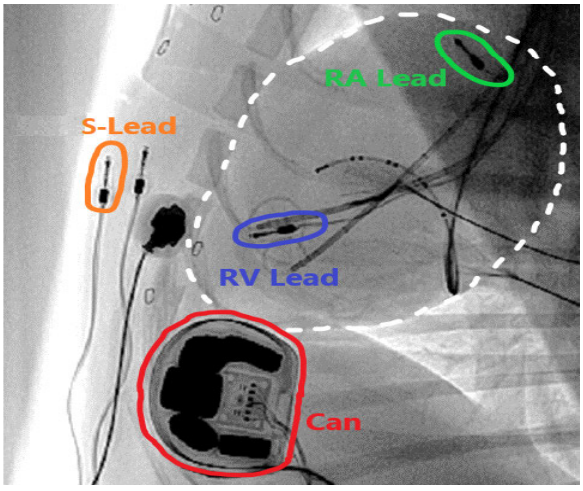


FIGURE 3. Median plane X-Ray of implanted leads in the right atrium (RA), right ventricle (RV), subcutaneous left parasternal space, and the subcutaneous can implanted along the mid axillary line. Other visible sensors were not relevant to this work. The figure is adapted from [34] .

B. SIGNAL ACQUISITION AND IBI EXTRACTION

The three physiological signals (AEGM, VEGM and S-ECG) were sampled at 1000 Hz using a multi-channel custom digital-acquisition platform. The recorded signals were exported to MATLAB ™ (Mathworks) for offline processing. Exemplary AEGM, VEGM, and S-ECG signals recorded during normal sinus rhythm are shown in Fig. 4.

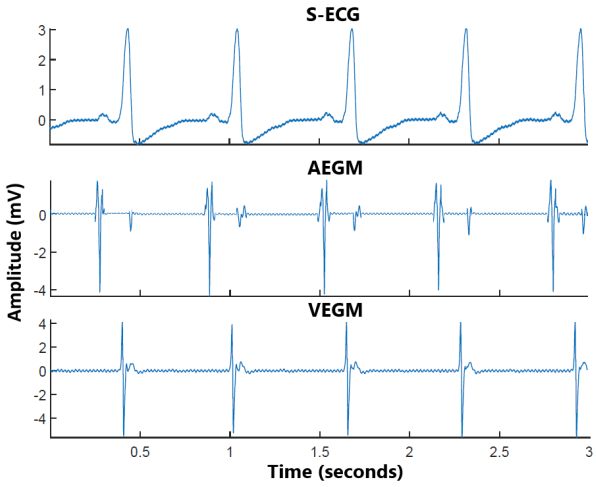


FIGURE 4. Recorded S-ECG, AEGM, and VEGM signals. The cross-talk of the ventricular depolarization on the AEGM were not counted in the beat detection process.

The IBI extraction from S-ECG was performed using the Pan-Tompkins algorithm [35]. IBIs 15% greater or smaller than the median of the last five IBIs were considered ectopic and discarded. This was to eliminate erroneous detections or premature-ventricular contractions. To extract the IBIs from EGM signals, we used the Multilevel-Teager Energy Operator (MTEO). More details on MTEO can be found in [36].

C. KEY GENERATION PROTOCOL

The block diagram of a key generation protocol for multi-nodal LCP is shown in Fig. 5. In Fig. 5, the normal fitting, binary encoder and parity check methods are adapted from [37] whereas the rest of the procedures utilized for IBI extraction and key generation are novel. This includes effective IBI extraction from EGM and ECG signals using Pan-Tompkins and Teager Energy operator and then utilizing the DIFF operation to reduce the intra series auto-correlation.

