Evaluation of Secrecy Capacity for Next-Generation Leadless Cardiac Pacemakers

Muhammad Faheem Awan, Pritam Bose, Ali Khaleghi, *Senior Member, IEEE,* Kimmo Kansanen, *Senior Member, IEEE,* and Ilangko Balasingham, *Senior Member, IEEE*

Abstract— **Secure communication can be considered as an integral part of the next generation implantable medical devices. With the advent of physical layer security (PLS) methods, confidential messages can be transmitted without the use of encryption keys. For analyzing the effectiveness of PLS for next-generation leadless cardiac pacemakers, we provide secrecy analysis using a performance metric of secrecy capacity. Secrecy capacity defines the secure transmission rate between legitimate nodes without leakage of information to an eavesdropper and depends on respective channel attenuations. The legitimate and eavesdropper channel attenuations are evaluated by 3D numerical electromagnetic simulations using a detailed human model. We do not assume eavesdropper to be located in specific directions or positions and considers it to be located anywhere around the body. We evaluate the secrecy capacity by defining a spherical grid for eavesdropper positions around the body with a radius of 1 m. The secrecy capacity of the entire space is evaluated by extrapolating the grid to different radial distances using free space path loss model. Moreover, by fixing application based secure communication rate, the entire space is divided into secure and in-secure volumes. The in-secure volume consists of all the eavesdropper positions from which the pacemaker can be eavesdropped. We also evaluated the angle from which the maximum leakage of information takes place and referred it as "Eve's sweet spot angle". Data for channel attenuations from phantom and in-vivo experiments is also utilized to validate and observe the differences between simulations and experiments. This work will help in design of the communication module of implanted leadless cardiac pacemakers with enhanced security on the physical layer.**

Index Terms— **Physical layer security; Secrecy capacity; Leadless cardiac pacemakers; Privacy and Security, Implantable medical devices**

Manuscript received 31 May, 2019; Revised 25,Oct, 2019; Accepted 03,Dec, 2019. This work was supported by the EU's H2020 MSCA:ITN grant for the Wireless In-Body Environment (WiBEC) project with grant no: 675353 and "Research council of Norway project — Wireless In-Body Sensor and Actuator Networks - WINNOW — with grant no. 270957/070. *(Corresponding author: Muhammad Faheem Awan.)*

Muhammad Faheem Awan and Kimmo Kansanen are with the Department of Electronic Systems, Norwegian University of Science and Technology, Trondheim, 7491 Norway e-mail: faheem.awan@ntnu.no and kimmo.kansanen@ntnu.no

Ali Khaleghi and Ilangko Balasingham are with the Intervention Center, Oslo University Hospital, NO-0027 Oslo and with the Department of Electronic Systems, Norwegian University of Science and Technology, 7491 Trondheim, Norway (e-mail: ali.khaleghi@rr-research.no and ilangko.balasingham@medisin.uio.no.

Pritam Bose is with Intervention Center, Oslo University Hospital, NO-0027 Oslo, Norway (e-mail: pritam.bose@studmed.uio.no

I. Introduction

The technological advancements in personal health systems have led to the development of different wearable and implantable medical devices and systems. These developments also motivate transformation of decades old implantable medical devices (IMD's) such as cardiac pacemakers and implantable cardioverter defibrillators (ICDs).

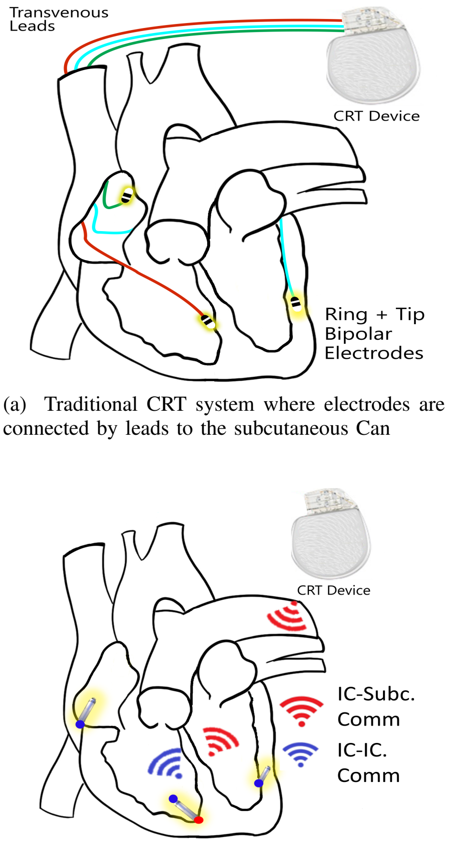
A. Cardiac Pacemakers

Pacemakers are medical devices that are implanted in patients with abnormal heart rhythms. About 1 million pacemakers are implanted annually worldwide [1]. Traditional pacemakers contain a subcutaneous implant (usually called "Can") implanted in the pectoral pocket below the shoulder. The Can is connected to the transvenous wires or 'leads' that pierce into, and run down, the subclavian vein where they are fixed to the inner walls of the heart. These leads contain electrodes to the distal ends that sense irregularities and provides electric excitation to maintain proper heart rhythm. Depending on the specific cardio-pathology, the electrodes can lie in the right ventricle, right atrium or in the coronary sinus above the left ventricle [2] . The transvenous leads are considered to be the weak side of a traditional pacemaker system because they can fracture, they may lead to infection, and also their explantation carries significant risk of mortality [3], [4]. Consequently, the next generation of these pacemaker systems is becoming wireless by getting rid of transvenous leads. Fig. 1 shows the traditional cardiac re-synchronization therapy (CRT) management system and one of the variant of next generation pacemaker system, hosting battery driven, physically small leadless capsules that may be placed in multiple heart chambers and being able to communicate with a subcutaneous implant wirelessly which can relay data to an external monitor[1]. These capsules need to be computationally less complex and consume less power than the traditional pacemakers. Besides unquestionable benefits, the wireless communication expose the leadless cardiac pacemaker (LCP) to the potential eavesdroppers compromising privacy, confidentiality and most importantly patient safety.

B. Motivation and Background

The comprehensive survey on privacy and security issues related to IMD's is provided in [5]. Similarly, [6] discusses

[1] EU Horizon 2020 Project WiBEC "Wireless In Body Environment.



(a) Traditional CRT system where electrodes are connected by leads to the subcutaneous Can

(b) Next generation multi-nodal leadless CRT system. IC-IC represents Intra-cardiac to Intra-cardiac communication, whereas IC-Subc, represents Intra-cardiac to Subcutaneous communication

Fig. 1: Comparison between traditional (a) and a variant (b) of the next generation CRT systems.

the challenges, goals, and need of securing IMD's. In order to show the security concerns, Halperin et al. in [7] performed eavesdropping attacks on an insecure communication link of ICD device to obtain the patient's data, using an off the shelf programmer, directional antennas and software defined radio. This work was followed by a number of scientific publications [8]–[11] to address the security concerns of IMD's.

Traditionally, the wireless communication networks are secured by conventional cryptographic methods at the upper layers of communication paradigm. However numerous challenges arise in key establishment and distribution for newly evolved paradigms like wireless in-body networks. Lately, physical layer security (PLS) has been identified as a feasible alternative to secure wireless transmissions via exploiting different characteristics of wireless channels [12]–[14]. The concept of PLS was first presented by Shannon [15] in 1949 which was further extended by Wyner in [16] with introduction to wire-tap channel. Csiszar et al. [17] broaden the idea by presenting the transmission of confidential messages over broadcast channels. These works demonstrated the benefits of using different secure transmission techniques at physical layer.

The approaches to achieve physical layer security can exist either as keyless or key based usually referred to as channel model and source model approaches respectively. Using the source model approach, the legitimate nodes utilize the correlated randomness of different wireless channel characteristics e.g. received signal strength (RSS), channel impulse response, phase, angle of arrival (AoA) or human biometrics in case of wireless body area network (WBAN) [18]–[22]. A comprehensive survey is provided in [23].

