Estimating Eavesdropping Risk for Next Generation Implants

Muhammad Faheem Awan
faheem.awan@ntnu.no

Kimmo Kansanen
kimmo.kansanen@ntnu.no

Department of Electronic Systems
NTNU, Trondheim
Norway

ABSTRACT
Implanted medical devices are expected to be wireless in near future. Wireless nature of sensing, controlling and transmission brings along different security threats. In this work, an analysis of eavesdropping risk is performed for an unencrypted data transmissions from an implanted medical device such as cardiac leadless pacemaker. This work utilizes statistical attenuation model along with measures of capacity, information rate and outage probability. Results show that eavesdropping risk depends on pathloss with shadow fading, distance and information rate (R). In addition, probability of successful eavesdropping increases if legitimate nodes transmits at lower rate. Thus, a proper tradeoff between information rate (R) and eavesdropping risk should be made. Numerical results show that at an information rate of 650 kbps, an IMD has a 5% risk of successful eavesdropping at a distance of 500 mm. This work also consider different transmission parameters like heart rate, blood pressure, ECG and EMG with their information rates and find probability of successful eavesdropping at different distances. This study provide basis for designing secure implantable cardiac leadless pacemaker with associated risks involved due to wireless nature of transmission.

Keywords
Implanted Medical Devices; Wireless leadless cardiac pacemaker; WBAN, Security and Privacy

1. INTRODUCTION
Rapid development in personal health systems based on implantable and wearable medical devices results in better quality of diagnosis. This along with automatically treating different medical conditions, improves quality of life. Implantable medical devices (IMD’s) continuously monitor and treat physiological conditions inside the body. Notable among these devices are cardiac pacemakers and implanted cardiac defibrillators (ICD’s). They help treating different types of cardiac arrhythmia’s. In 2001, there were approximately 25 Million patients with IMD’s [1] in the USA. With help of sensors these devices sense different conditions and provide proper actuation e.g. by maintaining heart rhythm.

IMD’s are mostly equipped with on-board transceivers to transmit wirelessly over certain distance. These transmissions facilitate remote monitoring of a patient. The wireless nature of modern IMD’s is a significant source of security risks. Security risk for an IMD increases, when patient is in non-medical or in an open environment. Wireless nature of an IMD makes it 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. Security and privacy of implantable medical devices received a lot of attention when it was revealed that US Vice President Dick Cheney disabled the wireless telemetry on his ICD [2][3]. The work of Halperin et al. [4] is considered as pioneer work in security analysis of IMD’s, followed by different research activities providing security for IMD devices. Most of research is focused on mitigating the security risks via providing different encryption mechanisms in order to protect data between sender and legitimate node [5] [6] [7].

Cardiac pacemakers are designed to facilitate proper functioning of human heart. Currently these pacemakers are mostly implanted using wired electrodes. The next generation of these pacemakers are expected to be wireless. Data transmitted by these devices include transmission of real time patient data, offline patient data and device information along with different indicators. Heart rate, blood pressure etc are considered to be real time data whereas patient name, patient date of birth, patient history lies under offline data transmission. Pacemakers also transmit device information like battery status, device number etc. Furthermore, it may transmit indicators with different diagnosed conditions along with therapies performed. These data transmissions are vital in order to keep pacemaker with right configurations and continuous remote monitoring of a patient. They also help physician to have an updated report regarding heart condition of a patient. Frequency of transmissions depends upon the configurations used for a pacemaker. In case of wireless capsule inside a heart and subcutaneous node under the skin as shown in Figure 1, the data is transmitted...
every heart beat whereas wireless subcutaneous node with leads, logs an activity to a bedside external device on daily basis or data is retrieved during a visit to a physician. Table 1 shows examples of different types of traffic and their typical information rate for an IMD [8].

| Sensing Parameter | Required Data rate |
|-------------------|--------------------|
| Heart rate        | 1 sample/s or 600bps |
| Medical image     | 2.4 Mbps           |
| Blood pressure    | 1.2 kbps           |
| EMG               | 600 kbps           |
| EEG               | 4.2 - 32 kbps      |
| ECG               | 1.2 - 250kbps      |

