A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security

Z. Esat Ankaralı[1], Qammer H. Abbasi[2], A.Fatih Demir[1], Erchin Serpedin[3], Khalid Qaraqe[2], Huseyin Arslan[1,4]

***Abstract*—Nowadays wireless communication is playing a vital role in implantable medical devices (IMDs) on health-care applications. It has many advantages in remote health monitoring, treatment and prediction for critical cases. However, any drawback in security of these devices against malicious attacks may lead to serious problems, such as theft of private information, wrong treatment and even death. In this paper, a comparative review of the current literature on IMD security research is provided to have a better understanding of the state of the art and the gaps in this direction.**

***Index Terms*—Body Area Networks, Implantable medical devices (IMDs), In-Vivo communication, Security.**

I. Introduction

Implantable medical devices (IMDs), e.g., pacemakers, implantable cardiac defibrillators (ICDs), drug delivery systems and neurostimulators, provide substantial improvement in healthcare by helping to manage many diseases [1] and saves innumerable lives [2]. They offer a great advantage to achieve the vision of pervasive healthcare that enables the identification, monitoring, and treatment of patients anywhere, anytime [3]. These devices have already been deployed in the body of many patients, and its usage is expected to be grown further in the future.

Many IMDs perform complex analyses and sophisticated decision-making algorithms in addition to storing detailed personal medical information, and communication capability automatically, remotely, and wirelessly. These functionalities improve the quality of healthcare but their susceptibility to the malware and malicious attacks emerges as a critical issue [4] [5]. Due to the growing demand of IMDs and increase in security risks, patients may not use these devices comfortably in the near future. Therefore, providing the security of each operation performed by medical devices is a serious need to ensure the patients' safety and privacy [6]. This requires a proper unification of technology and regulation. In this study, a review of the research on secure wireless communication for IMDs including the potential security threats, challenges in secure system design and the proposed techniques in this direction are provided with a special focus on the main security issues in wireless communication; eavesdropping, impersonation and jamming. Some studies on wireless body area network security compatible with IMDs are also included. In this paper, in addition to the survey, a comparison of the proposed techniques in terms of addressing the wireless security problems to understand current concepts, their drawbacks and advantages against different type of adversaries is presented.

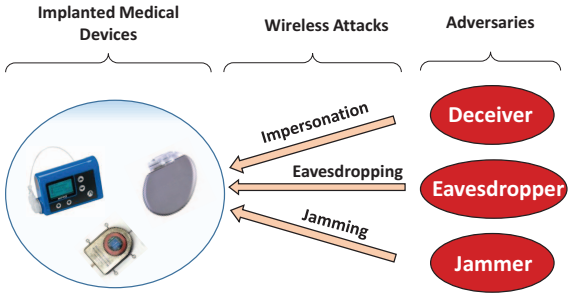

Fig. 1. Wireless adversaries may perform various malicious attacks and compromise the safety of IMD using patients

II. IMD Security Issues

Adversaries that likely exist around an IMD user may threat the patient in different ways. An adversary may passively wait to catch private health-related information transmitted by IMD or actively attempt to modify IMD parameters. It may be located nearby the patient or very close to the unit controlling the IMD from the hospital. Also, there may be a group of coordinated adversaries rather than a single one. Considering the existence of these adversaries, possible malicious attacks should clearly be revealed in order to construct a comprehensive framework for secure IMD design [2]. Various classifications of the IMD security issues are provided in the literature [1] [3] [7] [8]. In this paper, these issues are compiled under three main malicious attacks in wireless communication; eavesdropping, impersonation and jamming attacks.

Impersonation: Authentication can be considered as the most critical issue in IMD security and most of the related studies in the literature focuses on that [1]. If the access of a malicious node to the IMD cannot be prevented,

- Virus and malware type of softwares can be installed in an IMD to create malfunctions such as keeping IMD always open to decrease battery life [4] or ignoring some commands from the legitimate programmer.
- IMD can be hacked and fatal operations may be performed such as ordering an insulin pumps to apply an overdose insulin injection [9], [10], or an implantable

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.
[1]Department of Electrical Eng., University of South Florida, USA
[2]Department of Electrical and Computer Engineering, Texas A&M University at Qatar
[3]Department of Electrical and Computer Engineering, Texas A&M University, College station, USA
[4]School of Eng. and Natural Sciences, Istanbul Medipol University

MOBIHEALTH 2014, November 03-05, Athens, Greece

DOI 10.4108/icst.mobihealth.2014.257411

TABLE I
CONFLICTING REQUIREMENTS IN IMD DESIGN AND SECURITY.

IMD Needs	Security Needs
Limited energy consumption	Extra processing and signaling
Availability in emergencies	Protection against unauthorized access
No modification for implanted devices	Additional functionalities on IMD
Less software for low susceptibility against software bugs	Extra algorithms for security operations

cardiac defibrillator to emit a shock designed to induce a fatal heart rhythm [11].