In contrast to the source model approach, the keyless approach or channel model approach, information theoretically secure the transmissions by utilizing the physical medium (channel fluctuations, attenuations, and noises), and make use of the channel difference between legitimate receiver and eavesdropper to benefit the legitimate party. Different methods are proposed in the literature to secure standard wireless network transmissions using channel model approach with focus to degrade the Eve channel by making it noisier than legitimate channel. It can be achieved by using cooperative jamming, with external helpers, relays, full duplex receiver with multiple antennas or adding the artificial noise. Biao et al. in [24] secure the single antenna systems by introducing artificial noise. Similarly, in [25], different theoretical limits for practical design of PLS jamming in standard wireless networks are presented with introduction to transmit and receive jamming whereas [26], [27] explores different secrecy rate optimization techniques for multicast networks. A comprehensive survey on PLS channel model approaches is provided in [28], [29].

The key performance metric in channel model approaches is secrecy capacity, playing a central role in PLS. It characterizes the fundamental limit on secure communications over noisy channels and is mainly associated to a channel model referred as wire-tap channel. Secrecy capacity captures the maximum transmission rate *(R)* that can be achieved ensuring the reliability, and by considering the extreme case of no information leakage to eavesdropper. In contrast to capacity of a link which is a communication rate for reliable communication, secrecy capacity reflects both reliability and confidentiality with a cost of reduction in communication rate. It is a system performance metric that characterizes the bound based on the channel characteristics. Once the design limits are known, one can choose among different wiretap codes[2] for transmission of confidential information without encryption[3].

The wireless in-body network e.g. Leadless cardiac pacemaker, with an eavesdropper outside, motivates a similar scenario of a wiretap model. This is because the human body being a lossy medium for electromagnetic propagation can inherently provide high attenuations to off body links. Thence, utilizing channel model approach of PLS in context of in-body networks could have substantial benefits that includes from avoiding the key management and distribution challenges to existing along with traditional cryptographic methods to provide an extra layer of security at the physical layer for sensitive applications like pacemakers. Furthermore, to the best of authors knowledge, none of the work exist in context of detail

[2] e.g LDPC, Polar wiretap codes

[3] We do not delve in detail of encoding and decoding of wiretap coding, and kept the information theoretic part to as minimum as possible

evaluation of the secrecy capacity for in-body wireless sensors network where one can utilize the naturally available wiretap channel between in-body and off-body nodes (eavesdropper) to provide secrecy on the physical layer.

To reap the aforementioned benefits of channel model approach of PLS, the feasibility analysis of securing next generation leadless cardiac pacemaker has been explored. This is done by considering the wiretap scenario of Wyner's model, and modeling the legitimate and eavesdropper channel, using electromagnetic (EM) simulations, phantoms and in-vivo experiments. Considerable literature exists on channel modeling of WBAN. Sayrafian et. el. in [30] proposes a statistical path loss model for implant to implant communication, considering different in-body scenarios. Similarly, Antonietta et. al in [31] characterizes in-body to off-body link in medical implant communication systems (MICS) band for upper limb prostheses using electromagnetic simulations. Concepcion, et al in [32] discuss different approaches for propagation analysis in an ultrawide (UWB) frequency band. Similarly, earlier works [33], [34], based on EM simulations examines different antennas for implanted and on-body communication systems in industrial scientific and medical (ISM) and MICS frequency band. A comprehensive review on different propagation models, frequency bands, and communication scenarios is provided in [35] whereas [36] provides a review on human body communication as an alternative for communication between body area network nodes.

The channel modeling methods of this work introduces different forefronts over existing models. The EM simulations performed in this work considers the highly detail human model (Hugo model) and are specifically application based (Cardiac pacemakers). Furthermore, for experiments, a small battery powered antenna with transmitter is utilized instead of using conventional coaxial cables and vector network analyzer (VNA) for generation of sounding signal. This is because, in case of small dimensions of antenna, the adjoined coaxial cables also radiate which is being ignored by authors in the literature [37]. Another aspect of this work is that it evaluates the in-body to off-body link (Eve link) directly from deep implant (inside the right ventricle) and computes the channel attenuation of entire space around the body.

In this work, simulations and tests are performed in the ISM frequency band (2.4 GHz). The selection of ISM frequency band is done due to smaller antenna dimensions with good radiation efficacy and matching [38]. In addition, Federal Communications Commission (FCC) also includes ISM 2.36-2.40 GHz spectrum in medical device communication (MedRadio) for body area networks [39].

C. Contributions

To the best of authors knowledge, this work is the first to explore channel model approach of PLS methods for in-body wireless networks with an application of next generation leadless cardiac pacemaker. A popular three-node model is considered, where the legitimate node, Alice (Leadless pacemaker/capsule, A) in the right ventricle of a human heart is communicating with Bob (Subcutaneous implant, B). In contrast to considering Eve at a certain specific position as usually done in literature for free space wireless networks, in this work Eve is considered to be located anywhere at any angle in three dimensional space around the body and her location can be presented using spherical coordinates (r, θ, ϕ) — r is the radius, θ is the elevation angle and ϕ is the azimuth angle. The key contributions in the paper are:

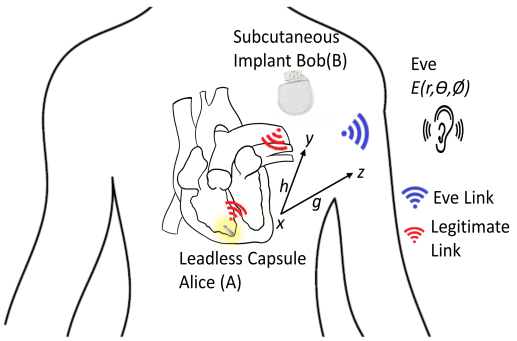


Fig. 2: Leadless capsule (Alice) communicating confidential message "X" through the in-body channel with a subcutaneous implant (Bob), and Eve, eavesdropping the communication through a channel which is a combination of in-body and free space

- Characterization of the Alice-Bob (AB) and Alice-Eve (AE) channels by numerical electromagnetic (EM) simulations using a detailed computational human model (HUGO Model), a phantom and in-vivo experiments.
- EM-Simulation based evaluation of secrecy capacity of the entire space around the body, first by defining a spherical grid for Eve at a radius of 1 m, then using the free space path loss model to extrapolate it over the entire space for different radial distances.
- EM-Simulation based evaluation of secure and in-secure volume around the body by considering the cardiac application based fixed secure transmission rate. The in-secure volume consists of all Eve's positions from which the leadless capsule can be eavesdropped.
- Worst-case analysis of secrecy capacity by considering eavesdropper at a sweet spot angle — the angle with maximum information leakage.
- For validation and comparison of EM-simulation results, the phantom and in-vivo experiments are also performed.

The paper is structured as follows. Section II provides System model and methodology whereas Section III, contains the results. Section IV discuses the results and finally Section V concludes the paper.

II. System Model and Methodology

In Fig. 2, a future LCP is depicted where Alice communicates with a subcutaneous implant Bob and Eve, outside the body, tries to eavesdrop the communication. Alice is located in the right ventricle (RV) of the heart whereas Bob is placed in the subcutaneous space under the shoulder. Eve is not assumed to be in any specific position and can be located anywhere, at any angle around the body in three-dimensional space presented in the spherical coordinate system.

Alice transmits a confidential message X to Bob. Thus, for a single channel realization, the input-output relation between Alice-Bob (AB) and Alice-Eve (AE) can be expressed as

$$\begin{aligned} y &= hx + n_1 \\ z &= gx + n_2, \end{aligned} \tag{1}$$

where x is the transmitted signal, y is the channel output to the Bob and z is the channel output to the Eve. The channel coefficients between Alice and Bob and Alice and Eve are represented by h and g where n_1 and n_2 are the complex Gaussian noises with mean μ and variance σ^2 and can be represented as $\mathcal{CN}(0,\sigma^2)$. We assume that x, n_1, and n_2 are stochastically independent. The signal to noise (SNR) ratio at Bob and Eve can be expressed as

$$\gamma_b = \frac{|h_{(x,y)}|^2 P}{\sigma^2}, \tag{2}$$

$$\gamma_e = \frac{|g_{(r,\theta,\phi)}|^2 P}{\sigma^2}, \tag{3}$$

where, $|h_{(x,y)}|^2$ and $|g_{(r,\theta,\phi)}|^2$ are the respective channel attenuations by considering Bob at position *(x,y)* and Eve at (r,θ,ϕ) respectively. Eve could have higher SNR outside the body at some respective angles than AB channel, even at larger distances. This is because the body provides more loss to EM radiations than free space. Thus, at some specific angles, the transmission path encounters more non-homogeneous medium (less in-body than free space) causing the power received outside the body to be higher. Therefore, our system model can be considered as a non-degraded version of Gaussian wiretap channel, in which the AE channel can have better SNR than the AB channel. In order to transmit securely between Alice and Bob, the secrecy capacity for non-degraded Gaussian wiretap channel [17], [40] can be expressed as

$$C_S = \begin{cases} [C_B - C_E]^+, & \text{if } \gamma_b > \gamma_e \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where C_B and C_E are the channel capacities of AB and AE link which can be expressed as

$$\begin{aligned} C_B &= \log_2(1+\gamma_b) \\ C_E &= \log_2(1+\gamma_e). \end{aligned} \tag{5}$$