Table 1: Data rate for IMD traffic

In order to perform the security analysis the first thing to do is analyzing different types of threats [9]. Providing a threat model is always considered to be starting point in security analysis. Among different threats one of the important threat is eavesdropping which provide basis for further attacks. Thus for the aforementioned purpose, this paper focus on finding probability of successful eavesdropping for legitimate transmission between leadless capsule inside human heart and subcutaneous implant. This work considers that an implant is using Medical Implant Communication system (MICS) band for telemetry between legitimate nodes with an assumption that encryption is not used in data communication. We find probability of successful eavesdropping by using a concept of outage probability. We show that eavesdropping risk depends upon information rate, distance, and antenna gains. We utilize statistical attenuation model [10] to find path loss between legitimate nodes and path loss between legitimate node and an eavesdropper. This helps finding the distribution of signal to noise ratio (SNR) at different distances \((d)\). We can then set different cutoff thresholds for SNR \((\gamma_{th})\) depending upon various information rates \((R)\) and find the corresponding outage probability. We finally provide the design details which help setting an appropriate information rate \((R)\) between legitimate nodes.

The rest of the paper is formulated as follows: Section II gives system model followed by eavesdropper model in section III; section IV provides numerical results, and finally we conclude and provides future work in section V.

2. SYSTEM MODEL

Our system consists of an eavesdropper, an IMD, and a subcutaneous node as shown in Figure 1. We consider implanted leadless capsule inside a right ventricle of human heart. This leadless capsule transmits unencrypted data to subcutaneous implant at a distance of 150 mm. We consider the famous Alice, Bob and Eve model which can be seen in Figure 1 for our case scenario.

In case of IMD’s, Eve can be categorized as

- An eavesdropper, eavesdropping legitimate transmission can be an active or passive node.
- There is possibility of single eavesdropper or it may be part of well organised group.
- Eavesdropper is most likely to be an external intruder but there can be the case where an eavesdropper is from inside the system e.g physician, hospital administration, equipment manufacturers etc because they have the benefit of being close to patient.

It can be seen that each eavesdropper may have different intentions or goals. There may be possibility that some one eavesdrop just to get the private information of a patient or there may be a case where there is competition between manufacturers and they would like to obtain information on an IMD equipment. Eavesdropper may have higher capabilities than that of legitimate node like higher computational power, higher antenna gains, etc. In this work we consider single passive eavesdropper having same capabilities as a legitimate node trying to eavesdrop the communication. We also consider a case where the eavesdropper has high gain antenna.

3. EAVESDROPPER MODEL

This section focus on providing the probability of successful eavesdropping by utilizing path loss model for MICS band. We need to predict the received power from a transmitted node along with associated path loss at a certain distance \((d)\). This helps finding distribution of signal to noise ratio (SNR). Then by considering different values of information rate \((R)\), we can set different cutoff thresholds and find probability of successful eavesdropping at a certain distance \((d)\).

3.1 Received Power/Attenuation

We consider that IMD (leadless pacemaker) is transmitting with power \(P_p\) to subcutaneous node at a distance of 150 mm. The eavesdropper is trying to listen the transmission and receives power \(P_e\) at a distance \((d)\) away from the IMD. The power received by the eavesdropper can be given as

\[
P_e = \frac{G_p G_e P_p}{w d^\alpha}
\]

In (1), \(G_p\) and \(G_e\) are antenna gains of implant and eavesdropper antenna whereas \(\alpha\) is path loss exponent and \(w\) is a random variable given by
Equation (2) is used to model log normal shadowing effect. Here $S_h$ is Gaussian random variable with zero mean and standard deviation $\sigma$ ranging from 4-12 dB[10][11]. This randomness is because of propagation through different materials (e.g. bone, muscle, etc.).

