20th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, IEEE CAMAD 2015, 7-9 September

Physical Layer Security for Wireless Implantable Medical Devices

Z. Esat Ankaralı[1], A.Fatih Demir[1], Marwa Qaraqe[2], Qammer H. Abbasi[3], Erchin Serpedin[2], Huseyin Arslan[1,4] and Richard D. Gitlin[1]

[1]Department of Electrical Engineering, University of South Florida, USA

[2]Department of Electrical and Computer Engineering, Texas A&M University, College Station

[3]Department of Electrical and Computer Engineering, Texas A&M University at Qatar

[4]Department of Electrical and Electronics Engineering, Istanbul Medipol University

***Abstract*—Wireless communications are increasingly important in health-care applications, particularly in those that use implantable medical devices (IMDs). Such systems have many advantages in providing remote healthcare in terms of monitoring, treatment and prediction for critical cases. However, the existence of malicious adversaries, referred to as nodes, which attempt to control implanted devices, constitutes a critical risk for patients. Such adversaries may perform dangerous attacks by sending malicious commands to the IMD, and any weakness in the device authentication mechanism may result in serious problems including death. In this paper we present a physical layer (PHY) authentication technique for IMDs that does not use existing methods of cryptology. In addition to ensuring authentication, the proposed technique also provides advantages in terms of decreasing processing complexity of IMDs and enhances overall communications performance.**

***Index Terms*—Body area networks, implantable medical devices (IMDs), *in-vivo* wireless communications, security.**

I. Introduction

In our vision of pervasive healthcare, implantable medical devices (IMDs), e.g., pacemakers, implantable cardiac defibrillators (ICDs), drug delivery systems and neurostimulators, have a vital importance. They provide a substantial advantage by enabling physicians to manage many diseases [1] with the identification, monitoring, and treatment of patients in anywhere, at anytime [2] and save innumerable lives [3]. Such IMDs have already been deployed in many patients, and their usage is expected to expand in the near future. For example, the number of insulin pump users in 2005 was about 245,000, and the expected growth rate for the insulin pump market is 9% from 2009 to 2016 as reported in [4].

While many IMDs are able to perform complex analyses and sophisticated decision-making algorithms in addition to storing detailed personal medical data, wireless signals conveying critical information need protection from a variety of attacks [5]. Considering the growing utilization of IMDs and increasing security risks, comprehensive techniques against wireless adversaries have emerged as an important requirement to ensure that the patients can use IMDs confidently and without harm. Authentication is critically important, since an adversary may wirelessly change various IMD parameters and cause a dangerous mistreatment of a patient. For example, an insulin pump user might face an overdose attack that may even result in death. In the literature, proposed protection techniques against such attacks can be classified to three main categories; cryptography, anomaly detection, and "friendly" jamming. A review of the literature on these approaches, along with their comparison is done in [6]. A brief description of these approaches can be given as follows:

- *Cryptography*: Relies on a secret key shared between IMD and the external device. However, cryptography may not be properly deployed if the limitations of IMDs are considered as mentioned in [7]. For example, cryptography based techniques conflict with the accessibility requirement of IMDs in the case of any emergency, since the closest physician may not have the secret key. Then, required urgent modifications on IMD cannot be done and patients may experience serious problems.
- *Anomaly detection*: Relies on identifying the legitimacy of received commands based on the variance of IMD parameter values that are observed over the time. However, such a mechanism is not agile in adapting new conditions of patients as it requires long time monitoring and data analyzing to achieve a reasonable performance.
- *Friendly Jamming*: This technique attempts to sense the existence of a malicious attack and prevents the reception of illegitimate commands by jamming the IMD with the help of an external device. Although, it does not have a direct conflict with IMD requirements, energy efficiency of the external device is a drawback as it performs very complex and power consuming operations, i.e., continuous spectrum sensing and jamming, and may preclude normal IMD operation.

