Information theoretic analysis for securing Next Generation Leadless Cardiac Pacemaker

Muhammad Faheem Awan, Kimmo Kansanen, and Deepak Palaksha

Norwegian University of Science and Technology,
NTNU, Trondheim, Norway
`faheem.awan@ntnu.no`

Abstract. Next generation of cardiac pacemakers are anticipated to be wireless that could lead to new security threats. This paper analyzes problem of secure data transmissions for future leadless cardiac pacemaker in terms of information theoretic security. Based on information theoretic approach for Gaussian broadcast channel, a communication channel can be secured if the legitimate receiver has better SNR than eavesdropper. By using attenuation as a key parameter this condition can be fulfilled for leadless cardiac pacemaker, assuming that legitimate receiver is always closer to leadless capsule than eavesdropper. In this work, capacity region for leadless cardiac pacemaker with and without secrecy constraints is characterized. Numerical results are obtained by setting different eavesdropping distance and finding corresponding secrecy transmission rates for legitimate receiver and eavesdropper by utilizing in-body channel model. Results also provides threat distance within which the eavesdropper must be to eavesdrop the communication which in turn depends on total power, information rates and power distribution factor between legitimate receiver and eavesdropper. It has also been shown that by reducing total power, two fold advantages can be achieved, one of saving energy for low power implanted devices and second it helps increasing the secure zone but it comes with a cost of reduction in information rate. Numerical results are provided by using medical implant communication systems (MICS) band for communication between implanted devices. Similarly, it has also been shown that for certain fixed total power, power distribution factor, and transmission rate of 3.5 bps/channel, the threat zone can be reduced to as low as 400 mm.

Keywords: Implanted Medical Devices · Leadless cardiac pacemaker (LCP) · WBAN · Security and Privacy · Physical layer security.

1 Introduction

The technological advancements in personal health systems results in number of wearable and implantable medical devices. These devices help the automatic

diagnosis and treatment of several medical ailments, thus improving the life quality.

Implantable medical devices (IMD's) are designed to monitor and treat regularly several physiological conditions of the body. The most significant among them are cardiac pacemakers and implantable cardioverter defibrillators (ICD's). Pacemakers and ICDs are used to treat cardiac arrhythmia's. These devices are equipped with sensors that senses the pathological conditions and delivers proper actuation, e.g. by retaining the cardiac rhythm.

Cardiac pacemakers are designed to maintain the regular heart rhythms. The current generation of these pacemakers consist of a subcutaneous implant, implanted in the pectoral pocket under the shoulder which is connected to the wired electrodes in the heart chambers through the subclavian vein. The traditional cardiac pacemakers are anticipated to be wireless in near future. These implanted devices transmit patient data (offline and real-time) along with other critical device information and indicators. In addition, the transmitted indicators may contain information about diagnosed ailments along with performed therapies. In order to maintain the proper configuration of a pacemaker along with regular patient monitoring, the data transmissions play a critical role. The physician is also continuously updated regarding the current status of a patient and alarms if the critical condition is detected. The frequency of data transmissions vary, depending upon different configurations. The most common configuration follows the retrieval of data, while visiting a physician. In some cases, a bedside external device is also provided, in which the data is logged automatically on everyday basis. However, the future leadless cardiac pacemaker is shown in Fig. 1, with a capsule inside the heart chamber and a subcutaneous implant will transmit the data on each heart beat.

The wireless communication in next generation IMDs could be a substantial source of security risks. It increases the visibility of IMD and can help eavesdropper to overhear the communication [5]. Thus, in case of an insecure communication channel, the eavesdropper can easily execute attacks on implants, as like they are performed in other communication networks and devices. If the eavesdropper succeeds in gaining access to the implanted device, she can fetch the patient data (medical or non-medical) or can forge or alter the information. Furthermore, the eavesdropper can modify the device configuration without knowledge of physician or a patient.