In order to compute the numerical results, we generally work with signal attenuation from sender to receiver, and then can utilize it into any case scenario. Here we consider sender as a legitimate node (IMD), where as the eavesdropper is considered as a receiver. Thus instead of received signal strength, attenuation between IMD and the eavesdropper can be given as

$$\delta(d) = \frac{P_r}{P_e} = \frac{w d^a}{G_e G_p}$$

In this paper, we utilizes path loss model provided by [10] in order to find attenuation at distance $d$. Thus, a path-loss/attenuation in logarithmic scale ($\text{dB}$) can be given as

$$PL(d)_{\text{dB}} = PL(d_o)_{\text{dB}} + G_e(d_{\text{dB}}) + G_p(d_{\text{dB}}) + 10\alpha \log_{10}(d/d_o) + S_h,$$  \hspace{1cm} (4)

In (4), $PL(d)_{\text{dB}}$ is the path loss at distance $d$ between the implant and the eavesdropper, $d_o$ is the reference distance and is equal to 50mm. Path loss exponent $\alpha$ is equal to 4.26 in [10]. Furthermore $PL(d_o)$ is the path loss at reference distance and is equal to 47.14 dB. Similarly, $S_h$ is random scattering around the mean and is equal to 7.85dB.

### 3.2 Outage Probability, Information rate and Detection threshold

The main focus of this section is outage probability (OP), information rate ($R$) and detection/cutoff threshold. This section also provide relation between these quantities for main link(link between legitimate nodes) and show how they provide eavesdropping risk. Outage probability is the probability that “When signal to noise ratio (SNR $\gamma$) at the input of a receiver chain fall below certain threshold level [12]”. It can be expressed as

$$P_{\text{out}}(\gamma_{th}) = P[\gamma < \gamma_{th}]$$

where $\gamma$ is signal to noise ratio (SNR) and $\gamma_{th}$ is the threshold SNR. For a communication between legitimate nodes, the value of SNR ($\gamma$) should be greater than threshold otherwise the communication link will be in outage. Based on this threshold, which can also be referred as cutoff threshold, we define the probability of successful eavesdropping at any distance ($d$). In (5) SNR ($\gamma$) can be expressed as

$$\gamma = \frac{P_r}{N_o B} = \frac{P_p}{\delta(d) N_o B}$$

where $P_r$, is received power at input of receiver chain, $P_p$ is power transmitted, $\delta(d)$ is attenuation at a distance ($d$), $B$ is bandwidth and $N_o$ is noise spectral density. In logarithmic (dB) scale (6) can be expressed as

$$\gamma_{dB} = P_{\text{pdBm}} - PL(d)_{\text{dB}} - (N_o B)_{\text{dBm}} = P_{\text{pdBm}} - (PL(d_o)_{\text{dB}} + G_e(d_{\text{dB}}) + G_p(d_{\text{dB}}) + 10\alpha \log_{10}(d/d_o)) - (N_o B)_{\text{dBm}},$$  \hspace{1cm} (7)

where, a constant per channel transmit power $P_{\text{pdBm}}$ and constant $(N_o B)_{\text{dBm}}$ is considered. In (7), $PL(d)_{\text{dB}}$ is mean path loss obtained from (4) at any distance ($d$). Furthermore $S_h$ is Gaussian random variable with zero mean and $\sigma_{dB} = 7.85dB$. Thus, (7) show that SNR ($\gamma_{dB}$) has Gaussian distribution with mean as

$$\mu_{\gamma_{dB}} = P_{\text{pdBm}} - (PL(d_o)_{\text{dB}} + G_e(d_{\text{dB}}) + G_p(d_{\text{dB}}) + 10\alpha \log_{10}(d/d_o)) - (N_o B)_{\text{dBm}},$$  \hspace{1cm} (8)

and standard deviation of $\sigma_{\gamma_{dB}} = 7.85dB$.

Our approach basically uses the concept of channel capacity as a measure. According to the concept of capacity, for a given information rate $R$, there exist a minimum received power to successfully decode the transmission based on certain threshold SNR. Using this concept, the capacity of a link is given by the famous Shannon capacity formula

$$C = B \times \log_2 (1 + \frac{\gamma_{th}}{\gamma})$$

Where $B$ is per channel bandwidth and is equal to 300kHz in case of MICS band and $C$ is capacity. In order to find threshold SNR $\gamma_{th}$, (9) can also be expressed as

$$\gamma_{th}(R) = 2^{\frac{\gamma}{B}} - 1$$

In logarithmic scale (10) can be expressed as

$$\gamma_{th_{dB}}(R) = 10 \log_{10} \gamma_{th}$$

Equation (10) shows that threshold SNR is function of information rate $R$. With variation in information rate ($R$), cutoff threshold ($\gamma_{th}$) varies and have different information rate $R$ due to different traffic transmitted by an IMD. If we solve (10), by taking $B = 300\text{kHz}$ and $R = 600\text{bps}$, we have $\gamma_{th_{dB}}$ as $-28\text{dB}$ which shows that we have successful, error free decoding at that threshold. By reducing information rate ($R$), the cutoff threshold reduces where as by increasing, it increases the detection or cutoff thresholds. Thus, at a same distance $d$ outage probability increases because of higher cutoff threshold and decreases because of lower cutoff threshold($\gamma_{th}$) (5).