By obtaining the physiological signals at different locations inside the body, we want to generate the symmetric key between different nodes of next-generation LCP systems. After signal processing and using the MTEO operator, the timing information of the IBIs was extracted at each node and this information was used to generate a secret key independently. Each node generates a series of IBI values from consecutive beats. Fig. 6a shows the extracted IBI values across the nodes. A strong correlation is observed in measured IBI's across all the nodes. The correlation between the IBI sequences can be expressed as

$$\rho(x, y) = \frac{1}{n-1} \sum_{i=1}^{n} \left(\frac{\overline{x_i - \mu_x}}{\sigma_x} \right) \left(\frac{y_i - \mu_y}{\sigma_y} \right), \qquad (1)$$

where x and y are the IBI values extracted from AEGM and VEGM, n is the total number of IBI values (120 samples)

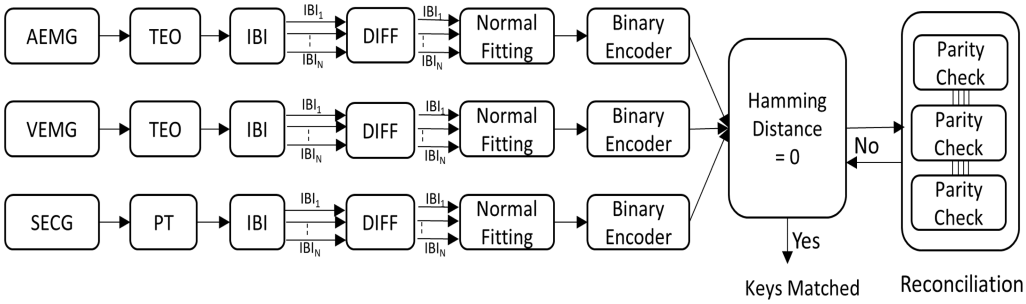
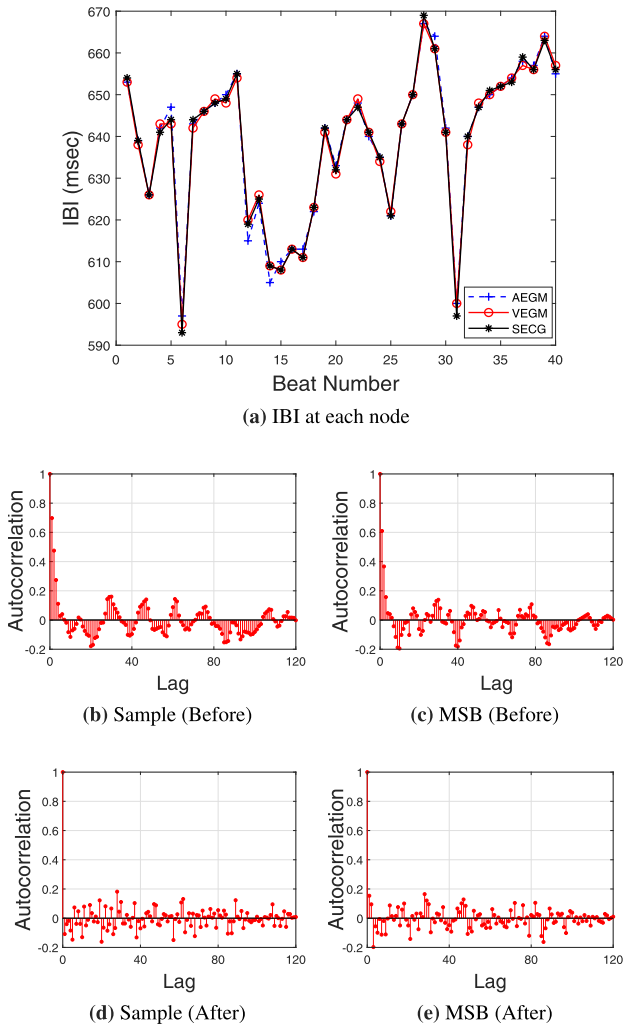


FIGURE 5. Block diagram of Key generation process, PT represents Pan-Tompkins algorithm, DIFF represents the difference operator.



