Experimental phantom-based evaluation of Physical Layer Security for Future Leadless Cardiac Pacemaker

Muhammad Faheem Awan[1], Sofia Perez-Simbor[2], Concepcion Garcia-Pardo[2], Kimmo Kansanen[1],
Pritam Bose[3], Sergio Castelló-Palacios[2] and Narcis Cardona[2]
[1]Department of Electronics, NTNU, Trondheim, Norway
[2]iTEAM, Universitat Politècnica de València, Spain
[3]University of Oslo, Norway
{faheem.awan}@ntnu.no

***Abstract*—Next generation of cardiac pacemakers are expected to be completely wireless bringing along new security threats. Thus, it is critical to secure the pacemaker transmissions between legitimate nodes from a third party or an eavesdropper. This work explores the potential of securing leadless cardiac pacemaker by using physical layer security methods. In this work, we perform phantom experiments to replicate the dielectric properties of human heart and measure the path loss models for in body to in body scenario and in body to off body scenario. These scenarios reflects the channel between legitimate nodes and that of channel between legitimate node and eavesdropper in frequency band ranging between 1.7 - 2.5 GHz. In our case, legitimate nodes are leadless cardiac pacemaker implanted in right ventricle of human heart transmitting to a legitimate receiver, which is subcutaneous implant beneath the collar bone under the skin, whereas third party outside the body trying to eavesdrop the communication. By using these models, potential of positive secrecy capacity has been shown along with its probability by varying eavesdropper distances. It has been seen that even if eavesdropper is at the same distance as of legitimate node, still we have about 45% probability of positive secrecy rate. The randomness in channel measurements is observed because of measurements at different angles from source, both for legitimate link and as well as eavesdropper link, which can reflect to propagation through different parts/organs of human body.**

I. Introduction

Rapid development in personal health systems due to wireless body area networks (WBAN) results in number of implantable and wearable medical devices. These on body and in body wireless medical devices continuously monitor different physiological conditions and provide proper diagnosis and treatment. Notable among these devices are cardiac pacemakers and implanted cardiac defibrillators (ICD's).

Pacemakers are used to treat different types of cardiac arrhythmia's. Annually there are about 0.7 million pacemaker implantations worldwide [1]. Pacemaker sense irregularities between heart beats and provides proper actuation via electrodes, thus facilitating proper functioning of human heart. Currently these pacemakers are mostly implanted having wired connection between subcutaneous implant and electrodes in right ventricle and right atrium of the human heart. Data transmitted by these devices include transmission of real time patient data, offline patient data and device information along with different indicators. The next generation of these pacemakers are expected to be wireless between subcutaneous implant and electrodes.

Being wireless in nature, a strong urge for communicating securely also arises because of sensitive nature of this application. The wireless nature of modern Implanted Medical Devices (IMD's) is a significant source of security risks. It makes IMD more visible and can facilitate an eavesdropper to listen. Thus an insecure communication channel makes it easier for an eavesdropper to perform attacks on an implant similar to attacks on other computing devices. Successful eavesdropping may result in retrieval of patient information (medical and non medical) or performing attacks like forging and data altering. In addition, it may enable the modification of implant configuration without knowledge of the patient or physician.

The work of Halperin et al. [2] is considered as pioneer work in security analysis of IMD's, followed by different research activities providing security for IMD devices [3]. Most of the research is focused on mitigating the security risks via providing different encryption mechanisms in order to protect data between sender and legitimate nodes [4] [5] [6].

In conventional wireless networks, security is considered as an independent feature with no or little connection to other tasks of communication network. State of the art encryption algorithms are developed for such purposes. But in case of wireless IMD's a little attention is given to security feature of these medical devices due to which IMD's are considered to be under high security threat.

Traditionally security in wireless networks is implemented and studied via cryptographic algorithms.(e.g RSA, AES, DES etc). These methods require high computational power and proper key management servers for implementation which cannot be the case for tiny implanted medical devices. Also, these techniques rely on intruders limited computational resources. A lightweight alternative could be secure communication via information theoretic measures which utilizes random characteristics of wireless channels.