The security analysis of IMD's was first provided by Halperin et al. [1], in which it has been shown that the insecure link between IMD's can be compromised. This work was succeeded by various research activities that mainly emphasize on various encryption mechanisms for confidentiality between authentic nodes [2–4, 6].

In traditional wireless networks, the security of a communication network is viewed as an independent task with no or limited association with other features of a network. This leads to the development of state-of-the-art algorithms for privacy and security of these networks. But IMD's majorly focuses on device application rather than features like security, due to which wireless IMD's have

weak security algorithms and are more prone to privacy and security threats.

Security and privacy in conventional wireless networks is studied and implemented via various traditional cryptographic algorithms that includes AES, RSA, DES etc. Cryptographic algorithms ensures confidentiality by encrypting data using secret keys. These keys helps, encrypt and decrypt the information at sender and receiver, which can be achieved by keys distribution among them. They work on an assumption that eavesdropper has limited computational resources. But sometimes it's difficult to implement these techniques in low power devices because of keys management issues and computational complexity. Another approach to secure data is using physical layer security, which relies on concepts of information theory. Security with information theoretic measures can be cryptanalytically unbreakable regardless of eavesdropper unlimited computational resources. Physical layer security is based on information theoretic measures which ensures that third party or eavesdropper is not able to eavesdrop communication. It can be additionally provided together with cryptographic methods.

The key idea of information theoretic security (ITS) is to utilize properties of the eavesdropper and legitimate receiver channels. The idea of ITS was pioneered by Shannon in [7]. Wyner in [8] further extended the concept by introducing a wiretap channel. It was shown in [8], that secrecy can be provided by wireless channel itself without depending on secret keys and can degrade the ability of eavesdropper to collect information. Notable mechanisms among them exploit channel attenuation, interference and fading in a communication channel. He added that perfect secrecy can be achieved, if the channel capacity of a link between source and legitimate receiver is greater than the channel capacity of link between source and eavesdropper. In Wyner model, eavesdropper is considered to have unlimited computational resources. Using the assumption, that an eavesdropper channel is a degraded version of the main channel, Wyner proved the existence of positive secrecy capacity. This work was extended by [9] for broadcast channels where non degraded version of eavesdropper channel was considered. These studies provide an important performance metric of secrecy capacity. Secrecy capacity is the maximum communication rate with which the legitimate nodes can communicate securely without leakage of information to the eavesdropper.

This work explores the potential of physical layer security methods for securing future leadless cardiac pacemaker (LCP). We utilize the strategy of sending information over the Gaussian broadcast channel in order to ensure secrecy. This can be achieved by manipulating transmission rates for different broadcast receivers. As the name suggests, broadcast scenario involves simultaneously transmission of information to multiple receivers, thus securing information involving Gaussian broadcast channel requires sending of information to two distant receivers in a way that one message X_1 is intended for receiver one and second message X_2 is intended for receiver two. Receiver one which can be regarded as legitimate receiver can decode both messages, if his signal to noise ratio is greater than receiver two, whereas receiver two can only decode second message

Fig. 1. Pacemaker Scenario with an Eavesdropper

X_2 with an inferior signal to noise ratio. Signal to noise ratio of both receivers vary due to channel attenuation ($|h|^2$). Receiver one's higher signal to noise ratio is achieved because it's close to leadless capsule, thus resulting in lower channel attenuation or path loss than that of receiver two, which is physically away from the body of implanted capsule. In this work, path loss model from [10] is utilized to formulate attenuation between nodes.

The rest of paper is organized as follows. System model is provided in section 2 whereas section 3 contains numerical results. Section 4 and 5 provides conclusions and acknowledgments respectively.