The resultant secrecy capacity by considering eavesdropper at any direction around the body can be expressed as

$$C_S(r,\theta,\phi) = \begin{cases} \left[\log_2 \frac{\left(1+\frac{|h_{(x,y)}|^2 P}{\sigma^2}\right)}{\left(1+\frac{|g_{(r,\theta,\phi)}|^2 P}{\sigma^2}\right)}\right]^+ & , |h_{x,y}|^2 < |g_{r,\theta,\phi}|^2 \\ 0, & \text{Otherwise} \end{cases} \tag{6}$$

After evaluating the secrecy capacity of all the AB-AE link channel attenuations in the entire space, we divide the space around the body into secure and in-secure volumes. For fixed AB attenuation and communication rate, we solve for all the AE attenuations that lie in the secure and in-secure volumes. The in-secure volume defines all the Eve distances from which LCP can be eavesdropped, and can be expressed as

$$d_{E_{(r,\theta,\phi)}} \leqslant r \times 10^{\left(\frac{P-\beta-10\log_{10}(2^{(C_B-C_S)}-1))-\sigma^2}{10n}\right)}. \quad \forall\ (r,\theta,\phi) \tag{7}$$

The derivation of (7) is provided in Appendix I for simplicity.

For a given power, AB attenuation and secrecy rate, (7) holds for all (r,θ,ϕ). Beyond the in-secure volume, communication is considered to be secure for a given secrecy rate. In (7), $d_{E_{(r,\theta,\phi)}}$ is the eavesdropper distance at a specific angle from Alice, C_B is the capacity of the AB link, C_S is the fixed secrecy rate for communication, r is the reference eavesdropper distance and is equal to 1 m, σ^2 is the noise power and β is the Eve channel attenuation at the reference eavesdropper distance.

The secrecy capacity depends on AB and AE channel attenuations as shown in (6) and (7).Thus, we simulate the in-body environment to evaluate the respective channel attenuations. To validate the EM-simulation results, experimental tests are also performed. This helps in assessing the differences and similarities between results from simulations and experimentation[4]. In addition, the experiments can also help validate whether the EM simulations in CST can efficiently predict the channel losses or not. Thus for channel modeling, EM simulations are presented first, followed by phantom and in-vivo experiments.

A. Electromagnetic (EM) Simulations

For estimating channel attenuations, EM simulations are performed by using the 3D EM simulation tool CST[5] [41]. This work utilizes the anatomical data set of the Visible Human Project [42], [43], from which the developed voxel model in CST is referred as HUGO model. The HUGO model is developed from a dissected male corpse that is segmented into multiple layers. These layers are then sampled and interpolated to provide a highly efficient computational model of the human body. The dielectric properties of each individual biological tissue have been considered in the model. The model offers different tissues and resolutions (1 mm to 8 mm) to select. Due to shorter wavelengths in 2.4 GHz, in this work, we opted for a resolution of 1 × 1 mm^2. The communication element, the capsule (Alice), is modeled as an ideal dipole antenna with 100 % efficiency. The antenna is 5 mm in length and 2 mm in diameter. The antenna is encapsulated inside a vacuum tube of 1 mm in width to avoid the direct contact with body tissues.

1) Legitimate/AB-link: The AB link is simulated by placing a capsule (dipole antenna, Alice) in the right ventricle (RV) of the heart along with the placement of other dipole antennas (Bobs) in the subcutaneous space as shown in Fig. 3. The subcutaneous space is the space under the skin beneath the shoulder. In addition, to observe the effect of antenna polarization on channel attenuation ($|h_{(x,y)}|^2$), two set of experiments are conducted, one by placing the dipole antenna in the horizontal direction (transverse plane) and the other in

[4] We concentrate only on antennas, not the entire TX/RX communication chain

[5] https://www.cst.com/

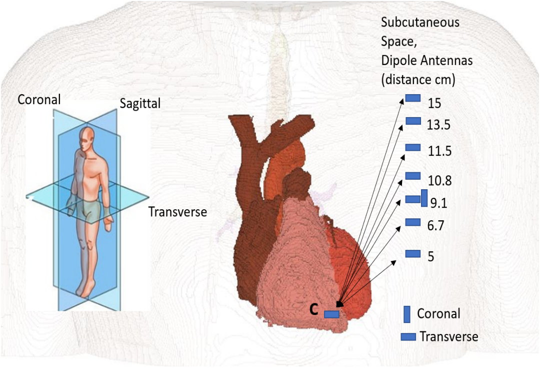


Fig. 3: Position of the leadless capsule (Alice) in the right ventricle, transmitting to the antenna (Bob) positioned at different distances in subcutaneous space. Reference representation of coronal, sagittal and transverse planes with respect to the human body

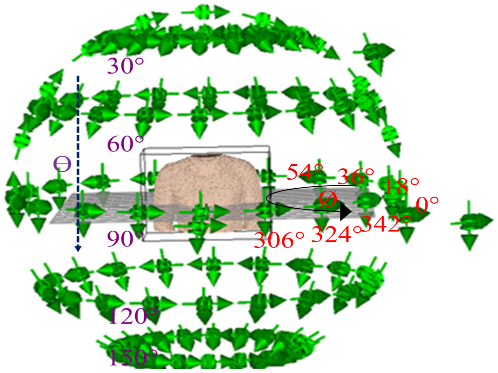


Fig. 5: Placement of electric probes around the body to receive electric field intensity. In total 100 electric probes are placed at a radius of 1 m, 20 probes along azimuth angle (ϕ), 18° apart and 5 elevation angles (θ) with 30° apart. The left arm is considered as 0° for azimuth angle and then rotated anticlockwise. Couple of probes are outside the sphere at a radius of 2 m

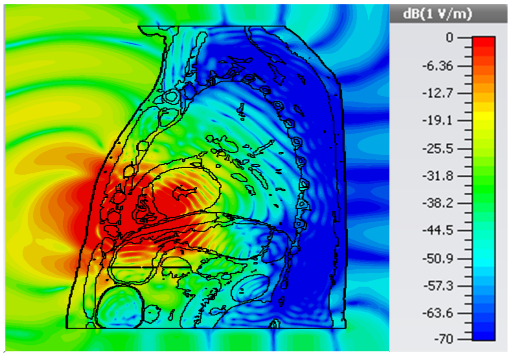


Fig. 4: Radiation of electric field strength, by placing the dipole antenna inside the right ventricle. The bar shows the field intensity (V/m), in and around the body. (Side view)

vertical direction (coronal plane). First, all the antennas are placed in the transverse plane to determine the attenuation between Alice and Bob. Then, the receiving antenna at one of the subcutaneous position is changed from transverse to coronal plane and the difference in the attenuation is observed. The results with EM simulations contain both the observations.