The concept of information theoretic security was first introduced by Shannon [7] which was further extended by Wyner [8] by introduction to wiretap channel. The focal point of information theoretic security or physical layer security is using the characteristics of wireless channels which can be achieved by measuring the channel transfer functions of legitimate link and eavesdropper link and estimating the channel capacities of the links. If the eavesdropper channel's signal to noise ratio (SNR) is inferior to that of the legitimate channel, then the difference between link capacities provide the secrecy rate for communication and defines a key performance measure of secrecy capacity which is maximum achievable transmission rate keeping eavesdropper uncertainty about source message to maximum and can be achieved by using different practical coding schemes.

Channel characterizations involving human body are usually done by software simulations and experimental measurements which include in-vivo experiments and phantom experiments. It is difficult to simulate these channels in practice using in-vivo experiments because of moral, ethical and physical integrity reasons. Similarly, software simulations are computationally very costly and requires a good deal of time. A cheap alternative to characterize human body channels is via phantom experiments. Phantoms are chemical solutions that can be used to mimic the electromagnetic behaviour of different human body parts provided by Gabriel [9].

In WBAN standard of IEEE 802.15.6, medical implant communication (MICS) band is allocated for implant to implant communication that spans between 402 MHz-405 MHz but a lot of research is also focussed on channel modelling in other bands as well [10] [11] [12] [13]. We focusses on communication between leadless cardiac pacemaker and subcutaneous implant in frequency band ranging between 1.7 - 2.5 GHz (Industrial Scientific and Medical radio band) and develop path loss models for In-Body to In-Body (IB2IB) scenario and In-Body to Off-Body (IB2OFF) scenario.

In this work, potential of securing future leadless cardiac pacemaker by means of physical layer security is analyzed. We develop phantom that mimics the dielectric properties of human heart provided by Gabriel [9] and model a channel between leadless capsule and subcutaneous implant. We also model a channel between leadless capsule and an off body device that could be potential eavesdropper. Once the channel transfer functions are obtained via phantom experiments, we used this information to measure the respective capacities of both links. Furthermore, secrecy capacity analysis is performed over both channels to examine the probability of positive secrecy rate. We also analyze the impact of eavesdropper distance from implanted node and how it effects secrecy rate.

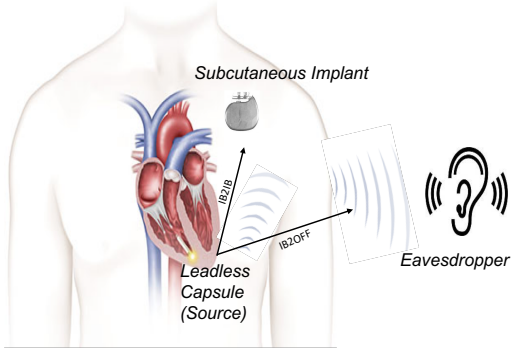

Fig. 1. Pacemaker Scenario with an Eavesdropper

The rest of the paper is organized as follows. Section 2 provides system model whereas secrecy capacity analysis for cardiac leadless pacemaker is provided in section 3. The conclusions and acknowledgements are given in section 4 and 5 .

II. System Model

This section provides a broader view of a system that includes leadless cardiac pacemaker inside the right ventricle of human heart that communicates with subcutaneous implant where as an eavesdropper wants to eavesdrop the communication as shown in Figure 1. In this paper, the link between pacemaker and subcutaneous implant is referred as legitimate link or IB2IB link, whereas the link between pacemaker and eavesdropper is referred as eavesdropper link or IB2OFF link. First, we provide the measurement setup to obtain the path loss models for the respective links. Later on, these models are used for secrecy rate analysis.