(a) IBI at each node

(b) Sample (Before)

(c) MSB (Before)

(d) Sample (After)

(e) MSB (After)

FIGURE 6. (a) Evolution tachogram (b)(c)(d)(e) represents correlation between adjacent samples and the corresponding correlation reflected on generated MSB, before and after the difference operator for Atrium IBI time series (AEGM) (b)(c) shows the adjacent IBI sample correlation and MSB correlation before difference operator (d) (e) shows the correlation between adjacent IBI sample correlation and MSB after difference operator.

and σ is the standard deviation from the mean. The observed correlation is about 0.9937. Similarly, almost the same correlation is found between intra-cardiac EGMs (AEGM) and S-ECG signal and is 0.9946. In order to generate a completely random sequence of bits from a given source, the correlation within each of the time series IBI sequence samples should be zero. Fig. 6b shows the auto-correlation between the time series IBI samples generated from the node in the right atrium. A high correlation of 0.7, 0.5, and 0.3 is observed between the adjacent IBI samples (see Fig. 6b), which is not considered as a favorable scenario to generate completely random bits from each sample. This adjacent sample correlation is also reflected on the bits generated, specifically on most significant bits (MSBs) (see Fig. 6c). In order to reduce the auto-correlation between the adjacent IBI samples to a level that it can be treated as independent identical distributed (i.i.d), the strategy of difference operator is applied. The difference sequence is evaluated by taking the difference between adjacent IBI samples which can be expressed as,

$$IBI_{diff} = [IBI(2) - IBI(1) \;\; IBI(3) - IBI(2) \;\; \ldots \;\; \ldots \;\; IBI(n) - IBI(n-1)] \quad (2)$$

The reduction in adjacent sample correlation can be observed in both sample (see Fig. 6d) and MSB (see Fig. 6e) after the difference operator.

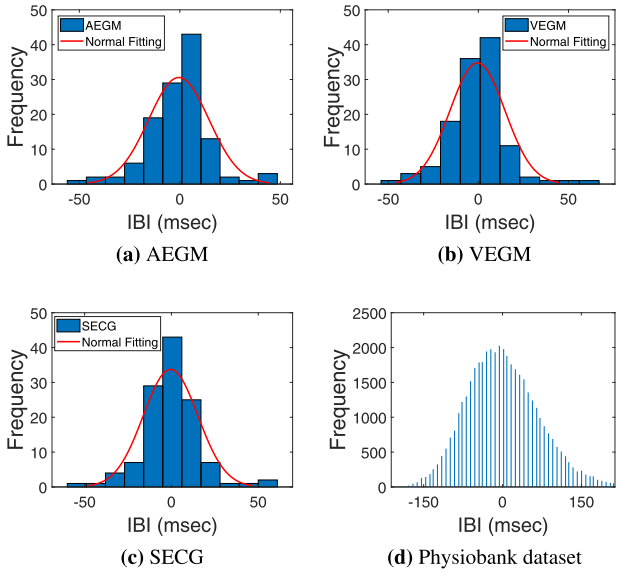
From a statistical point of view, the IBI values at each node can be fitted with the normal distribution [38]. The histogram of the IBI values accumulated from 120 cardiac cycles is shown in Fig. 7. With a large sample size, the IBI values can be assumed as normally distributed as shown in Fig. 7d, which is the histogram of large data set obtained from online repository.[2] The fitting parameters evaluated are transformed to zero mean with standard deviation of 0.015 seconds and can be expressed as $\mathcal{N}(0, 0.015)$.

1) QUANTIZATION ALGORITHM

The entropy of a random source evaluates the number of random bits that can be generated from each IBI sample. In case of normally distributed independent identical (i.i.d.) source with standard deviation σ, the entropy can be expressed as

$$\mathbb{H} = 1.44 \times \ln(\sigma\sqrt{2\pi e}) \approx 4 \; bits, \quad (3)$$

[2]https://physionet.org/physiobank/database/nsr2db/



(a) AEGM (b) VEGM (c) SECG (d) Physiobank dataset

FIGURE 7. Extracted IBI samples from experimental data set with normal fitting (d) shows the histogram of large data set of IBI values downloaded from Physiobank.