2) Eavesdropper/AE-link: The electromagnetic radiations from the Alice radiate in all directions outside the body as shown in Fig. 4. We place in a total of 100 electric probes in three-dimensional space around the body with a sphere of radius 1 m. The entire sphere is partitioned in five elevation angles (θ), each of which is further partitioned into twenty azimuth angles (ϕ) (Fig. 5), totaling a spherical grid of 100 Eve positions to observe the field strength. Couple of electric probes are also positioned at large radial distances in order to verify the applicability of the free space path loss model. This helps in extrapolating the spherical grid to different radial distances. The electric probes are used because by placing dipole antennas outside the body at the distance of 1 m, results in a very huge mesh size to resolve. Therefore, due to the extensive computational cost of using dipole antennas, electric probes are used to determine the electric field intensity which is then transformed to the power density using

$$S(r,\theta,\phi) = \frac{1}{2}\frac{|E(r,\theta,\phi)|^2}{Z_o}, \tag{8}$$

where S is the received power density (W/m^2) at each probe, E is the received electric field and Z_o is the intrinsic impedance of free space. The total power received at each probe depends upon the effective aperture of an antenna and can be expressed as

$$P(r,\theta,\phi) = S(r,\theta,\phi) \times A_{eff}, \tag{9}$$

where $P(r,\theta,\phi)$ is the total power received, S is the power density and A_{eff} is the effective aperture of the antenna. From received power, the Eve channel attenuation $(|g_{(r,\theta,\phi)}|^2)$ is evaluated. The AE-link attenuation can be expressed as

$$\beta = |g_{(r,\theta,\phi)}|^2_{dB} = P - P(r,\theta,\phi), \qquad \forall\ (\theta,\phi) \tag{10}$$

where r is the reference distance of 1 m, θ and ϕ are reference angles in the spherical coordinates, and P is the transmit power which for simplicity is considered as 0 dBm. In order to extrapolate the path loss over the entire space for different radial distances, the free space path loss model is utilized which can be expressed as

$$PL_{r,\theta,\phi}(d_E) = \beta + 10 \times n \times \log_{10}\left(\frac{d_E}{r}\right), \tag{11}$$

where, n is the free space path loss exponent with a value of 2. d_E is the distance to extrapolate beyond 1 m with the reference β, evaluated using (10) from the EM simulations.

B. Phantom Experiment

The methodology used in the phantom experiments is adapted to corroborate the results obtained from simulations. It also helps to observe the differences by implementing the setup in practical scenarios using realistic antennas. To evaluate channel attenuations, the phantom with dielectric

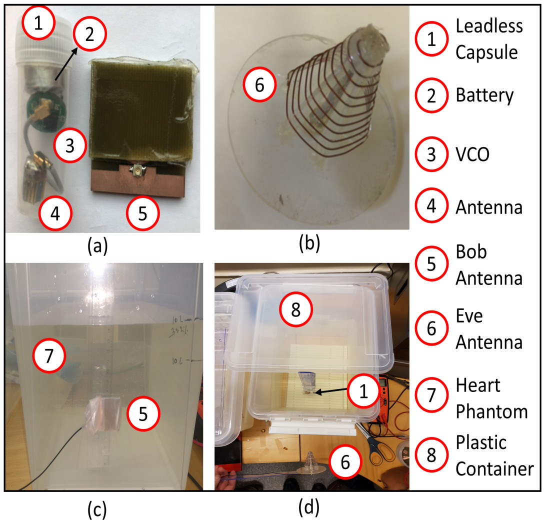


Fig. 6: Phantom experiment setup (a) Legitimate link antennas (Alice and Bob) (b) Eve antenna (c) legitimate link setup (d) Eve link setup

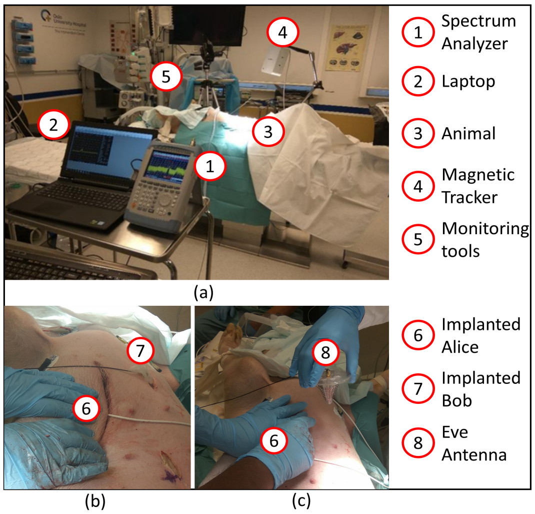


Fig. 7: In-vivo experiment setup (a) Operating room (b) Legitimate link (c) Eve link

properties of the human heart was developed. The phantom was prepared using 39.2 % of sucrose in water, provided in [44]. The transmitter antenna (Alice) was a 1 mm in radius meander-shaped, connected to voltage control oscillator (VCO). VCO generates a sinusoidal signal at 2.4 GHz and operates on a button cell. The antenna, VCO and cell battery were encapsulated by a small plastic container to avoid direct contact with the phantom. Subcutaneous antenna (Bob) was a wideband patch antenna with dimensions of 3×3 cm^2. These two antennas replicate the AB link. Similarly, an off-body circular polarized spiral antenna is utilized to replicate the Eve. Fig. 6 shows the container with liquid phantom, antennas placement and antennas itself. More details on antennas can be found in [38].

1) Legitimate/AB-link: Fig. 6a shows the AB link antennas and Fig. 6c shows the setup for AB link where the leadless capsule was implanted inside the phantom filled container with the help of a ruler and the subcutaneous antenna was mounted on a wall of the container.

2) Eavesdropper/AE-link: Fig. 6b shows the eavesdropper antenna whereas Fig. 6d shows the AE link. The leadless cardiac pacemaker (LCP/capsule) was fixed inside the phantom with a ruler at a depth of 10 cm, and the Eve antenna attached with another ruler was moved to different positions outside the container.

C. In-vivo Experiment

The animal experiment was carried out in an operating room at the Intervention Center, Oslo University Hospital, Oslo, Norway, which is qualified to perform such procedures. All the experiments were performed according to ethical standards and regulations provided by the responsible agencies. The experiment was performed on a female pig weighing about 61 Kg. Fig. 7a shows the operating room along with the pig, which had been given general anesthesia for the experiment. We did not take into account the posture change of the animal during the experiments that might effect the antenna coupling. However, we believe that to some extent the coupling effects have been compensated by changing the antenna positions. Similar set of antennas were used in in-vivo experiments, as described in section II-B.

1) Legitimate/AB-Link: An antenna (Alice) within a plastic container was placed behind the right ventricle of a pig heart whereas subcutaneous antenna (Bob) was positioned under the skin below shoulder as shown in Fig. 7b. An electromagnetic distance measurement system, *Medical Aurora by NDI Medical, Canada*, was used to evaluate the distance between transmitting and receiving antenna. We moved the in-body antenna at different positions (in mm) within the subcutaneous space and took multiple measurements around the same distance which was averaged to minimize the measurement errors.

2) Eavesdropper/AE-Link: For AE link, the Alice was placed at the same position as in case of AB link, and the Eve antenna was held outside the pig body as shown in Fig. 7c. The Eve antenna coupling was evaluated across different angles over the chest of the animal, and later considered the best-case scenario for an Eve (worst case for a pacemaker).

III. Results

This section focuses on results based on the system methodology. First, we present the channel measurements using EM simulations in CST. We evaluate the legitimate link channel attenuation and the attenuation of each eavesdropper position on the spherical grid from the leadless capsule in the RV. Afterwards, the distance of the legitimate link is fixed and the secrecy capacity of the defined spherical grid at a radial distance of 1 m is evaluated. In order to cover the entire space around the body, path loss model for free space is utilized to extrapolate the secrecy capacity. Moreover, the results for the in-secure volume are presented by fixing the cardiac application based secrecy rate. The results are concluded by presenting the phantom and in-vivo results.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBME.2019.2958748, IEEE Transactions on Biomedical Engineering

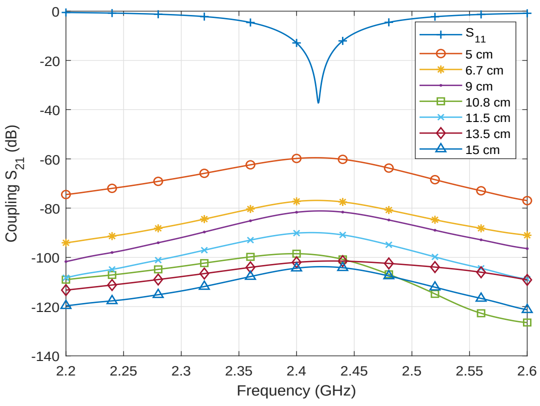


Fig. 8: Antennas coupling. Alice is in RV whereas Bob is place at different positions in the subcutaneous space. The S_{11} around 2.4 GHz, shows the efficient matching between antennas.