A popular approach in IMD communications and in aforementioned security techniques is the usage of a wearable external device (WED) attached on the patient body. These devices act as a relay between the IMD and the central

This publication was made possible by NPRP grant # NPRP 6-415-3-111 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

Corresponding author's e-mail: zekeriyya@mail.usf.edu

external node, and provide a substantial advantage in terms of the IMD's energy consumption for signal transmission and processing. In this study, we propose a pre-equalization based wireless communication system between the IMD and the WED in order to improve performance in terms of channel estimation, decrease the processing burden on the IMD and importantly provide authentication at the physical layer. An illustration of the proposed scenario is given in Fig.1. Considering the small distance between the IMD and the WED, the resulting path loss lower than that experienced by the nodes located relatively far away from the patient. These more distant nodes may be adversaries and our goal is to prevent any adversary (AD) from controlling the IMD. Basically, the IMD sends pilot signals to enable the WED to estimate the channel. By using this estimation, the WED pre-equalizes the data signal that is transmitted to the IMD. Assuming that an adversary cannot be closer to the IMD than the WED, the pilot signals will reach the adversary with much less power and greater dispersion and lead to erroneous channel estimation. Since pre-equalization with such an estimation leads to a significant distortion in the AD's signal, an adversary's attempt to communicate with IMD will fail even if the transmitted signal is extremely powerful. In this way, adversaries trying to control or mislead IMDs from relatively distant locations can be prevented from achieving impersonation attacks.

However, these aforementioned techniques may not ensure security if ADs deploy highly advanced signal processing algorithms or hardware having a very small noise floor. Then, they might still be able to estimate the channel, properly. In case of such scenarios, we also introduce a friendly jamming mechanism to our system. In order to achieve this, we design the pilot signal transmitted by IMD as a "wake-up" signal for WED. If the pilot signal is transmitted upon the request of an unauthorized user, the WED is activated and sends a jammer signal to IMD for preventing it from decoding any AD's signal. This capability is extremely important for the IMDs to retain the ability to treat the patient and resist the AD attack. Any wrong treatment, e.g., high voltage injection for a pacemaker and overdosing of an insulin pump, may result in serious problems including death. Also, since equalization is performed in the WED, the proposed technique works in a power efficient way in terms of processing. Also, since more advanced components can be deployed on WEDs because of its size flexibility as compared to IMD, channel estimation performance can be considerably enhanced.

The paper is organized as follows. Section II provides the system model for the proposed technique. In Section III, channel effects for WED and AD are presented. Finally, numerical results are given in Section IV, and Section V concludes the paper.

II. System Model

Channel estimation performed by a WED can be much better than that performed by an IMD because of the greater

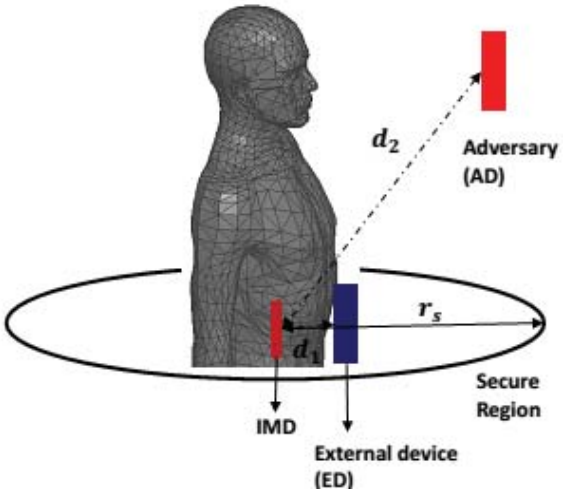

Fig. 1. Wireless adversaries may perform various malicious attacks and compromise the safety of IMD using patients

