External Relaying Based Security Solutions for Wireless Implantable Medical Devices: A Review

Selman Kulaç, Murat H Sazli, H. Gökhan Ilk

External Relaying Based Security Solutions for Wireless Implantable Medical Devices : A Review

Selman Kulaç
Department of Electrical and Electronics Engineering
Faculty of Engineering
Duzce University
Konuralp, Duzce 81620, TURKEY
Email: selmankulac@duzce.edu.tr

Murat H. Sazlı
Department of Electrical and Electronics Engineering
Faculty of Engineering
Ankara University
Gölbaşı, Ankara 06830, TURKEY
Email: sazli@eng.ankara.edu.tr

H. Gökhan İlk
Department of Electrical and Electronics Engineering
Faculty of Engineering
Ankara University
Gölbaşı, Ankara 06830, TURKEY
Email: ilk@ieee.org

***Abstract*—The use of wireless applications is increasing in health care services. One of these areas is communicating with wireless Implantable Medical Devices (IMD). For existing or already implanted IMDs, wireless communication security and privacy is very important when it is against active and passive adversaries. In this study, current proposed solutions with external relaying devices that protect the wireless communication data of IMDs are explained. The advantages and disadvantages of these solutions are emphasized comparatively.**

***Index Terms*—IMD Telemetry Communications, Remote Control, Physical Layer Security, Security for IMDs**

I. Introduction

THE demand of the usage of wireless devices increases in biomedical applications. Because of having many advantageous such as tracking and controlling the patients remotely or being utilized in various disorder treatments, implantable medical devices (IMD)s have received considerable interest by the researchers and medical doctors. These devices should be designed by taking into consideration the fact that they are being placed within the human body. This fact provides that IMDs should be biocompatible, less complex, physically small, reliable, power efficient, and should guarantee secure communication [1]. Since the communication is carried out in wireless manner in IMDs, which can be utilized in different tasks such as deep brain neorostimulators (DBS), implantable cardiac defibrillators (ICD), insulin pumps; satisfying the secure communication becomes a critical task. For instance, in deep brain neorostimulators (DBS), physician can monitor the neurochemical changes in the specific part of the patient's brain and send the stimulation data, i.e., command or remote control data to the IMD based on the therapy to produce electrical impulses. If there is another device between physician and patient, this device can also perform the same duty by working as relay node. On the other hand, different types of query or command data can be sent to IMD, too. For instance, changing the therapy parameters of IMDs, turn-off device, treatment modifications, deliver command shock can be given as some critical examples/commands [2]–[4]. It is important to protect these data from the adversaries. If an adversary knows any of those data, it can easily manipulate the IMD to injure or even kill the patient.

ISBN 978-3-903176-03-4 2018 IFIP

This study only focuses on the relaying devices and the solutions which provide wireless secure communication capability for IMD systems. Therefore, this study reviews all external relaying solutions obtained in recent literature.

The remainder of this paper is organized as follows. General technical information about wireless implantable medical device communication is given in Section II. Section III comprises attack scenarios for existing wireless implantable medical devices. Section IV expresses external relaying based security solutions for wireless implantable medical devices in detail, and finally, conclusions are drawn in Section V.

II. Wireless Implantable Medical Device Communication

Wireless frequency band between 402 - 405 MHz has been allocated for wireless implantable medical device communication in USA since 1999 and called medical implantable communications service (MICS) band [5]. Communications with IMDs from external programmers in this band has been allowed with maximum 25 μW (an EIRP level of -16 dBm) transmission power, because suitable signal propagation in the human body, higher data rate transmission, international acceptability and higher operating ranges about several meters are possible with using this band. Frequency agility (FA) and listen before talk (LBT) is also necessary for MICS operation [5], [6] and [7].

MICS band has 3 MHz bandwidth between 402 MHz and 405 MHz and 10 channels. These are used to avoid interferences and to support the simultaneous operation of multiple devices (such as hospitals with multiple rooms) in the same area. It has been shown that even at 3 MHz, one or two channels can be used in many environments [6]. Modulation type is also defined as frequency shift keying (FSK) in [6].