It can be seen from (3) that approximately 4 random bits can be generated per IBI sample. In this work, the utilized quantization algorithm is modeled in a way that it generates only 3 bits per IBI sample. This is to reduce the potential mismatches between generated bits across the nodes. Thus, based on the assumption that IBIs follow a normal distribution with given (μ, σ), the probability density function is divided into eight regions. The regions are segregated in such a way that cumulative distribution function of each region is $\frac{1}{8}$. For evaluated values of μ and σ, the segregated regions are listed in Table 1. During a cardiac cycle, the quantization algorithm of all the nodes, samples the physiological signal and extracts the IBI. The sampled IBI is then matched to a region it belongs. The resultant gray code of a region is generated for a given IBI sample. Thus, each IBI sample generated from two consecutive cardiac cycles is sampled to 3 bits by quantization algorithm. We have assumed that all the nodes are synchronized and sample the same IBI index. Realistically it is quite difficult to completely synchronize all the modules, but the design of future leadless cardiac pacemakers will guarantee a certain level of synchronization in order to effectively perform CRT therapy [39]. This synchronization between the leadless modules will be within a few 10s of milliseconds (ms) and not within 100 ms,

TABLE 1. Segregated Regions for Normally distributed sequence of IBI samples.

	Regions		Regions
1	$(-\infty$ — $\mu - 1.151\sigma)$	5	$(\mu$ — $\mu + 0.319\sigma)$
2	$(\mu - 1.151\sigma$ — $\mu - 0.675\sigma)$	6	$(\mu + 0.319\sigma$ — $\mu + 0.675\sigma)$
3	$(\mu - 0.675\sigma$ — $\mu - 0.319\sigma)$	7	$(\mu + 0.319\sigma$ — $\mu + 1.151\sigma)$
4	$(\mu - 0.319\sigma$ — $\mu)$	8	$(\mu + 1.151\sigma$ — $\infty)$

Algorithm 1 Algorithm for Key Generation

n-sample
Input: (IBI intervals) of a physiological signal
Output: 3n-bit of a binary key string
Steps:
1: 'can'- Generate network wide synchronization signal indicating beginning of key generation
2: All the nodes capture physiological signal (EGM/SECG)
3: Extraction of IBI from consecutive cardiac cycles $IBI_i | 1 \leq i \leq n$
4: Difference operation on adjacent IBIs
5: Histogram of difference IBI sequence
6: Fitting Normal Distribution
7: Extraction of σ
8: Segmenting into Regions R_1, R_2, R_3,R_4,R_5,R_6,R_7 and R_8
9: Gray code for each region '$GC_1 = 000$','$GC_2 = 001$','$GC_3 = 011$','$GC_4 = 010$','$GC_5 = 110$','$GC_6 = 111$','$GC_7 = 101$','$GC_8 = 100$'
Output = []
10: **for** i =1 *to* n **do**
11: **for** k =1 *to* 8 **do**
12: **if** $(IBI_i \epsilon R_k)$ **then**
13: Output = strcat(Output,GC_k)
14: **end if**
15: **end for**
16: **end for**
17: **return** *Output*
18: Reconciliation - Parity Check bit

resulting in sampling the same IBI index (even if they sample it at a different point in time within the cardiac beat). As a single IBI results in 3 bits, thus in order to generate the secret key of 128 bits, a total of 43 cardiac cycles are required. The generated keys across multiple nodes always have slight mismatching, which must be reconciled before using it for data encryption.

2) KEY-RECONCILIATION

The parity check method for key reconciliation is used, since it is simple and efficient. For each IBI sample, the nodes generate 3-bit gray code along with a parity bit. The parity bit is shared across the nodes. If parity across the nodes for a given gray code is different, the nodes discard the generated block. If the parity bit is identical, then the first 3-bits are extracted from a given block. The process continues until 128-bits of reconciled key is generated across all the nodes. The key generation algorithm is provided in Algorithm 1.