capabilities of the external device. For example, more advanced device components with a lower noise floor can be used in the design of WEDs and the channel estimation error can be reduced. In this regard, pre-equalization might be a very useful method for IMD communications. In Fig. 1 wireless adversaries (AD) may perform various malicious attacks and compromise the safety of IMDs. In our proposed scenario, the IMD transmits a pilot signal, $p(t)$, that is used to enable the WED to estimate the channel. Then channel estimation is performed as

$$h_\epsilon(t) = h(t) + w(t)p^{-1}(t) \tag{1}$$

where $w(t)$ is the additive noise. Note that, h_ϵ is defined as a scalar value, i.e, a one-tap channel estimation is performed for pre-equalization considering the non-dispersive medium between IMD and wearable external device (WED). Then, we can give the analytical expression of the baseband signal, transmitted from WED as

$$x(t) = h_\epsilon^{-1} \sum_{n=-\infty}^{\infty} X_n g(t - n\tau_0), \tag{2}$$

where n, $g(t)$ and τ_0 indicate the index of QAM symbol, pulse shaping filter and time spacing between the symbols, respectively. After passing through the linear time-variant channel, $h(t)$, received signal including the additive noise can be written as

$$y(t) = \int_{-\infty}^{\infty} h(\tau)x(t-\tau)d\tau. \tag{3}$$

Assuming the channel is a one-tap channel due to the small distance between communicating nodes, the received signal can be shown as

$$r(t) = h(t)x(t) + w(t) \tag{4}$$

TABLE I
PATH LOSS MODEL PARAMETERS [8]

Parameter	Parameter Value
n	1.48
d_0	0.01 m
P_{0dB}	39.37 dB

where $h(t)$ denotes the channel gain as a function of time, $w(t)$ is the additive noise.

In channel estimation, received pilot symbols are also subject to the channel impairments. Therefore, the estimated channel response can be given as

$$\hat{h} = h + \underbrace{w(t)/P}_{\epsilon}, \tag{5}$$

where P indicates the pilot symbol and ϵ stands for the error in channel estimation. Its effect on bit-error-rate (BER) performance should be investigated to identify the secure region around the patient's body. Considering more sophisticated attacks where ADs are equipped with highly advanced devices, we propose an additional mechanism to ensure authentication. Here, the pilot signal sent by IMD is regarded as a "wake-up" message for the WED. If an AD requests a pilot transmission before sending an unauthorized command to the IMD, the WED activates as soon as IMD sends the pilot signal. Since the WED can easily understand that an unauthorized user made this request, it sends a jamming signal and blocks reception by the IMD. However, the AD may send its signal at the same time with WED and may dominate WED's command with a very high power. In order to overcome this issue, IMD applies a power threshold criteria not to decode a received message exceeding a certain power level. If the WED sends its jamming signal close to this power level, additional AD signals will likely result in exceeding the pre-determined power threshold and the IMD's reception will be blocked. In this way, the AD will be disabled from maliciously controlling the IMD.

III. Channel Models for WED and Adversary

The major effect on a narrow band wireless signal is path loss for in body communications as dispersion in time is generally small compared to the data symbol duration. Also, considering a stationary environment, the frequency dispersion effect of the channel may not need to be taken into account. Note that accounting for dispersion gives us more degrees of freedom to provide security. Therefore, the one-tap technique may be viewed as a worst case scenario. In order to investigate the channel effect on legitimate and malicious nodes, a path loss channel model obtained as the function of distance for body centric communication environment should be used. The general expression for such a model is given as

$$P_{\mathrm{dB}} = P_{0dB} + n\left(\frac{d}{d_0}\right) \tag{6}$$

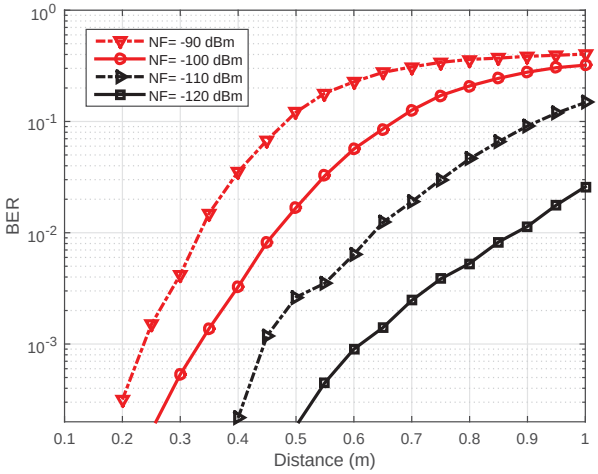

Fig. 2. BER performance versus distance for different noise floors (NFs)