- Data stored in IMD can be reached by unauthorized nodes which may leads to identity thefts [12].

Rather than a malicious attack, a legitimate node may access to wrong IMD accidentally, which may create problem for not only the wrong IMD but also the intended one. Therefore, a robust mechanism controlling the access to the IMDs should be deployed to maintain their safety and reliability.

Eavesdropping: Eavesdropping attacks compromise the secrecy of transmitted private data e.g., patients' personal information, medical measurements, user location, and information that may be used to perform additional attacks such as cloning as mentioned in [3] and [13]. Although, such attacks do not look as dangerous as impersonation attacks, harvested information may enable unauthorized users to access medical devices or IMD controller units. Therefore, protection of the data privacy is a critical issue for a secure system design.

Jamming: Besides the aforementioned attacks, medical devices may encounter jamming attacks that aim denial of service (DoS) [14] by flooding the operating frequency of medical devices with an irrelevant signal. Maintaining the transmission of IMD under such attacks is quite difficult [3] and should be studied carefully.

III. CHALLENGES IN IMD SECURITY

Secure communication is considered as one of the most critical issue for IMDs and many studies have already been presented in the literature. However, some issues conflicting with basic IMD requirements emerge in secure system design [3]. In order to develop a reasonable system these challenges should be considered carefully. They are itemized as follows:

- *Battery Life* : An IMD should last for many years inside a patients body as replacing the device or any piece of it requires surgery [4]. Therefore, battery life should be long enough. However, security algorithms degrade battery life due to their operational complexity.
- *Adaptability* : In order to provide security for any medical device, adaptable techniques that do not require any modification on IMDs are crucial, especially for the previously implanted devices.
- *Availability* : While authentication algorithms should prevent the access of unauthorized users to the IMD, in the case of an emergency, where the patient is not able to disable authentication mechanism, IMD should be available to a doctor for an urgent treatment, even if he/she is not authorized previously.
- *Reliability* : Security mechanisms introduce extra components to the system or run extra algorithms which increases the susceptibility of IMDs against software bugs and hardware impairments, and lead to malfunctions. Therefore, security mechanisms should be robust enough to ensure system reliability.

IV. REVIEW OF THE LITERATURE

Most common techniques in wireless communication security are based on cryptography for eavesdropping and impersonation [15]. However, conventional approaches may not be properly deployed in IMDs. For example, secret key storage and data encryption are memory demanding operations [16] and one may question the feasibility of regular encryption considering the limited memory of the IMDs, which should be used inside the body for years. Also, encryption with preshared and stored keys conflicts with accessibility requirement of IMDs in the case of an emergency as a doctor should be able to treat the patient even if he/she is not authorized previously. In order to overcome these challenges, usage of physiological signals is first introduced in [17], and practiced for electrocardiogram (ECG) and photoplethysmogram (PPG) signals in [18]. Alternatively, inter-pulse intervals (IPIs) of heartbeats are exploited to generate secret keys in [19]. However, ECG based secret key generation dominates the others in the literature [20] [21], because of its higher randomness as compared to other physiological signals (PVs) such as heart rate, blood pressure and temperature along with the aforementioned ones.

For managing the secure communication between IMD and programmer considering the accessibility requirement, Denning et al. discussed the usage of wearable external devices [22] and introduced *Cloakers* [23], as a new direction in IMD security. While Cloakers does not allow unauthorized access to the IMD, security mechanism can be disabled by removing the external devices in the case of an emergency. So that, the access of any doctor becomes possible for urgent treatments. Then, various methods related in this context are proposed in the literature.

Another trend targeting to prevent spoofing attacks is anomaly detection based authentication, which observes the IMD related activities either in the body or between transceivers to understand legitimacy of coming commands. In this section, an evaluation and comparison of the present IMD security methods, in terms of robustness against malicious wireless attacks are provided, along with an overview.

A. Privacy against Eavesdropping Attacks

Strengthening the secrecy of wireless data with cryptography can be made possible with a strong secret key, since an eavesdropper can record the transmitted data and can attempt to decode it by trying many combinations of secret key in a long time. Due to the aforementioned challenges of conventional secret key usage, PVs are proposed to be utilized as an entropy source for IMDs. It has many benefits such as continuous key generation and secure key sharing between nodes having touch to the body. However, randomness of PVs is still an open question for practical scenarios [24].

Besides, Chang et al. pointed out that ECG measurements are location sensitive, in addition to having a noisy and distorted behavior [25]. Also, it is claimed that several remotely measurable body values have a strong correlation with ECG signals. For example, pulse oximetry [26] using light-emitting diodes can measure the oxygen saturation in the blood and extract the heart rate that gives information about ECG signals. Considering these facts, an artificial voltage injection, below the harmful limit, to the body is proposed for a robust key establishment. However, achieved bit rates for secret key generation in the experiments are very limited, i.e., 0.469 to 5.429 bits per hour.