III. RESULTS

In this section, the generated key is evaluated for a randomness test. The key mismatch rate and the possibility of similar key generation from patients medical history is also examined.

A. KEY RANDOMNESS ANALYSIS

The 128-bit generated key must be tested for a required degree of randomness. National Institute of Standards and Technology (NIST) provides the widely used set of randomness tests. We run the NIST randomness test suite [40] for evaluating the randomness in the generated key string. In total 15 NIST tests are available, 6 of them are for long bit strings whereas the rest are for short key strings. Our generated key passes all the NIST tests suitable for short keys. For NIST test suite the decision rule is provided in terms of p-value. The randomness hypothesis is rejected if p-value is less than the threshold (1%). Table 2 lists the p-value evaluated for generated keys. The details of the tests are provided in Appendix.

TABLE 2. NIST Randomness Tests.

Randomness Test	P-value (Test hypothesis 1%)
Approximate Entropy Test	0.6973
Block Frequency Test	0.1471
Frequency Test	0.1564
Runs Test	0.8738
Longest runs of ones	0.6529
DFT	0.2428
Non-Overlap	0.233
Cumulative frequency test	0.1176/0.2307

B. TEMPORAL VARIATION

To evaluate the temporal variation, we utilize the hamming distance, which evaluates the independence among the keys generated from past measurements. Hamming distance is the number of bits that varies between two key strings. For keys to be random, they must follow the binomial distribution, according to which the hamming distance should be around half of the key length, representing maximum distance between the keys. Fig. 8 shows the hamming distance between the keys with comparison to actual binomial distribution. The hamming distance is concentrated around 60 providing an evidence of being independent keys.[3] This proves that the keys generated at different time instant will be different and the Eve will not be able to take an advantage from the previous patient records.

[3]for temporal test purpose, we utilize key strings of 120-bits

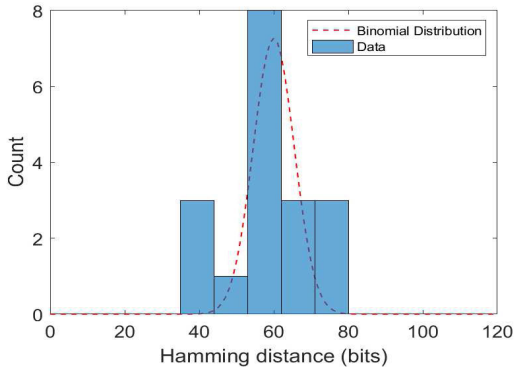


FIGURE 8. Hamming distance between keys from past records.

C. KEY MISMATCH RATE

To evaluate the key mismatch rate before the reconciliation phase, the same metric of hamming distance is used. The hamming distance for perfectly matched keys should be zero. We determine the hamming distance between generated keys across the nodes. The key mismatch rate between the 128-bit key generated in the atrium and subcutaneous relay is 3.89 % whereas the mismatch rate between the keys in the right ventricle node and subcutaneous relay is 2.2 %. The key mismatch rate requires a single round of reconciliation phase.

D. KEY GENERATION RATE

The system requires single IBI to generate 3-key bits. Thus if the normal heart beat rate of 70 bpm is considered then on average 37 seconds will be required to generate the 128-bit secret key. Similarly, by considering the two extremes e.g. in case of 30 bpm, on average the key generation process will require 86 seconds whereas for elevated heart rate of 120 bpm, it will require on average 21 seconds.

IV. DISCUSSION

The results from animal experiment are encouraging and support the process of effective cryptographic key generation from IBIs for next-generation multi-nodal leadless cardiac pacemaker. The entire process can be initiated by the S-relay that generates a network wide synchronous signal for key generation. Each individual node collects the local physiological signal for a sequence of IBI extraction. From each IBI, nodes generate a block of 3-bit gray code, followed by a parity bit for reconciliation. Parity bit is then shared between the nodes. If the parity across the nodes is the same, the block is stored otherwise it is discarded. The process continues until all the nodes of multi-nodal leadless pacemaker system have generated a 128-bit key. Once the key is generated, the pacemaker system will utilize the key for a specific duration that may consist of either multiple sessions or a fixed duration of 30 minutes to an hour. Afterwards, the keys are refreshed again by the S-relay. The method can be extended to off-body programmers with ECG recording.