A. Measurement Setup

The measurement setup is shown in Figure 2 [13]. It contains an anechoic chamber, Vector Network analyzer (VNA), 3D spatial positioner, a phantom container and a magnetic tracker. Anechoic chamber is used to reduce surrounding environmental contributions, the magnetic tracker measures distance between transmitter and receiver antenna at different measuring points, whereas the positioner is used to move an antenna to different measuring points. Soft control of VNA is done via laptop

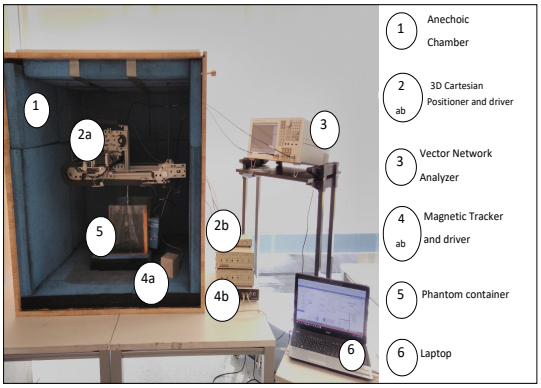

Fig. 2. Measurement Setup

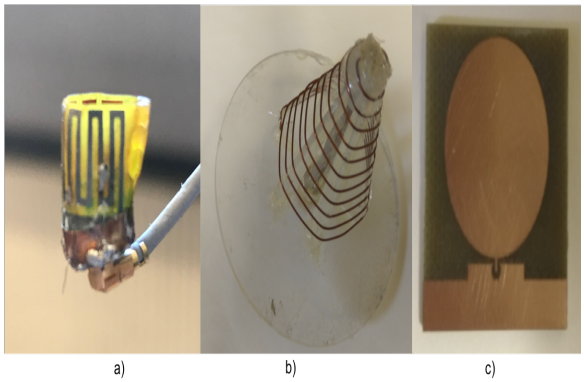

Fig. 5. TX and RX antennas a) Tx b) Rx2 c) Rx1

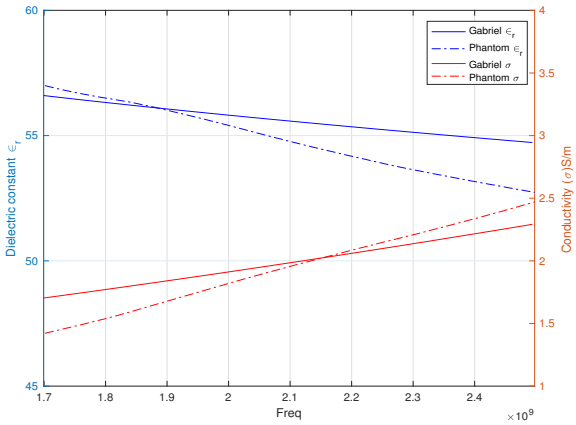

Fig. 3. Dielectric Properties of Heart Phantom

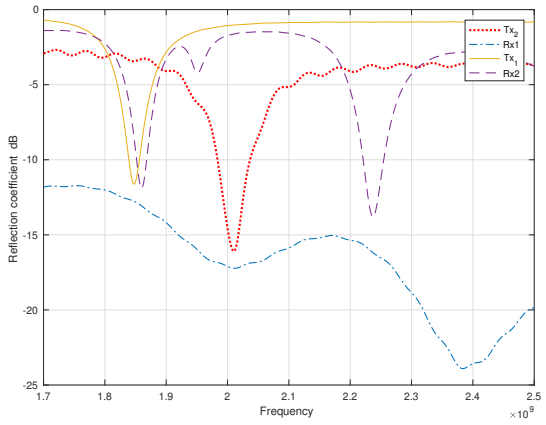

Fig. 4. S11/S22 for IB2IB and IB2OFF communication

with well designed software that performs initial calibration of components before measurement. Afterwards, it automatically measures the coupling between antennas at specified grid points. More details about anechoic chamber and measurement setup can be found in [13].