### 3.3 Probability of successful eavesdropping

In order to find the probability of successful eavesdropping, we use the concept of outage probability as shown in (5). We have to take certain cutoff threshold represented by $\gamma_{th_{dB}}$. Eavesdropper is able to eavesdropped communication with certain probability, when SNR ($\gamma_{dB}$) between Alice and Eve is greater than set cutoff threshold $\gamma_{th_{dB}}$. Here we express both SNR($\gamma$) and cutoff threshold ($\gamma_{th}$) in dB scale, i.e. $\gamma_{dB} > \gamma_{th_{dB}}$ (7)(11). The probability of successful eavesdropping can be given as

$$P_{SE} = 1 - P_{\text{out}}(\gamma_{th_{dB}})$$

As SNR ($\gamma_{dB}$) is Gaussian distributed (7) with mean $\mu_{\gamma_{dB}}$ (8) and standard deviation $\sigma_{\gamma_{dB}}$, we can express (12) by Q-function as
\[ P_{SE} = 1 - \left(1 - Q\left(\frac{\gamma_{thdB} - \mu_{dB}}{\sigma_{dB}}\right)\right) \]  
(13)

Where, \( P_{SE} \) is probability of successful eavesdropping, \( \gamma_{thdB} \) is cutoff threshold depending upon \( R \) (10) and \( \mu_{dB} \) is mean of signal to noise ratio (\( \gamma_{dB} \))(8) at any distance (d). Equation (13) can also be expressed as

\[ P_{SE} = Q\left(\frac{\gamma_{thdB} - \mu_{dB}}{\sigma_{dB}}\right) = 1 - \varphi\left(\frac{\gamma_{thdB} - \mu_{dB}}{\sigma_{dB}}\right) = 1 - \frac{1}{2} \left(1 + \text{erf} \left(\frac{\gamma_{thdB} - \mu_{dB}}{\sigma_{dB}\sqrt{2}}\right)\right) \]  
(14)

The eavesdropper can increase probability of successful eavesdropping by using high gain antennas. An antenna with high gain, have a reception from greater distances and have higher SNR. But nothing comes without cost, higher gain results from larger dimensions of an antenna. In case of MICS band the transmitting antenna gain is considered to be part of path loss model [10]. Different antennas has different antenna gain and aperture relation but in general it can be expressed as

\[ A_e = \frac{\lambda^2 G_e}{4\pi} \]  
(15)

From the eavesdropper perspective, she wants to eavesdrop without noticing. But with large aperture antennas it can not happen easily. So, the gain of an antenna can not be increased above certain limits e.g. if we are using MICS band and want to have an antenna gain of 20dBi then the effective aperture of an antenna will be around 4.4m² which can not go without noticing within short distance of a patient.

4. NUMERICAL RESULTS

This section focus on numerical results by considering scenario as shown in Figure 1 which focus on communication between implanted leadless capsule(pacemaker) and a subcutaneous node under the skin. For communication between the implant and subcutaneous node, we are interested to find the probability of successful eavesdropping. First, channel attenuation is predicted by utilizing pathloss model in [10], which give an SNR \( \gamma_{dB} \) distribution (7). Then different cutoff thresholds \( \gamma_{thdB} \) for an SNR are considered based on information rates (10)(11).

We take different cutoff values by considering information rates from Table 1, whereas Table 2 provides different information rates with corresponding threshold SNR. Now, by looking into different threshold values, we utilize (14) and find probability of successful eavesdropping \( P_{SE} \). Figure 2 shows probability of successful eavesdropping for different information rates (\( R \)) at different distances.