where d is the distance, d_0 is the reference distance and P_{0dB} is the path loss for reference distance. These parameters for a body model is given in [8] as shown in the Table 1. In order to investigate the performance of the users located far away, different channel models might be superposed with the given model. However, we only consider the users nearby the patient. Therefore, only given model will be taken into account.

IV. Numerical Results

Performance of the proposed technique is presented using MATLAB simulations. Firstly, we investigate the effect of distance between the IMD and other devices on the BER performance. As we mentioned before, a greater distance corresponds to a further path loss. As a device is moving away from the IMD, the power of the received pilot signal become weaker and this will lead to error in channel estimation. A command signal pre-equalized with a erroneous channel estimation will naturally cause a distortion in the signal independent of the signal's SNR. In Fig.2, BER results of a command signal sent from different distances is given, where the SNR of the transmitted signal is specified as 100 dB in order to see the effect of channel estimation error only. As shown in Fig.2, increasing distance of the AD from the IMD and resulting increased channel estimation error dramatically degrade BER performance. For example, if an adversary is located 90 cm away from the IMD, more than 1% error probability is experienced for 0 dBm transmission power and -120 dBm noise floor (NF) at the AD.

Considering some scenarios where the AD performs a strong signal processing and uses more advanced hardware having very low noise floors, we also deployed our self-jamming approach to ensure authentication. As mentioned earlier, IMD applies a power-limitation criterion in order to prevent the AD from dominating WED's jamming signal. While determining the WED's jamming signal power,

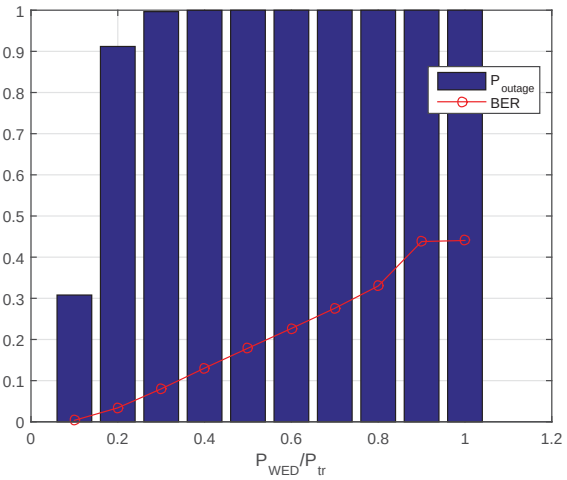

Fig. 3. Adversary outage probabilities for different jammer signal powers

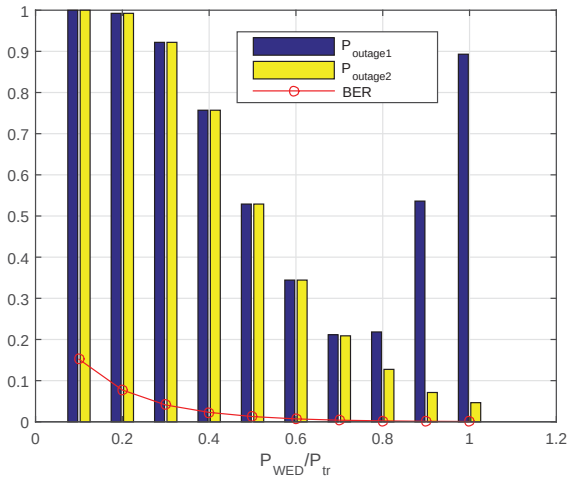

Fig. 4. Outage probabilities of WED's command with and without proposed technique represented by $\mathrm{P}_{\mathrm{outage1}}$ and $\mathrm{P}_{\mathrm{outage2}}$, respectively