The described key generation method has two advantages. One, it removes the need of complex key generation and distribution methods as per traditional cryptography. Second, it can be stacked to provide extra layer of security at the physical layer. In addition, instead of utilizing a 128-bit key for data encryption, the proposed method can generate 64-bit key for authentication purposes.

There are also some limitations to the current key generation method. The described method fails if the Eve with knowledge about key-generation method can collect the IBIs at the same time instant as of legitimate nodes of the system. But in order to robustly extract IBIs, the Eve needs to be in physical contact with the patient or use remote sensing techniques based on radar [41] for example which can sense the sub-millimeter movement due to heartbeats.

The results of this work are based only on a single animal, which constitutes a limited test size. For this reason, we would like to replicate the results with more animals, and eventually human patients. Also, the conditions in which we perform the test were in normal sinus rhythm. The methods are not tested on different conditions that could include elevated heart rate, atrial fibrillation, or desynchronized ventricles. Moreover, in case of operating pacemaker, depending on the cardiac pathology, in some cases the heart rhythms will not be normally distributed e.g. the case of pacing at a fixed rate. For those cases, the pacemaker can be programmed for key generation without the assumption of being normally distributed.

Our future work will focus on prototyping the IBI based encryption algorithm. A comparison will be provided between traditional cryptographic and IBI-based methods in terms of system complexity, level of privacy and device longevity. Furthermore, the variation in time required for key generation based on heartbeats will also have an impact on energy consumption and will deserve a specific study. In addition, key generation method in case of different cardiac pathologies will also be tested.

V. CONCLUSION

In this article, a proof of concept in a single animal is provided, for evaluating the potential of securing next generation multi-nodal leadless cardiac pacemaker systems using inherent cardiac physiological signals (intracardiac EGM as well as subcutaneous ECG signals in the presence of a subcutaneous relay). A symmetric group key is generated across all the nodes that includes: right ventricle, right atrium, and a subcutaneous relay. The proposed key generation method provides a promising alternative to establish symmetric keys for data encryption between legitimate nodes, thus avoiding need of key management and distribution servers and conserving substantial computational resources. For an average healthy heart rate of 70 bpm, the proposed method generates 3.65 key bits per second with an average mismatch rate of approximately 3% for a key length of 128-bits. The method can be extended to off-body programmers with ECG recording.

APPENDIX
NIST TEST SUITE

The tests performed are:

A. THE FREQUENCY (Monobit) TEST

This test provides the distribution of zeroes and ones in an entire bit string. The test evaluates that the proportions of zeroes and ones are approximately the same, which is the requirement of a random sequence.

B. BLOCK FREQUENCY TEST

This test evaluates the portions of zeroes and ones in an M-bit defined blocks with in a key sequence.

C. THE RUNS TEST (R-TEST)

This test evaluates the total number of runs in a binary sequence, where a run is the uninterrupted sequence of identical bits.

D. LONGEST-RUN-OF-ONES IN A BLOCK

This test evaluates the longest runs of ones with in M-bit blocks.

E. APPROXIMATE ENTROPY

The purpose of the test is to evaluate and compare the frequency of overlapping blocks of adjacent lengths against the expected result for a random sequence.

F. DISCRETE FOURIER TRANSFORM

The test is performed to evaluate the peak heights in the discrete Fourier transform of the sequence in order to predict the periodic features.

G. NON-OVERLAPPING TEMPLATE MATCHING TEST

It evaluates number of occurrences of pre-specified target strings.

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 Clin. Electrophysiol.*, vol. 34, no. 8, pp. 1013–1027, Aug. 2011.