The results in Figure 2, shows that if an eavesdropper is exactly at same distance as that of subcutaneous node i.e 150mm for an information rate of 650kbps, then in practice the probability of successful eavesdropping is about 100%. But when an eavesdropper distance is increased the probability of successful eavesdropping reduces with distance e.g. for the same case at 400mm, the probability of successful eavesdropping is reduced to around 19%. Each curve shows probability of successful eavesdropping for certain information rate (\( R \)) over different distances. An eavesdropper can also increase its receiver sensitivity against path loss by using high gain antennas, resulting in successful eavesdropping over larger distance because of higher SNR e.g as shown in Figure 2 the dashed lines show that probability of successful eavesdropping is increased over a distance by using an antenna gain of 4dBi for the same respective cases without antenna gain (green and red curve). Here it is notable to mention that from a design perspective, a proper tradeoff is required between information rate and eavesdropping risk.

| Sensing Parameter | Required Data rate | Threshold SNR (\( \gamma_{thdB} \)) |
|-------------------|-------------------|-------------------------|
| Heart rate        | 600 bps           | -28.5dB                 |
| Blood pressure    | 1.2 kbps          | -25.56dB                |
| EMG               | 600 kbps          | -4.77dB                 |
| ECG               | 250kpbs           | -1.1dB                  |

Table 2: Cutoff threshold SNR for IMD traffic
We refer to the same example by considering 650kbps information rate, which shows successful eavesdropping probability of 19% at 400mm. But in case, if information rate is reduced to 0.6kbps, at a same distance of 400 mm probability of successful eavesdropping is close to 100%.

Figure 4: Probability of successful eavesdropping with varying outage probability of Alice-Bob link at fixed distances.

Figure 3 gives probability of successful eavesdropping for different information rates, against certain fixed distance. Alice and Bob link is considered as 150mm whereas Alice and Eve link is changed. For our case, we consider Alice-Eve distance of 150mm, 350mm, 550mm, 750 and 1000mm. The eavesdropping risk is calculated for these distances with different information rates (R). For each information rate, we calculated corresponding cutoff SNR (γ_{th,AB}) and then find P_{SE} by (14). Figure 3 shows that if we have Alice-Eve distance of 1 meter and an Information rate of 1kbps, probability of successful eavesdropping is 85% and reduces to 10% at a rate of 60kbps. Thus by increasing information rate, probability of successful eavesdropping reduces.

We also provide results of eavesdropping risk against outage probability of main link (Alice-Bob). Figure 4 is in logarithmic scale, which shows that as outage probability of Alice-Bob link increases, probability of successful eavesdropping reduces. It can also be seen that for Alice-Bob link outage probability of 0.01, the minimum distance should be approximately 1.5m for having the eavesdropping risk of 0.001.

5. CONCLUSION & FUTURE WORK

In this paper we perform analysis of eavesdropping risk for a communication between an implant and subcutaneous node. We analyze probability of successful eavesdropping for different distances with different information rates. We analyze that proper tradeoff is required between information rate and corresponding eavesdropping risk. Our numerical results show that for the information rate (R) of 650kbps, there is 5% probability of successful eavesdropping at a distance of 500mm. If the information rate is reduced, eavesdropping risk increases over a larger distance. Our results also show that path loss reduces eavesdropping risk whereas antenna gains increases the risk. In future, it will be interesting to take different scenarios where we can consider transmission from subcutaneous node to external programmer or directly from leadless capsule to a programmer. We would also like to perform risk analysis using UWB band and finding probability of successful eavesdropping.

6. ACKNOWLEDGMENTS

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

7. REFERENCES

[1] A. Pope, P. Bouxsein, F. J. Manning, K. E. Hanna et al., Innovation and invention in medical devices: workshop summary. National Academies Press, 2001.
[2] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, “Sok: Security and privacy in implantable medical devices and body area networks,” in Security and Privacy (SP), 2014 IEEE Symposium on. IEEE, 2014, pp. 524–539.
[3] N. Y. Times, “Vice president news,” http://www.nytimes.com, October 2013.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay, “Privacy risk models for designing privacy-sensitive ubiquitous computing systems,” in Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques. ACM, 2004, pp. 91–100.
[10] K. Sayrafián-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] J. Wang and Q. Wang, Body area communications: channel modeling, communication systems, and EMC. John Wiley & Sons, 2012.
[12] D. Tse and P. Viswanath, “Fundamentals of wireless communications,” 2004.