2 System Model

This section focuses on providing system model used in the analysis. For our scenario, the system model consists of an LCP implanted in the right ventricle of human heart. The LCP wants to communicate with a subcutaneous implant whereas an eavesdropper tries to overhear the communication as shown in Fig. 1. The subcutaneous implant is considered to be placed at a distance of 150 mm below the collarbone under the skin, thus having lower channel attenuation than eavesdropper. The eavesdropper is assumed to be physically away from a body in which leadless capsule is implanted. As mentioned earlier, in order to ensure secrecy we utilized strategy of Degraded Gaussian Broadcast Channel (DGBC) with confidential messages, which can be presented schematically in Fig. 2. This method is utilized because of its resemblance to our scenario, where eavesdropper channel is always degraded version of legitimate channel. In context of DGBC, subcutaneous implant is considered as the receiver one, whereas the eavesdropper is considered as receiver two. Leadless capsule will transmit two different messages intended for two receivers. Message 1 (X_1) will be confidential infor-

Fig. 2. Gaussian broadcast channel with Confidential information

mation intended for receiver one and message 2 (X_2) will be dummy message or jamming signal intended for receiver two.

2.1 Encoding

In order to encode messages, the encoder of leadless capsule will encode message X_1 with rate R_1 and power (αP) for receiver one and X_2 with rate R_2 and power $(1 - \alpha)P$ for receiver two where α is the power allocation factor that distributes total power between confidential message X_1 and jamming signal X_2 . Transmitter then calculates sum of useful information and jamming signal and transmit sum X over a channel as shown in Fig. 2. The transmitted signal along with signals received by the two receivers are expressed respectively as

$$X = X_1 + X_2 \quad (1)$$

$$\begin{aligned} Y_1 &= \sqrt{P}h_1X + n_1 \\ Y_2 &= \sqrt{P}h_2X + n_2 \end{aligned} \quad (2)$$

X is subject to average power constraint $\frac{1}{n} \sum_{i=1}^n E[X_i]^2 \leq P$, h_1, h_2 are channel gains, and $n_1 \sim \mathcal{N}(0, N_1)$, $n_2 \sim \mathcal{N}(0, N_2)$ is additive white Gaussian noise (AWGN). Multipath small scale fading is assumed to be negligible and channel gain only constitutes path loss which can be expressed in logarithmic scale as

$$\begin{aligned} PL(d)_i &= PL(d_o) + 10\gamma \log_{10}(d_i/d_o), \\ d &\geq d_o, i \in (1, 2) \end{aligned} \quad (3)$$

$$|h_i|^2 = 10^{\frac{PL(d)_i}{10}}, i \in (1, 2) \quad (4)$$

In (3), $PL(d)_2$ is path loss at distance d_2 between implant and receiver two (eavesdropper) and $PL(d)_1$ is path loss between implant and receiver one at distance d_1 . d_o is the reference distance where $PL(d_o)$ is path loss at reference distance and γ is path loss exponent.

2.2 Decoding

The respective receivers then decodes messages. Our aim is to maximise mutual information $I(X; Y_1)$ between capsule and receiver, keeping mutual information between eavesdropper and capsule to zero s.t. $I(X; Y_2) = 0$. First, consider receiver two, which is the eavesdropper. She will try to map a received sequence to a message pair (X_1, X_2) . Her effective signal-to-noise ratio of X is $\frac{(1-\alpha)P|h_2|^2}{(\alpha P|h_2|^2 + N_2)}$, where $\alpha P|h_2|^2$ acts as noise. Thus, she will be able to decode only X_2 . Receiver one which is subcutaneous implant, first decodes X_2 , which he can accomplish because of his higher SNR i.e. $\frac{\alpha P|h_1|^2}{N_1}$. Then he will decode the confidential message X_1 intended for himself. Thus, in order to have confidential messages, information rates R_1 and R_2 must satisfy secrecy condition.