III. Attack Scenarios for Existing Wireless Implantable Medical Devices

There are two types of attack scenarios that can be made against IMDs and these can be called passive and active attack

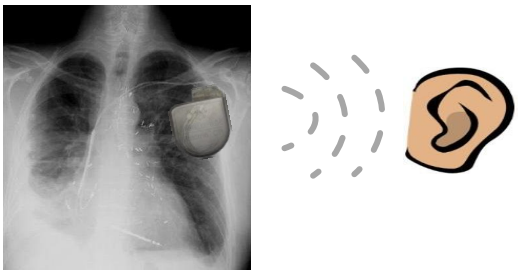

Fig. 1. Passive attack scenario

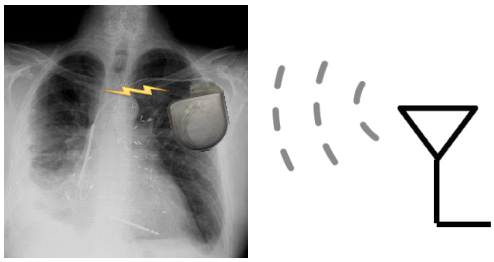

Fig. 2. Active attack scenario

scenarios.

In a passive attack scenario, a malicious audience known as eavesdropper can get device status and history information, disease diagnosis and history information, patient privacy information, and patient vital information by listening as in Fig.1.

In the active attack scenario, an adversary can send the unwanted commands to the implant device, which can hurt the patient, change the treatment parameters of the IMD, send the shock command, turn off the device, change the functions of the device as in Fig.2

IV. External Relaying Based Security Solutions for Wireless Implantable Medical Devices

In this section, recent proposed solutions with external relaying devices providing security for the already implanted IMDs are expressed comparatively.

In the first study, a relaying device named Communication Cloaker is suggested in [8]. It can be thought as medical alert bracelets. It is aimed to balance safety with security for IMDs. Cloaker acts like a relay after being worn. This relaying process includes cryptographic method and it is needed to change the design of Wireless IMD a bit. Wireless IMD should detect the existence of Cloaker by pinging using keep-alive messages. This is also not power efficient way for wireless IMDs. But it helps to save battery power of IMD against adversary attacks.

Another external relaying device named IMDGuard which provides secure communication is proposed in [9]. In this solution, mutual cryptographic key management and authentication process based on patient's ECG signals is used as in Fig.3. IMDGuard has also jamming capabilities of all

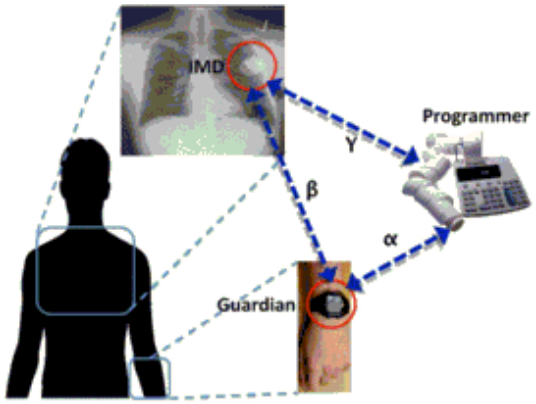

Fig. 3. IMDGuard system model [9]

IMD transmissions. Existing IMDs should be changed due to cryptographic applications for IMDGuard and Communication Cloaker solutions. As a result, cryptographic application requires that the pre-placed IMDs be replaced, increases the unwanted hardware and computational complexity and need extra power consumption.

The other relaying device, named MedMon, considers anomaly detection technology [10]. MedMon does not act as a relaying device, only focuses on the physical properties of the transmitted signals. If the abnormality is perceived, the patient is only warned as in Fig.4 (a) in case of low potential damage or the signals are also jammed as in Fig.4 (b) in addition to warning in case of high potential damage. MedMon provides good protection against adversaries, but does not provide protection to eavesdroppers.

In [2], another similar relaying device, namely shield and carried on the patient, designed by the authors is introduced to protect data against adversaries. This device is placed between IMD and its programmer to fulfill secure communication by jamming as in Fig.5. The shield can be used to protect IMD against spoofing attacks. When an adversary sends the spoofing data, the shield would detect it and transmit a jamming signal as in previous case. Since the jamming would make the spoofing data meaningless, IMD will not be able to decode it, and thus the security would be provided. This shield can also ensure security communication against eavesdroppers. When IMD sends the data to its programmer as a reply, at the same time, shield transmits the jamming signal to protect the data from eavesdroppers. But, as shown in [11], the data under jamming can still be extracted by the eavesdroppers via utilizing multiple-input multiple-output (MIMO)-based attack. Furthermore, there is a weakness of the security when transmitting commands in [2]. When shield sends a query or command data to the patient, this transmission will not be jammed but only reply of IMD will be jammed. In [1] and [12], authors also define that when the shield transmits commands to the IMD, confidentiality is not guaranteed. If