[2] R. G. Hauser, W. T. Katsiyiannis, C. C. Gornick, A. K. Almquist, and L. M. Kallinen, "Deaths and cardiovascular injuries due to device-assisted implantable cardioverter-defibrillator and pacemaker lead extraction," *Europace*, vol. 12, no. 3, pp. 395–401, Mar. 2010.

[3] *Medtronic Micra Leadless Pacemaker*. Accessed: Nov. 20, 2018. [Online]. Available: https://www.medtronic.com/us-en/patients/treatments-therapies/pacemakers/our/micra.html

[4] L. Mucchi, M. Hämäläinen, S. Jayousi, and S. Morosi, "Body area networks: Smart IoT and big data for intelligent health management," in *Proc. 14th EAI Int. Conf.*, Florence, Italy, Oct. 2019, p. 297.

[5] R. Altawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.

[6] 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 *Proc. IEEE Symp. Secur. Privacy*, May 2008, pp. 129–142.

[7] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015.

[8] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[9] S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 7, p. e3142, Jul. 2017.

[10] L. Mucchi, L. S. Ronga, and L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems," *Wireless Pers. Commun.*, vol. 51, no. 1, pp. 67–80, Oct. 2009.

[11] L. Mucchi, L. S. Ronga, and E. Del Re, "A novel approach for physical layer cryptography in wireless networks," *Wireless Pers. Commun.*, vol. 53, no. 3, pp. 329–347, May 2010.

[12] M. F. Awan, S. Perez-Simbor, C. Garcia-Pardo, K. Kansanen, P. Bose, S. Castello-Palacios, and N. Cardona, "Experimental phantom-based evaluation of physical layer security for future leadless cardiac pacemaker," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2018, pp. 333–339.

[13] M. Bloch, "Physical-layer security," Ph.D. dissertation, School Elect. Comput. Eng., Georgia Inst. Technol., Atlanta, GA, USA, 2008.
[14] M. F. Awan, P. Bose, A. Khaleghi, K. Kansanen, and I. Balasingham, "Evaluation of secrecy capacity for next-generation leadless cardiac pacemakers," *IEEE Trans. Biomed. Eng.*, vol. 67, no. 8, pp. 2297–2308, Aug. 2020.
[15] M. Bloch and J. Barros, *Physical-Layer Security: From Information theory to Security Engeering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[16] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[17] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, "A new metric for measuring the security of an environment: The secrecy pressure," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3416–3430, May 2017.
[18] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.
[19] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[20] M. F. Awan, K. Kansanen, S. Perez-Simbor, C. Garcia-Pardo, S. Castello-Palacios, and N. Cardona, "RSS-based secret key generation in wireless in-body networks," in *Proc. 13th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, May 2019, pp. 1–6.
[21] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," *Int. J. Inf. Secur.*, vol. 1, no. 2, pp. 69–83, Feb. 2002.
[22] H. Feng and C. Choong Wah, "Private key generation from on line handwritten signatures," *Inf. Manage. Comput. Secur.*, vol. 10, no. 4, pp. 159–164, Oct. 2002.
[23] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Cryptographic key generation using handwritten signature," in *Proc. SPIE* , vol. 6202, Oct. 2006, Art. no. 62020N.
[24] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, "Biometric key binding: Fuzzy vault based on iris images," in *Proc. Int. Conf. Biometrics*, 2007, pp. 800–808.
[25] Z. Jin, A. B. J. Teoh, B.-M. Goi, and Y.-H. Tay, "Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation," *Pattern Recognit.*, vol. 56, pp. 50–62, Aug. 2016.
[26] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.
[27] K. V. R. Ravi, R. Palaniappan, C. Eswaran, and S. Phon-Amnuaisuk, "Data encryption using event-related brain signals," in *Proc. Int. Conf. Comput. Intell. Multimedia Appl.*, Dec. 2007, pp. 540–544.
[28] C. C. Y. 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 Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.
[29] 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 Trans. Biomed. Eng.*, vol. 65, no. 12, pp. 2751–2759, Dec. 2018.
[30] H. Garcia-Baleon and V. Alarcon-Aquino, "Cryptographic key generation from biometric data using wavelets," in *Proc. Electron., Robot. Automot. Mech. Conf. (CERMA)*, 2009, pp. 15–20.
[31] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proc. IEEE Mil. Commun. Conf.*, Nov. 2008, pp. 1–7.
[32] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ECG)," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 6, pp. 1400–1411, Jun. 2017.
[33] C. Camara, P. Peris-Lopez, H. Martín, and M. Aldalaien, "ECG-RNG: A random number generator based on ECG signals and suitable for securing wireless sensor networks," *Sensors*, vol. 18, no. 9, p. 2747, Aug. 2018.
[34] R. C. Alvarez, P.-Y. Joubert, F. Ziglio, A. Amblard, and D. Feuerstein, "Cardiac hemodynamic monitoring in the subcutaneous space : A preclinical proof-of-concept," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Jun. 2018, pp. 1–6.
[35] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Trans. Biomed. Eng.*, vols. BME–32, no. 3, pp. 230–236, Mar. 1985.
[36] H. Sedghamiz and D. Santonocito, "Unsupervised detection and classification of motor unit action potentials in intramuscular electromyography signals," in *Proc. E-Health Bioengineering Conf. (EHB)*, Nov. 2015, pp. 1–6.
[37] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
[38] Y. Ostchega, "Resting pulse rate reference data for children, adolescents, and adults: United States, 1999-2008," U.S. Dept. Health Hum. Services, Centers Disease Control Prevention, Nat. Center Health Statist., Tech. Rep., 2012.
[39] D. Palaksha, K. Kansanen, Z. Filippo, J. Bergsland, I. Balasingham, and D. Feuerstein, "Patient specific strategies to enhance leadless pacemaker lifetime in synchronized dual chamber system," *IEEE Access*, vol. 8, pp. 49363–49376, 2020.
[40] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen Hamilton Inc., McLean, VA, USA, Tech. Rep. ADA393366, 2001.
[41] O. Aardal, S.-E. Hamran, T. Berger, Y. Paichard, and T. S. Lande, "Chest movement estimation from radar modulation caused by heartbeats," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, Nov. 2011, pp. 452–455.