2.3 Secrecy Capacity

Secrecy capacity region is the set of information rates that can be achieved by keeping confidentiality of secret information to maximum from eavesdropper. The secrecy capacity region for one confidential message and one dummy message or jamming signal can be expressed as

$$C_s = \bigcup_{0 \leq \alpha \leq 1} \left\{ \begin{array}{l} R_1, R_2 : \\ R_1 \leq \left[\frac{1}{2} \log \left(1 + \frac{\alpha P|h_1|^2}{N_1} \right) - \frac{1}{2} \log \left(1 + \frac{\alpha P|h_2|^2}{N_2} \right) \right]^+ \\ R_2 \leq \min \left\{ \begin{array}{l} \frac{1}{2} \log \left(1 + \frac{(1-\alpha)P|h_1|^2}{N_1 + \alpha P|h_1|^2} \right), \\ \frac{1}{2} \log \left(1 + \frac{(1-\alpha)P|h_2|^2}{N_2 + \alpha P|h_2|^2} \right) \end{array} \right\} \end{array} \right\} \quad (5)$$

Equation (5)¹ provides secrecy rate pairs (R_1, R_2) depending upon different values of α and channel attenuation $(|h_i|^2)$, $i \in (1, 2)$. Noise variance for receiver one is N_1 and N_2 of receiver two. For simplicity, $N_1 = N_2 = N_0$ is considered, suggesting same noise for both receivers. The only thing that varies SNR for both receivers is channel attenuation and power allocation factor α . As α increases, information rate R_1 will increase whereas R_2 will reduce. In Equation (5), R_1 is positive confidential information rate when inequality holds.

2.4 Analysis of the strategies

The strategy above provides the secrecy operating regions for leadless cardiac capsule where our motive is to keep confidential information secret from receiver two. In our analysis, we focus on fixing certain information rate R_1 for legitimate

¹ all bases are $\log_2$, else specified

receiver and find the value of α where eavesdropper distance is maximum which can then be related to maximum threat distance. Consider, fixed secrecy information rate $R_1 = R_1^*$, which is chosen to be decodable at channel attenuation ($|h_1^*|^2$) (corresponds to distance d_1). Eavesdropper threshold attenuation ($|h_2|^2$) can be expressed from (5) as

$$\log(2^{R_1^*}) + \frac{1}{2} \log \left(1 + \frac{\alpha P |h_2|^2}{N_0} \right) \leq \frac{1}{2} \log \left(1 + \frac{\alpha P |h_1^*|^2}{N_0} \right) \quad (6)$$

Using, properties of log, (6) transforms into,

$$\log \left(2^{R_1^*} \left(1 + \frac{\alpha P |h_2|^2}{N_0} \right)^{\frac{1}{2}} \right) \leq \log \left(1 + \frac{\alpha P |h_1^*|^2}{N_0} \right)^{\frac{1}{2}} \quad (7)$$

For simplicity, we put inequalities to equality. After simplification,

$$\begin{aligned} |h_2|^2 &= \frac{N_0}{\alpha P} \left(\left(1 + \frac{\alpha P |h_1^*|^2}{N_0} \right) \frac{1}{2^{2R_1^*}} - 1 \right) \\ |h_2|^2 &= \frac{N_0}{\alpha P} \left(\frac{1}{2^{2R_1^*}} - 1 \right) + \frac{|h_1^*|^2}{2^{2R_1^*}} \end{aligned} \quad (8)$$

Equation (8), provides maximum eavesdropper threshold attenuation for fixed R_1^* and $|h_1^*|^2$, which can be transformed to maximum eavesdropper distance by using (3) and can be expressed as

$$10 \log_{10} |h_2|^2 = 10 \log_{10} K \quad (9)$$

where $K = \frac{N_0}{\alpha P} \left(\frac{1}{2^{2R_1^*}} - 1 \right) + \frac{|h_1^*|^2}{2^{2R_1^*}}$. From (3), (9) can be expressed as