Similar to [23], deploying an external wearable device paired with IMD called Guardian is proposed in [21]. IMD and Guardian locally measure ECG signal simultaneously, and secret key generation is performed with a multi-staged algorithm introduced in this study. Although, presented algorithm exploits the entropy of ECG signals better, noisy measurements still remain as a problem in terms of agreeing on a secret key. Considering this issue, a key sharing method is presented in [27]. Basically, each node measures a PV locally and simultaneously and collect the measurements to form a set of sequence named as *feature*. Then these features are organized in an order known by each device, to set a feature vector. One node hashes its feature vector with a noise data called *chaff* and send the resulting data, called *coffer*. The receiver node compares this data with its own feature vector and finds the matching parts to generate the key.Then, receiver sends the indexes of matching data points to the sender to enable it to construct exactly the same key.

Unlike cryptography based and external device assisted approaches, *shield* is proposed in [28] for data privacy of IMD in physical layer with a friendly jamming mechanism discussed in [29]. When IMD starts transmission, shield jams the channel to prevent any malicious eavesdropper from getting the data. As shield knows the jamming signal, by performing a self-interference cancellation operation, shield can receive the signal and relays to the programmer.

B. Authentication against Impersonation Attacks

As mentioned earlier, cryptography is also considered against impersonation attacks and PV based secret keys are used to establish an authenticated secure channel between IMD and programmer [30]. Alternatively, in [21] and [28] authentication is done with a friendly jamming mechanism. When Guardian detects a spoofing attack by adversaries attempting to hide the existence of Guardian and gain access to the IMD, Guardian activates a defensive jamming mechanism to notify IMD about the threat. Note that, this protocol requires a collaboration with IMD and Guardian. In [28], shield targets to prevent spoofing attacks without running any extra algorithm in IMD. Basically, shield keeps sensing the channel and whenever a spoofing attack is detected, it jams the channel for avoiding IMD to decode the illegitimate command. Self-interference cancellation is also performed to understand if spoofing is going on or not.

Unlike cryptography and external device deploying approaches, anomaly detection based methods as presented in [25] [31] utilize the changing patterns of various parameters [32], such as physical anomalies e.g., received signal strength indicator and time of arrival, or behavioral anomalies like drug dose amount, vital signs, etc. For example, an access control scheme for wireless insulin pumps is proposed to avoid malicious overdose attacks in [10]. Insulin pump performs a supervised learning algorithm based on the patient's infusion pattern consist of insulin dosage amount, rate and infusion time. After collecting the pattern related data for a certain amount of time, insulin pump set a safety infusion rate and does not accept the commands attempting to exceed the safety region.

C. Maintainability against Jamming

Jamming is a challenging attack for IMDs and not studied enough in the literature. Well-accepted jamming resistant methods are direct sequence-spread spectrum (DSSS) and frequency hopping (FH) in the literature and they are implemented in [33], for a cardiac pressure sensing system. Although these techniques also improve the communication security against eavesdropping and impersonation attacks, their feasibility for IMDs is very questionable in practical cases considering the hardware design limitations and band regulations [34].

V. Evaluation of the Techniques

Proposed methods should be evaluated according to most critical threats for the given scenario since addressing all the issues is not an easy task. In eavesdropping resistant methods, PV based cryptography techniques provide important advantages upon regular cryptography such as accessibility, no need for key storage and pre-sharing, however they suffer from low randomness and noisy measurements. Although [27] and [21] deal with these issues, they still have vulnerabilities against intelligent attackers as presented in [35]. Also they require modification in IMD algorithms. The friendly jamming approach in [28] protects the signal without these issues. It is also more power efficient for IMDs as all the security activities are done by external device. However, jamming signal power should be determined carefully not to overwhelm the actual signal.

PV based key generation may be more convenient in authentication than secrecy against eavesdroppers, since it is a kind of real time operation and not requires high entropy. However, other issues are valid for authentication and should be considered. Friendly jamming presented in [21] and [28] provides alternative solutions for them. Even if external devices are highly power consuming, it is not a critical problem. Anomaly detection requires data monitoring and analyzing to understand the pattern of legitimate activities. Although it offers an interesting approach, it is not applicable for already deployed devices and its effect on IMDs battery life is questionable. In order to overcome these issues, all the operation is done by an external device in [32].

Other than aforementioned issues, maintaining IMD communication against jamming attacks is still an open problem. Additionally, one may note that almost no study mentions the

TABLE II
CURRENT TRENDS ADDRESSING VARIOUS THREATS FOR IMD SECURITY.