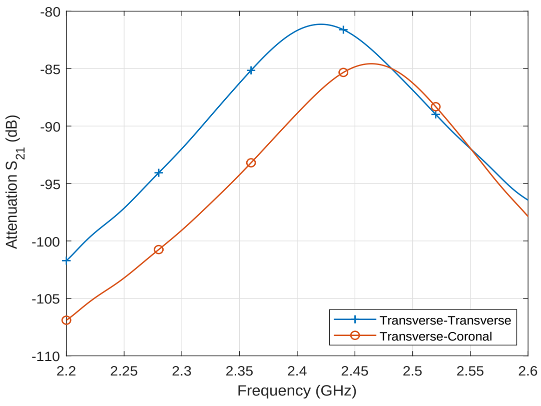


Fig. 10: The difference in the coupling between antennas by changing the direction of the antenna from Transverse to Coronal plane

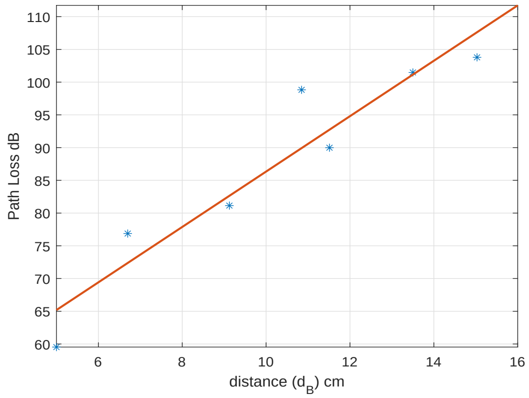


Fig. 9: AB link path loss model w.r.t subcutaneous distance (Bob distance)

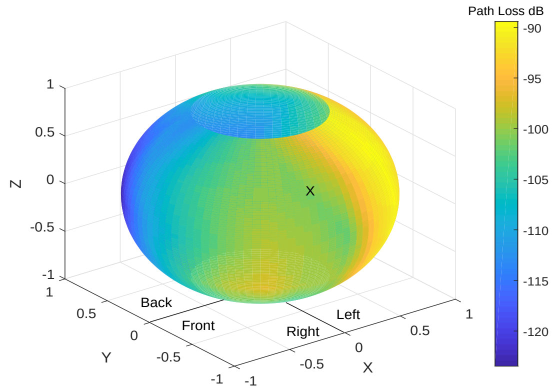


Fig. 11: Channel attenuation between Alice and Eve in 3d Sphere with a radius of 1 m. The axis is converted from spherical coordinates into Cartesian coordinates. Front represents the frontal side of the human body. The cross (X) represents the approximate heart position inside the sphere

A. EM simulation results

1) Legitimate/AB-link: Fig. 8 shows the channel attenuation between an antenna in the right ventricle and the antennas in the subcutaneous space. The antennas (transmitter and receiver antennas) are matched at 2.42 GHz represented as S_{11} and is shown in Fig. 8. Fig. 9 shows the extracted path loss model where dots represents the attenuation at a respective distance from Alice and the straight line shows the linear fitted model which can be expressed as

$$PL(d_B) = P_1 \times d_B + P_2, \tag{12}$$

where P_2 = -44.03 dB, P_1 = -4.231 dB/cm and d_B is the distance in cm between Alice and Bob. This path loss is valid for the distance between 5 cm $\leq d_B \leq$ 16 cm. As mentioned earlier, $|h_{(x,y)}|^2$ is the AB link attenuation in linear scale, thus in dB scale, it can be expressed as

$$\alpha = |h_{(x,y)}|^2_{dB} = PL(d_B). \tag{13}$$

The extracted path loss model for the AB link is obtained by placing the antennas (in the right ventricle and the subcutaneous space) in the transverse plane. Aforementioned, to observe the effects of the antenna polarization, simulation is also performed by placing the antenna in the coronal plane. Fig. 10 shows the difference observed in the attenuation by changing the direction of the antenna at the distance of 9.1 cm from the transverse plane to the coronal plane. It has been observed that the attenuation is increased by 3 dB due to polarization mismatch. Thus, placing the antennas in the transverse plane is efficient and results in less attenuation between antennas as compared to the coronal plane. The channel attenuations are comparable to the results presented in [45], [46] with slightly higher values of attenuation due to the use of a highly accurate Hugo model for transmission through heterogeneous medium.

2) Eavesdropper/AE-link: The attenuation determined at each electric probe after conversion from E-field using (9) is expressed in three-dimensional space around the body in Fig. 11. It has been observed that at $\theta = 60°, \phi = 306°$, the eavesdropper has the minimum attenuation with the leadless capsule and is considered as the Eve sweet spot angle. To

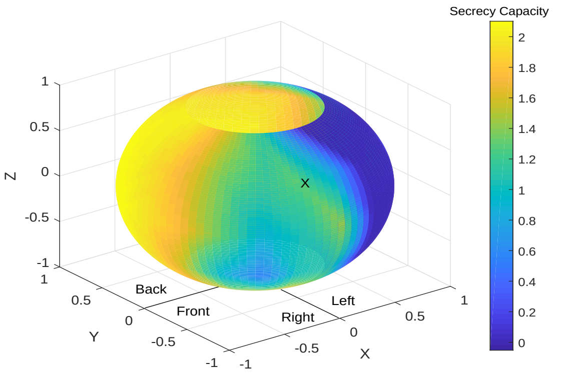


Fig. 12: Secrecy capacity across all the spatial positions surrounding the body at a distance of 1 m. The axis is converted from spherical coordinates into Cartesian coordinates. Front represents the frontal side of the human body. The cross (X) represents the approximate heart position inside the sphere

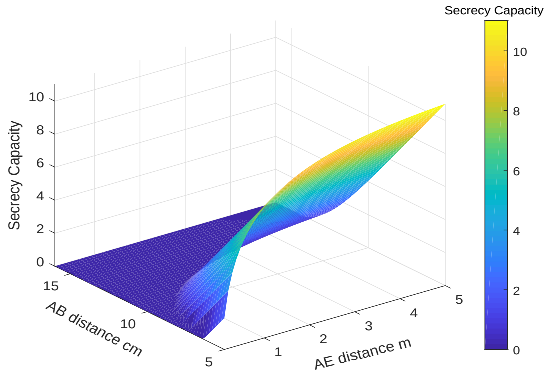


Fig. 13: Secrecy capacity with variation in both AB and AE distance, for eavesdropper at sweet spot angle ($\theta = 60°, \phi = 306°$)

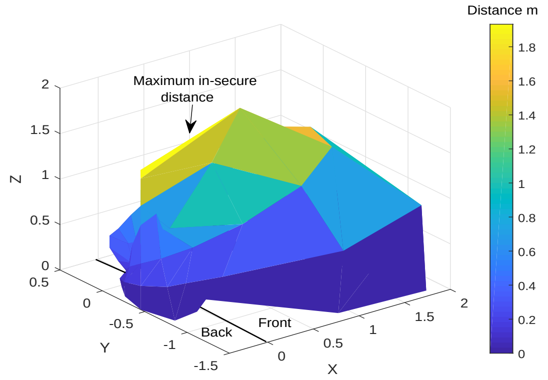


Fig. 14: Boundary of in-secure volume around the body for fixed secrecy rate of 0.5 bpcs/Hz

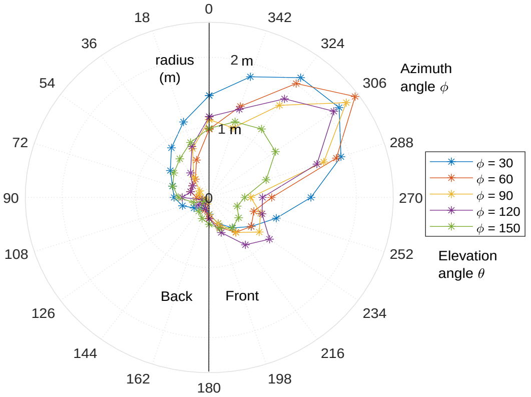


Fig. 15: 2-D representation of in-secure volume around body for fixed secrecy rate of 0.5 bpcs/Hz

observe the difference in the AE link attenuation by changing the orientation of the antenna from transverse to the coronal plane, we change the orientation of the leadless capsule inside the right ventricle. As the transmitting antenna is very small in size, thus changing the orientation doesn't effect the attenuation values at larger distances (1 m).