Regarding the phantom-based experiments, a container is filled with required liquid phantom. Thus, the first step involves the preparation of a phantom that mimics the dielectric properties of a required human muscle/body organ, which one wants to replicate. Considering the scenario of leadless cardiac pacemaker, the muscle involved is human heart. Thus, a phantom with dielectric properties of human heart is developed. As the dielectric properties of human muscles vary with frequency, thus we make a phantom that mimics dielectric properties of human heart in a required frequency band. Figure 3, shows the dielectric properties of a replicated phantom with its counterpart reported in [9], widely used in literature. It shows a good approximation of dielectric properties of heart muscle around 2 GHz, which is the required band for measurements. The heart phantom is mainly composed of sugar (39.2%) with remaining percentage of water [14].

We used three sets of antennas to perform our measurement campaign. An in-body antenna (Transmitter, Tx_1 (orange color)) that replicates the leadless pacemaker transmission, a subcutaneous antenna (Receiver 1, Rx1 (blue color)) that is used as a subcutaneous implant or legitimate receiver, and an external antenna (Receiver 2, Rx2 (purple)) that replicates an eavesdropper link. Figure 4 shows reflection coefficients of the antennas. IB2OFF and IB2IB measurements were performed on different days. For IB2OFF, the Tx_1 and Rx1 antennas resonates around 1.85 GHz, due to which we only use that part of a frequency band for path loss modelling. As the measurements were performed on different days, For IB2IB link the same reflection coefficient (Tx_1), shifts towards 2 GHz and is represented by Tx_2 (red color). The losses can be considered the same in both frequencies because they are relatively near. This is further explained in Section III-A. All the antennas used are directional and provided in Figure 5. More details on antennas can be found in [15].

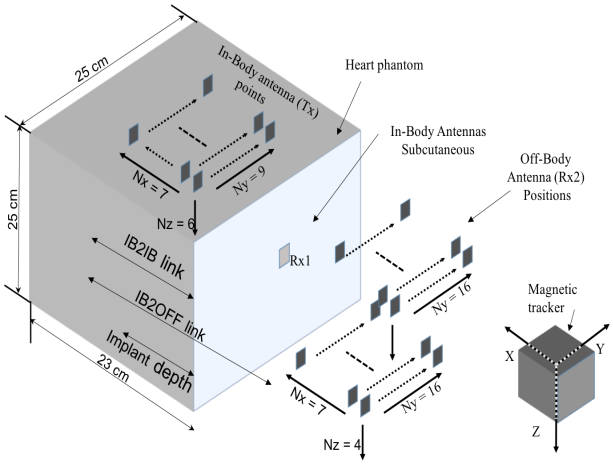

Fig. 6. Measurement Grid points

B. Channel Measurements

In order to perform the measurements, we place the container inside the anechoic chamber and fill it with heart phantom. VNA is calibrated with *Rosenberger calibration kit RPC - 3.50* in order to remove the losses due to coaxial cables. The phantom temperature is maintained at 24°C because of its variation due to temperature change. Table I, shows the set of parameters used for measurements. We perform measurements for legitimate link (IB2IB) and move in body antenna to different positions in a grid. For eavesdropper link measurement, we set different grid points/measuring points outside the phantom container. Figure 6 shows sample IB2IB and IB2OFF measuring points in 2D and 3D grid.

Furthermore, for legitimate link measurements implanted antenna (Tx) is moved in different grid points with $\Delta x = \Delta y = \Delta z = 1cm$ with total grid points of (Nx, Ny, Nz) = (7,9,6), whereas subcutaneous antenna is fixed on the phantom container, on an inside as shown by Rx1 in Figure 6. Both antennas are covered with latex to protect from short circuiting. Similarly, for eavesdropper link an implanted antenna (Tx) is fixed inside the phantom with an implant depth of 11.5 cm and external antenna (Rx2) is moved in different grid points outside the container shown in Figure 6 . The total measuring points for off body antenna are $(Nx, Ny, Nz) = 2 \times (7, 16, 4)$. It is multiplied by 2, because first we cover the upper space and then the lower space as shown in Figure 6. In addition, for each measuring point five snapshots are taken and then averaged to enhance the signal to noise ratio (SNR).