METHODS	Eavesdropping	Impersonation	Jamming
Cryptography (Regular or PV based)	X	X	
External Device deployment	X	X	
Anomaly Detection (e.g., RSS, dose pattern)		X	
FHSS and DSSS	X	X	X

need for secure waveform design. These are open research areas and should be considered for future directions.

VI. CONCLUSION

In this paper, a comparative review of the current literature on wireless communication security techniques for IMDs is provided. Unlike similar studies, the proposed techniques are also evaluated in terms of their adequateness against specific wireless attacks. Thus, required improvements for each method can be understood easily and stated issues can be handled considering the application scenarios.

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] W. Maisel, "Safety issues involving medical devices," *J. Am. Medical Assoc*, vol. 294, pp. 955–985, 2005.

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

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

[5] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: Security and privacy for neural devices," *Journal of Neurosurgery: Pediatrics*, vol. 27, p. E7, 2009.

[6] 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.

[7] V. Pournaghshband, M. Sarrafzadeh, and P. Reiheret, *Wireless Mobile Communication and Healthcare*. Springer, 2013, ch. Securing legacy mobile medical devices, pp. 163–172.

[8] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," *BT Technology Journal*, vol. 24.2, pp. 138–144, 2006.

[9] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *IEEE Int. Conf. on e-Health Networking Applications and Services (Healthcom)*, 2011.

[10] X. Hei, X. Du, S. Lin, and I. Lee, "Pipac: patient infusion pattern based access control scheme for wireless insulin pump system," in *IEEE INFOCOM*, 2013.

[11] N. Leavitt, "Researchers fight to keep implanted medical devices safe from hackers," *Computer*, vol. 43.8, pp. 11–14, 2010.

[12] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel., "Security and privacy for implantable medical devices," *Pervasive Computing, IEEE*, vol. 7.1, pp. 30–39, 2008.

[13] K. Malasri and L. Wang, "Design and implementation of a secure wireless mote-based medical sensor network," in *Proc. 10th Int'l. Conf. Ubiquitous Computing*, 2008.

[14] J. Misic and V. B. Misic, "Implementation of security policy for clinical information systems over wireless sensor networks," *Ad Hoc Net.*, pp. 134–144, 2007.

[15] M. Bellare and N. Chanathip, *Advances in Cryptology-ASIACRYPT*. Springer, 2000, ch. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm, pp. 531–545.

[16] F. Strenzke, *Information Security*. Springer, 2012, ch. Solutions for the storage problem of mceliece public and private keys on memory-constrained platforms, pp. 120–135.

[17] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Int. Conference on Parallel Processing Workshops*, 2003.

[18] C. Poon, Y. Zhang, and S. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44(4), pp. 73–81, 2006.

[19] S. Bao, C. Poon, Y. Zhang, and L. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Trans Inf Technol Biomed.*, vol. 12(6), pp. 772–9, 2008.

[20] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14.1, pp. 60–68, 2010.

[21] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *IEEE INFOCOM Proc.*, 2011.

[22] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," in *in Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI'10)*, 2010.

[23] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *HotSec*, 2008.

[24] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "Sok: Security and privacy in implantable medical devices and body area networks."

[25] S. Chang, Y. C. Hu, H. Anderson, T. Fu, and E. Y. Huang, "Body area network security: robust key establishment using human body channel," in *Proc. of the USENIX conference on Health Security and Privacy*, 2012.

[26] K. K. Tremper, "Pulse oximetry," *CHEST Journal*, pp. 713–715, 1989.

[27] H. Chunqiang, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *IEEE INFOCOM Proc.*, 2013.

[28] 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.

[29] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S.Capkun, "On limitations of friendly jamming for confidentiality," in *IEEE Symp. on Security and Privacy*, 2013.

[30] V. I. Ivanov, L. Y. Paul, and J. S. Baras, "Securing the communication of medical information using local biometric authentication and commercial wireless links," *Health informatics journal*, vol. 16.3, pp. 211–223, 2010.

[31] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41.3, p. 15, 2009.

[32] M. Zhang, A. Raghunathan, and N. K. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," *Biomedical Circuits and Systems, IEEE Transactions on*, vol. 7.6, pp. 871–881, 2013.

[33] E. Y. Chow, A. L. Chlebowski, S. Chakraborty, W. J. Chappell, and P. P. Irazoqui, "Fully wireless implantable cardiovascular pressure monitor integrated with a medical stent," *Biomedical Engineering, IEEE Trans. on*, vol. 57.6, pp. 1487–1496, 2010.

[34] *FCC rules and regulations, MICS Band Plan, 2003*.

[35] M. Rostami, A. Juels, and F. Koushanfar, "Balancing security and utility in medical devices?" in *ACM 50th Annual Design Automation Conf.*, 2013.