3) Secrecy Capacity: For evaluation of the secrecy capacity, AB link distance of 12 cm is fixed. Using (6), Fig. 12 shows the secrecy capacity of a spherical grid at the radial distance of 1 m around the body. It has been observed that most of the sphere has positive secrecy capacity except the low attenuation eavesdropping angles (17 out of 100). Thus, to find the distance where the secrecy capacity is positive across all Eve angles, the secrecy capacity of the spherical grid is computed with the radial distance of 2 m by using (11). It has been found that at the distance of 2 m, the positive secrecy capacity is observed over the entire spherical grid.

The variation in secrecy capacity is also viewed by changing both the AB and AE link distance. For the AE link, Eve is considered at the "sweet spot angle". Fig. 13 shows the resultant secrecy capacity, where x-axis is AE distance and varies from 0.12 – 5 m, y-axis is the AB distance and varies from 5 – 16 cm and z-axis is the resultant secrecy capacity. The movement of Eve, away from the legitimate nodes results in higher secrecy capacity.

4) In-Secure Volume: The in-secure volume is the volume that contains all the Eve positions from which the leadless pacemaker can be eavesdropped and is expressed in (7). Equation (7) provides the minimum Eve distance required across different angles in order to achieve the fixed communication secrecy rate. The pacemaker usually requires the transmission rate of approximately 100 kbps in order to transmit the cardiac parameters (ECG, pulse rate, respiratory rate, blood pressure, etc.) [47]. Thus, we fix the secrecy rate to 0.5 bpcs/Hz (bits per complex symbol), which for the bandwidth of 1 MHz is around 250 kbps. Similarly, the AB distance is fixed to 12 cm and the minimum Eve distance required to support the secure communication rate is evaluated across all the angles. Fig. 14 shows the in-secure volume around the body. The volume is uneven because the attenuation values across different angles through the body provides different secrecy capacity. For more visual clarity the same information is provided in 2-dimensional space in Fig. 15. Thus, to transmit 0.5 bpcs/Hz securely with transmit power of 0 dBm, the Eve at the "sweet spot angle" (worst case scenario for the pacemaker) with receiver [6] sensitivity of -100 dBm should be at a distance of 2.5 m or beyond. The boundary of the in-secure volume is considerably less for other angles e.g at $\theta = 150°, \phi =$306°, the insecure volume stretches till 1.1 m. Regarding the back side of the human body, the boundary of the in-secure volume stretches till 1 m for the worst case representing the distance from RV of the human heart. The worst case angle to the back side is $\theta = 30°$, $\phi = 18°$. It is worth mentioning that the implanted nodes generally transmit with power ranging between -16 – -27 dBm due to which the in-secure volume at Eve sweet spot angle will be reduced. e.g for the transmit power of -16 dBm, the in-secure distance at Eve sweet spot angle reduces from 2.5 m to 2.1 m.

5) Worst-Case Analysis: In order to observe variation in the Eve distance with respect to the secrecy rate, we evaluate a bound on the minimum and the maximum Eve distance for a certain fixed AB distance. The analysis is done by considering Eve at the "sweet spot angle" or the worst case scenario for the pacemaker. When the secrecy rate approaches to zero, the Eve distance can be expressed as

$$\lim_{C_S \to 0} d_E(C_S) = r \times 10^{\frac{P_1 \times d_B + P_2 - \beta}{10 \times n}}, \tag{14}$$

where P_1 and P_2 are constants (see (12)), r is the reference Eve distance (1 m), d_B is the AB distance and β is the eavesdropper reference attenuation at the "sweet spot angle". As C_S approaches to zero, this means AB and AE link have the same capacity, which apparently represents the same distance [7]. This could be true for free space wireless channels with homogeneous loss. But for the in-body networks where the eavesdropper is outside the body and legitimate receiver (Bob) is inside the body, we could have less attenuation at some angles around the body at Eve than that of the Bob. This is because of higher in-body loss than free space. Thus, the transmission path to the eavesdropper may encounter less in-body portion and larger free space portion resulting in a non-homogeneous loss. The Eve at the "sweet spot angle", should be at a distance of 1.872 m for the secrecy capacity to be positive.

Similarly, when the secrecy rate approaches to the AB link capacity C_B, then the Eve distance approaches to infinity and can be expressed as

$$\lim_{C_S \to C_B} d_E(C_S) \to \infty. \tag{15}$$

Fig. 16 shows the minimum and maximum Eve distance with variation in secrecy capacity as a fraction of the legitimate (AB) link capacity.

B. Phantom Experiment Results

This section focuses on providing the secrecy capacity using path loss models developed from the phantom experiments in order to evaluate the AB and AE channel attenuations. The pathloss models has also been reported in earlier work [48]. We use directional antennas as mentioned in section II-B.

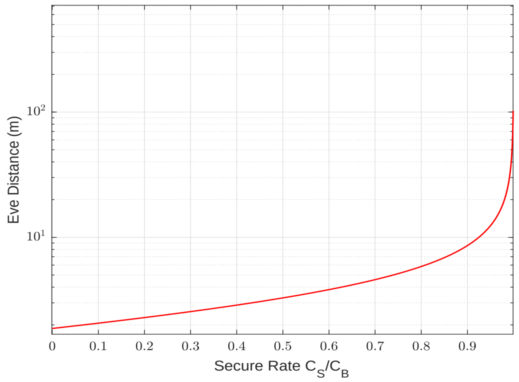


Fig. 16: Minimum and maximum eavesdropper distance at Eve sweet spot angle for pacemaker worst-case analysis

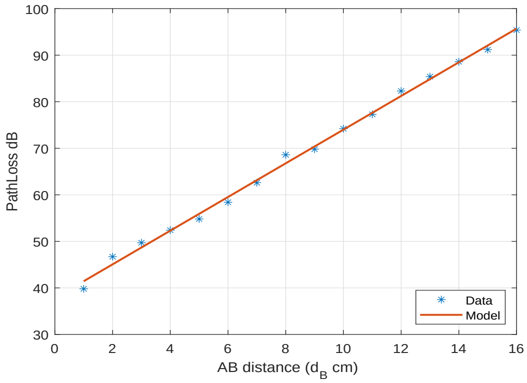


Fig. 17: Phantom Experiment: AB link attenuation and path loss model

For phantom experiments, we didn't consider different spatial positions for the eavesdropper. Albeit, we evaluate the secrecy capacity by considering Eve at the sweet spot angle (worst case scenario for a pacemaker).

1) legitimate/AB-link: In case of AB link, the implanted antenna (capsule) was moved in the distance range of 1 cm to 16 cm from subcutaneous antenna and the corresponding received power was measured via spectrum analyzer connected to the subcutaneous antenna. Fig. 17 shows the measured values along with the fitted model. The AB link path loss follows a linear model and can be expressed as

$$PL(d_B) = P_1 \times d_B + P_2, \tag{16}$$

where P_1 = -3.618 dB/cm, P_2 = -37.82 dB and d_B is the AB distance. The path loss model is valid for 1 cm $\leq d_B \leq$ 16 cm.

2) Eavesdropper/AE-link: The AE link path loss model is shown in Fig. 18, where dots represent the measured values and line shows the fitted model which can be expressed as

$$PL(d_E) = PL(d_o) + 10 \times n \times \log_{10}\left(\frac{d_E}{d_o}\right), \tag{17}$$

where $PL(d_o)$ = 68.4 dB is the path loss at a reference distance of 11 cm (10 cm implant depth + 1 cm from the

[6] 0 dBi antenna gain

[7] If only the attenuation with distance is considered as a variation parameter for homogeneous loss

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBME.2019.2958748, IEEE Transactions on Biomedical Engineering

TABLE I: Summary of Simulation and experimental measurements for eavesdropper distance

Parameters	C_S = 0 bpcs/Hz				C_S= 0.5 bpcs/Hz		
	AB Distance	AE Distance			AE Distance		
		In-Body	From Body Surface	Total	In-Body	From Body Surface	Total
EM Simulations (Worst Case, Ideal Antenna)	12 cm			1.8 m			2.5 m
EM Simulations (Worst Case, Realized Antenna)	12 cm			13 cm			15 cm
Phantom Exp (Extrapolated)	12 cm	12 cm	2.5 cm	14.5 cm	12 cm	3.5 cm	15.5 cm
In-vivo Exp	12 cm	8 cm	4 cm	12 cm	8 cm	5 cm	13 cm