MUHAMMAD FAHEEM AWAN received the B.S. degree in electrical engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2008, the M.S. degree in communications systems engineering from the National University of Science and Technology (NUST), Pakistan, in 2014, and the Ph.D. degree from the Norwegian University of Science and Technology (NTNU). His research interests include signal processing, channel modeling for in-body networks, and information security.

RAFAEL CORDERO received the B.Eng. and M.Eng. degrees in biomedical engineering from the Imperial College London, in 2014 and 2015, respectively, and the joint Ph.D. degree in signal processing for subcutaneous cardiac monitoring applications from the Université Paris-Saclay and Microport, Sorin CRM, Paris, France. He then worked as an Associate Research and Development Engineer in the field of neurocardiology with the Medtronic Bakken Research Centre, Maastricht, The Netherlands.

KIMMO KANSANEN (Senior Member, IEEE) received the M.Sc. (EE) and Dr.Tech. degrees from the University of Oulu, Finland, in 1998 and 2005, respectively. He was a Research Scientist and the Project Manager of the Centre for Wireless Communications, University of Oulu. Since 2006, he has been with the Norwegian University of Science and Technology, Trondheim, Norway, where he has been a Full Professor, since 2016. He leads the Signal Processing Group, Department of Electronic Systems. His research interests include wireless communications and signal processing. He is an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

DELPHINE FEUERSTEIN (Senior Member, IEEE) received the Ph.D. degree in bio-engineering from the Imperial College London, in 2009. She then moved to neurological research at the Max Planck Institute, Cologne, as a Humboldt Fellow. She returned to France to join Microport, Sorin CRM, in 2013. She trained as a Multidisciplinary Engineer with Ecole Centrale Lyon, France. She is currently the Biomedical System Leader for innovative active medical devices.