$$\begin{aligned} 10 \log_{10}(K) &= PL(d_o) + 10\gamma \log_{10}(d_2/d_o) \\ d_2 &= d_o \times 10^{\left(\frac{1}{10\gamma} (10 \log_{10}(K) - PL(d_o)) \right)} \\ d_2 &= d_o \times 10^{\left((\log_{10}(K))^{\frac{1}{\gamma}} - \frac{0.1}{\gamma} PL(d_o) \right)} \\ d_2 &= d_o \times \frac{K^{\frac{1}{\gamma}}}{10^{\frac{1}{10\gamma} PL(d_o)}} \\ d_2 &= d_o \times \frac{\left(\frac{N_0}{\alpha P} \left(\frac{1}{2^{2R_1^*}} - 1 \right) + \frac{|h_1^*|^2}{2^{2R_1^*}} \right)^{\frac{1}{\gamma}}}{10^{\frac{1}{10\gamma} PL(d_o)}} \end{aligned} \quad (10)$$

Equation (10), provides eavesdropper threshold distance, for a fixed secrecy rate R_1^* . Thus, at this distance, eavesdropper will be able to decode only R_2^* . When eavesdropper is closer, she will be able to partially decode R_1^* as well.

Fig. 3. Secrecy Capacity Region C_s

Eventually a point will reach when eavesdropper attenuation becomes equal to receiver one, where she will be able to decode both R_1^* and R_2^* . Thus d_2 from (10) is the distance from which eavesdropper can eavesdrop the confidential message for a given fixed information rate R_1 . So, eavesdropper should be outside this threat distance d_2 for data confidentiality. Beyond d_2 , entire region will be in secure zone.

3 Numerical Results

The system model of Fig. 1 is considered, with a leadless capsule and subcutaneous implant at a distance $d_1 = 150$ mm, where an eavesdropper attempts to eavesdrop communication at a distance $d_2 \geq 150$ mm. The main interest is to find secrecy capacity region (C_s) for different values of α and eavesdropper distance. In addition, a threat zone around implanted body will also be found for fixed information rate R_1 .

For numerical results, we consider that legitimate nodes are communicating in Medical implant communication (MICS) band. MICS band ranges between 402-405 MHz with authorized channel bandwidth of 300 kHz. Implanted medical devices operate on low operational power usually between -16 dBm to -25 dBm due to which transmitted power of $P = -16$ dBm is considered [11]. In addition, noise power spectral density (PSD) of -100 dBm/channel is considered for both receivers. Channel attenuation is obtained from (3) in which path loss $PL(d_o)$ at reference distance of 50 mm is 47.14 dB and path loss exponent (γ) is 4.26 [10]. This is the case for communication between leadless capsule and subcutaneous implant whereas for an eavesdropper link, a reference distance of 150 mm is considered, and beyond it free space path loss is applied with path loss exponent

Fig. 4. Secrecy Capacity Region C_s for varying Eve distance

$\gamma = 2$.

Fig. 3 shows capacity and secrecy capacity region (R_1, R_2) for a particular distance pair (150 mm, 300 mm). In this case, receiver two is considered at a distance of 300 mm, resulting in channel attenuation of 73.48 dB. It can be seen that when power allocation factor α increases, information rate R_1 to legitimate receiver increases while information rate R_2 to receiver two reduces. In addition, cost for making communication secure can also be seen by observing a difference between capacity region and secrecy capacity region. Now consider a case, when $\alpha = 0.9$, receiver two (eavesdropper) is at a distance of 300 mm, and receiver one is at mentioned fixed distance of 150 mm. The secrecy rate pair (R_1, R_2) is approx (1,0.4) bps/channel. Now, if eavesdropper move closer towards receiver one, it's channel SNR improves, this results in decoding a part of confidential message as well. Thus, 300 mm is threshold distance for an eavesdropper to support that secrecy capacity region. If eavesdropper move closer than 300 mm, rate R_1 should be reduced by reducing alpha (α) and feeding more power to jamming signal, otherwise eavesdropper will be able to eavesdrop communication partially and will be able to decode completely when she reach the same distance as legitimate receiver.