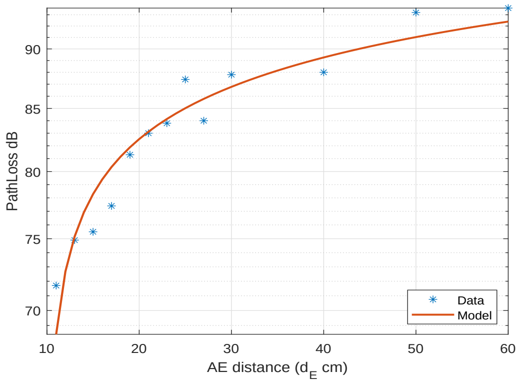


Fig. 18: Phantom Experiment: Eve link attenuation and path loss model

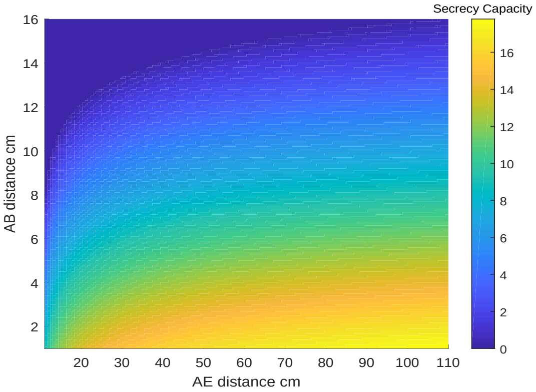


Fig. 19: Achievable secrecy rate from a phantom experiment

container surface), d_E is the Eve distance from the implant and n is the path loss exponent with a value of 1.411. The path loss model is validated only for a distance between 11 - 60 cm. After 60 cm free space path loss can be considered with n = 2.

3) Secrecy Capacity: The secrecy capacity for the phantom experiment is shown in Fig. 19. Considering the AB distance of 10 cm, and Eve at a distance of 16 cm from Alice, the secrecy rate is about 1.4 bpcs/Hz.

C. In-vivo Experiment Results

For AB link, the average attenuation found between an antenna (Alice) behind the RV and the subcutaneous antenna (Bob) at 12 cm was about -82.37 dB. Similarly, by holding the Eve antenna, 6 cm above the body surface (see Fig. 7c) with the in-body antenna depth of 8 cm, the attenuation measured was -86.20 dB. The secrecy capacity that can be achieved is 1.2 bpcs/Hz at the total Eve distance of 14 cm from Alice. Similarly, path loss model for free space is utilized to extrapolate the secrecy capacity for different Eve distances.

IV. Discussions

So far, the secrecy capacity is evaluated separately by adopting simulations and experiments, here the inter-correlation between results from different methodologies is discussed. Table I lists the summary of the results with corresponding Eve distance to achieve the secure communication rate by use of different evaluation methodologies. For EM simulations, if we consider worst case scenario for the pacemaker or the angle ($\theta = 60°$, $\phi = 306°$) where the leakage of information is maximum, the fixed secrecy rate of 0.5 bpcs/Hz is achievable at a distance of 2.5 m. In case of phantom and in-vivo experiments the same rate is achieved at 15.5- and 13 cm respectively. The experimental measurements have high correlation but differ from simulations. This is due to the use of different types of antennas for simulations and experiments. Simulations assume theoretical ideal antenna of small size with 100 % efficiency whereas in the practical scenario we can not realize such an ideal small antenna of size 5 mm (i.e. $\frac{\lambda}{25}$ (λ is the wavelength at 2.4 GHz)) due to the theoretical limitation of small antennas efficiency. Therefore lower antenna efficiency reduces the radiated power density in practical implementations compared to ideal simulations. The typical efficiency for such an antenna is about -10 – -15 dB. Thus the calculated secrecy capacity should be scaled to include the implant antenna effects. For conducting experiments, we have designed a meander antenna for the implant in which a capacitive coupling mechanism is applied [49] to provide high efficiency and impedance matching at 2.4 GHz. However, the efficiency (about -12 dB) results in the reception of low power outside the body compared to the ideal antenna in the simulation. If the ideal antenna is scaled with respect to a realized antenna, then the Eve distance to achieve the secrecy capacity of 0.5 bpcs/Hz is reduced from 2.5 m (250 cm) to about 15 cm $(10^{-1.2} \times 250)$, approximately same as computed in the experiments. Thus, the simulations and the experimentation results show similar Eve distance in order to achieve the same secrecy capacity if the efficiency drop in case of realized antennas is taken care off. Thus, by considering a patient personal space of 50 cm with a maximum leakage angle to the front, it will be difficult for an Eve to enter into the space without going un-noticed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBME.2019.2958748, IEEE Transactions on Biomedical Engineering

The evaluated secrecy communication rate reflects both confidentiality and reliability. To draw a theoretical comparison of reliability with the reference provided in IEEE 802.15 standard, the required SNR should be approx. 2 dB [50] for the BER of 10^{-3} in case of DBPSK[8] modulation scheme (commonly used for resource constrained devices [7]). The mentioned threshold SNR is achievable for legitimate link which for *R* of 250 kbps and bandwidth of 1 MHz is approx. 5 dB[9]. For AE link, after considering the realized antenna effects, the best case scenario of Eve at sweet spot angle has SNR of approx. 0 dB, which corresponds to BER of 10^{-1} and will be further degraded by use of channel coding, based on evaluated secrecy capacity.

The results of this work are promising and motivates to secure the next generation of leadless cardiac pacemaker via PLS methods. The results can also be utilized for other in-body sensor network applications. Nevertheless, PLS methods can be stacked with traditional cryptographic methods to provide extra layer of security at the physical layer to secure the sensitive application of a pacemaker.

V. Conclusion

In this work, we analyze the effectiveness of securing next generation leadless cardiac pacemaker using the channel model approach of PLS. The is done by evaluating the performance metric of secrecy capacity for a pacemaker implant inside the heart. The adopted methodology utilizes numerical electromagnetic simulations and the results are validated through measurements in phantom model and in-vivo experiments. From EM simulations, the angle where Eve has the minimum channel attenuation is found to the left from front, just above the heart and is termed as the “Eve sweet spot angle”. Eve sweet spot angle has the least secrecy capacity among all the eavesdropper spatial positions with human heart as the reference position. In addition, by fixing cardiac application based secrecy rate of 250 kbps, the in-secure volume is provided across different angles around the body. By considering an ideal antenna for EM simulations, the in-secure volume has a maximum distance of 2.5 m at Eve sweet spot angle for a transmit power of 0 dBm and receiver sensitivity of -100 dBm. However, by considering a realistic scenario with implant antenna effects, the secrecy distance reduces to 15 cm which is in correlation with the experimental measurements (Phantom and in-vivo).

[8] Differential binary phase shift keying

[9] SNR = $\frac{E_b}{N_o} \times \frac{R}{BW}$,($\frac{E_b}{N_o}$ is the energy per bit, R is rate, and BW is bandwidth)

Appendix I
Derivation for an in-secure volume

$$
\begin{aligned}
C_S &= C_B - C_E \\
\log_2(1 + \frac{PL_{r,\theta,\phi}(d_E)P_t}{\sigma^2}) &= C_B - C_S \\
\frac{PL_{r,\theta,\phi}(d_E)P_t}{\sigma^2} &= 2^{(C_B - C_S)} - 1 \\
P_t - PL_{r,\theta,\phi}(d_E) - \sigma^2 &= 10 \times \log_{10}(2^{(C_B - C_S)} - 1) \\
P_t - \left(\beta + 10n\log_{10}\left(\frac{d_E}{r}\right)\right) - \sigma^2 &= \\
&10 \times \log_{10}(2^{(C_B - C_S)} - 1) \\
d_{E_{(r,\theta,\phi)}} \leq r \times 10^{\left(\frac{P_t - \beta - 10\log_{10}(2^{(C_B - C_S)} - 1)) - \sigma^2}{10n}\right)}
\end{aligned}
$$

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, Aug, 2011.

[2] M. Albatat, J. Bergsland, H. Arevalo, H. Odland, P. Bose, P. Halvorsen, and I. Balasingham, “Technological and clinical challenges in lead placement for cardiac rhythm management devices,” *Annals of Biomedical Engineering*, pp. 1–21, Sept, 2019.