TABLE I
SETUP PARAMETERS

Phantom	Sugar (Heart)
Frequency band	f= [1.7-2.5] GHz
Resolution points	1601
Resolution Frequency	0.5 MHz
Intermediate Frequency	3 KHz
Output power	8 dBm
Snapshots per position	Ns = 5

III. Secrecy Capacity analysis

In this section, we discuss about the secrecy capacity of a leadless cardiac pacemaker and its dependence on different parameters. Path loss models for the legitimate link and eavesdropper link are depicted to measure the SNR of both links at different distances, which helps in evaluation of the secrecy capacity. Secrecy capacity is the maximum attainable communication rate between legitimate nodes without any leakage of information to eavesdropper and can be practically achieved by different coding schemes (not in a scope of this paper).
Consider the wireless system depicted in Figure 1, where leadless pacemaker communicates with subcutaneous implant and eavesdropper attempts to eavesdrop the communication. By recalling [16] for additive gaussian wiretap channel, where both channels are corrupted by gaussian noise in a way that Eve channel is noisier than legitimate channel i-e $W_e > W_r$. Then the instantaneous secrecy capacity is given as,

$$C_s = C_r - C_e \tag{1}$$

where,

$$C_r = \frac{1}{2}\log_2(1+\gamma_r) \tag{2}$$

is the instantaneous channel capacity of legitimate link and

$$C_e = \frac{1}{2}\log_2(1+\gamma_e) \tag{3}$$

is the instantaneous channel capacity of eavesdropper link, which follows instantaneous secrecy capacity as,

$$C_s = \begin{cases} \frac{1}{2}\log_2(1+\gamma_r) - \frac{1}{2}\log_2(1+\gamma_e), & \text{if } \gamma_r > \gamma_e. \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

γ_r is legitimate channel (IB2IB) SNR and γ_e is eavesdropper channel (IB2OFF) SNR. C_s is positive when $\gamma_r > \gamma_e$, which means that the legitimate nodes can communicate securely at that positive secrecy rate. Furthermore, SNR of each link can be given as;

$$\gamma_i = \frac{P \times |h_i|^2}{W_i}, \quad i\epsilon(r,e) \tag{5}$$

where, P is transmitted power, $|h_r|^2$,$|h_e|^2$ are channel attenuations of respective links and W is noise power. For our scenario, we consider a fixed transmit power of -16 dBm (mostly the case of low power

implanted devices like pacemaker) [17], the noise power to be constant and channel attenuations be the source behind variation in channel capacities. Thus, to analyze the secrecy capacity rate, channel transfer functions are measured via measurement campaign explained in previous section to obtain the path loss/attenuation.

A. Path Loss

From channel transfer function of each respective link, path loss is obtained. As we measured the forward transmission coefficient S_{21} for N resolution points (see Table I), the path loss per spatial position can be expressed as,

$$PL_i(dB) = |h_i|^2 = 10 \times \log_{10}\left(\sum_{k=N} \frac{|H(f)_k|^2}{N}\right), \quad i\epsilon(r,e) \tag{6}$$

$H(f) = |S_{21}|e^{-j\angle S_{21}}$, where $|S_{21}|$ and $\angle S_{21}$ are module and phase of transmission coefficient.

1) IB2IB Path loss model (legitimate link): In order to find the IB2IB path loss model, the in-body antenna is fixed on the inner surface of the container's wall and transmitting antenna is moved in different grid points inside the phantom. This is to replicate the scenario where human heart beats continuously due to which distance between the leadless pacemaker and subcutaneous implants changes with each beat. Leadless pacemaker is considered as implanted antenna whereas antenna fixed on the wall of a container is considered as subcutaneous implant. As mentioned earlier, the measured frequency band is 1.7 GHz to 2.5 GHz, but we only take that narrowband part in which transmitter's S11 is below -6 dB. Thus, only those measurements of S21, for which the S11 reflection coefficient is below -6 dB are taken. The resulting measured frequency band is 1.946-2.072 GHz. The obtained path loss can be modelled as distance dependant logarithmic function and for legitimate link, can be expressed as