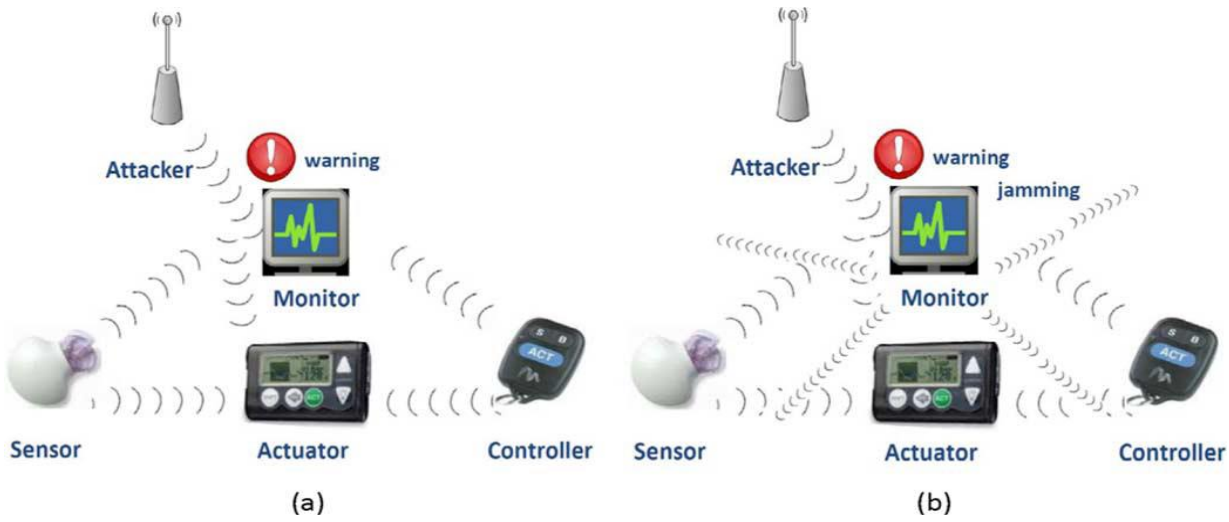

Fig. 4. MedMon working mechanism [10]

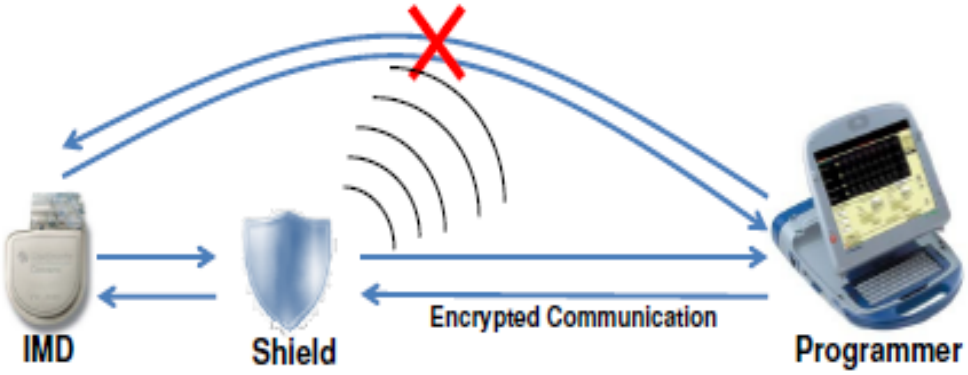

Fig. 5. Relaying and external device named Shield [2]

eavesdropper decodes the command data, he or she can easily deceive IMD.

Since the other external relaying solution named Security Belt focuses on secure full duplex transmissions of wireless IMD systems, a new secure design integrable to existing unsafe systems has been proposed in [13]. This security belt is a wearable device and looks like a belt as in in Fig.6. However, some advanced transceiver antennas have been installed on this belt in order to provide effective both way transmissions and physical layer security in Fig.7. In this study, when transmissions are carried out to the IMD, beam-focused multi-antennas in the most appropriate positions on the belt are randomly switched and run. Multi-jammer switching is applied with MRC combining or majority-rule based reception techniques when transmissions from the IMD are performed. In this approach, energy consumption of the IMDs may also be reduced and the battery life of the IMD may be prolonged. In this solution, all messages containing the commands sent by the physician as understood from the Fig.8 and also remote control data involving patient health and device history are protected.