[3] R. E. Kirkfeldt, J. B. Johansen, E. A. Nohr, O. D. Jørgensen, and J. C. Nielsen, “Complications after cardiac implantable electronic device implantations: an analysis of a complete, nationwide cohort in denmark,” *European heart journal*, vol. 35, no. 18, pp. 1186–1194, Dec, 2013.

[4] 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, Nov, 2009.

[5] 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, Jun, 2015.

[6] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, “Security and privacy for implantable medical devices,” *IEEE pervasive computing*, vol. 7, no. 1, pp. 30–39, Jan, 2008.

[7] 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 *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, May, 2008, pp. 129–142.

[8] C.-S. Park, “Security mechanism based on hospital authentication server for secure application of implantable medical devices,” *BioMed research international*, vol. 2014, Jun, 2014.

[9] J. Astorga, J. C. Astorga, E. Jacob, N. Toledo, and M. Higuero, “Securing access to next generation ip-enabled pacemakers and icds using ladon,” *Journal of ambient intelligence and smart environments*, vol. 6, no. 2, pp. 157–177, Jan, 2014.

[10] M. Zhang, A. Raghunathan, and N. K. Jha, “Medmon: Securing medical devices through wireless monitoring and anomaly detection,” *IEEE Transactions on Biomedical circuits and Systems*, vol. 7, no. 6, pp. 871–881, Apr, 2013.

[11] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, “They can hear your heartbeats: non-invasive security for implantable medical devices,” in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, Aug, 2011, pp. 2–13.

[12] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. Crc Press, Apr, 2016.

[13] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: A tutorial,” *IEEE wireless Communications*, vol. 18, no. 2, pp. 66–74, Apr, 2011.

[14] Y. Liang, H. V. Poor, S. Shamai *et al.*, “Information theoretic security,” *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, Jun, 2009.

[15] C. E. Shannon, “Communication theory of secrecy systems,” *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, Oct, 1949.

[16] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, Oct, 1975.

[17] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, May, 1978.

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

[19] M. F. Awan, K. Kansanen, S. Perez-Simbor, C. Garcia-Pardo, S. Castelló-Palacios, and N. Cardona, "Rss-based secret key generation in wireless in-body networks," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, May, 2019, pp. 1–6.

[20] 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, Sep, 2016.

[21] S. Pirbhulal, H. Zhang, W. Wu, S. C. Mukhopadhyay, and Y.-T. Zhang, "Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks," *IEEE Transactions on Biomedical Engineering*, vol. 65, no. 12, pp. 2751–2759, Mar, 2018.

[22] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: algorithms and rate optimization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, Apr, 2016.

[23] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 332–341, Jan, 2015.

[24] B. He, Y. She, and V. K. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9577–9581, May, 2017.

[25] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, Dec, 2016.

[26] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a mimo secrecy channel with a multiple-antenna eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, Oct, 2013.

[27] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1417–1432, Aug, 2016.

[28] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Feb, 2014.

[29] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, May, 2008.

[30] K. Sayrafian-Pour, W.-B. Yang, J. Hagedorn, J. Terrill, and K. Y. Yazdandoost, "A statistical path loss model for medical implant communication channels," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, Sep, 2009, pp. 2995–2999.

[31] A. Stango, K. Y. Yazdandoost, F. Negro, and D. Farina, "Characterization of in-body to on-body wireless radio frequency link for upper limb prostheses," *PloS one*, vol. 11, no. 10, p. e0164987, Oct, 2016.

[32] C. Garcia-Pardo, C. Andreu, A. Fornes-Leal, S. Castelló-Palacios, S. Perez-Simbor, M. Barbi, A. Vallés-Lluch, and N. Cardona, "Ultrawideband technology for medical in-body sensor networks: An overview of the human body as a propagation medium, phantoms, and approaches for propagation analysis," *IEEE Antennas and Propagation Magazine*, vol. 60, no. 3, pp. 19–33, Apr, 2018.

[33] J. Kim and Y. Rahmat-Samii, "Implanted antennas inside a human body: Simulations, designs, and characterizations," *IEEE Transactions on microwave theory and techniques*, vol. 52, no. 8, pp. 1934–1943, Aug, 2004.

[34] P. S. Hall, Y. Hao, Y. I. Nechayev, A. Alomainy, C. C. Constantinou, C. Parini, M. R. Kamarudin, T. Z. Salim, D. T. Hee, R. Dubrovka *et al.*, "Antennas and propagation for on-body communication systems," *IEEE Antennas and Propagation Magazine*, vol. 49, no. 3, pp. 41–58, Aug, 2007.

[35] D. B. Smith, D. Miniutti, T. A. Lamahewa, and L. W. Hanlen, "Propagation models for body-area networks: A survey and new outlook," *IEEE Antennas and Propagation Magazine*, vol. 55, no. 5, pp. 97–117, Oct, 2013.

[36] J. F. Zhao, X. M. Chen, B. D. Liang, and Q. X. Chen, "A review on human body communication: signal propagation model, communication performance, and experimental issues," *Wireless Communications and Mobile Computing*, vol. 2017, Sep, 2017.

[37] 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, Dec, 2018.

[38] P. Bose, A. Khaleghi, M. Albatat, J. Bergsland, and I. Balasingham, "Rf channel modeling for implant to implant communication and implant to sub-cutaneous implant communication for future leadless cardiac pacemakers," *IEEE Transactions on Biomedical Engineering*, Mar, 2018.

[39] Federal Communications Commission, "Medical Body Area Network (MedRadio)," https://www.fcc.gov/document/medical-body-area-networks, May,2015, online; accessed 3/02/2018.

[40] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, Jul, 1978.

[41] M. Studio, "Cst-computer simulation technology," *Bad Nuheimer Str*, vol. 19, p. 64289, 2008.

[42] M. J. Ackerman, "The visible human project," *Proceedings of the IEEE*, vol. 86, no. 3, pp. 504–511, Mar, 1998.

[43] V. Spitzer, M. J. Ackerman, A. L. Scherzinger, and D. Whitlock, "The visible human male: a technical report," *Journal of the American Medical Informatics Association*, vol. 3, no. 2, pp. 118–130, Mar, 1996.

[44] S. Castelló-Palacios, A. Vallés-Lluch, C. Garcia-Pardo, A. Fornes-Leal, and N. Cardona, "Formulas for easy-to-prepare tailored phantoms at 2.4 ghz ism band," in *Medical Information and Communication Technology (ISMICT), 2017 11th International Symposium on*. IEEE, Feb, 2017, pp. 27–31.

[45] R. Chávez-Santiago, C. Garcia-Pardo, A. Fornes-Leal, A. Vallés-Lluch, G. Vermeeren, W. Joseph, I. Balasingham, and N. Cardona, "Experimental path loss models for in-body communications within 2.36-2.5 ghz," *IEEE journal of biomedical and health informatics*, vol. 19, no. 3, pp. 930–937, Apr, 2015.

[46] D. Kurup, W. Joseph, G. Vermeeren, and L. Martens, "Path loss model for in-body communication in homogeneous human muscle tissue," *Electronics letters*, vol. 45, no. 9, pp. 453–454, Apr, 2009.

[47] J. Wang and Q. Wang, "Body area communications: Channel modeling, communication systems, and emc," Nov, 2012.

[48] P. Bose, A. Khaleghi, and I. Balasingham, "In-body and off-body channel modeling for future leadless cardiac pacemakers based on phantom and animal experiments," *IEEE Antennas and Wireless Propagation Letters*, vol. 17, no. 12, pp. 2484–2488, 2018.

[49] A. Khaleghi and I. Balasingham, "Wireless communication link for capsule endoscope at 600 mhz," in *Engineering in Medicine and Biology Society (EMBC), 2015 37th Annual International Conference of the IEEE*. IEEE, Aug, 2015, pp. 4081–4084.

[50] A. Ba, M. Vidojkovic, K. Kanda, N. F. Kiyani, M. Lont, X. Huang, X. Wang, C. Zhou, Y.-H. Liu, M. Ding *et al.*, "A 0.33 nj/bit ieee802. 15.6/proprietary mics/ism wireless transceiver with scalable data rate for medical implantable applications," *IEEE journal of biomedical and health informatics*, vol. 19, no. 3, pp. 920–929, Mar, 2015.