$$PL_{dB} = PL_{d_0} + 10 \times n \times log_{10}(\frac{d}{d_0}) + \mathcal{N}(\mu, \sigma) \quad (7)$$

where, d_0 = 2.7 cm, PL_{d_0} = 22.9284 dB , $n = 4.12$ and $\mathcal{N}(\mu, \sigma) = (-3.42 * 10^{-15}, 7.3002) \approx (0, 7.3002)$. Figure 7 shows the path loss model in which dots are path loss measurements and the line is a fitted model. This model is valid for legitimate link distance between 2.7 cm to 12 cm. It is also noted that our measurements agree with [12] in the respective band. The randomness observed is because of measurements at different angles from the transmitting antenna.

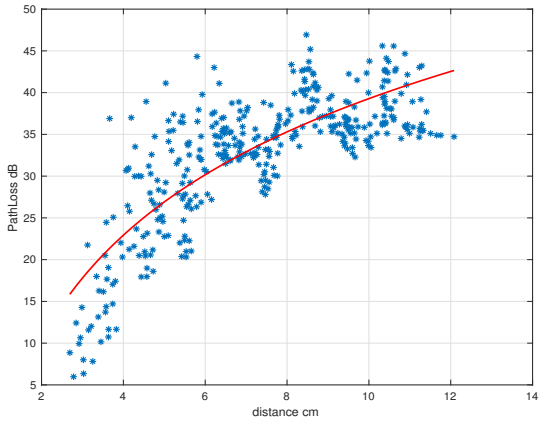

Fig. 7. Path loss legitimate link (IB2IB)

2) IB2OFF Path loss Model (Eavesdropper Link): Similarly, in order to find path loss for off body link, we fixed the implanted antenna inside the heart phantom at an implanted depth of 11.5 cm and move the external antenna as mentioned earlier in II-B. This replicates the scenario where, leadless pacemaker is implanted at a depth of 11.5 cm inside the body, transmitting to subcutaneous implant and eavesdropper outside the body trying to eavesdrop the communication. Similarly to IB2IB, we take S21 measurements for narrowband where matching occurs. Thus the measured frequency band range between 1.8255-1.8715 GHz. The narrowband frequency range in IB2IB and IB2OFF measurements should supposed to be same but as the measurements are performed on different days, a small deviation is observed. This slight deviation in frequency will not affect the measured path loss values and thus, the models. In a real scenario, both the links will be operating at the same frequency. Furthermore, the path loss model obtained, expressed in terms of distance dependent logarithmic function can be expressed as

$$PL_{dB} = PL_{d_0} + 10 \times n \times log_{10}(\frac{d}{d_0}) + \mathcal{N}(\mu, \sigma) \quad (8)$$

where, d_0 = 17.45 cm, PL_{d_0} = 46.97dB , $n = 3.352$ and $\mathcal{N}(\mu, \sigma) = (-1.17 * 10^{-15}, 4.40235) \approx (0, 4.40235)$. Figure 8 shows the path loss model for mentioned implant depth. This path loss model is valid for external distance of 17.5 cm - 40 cm. After 40 cm, free space path loss model can be applied. Table II provides the summary of path loss models.

B. Probability of Positive Secrecy Capacity

When the legitimate link SNR is better than the eavesdropper link, the secrecy capacity is positive and can be referred as positive secrecy capacity. Table II provides the summary of path loss models which shows