Similarly, in Fig. 4 it is shown that if eavesdropper distance (d_2) increases, attenuation increases due to which information rate R_2 reduces whereas R_1 increases. Thus, making information rate adaptable by estimating eavesdropper distance can help increasing the secrecy capacity. Fig. 5 shows change in information rate R_1 with changing Eve distance for different values of α . It is evident that, if eavesdropper distance increase, rate R_1 can be increased.

Furthermore, by using (10) maximum eavesdropping distance is depicted for different values of total power (P), information rate (R_1) and α in Fig. 6, mirroring the threat zone around the implanted node. The region beyond threat zone

Fig. 5. Information rate R_1 versus Eve distance

Fig. 6. Eavesdropping distance with changing Information Rate (R_1), α and total power (P)

is considered to be in secure zone. Secure zone can be increased by reducing the total power which has two fold advantages, one by conserving energy for low power implanted devices such as cardiac pacemaker that help increasing the longevity of a device and also results in increased secure zone. The eavesdropper then needs to move closer to eavesdrop the legitimate transmission. As shown in Fig. 6, with $\alpha = 0.2$, $P = -16$ dBm and $R_1 = 3.5$, the threat zone can be reduced to about 400 mm.

4 Conclusions

This work includes information theoretic security analysis of leadless cardiac pacemaker, transmitting data over a wireless channel to a subcutaneous implant, with an eavesdropper in the near premises to overhear the communication. For securing leadless cardiac pacemaker (LCP), we intend to use degraded Gaussian broadcast channel approach in which a node broadcasts the information to different receivers in a way that legitimate node can decode all the information whereas other receivers can only decode the information intended for them.

The secure information rates region is depicted where LCP can communicate securely with legitimate receiver in the presence of eavesdropper. A fixed distance between legitimate nodes is considered whereas eavesdropper distance is varied. LCP sends confidential message to legitimate receiver whereas noise signal or common signal is used to jam the eavesdropper. Legitimate receiver with lower attenuation and higher SNR will be able to decode both the messages whereas eavesdropper with inferior SNR will be able to decode only the common signal. In order to find channel attenuation between nodes, a pathloss model from [10] is used. Total power is distributed between both messages by power distribution factor (α). By increasing α information rate to legitimate receiver is increased whereas information rate to eavesdropper decreases. We also fixed certain information rate between legitimate nodes and find the maximum eavesdropping distance in order to decode confidential information by eavesdropper. If eavesdropper is at maximum eavesdropper distance for certain fixed value of α , it will not be able to decode any information, but when it starts getting close to legitimate receiver it will be able to partially decode the confidential information, until it reaches to a point where she will decode entire information. It has been seen that if distance between eavesdropper and legitimate node is increased, information rate between legitimate nodes is increased whereas information rate for noise signal can be reduced. Similarly, by increasing information rate and total power between the legitimate nodes, the threat zone increases. In this work, maximum eavesdropping distance reflects the threat zone around the pacemaker, beyond which the region can be considered secure.

5 Acknowledgments

This work was funded by the European Union's H2020:MSCA:ITN program for the Wireless In-body Environment Communication-WiBEC project under the grant agreement no. 675353.

References

1. 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.
2. 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.
3. 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.
4. 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.
5. M. F. Awan and K. Kansanen, "Estimating eavesdropping risk for next generation implants," in *Advances in Body Area Networks I*. Springer, 2019, pp. 387–398.
6. M. F. Awan, S. Perez-Simbor, C. Garcia-Pardo, K. Kansanen, P. Bose, S. Castelló-Palacios, and N. Cardona, "Experimental phantom-based evaluation of physical layer security for future leadless cardiac pacemaker," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2018, pp. 333–339.
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. I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.
10. 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 *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*. IEEE, 2009, pp. 2995–2999.
11. M. N. Islam and M. R. Yuce, "Review of medical implant communication system (mics) band and network," *ICT Express*, vol. 2, no. 4, pp. 188–194, 2016.