P_{WED}, we used a power threshold P_{tr} as a metric, i.e., P_{WED} is specified in terms of P_{tr}. Command signals are designed as packets consisting of 150 QPSK symbols and the outage probability of these packets will be used as the performance measure. In Fig. 3, outage probabilities for different jamming powers indicated as P_{WED}/P_{tr} are given for the AD along with the bit-error probabilities. Note that we assumed that AD has perfect channel estimation and its signal has a 20 dB SNR for this case. Even in such an extreme case, the AD's packets are all distorted when P_{WED} is 30% of P_{tr}. Then, we can ensure proper authentication, i.e., blockage of AD, once P_{WED}/P_{tr} is 0.3 or more.

We also investigate the effect of the proposed technique on the desired communication between the IMD and the WED. The power of the WED's signal is very critical here since IMD stops reception based on the received power. If WED's signal power exceeds P_{tr} after being combined with noise, legitimate commands will be eliminated as well. In Fig.4, outage probabilities are given as $\mathrm{P}_{\mathrm{outage1}}$ and $\mathrm{P}_{\mathrm{outage2}}$ for the WED's command with and without proposed technique, respectively. For small power values, outage probability for both cases are almost equal to each other. Here, P_{WED} is given as 0 dBm and if the P_{WED}/P_{tr} ratio is 1, the SNR of the received signal is specified as 20 dB, i.e., noise floor of IMD is adjusted for having 20 dB SNR. Then, if P_{WED}/P_{tr} ratio is 0.1, the SNR become 10 dB and the outage probability approaches to unity. The proposed technique does not degrade the successful transmission performance of WED unless P_{WED}/P_{tr} is greater than 0.7. After that level, the probability of blocking the WED packets increases since transmission power gets close to the threshold. Therefore, jamming power of WED P_{WED} should carefully be selected considering WED's performance and authentication requirements.

V. Conclusions

In this study, a physical layer authentication technique based on pre-equalization is proposed for IMDs. Besides authentication, our approach can enhance channel estimation performance by utilizing more advanced hardware and signal processing complexity in the WED because of its external location and not being limited in size as IMDs. Since only path loss was considered for the in vivo channel estimation, including other channel effects, e.g., dispersion in time and frequency will likely enable increase reliability. This will be investigated in our future studies.

References

[1] D. T. 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 *IEEE Symposium on Security and Privacy*, 2008.

[2] K. Malasri and L. Wang, "Securing wireless implantable devices for healthcare: Ideas and challenges," *IEEE Comm. Mag.*, vol. 47.7, pp. 74–80, 2009.

[3] W. H. Maisel and K. Tadayoshi, "Improving the security and privacy of implantable medical devices," *New England journal of medicine*, vol. 362.13, p. 1164, 2010.

[4] *Insulin pumps - global pipeline analysis, opportunity assessment and market forecasts to 2016, globaldata. Global Data (2010).*

[5] K. Fu, "Inside risks: Reducing risks of implantable medical devices," *Communications of the ACM*, vol. 52.6, pp. 25–27, 2009.

[6] Z. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on*. IEEE, 2014, pp. 246–249.

[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. 41.4, pp. 2–13, 2011.

[8] A. F. Demir, Q. H. Abbasi, Z. E. Ankarali, E. Serpedin, H. Arslan *et al.*, "Numerical characterization of in vivo wireless communication channels," in *RF and Wireless Technologies for Biomedical and Healthcare Applications (IMWS-Bio), 2014 IEEE MTT-S International Microwave Workshop Series on*. IEEE, 2014, pp. 1–3.