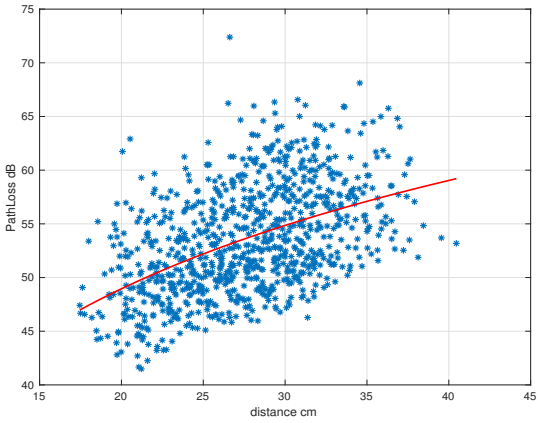

Fig. 8. Path loss Eavesdropper link (IB2OFF)

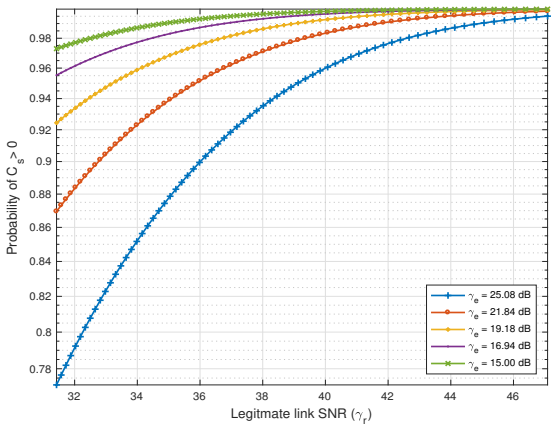

Fig. 9. Positive secrecy capacity with legitimate link SNR

that both the links, legitimate link and eavesdropper link have log normal randomness because of measurement points at different angles from the source. Because of randomness in channel, we are interested in finding the probability of positive secrecy capacity.

For log normal channels, the probability of positive secrecy capacity can be expressed in terms of Q-function as [18];

$$\mathcal{P}(C_s > 0) = Q\left(\frac{\ln E(\gamma_e) - \ln E(\gamma_r)}{4\sqrt{a^2 + b^2}}\right) \qquad (9)$$

where, $\ln E(\gamma_e)$ is the mean SNR of eavesdropper link and $\ln E(\gamma_r)$ is mean SNR for legitimate link (see Equation(5)). In addition, $a = \frac{\sigma_r ln10}{40}$ and $b = \frac{\sigma_e ln10}{40}$, where σ_e is the channel deviation of EVE link and σ_r is of legitimate link provided in table II. Thus, by using (9), we plotted probability of positive secrecy capacity for different values of legitimate channel SNR (in dB) against eavesdropper SNR as shown in Figure 9. With better legitimate link SNR, an increase in probability of positive secrecy capacity is observed. Similarly, probability of positive secrecy capacity is also plotted against Eve distance in Figure 10. Two fixed distances for legitimate link are considered and for each distance, probability of positive secrecy capacity is plotted against varying Eve distance. Figure 10, shows that as the Eve distance increases, probability of positive

TABLE II
SUMMARY OF PATHLOSS MODELS

Parameters	Legitimate Link	Eve link
PL_{d0}	22.92 dB	46.97 dB
Path loss exponent (n)	4.12	3.352
σ	7.3002	4.4023
μ	0	0
d_0	2.7 cm	17.45 cm
Maximum distance	2.7 cm-12 cm	17.5 cm-40 cm

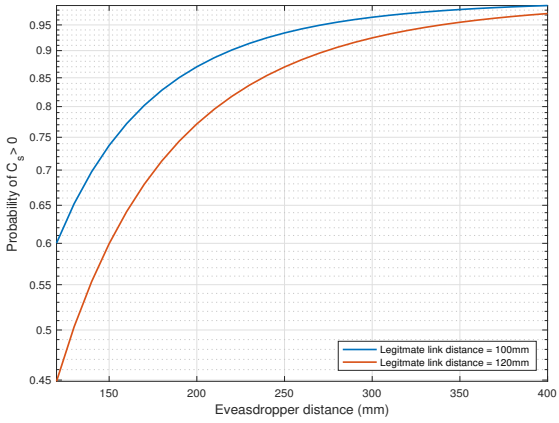

Fig. 10. Positive secrecy capacity with varying Eavesdropper distance from implanted node

secrecy capacity approaches to one. It also shows that if eavesdropper is exactly at the same distance to that of legitimate node i-e 120 mm, there is still about 45 % probability of positive secrecy capacity and it approaches to approximately 97 % at Eve distance of 400 mm.