As a result, all transmissions involving the physician's prescription and the patient's privacy data should be protected. The eavesdropper should not resolve the analysis of the doctor's treatment and patient outcomes. All prescription, patient related and device data etc. transmitted wirelessly needs to be protected for the already implanted IMDs with external relaying devices.

V. Conclusion

Some health services are increasingly using wireless applications. One of these areas is in communication with the wireless Implanted Medical Devices (IMD). For existing or already

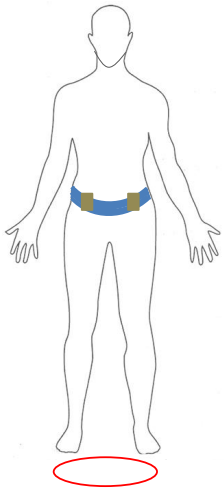

Fig. 6. Security belt solution [13]

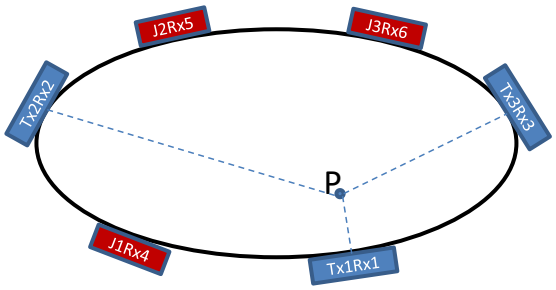

Fig. 7. All transceiver antennas on Security Belt, some of which are used for jamming [13]

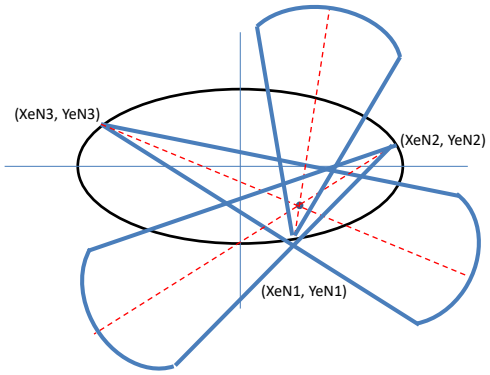

Fig. 8. Secure transmission to IMD in security belt solution [13]

implanted IMDs, wireless communication security and privacy is very important when facing active and passive attackers. In this paper, the existing proposed solutions with external relaying devices that protect the wireless communication data of IMDs are expressed comparatively.

REFERENCES

[1] M. Zhang, A. Raghunathan, and N. Jha, "Trustworthiness of medical devices and body area networks," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug 2014.

[2] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.

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

[4] S. E.Marin, D.Singelee, "Security analysis of an implantable cardioverter defibrillator," in *34th WIC Symposium on Information Theory & 3rd Joint WIC/IEEE Symposium on Information Theory and Signal Processing VLSI (ISVLSI)*, May 2013, pp. 216–221.

[5] *MICS Medical Implant Communication Services, FCC 47CFR95.601–95.673 Subpart E/I Rules for MedRadio Services*, Federal Communications Commission Std.

[6] *ITU-R Recommendation RS.1346: Sharing between the meteorological aids service and medical implant communication systems (MICS) operating in the mobile service in the frequency band 401–406 MHz, 1998.*, International Telecommunications Union. Std.

[7] Y.-H. Liu, C.-J. Tung, and T.-H. Lin, "A low-power asymmetrical mics wireless interface and transceiver design for medical imaging," in *IEEE Biomedical Circuits and Systems Conference (BioCAS)*, Nov 2006, pp. 162–165.

[8] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proceedings of the 3rd Conference on Hot Topics in Security*, ser. HOTSEC'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 5:1–5:7. [Online]. Available: http://dl.acm.org/citation.cfm?id=1496671.1496676

[9] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 1862–1870.

[10] M. Zhang, A. Raghunathan, and N. 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, Dec 2013.

[11] N. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *IEEE Symposium on Security and Privacy (SP)*, May 2013, pp. 160–173.

[12] M. Zhang, A. Raghunathan, and N. 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, Dec 2013.

[13] S. Kulaç, "Security belt for wireless implantable medical devices," *Journal of Medical Systems*, vol. 41, no. 11, p. 172, Sep 2017. [Online]. Available: https://doi.org/10.1007/s10916-017-0813-5