IV. CONCLUSIONS

This work analyze, the potential of securing next generation leadless cardiac pacemaker communicating wirelessly between implanted nodes via physical layer security (PLS) methods. We consider a scenario, where a leadless pacemaker is implanted in the right ventricle of human heart and communicates with subcutaneous implant wirelessly whereas third party or an eavesdropper attempts to eavesdrop the communication. Human heart like liquid phantoms are developed to mimic the behaviour of electromagnetic waves propagation through the heart. Phantoms developed closely reflects the dielectric properties of heart. Using these phantoms along with automated channel measurement mechanism, channel

transfer functions are obtained for a legitimate link and also link between implanted node and that of an eavesdropper. Furthermore, these channel transfer functions are used to develop path loss models for both IB2IB link (legitimate link) and IB2OFF link (eavesdropper link). After obtaining the path loss models, secrecy capacity analysis is applied to highlight the potential of PLS security methods for wireless cardiac implants. It is being analyzed that the positive secrecy capacity still can be achieved, even when eavesdropper is as close as 12 to 15 cm from an implanted node. It is been found that even if eavesdropper is exactly at the same distance as an implanted node to which leadless capsule is transmitting, still probability of positive secrecy capacity is about 45% and approaches to approximately 97 % at Eve distance of 400 mm. With advent of positive secrecy capacity, different practical coding schemes can be used to achieve this secrecy rate.

V. Acknowledgments

"This work was supported by the Marie Curie Research Grants Scheme, with project grant no 675353 WIBEC ITN".

We would also like to thank Dr. Ali Khaleghi (NTNU, Trondheim, Norway) for valuable discussions and providing an external antenna.

References

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

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

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

[4] 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, 2013.

[5] S. Son, K. Lee, D. Won, and S. Kim, "U-healthcare system protecting privacy based on cloaker," in *Bioinformatics and Biomedicine Workshops (BIBMW), 2010 IEEE International Conference on*. IEEE, 2010, pp. 417–423.

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

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[8] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] C. Gabriel, "Compilation of the dielectric properties of body tissues at rf and microwave frequencies." KING'S COLL LONDON (UNITED KINGDOM) DEPT OF PHYSICS, Tech. Rep., 1996.

[10] C. Garcia-Pardo, A. Fornes-Leal, N. Cardona, R. Chávez-Santiago, J. Bergsland, I. Balasingham, S. Brovoll, Ø. Aardal, S.-E. Hamran, and R. Palomar, "Experimental ultra wideband path loss models for implant communications," in *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2016 IEEE 27th Annual International Symposium on*. IEEE, 2016, pp. 1–6.

[11] C. Garcia-Pardo, R. Chávez-Santiago, N. Cardona, and I. Balasingham, "Experimental uwb frequency analysis for implant communications," in *Engineering in Medicine and Biology Society (EMBC), 2015 37th Annual International Conference of the IEEE*. IEEE, 2015, pp. 5457–5460.

[12] 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, 2015.

[13] S. P. Simbor, M. Barbi, C. Pardo, S. C. Palacios, and N. Cardona, "Initial uwb in-body channel characterization using a novel multilayer phantom measurement setup," *IEEE Wireless Communications and Networking Conference, WCNC*, April 2018.

[14] 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, 2017, pp. 27–31.

[15] 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*, 2018.

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

[17] A. B. Amar, A. B. Kouki, and H. Cao, "Power approaches for implantable medical devices," *Sensors*, vol. 15, no. 11, pp. 28 889–28 914, 2015.

[18] X. Liu, "Secrecy capacity of wireless links subject to log-normal fading," in *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on*. IEEE, 2012, pp. 167–172.