Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 773–778
ISBN 978-83-60810-48-4

Energy-Efficient Security in Implantable Medical Devices

Krzysztof Daniluk
Warsaw University of Technology, Institute of Control and Computation Engineering
Email: K.Daniluk@stud.elka.pw.edu.pl

Ewa Niewiadomska-Szynkiewicz
Warsaw University of Technology, Institute of Control and Computation Engineering
Research and Academic Computer Network (NASK)
Email: ens@ia.pw.edu.pl

***Abstract*—In this paper a survey of selected topics concerning development of wireless sensor network systems formed by implantable medical devices (IMDs) located on the patient's body are presented and discussed. The focus is on security aspects and effective management of power resources available in implanted sensors. Implantable medical devices are very sensitive to the energy constraints. Moreover, most applications of IMDs require protection against injection or modification of disseminated measurements. Therefore, the transmission between IMDs and external devices, which aim is to monitor and control of IMDs has to be protected. The approaches to provide a security and ensure a privacy during monitoring, controlling, drug disposition and implant identification are discussed. The concept of novel energy-efficient security system for wearable devices to monitor the patient's health is presented in the final part of this paper.**

I. Introduction

Nowadays wireless sensor networks (WSNs) are becoming part of everyday life. They can be used in different environments and situations, in which traditional networks are inadequate, and can perform different tasks. The popular applications include monitoring of environmental conditions, battlefield, home, office or factory, vehicle tracking and others. Every year, new solutions and applications of WSNs are proposed.

During the last decade the WSN systems have become extremely popular in the medical diagnostics. The medical devices that can be used to construct a WSN are divided into two main categories: **implantable and external devices**. Implantable devices can be deployed on a patient's body to measure different characteristics. The measurements are transmitted to the external devices (base stations) that collect and process all data. Nowadays, the extensive research is being conducted to develop the secure and robust network systems for medical diagnostics. The commonly used implantable medical devices like pacemakers, glucose meters, etc. can form a sensor network on our body. It should be pointed that such network similarly to other WSNs has many limitations concerned with power resources and low level security. To develop a robust and secure system we have to extend its architecture with additional solutions that assure reliable, secure and energy-efficient communication and protect the network against injection or modification of measurements transmitted to the external devices.

The remainder of this paper is organized as follows. The typical applications and functionalities of medical devices like monitoring, controlling, drug disposition and implant identification are described in **chapter II.** The use case of implantable medical device with focus on the transmission protocols are presented in **chapter III**. The security aspects and privacy risks are discussed in **chapters IV** and **V**. Finally, in **chapter VI** the concept of secure energy-efficient wireless sensor networks for health-monitoring is described. The paper concludes in **chapter VII**.

II. The applications of Implantable Medical Devices

During the last decade a broad spectrum of activities in medical diagnostics have been undertaken both in the research and industry domain. Implantable medical devices are becoming increasingly popular. For example there are millions of people in U.S. who already have installed wireless IMDs and about 300.000 such IMDs are implanted every year in U.S.

Due to the feeding methods we can divide the medical devices into two groups [7]:

- devices equipped with the internal non rechargeable batteries (e.g. pacemakers [1]),
- devices powered inductively (e.g. cochlear implants [2]).

Most of IMDs are small battery-fed devices, which means their power source is limited. Each battery powered device, participating in a network needs to manage its power in order to perform its duties as long, as effective is possible. It is obvious that the replacing of implanted devices or their batteries requires a surgical intervention and the frequent repetition of such operation is unacceptable [5, 6].

Moreover, due to wireless transmission the throughput of a network formed by IMDs is also limited. The quality of wireless transmission depends on numerous external factors, like weather conditions or landform features. Due to high requirements for the accuracy of the transmitted data and potential interference all measurements should be sent in short bursts [7]. It conserves power and reduces the potential

time window for interference. Hence, it is often necessary to buffer data. Therefore, design and development of networks formed by IMDs is a non-trivial task. The main direction in current research include increasing the potential of hardware components, more accurate sensors and techniques for energy-efficient and secure communication.

It is worth to mention, that currently used standard for communication with implantable medical devices was defined by the U.S. Federal Communications Commission (FCC) and European Telecommunications Standards Institute (ETSI). The specification for using a frequency band between 402 and 405 MHz in communication with medical implants is provided in Medical Implant Communication Service (MICS). It allows bi-directional wireless communication with electronic implants. Fig. 1 demonstrates the cardiac pacemaker together with the monitoring base station. Wake-up link operates in 2.45GHz band and RF data link operates in 402-405 MHz.

The currently available medical devices can provide different functionalities, and thus can perform different tasks. The widely used applications are:

- monitoring of the typical characteristics of the patient's body,
- monitoring and controlling, which covers monitoring but provides additional functionality, i.e., directly programming or programming the implantable devices over the Internet,
- drug disposition - controlling the delivery of drugs to a human body,
- identification of the implant, which determines whether a patient has any implant and of which type.

A. Monitoring

Monitoring of the patient's health conditions is the widely used application of implantable medical devices. The measurement results can be directly read from the medical device or taken from the Internet. In case of direct readout IMD has to be directly connected to the external device (base station) or the measurements should be transmitted using wireless connection to the external device located not far from a given IMD. Such situation occurs when the patient is visiting a doctor to evaluate his state of health. In case of readout of measurements from the Internet, the medical examination is conducted remotely.

B. Control

In some situations it is necessary to affect the operation of the implantable medical device. We can control the device via **direct programming** or **programming over the Internet**.

In case of direct programming, the patient has to be directly connected or located in the transmission range of the wireless external device that is responsible for IMD software modification (e.g. updating the firmware of implantable medical device [8]). In case of programming over the Internet, the external device has to have access to the implantable medical device via Internet, often using some kind of intermediate devices for transmission. In this way the measurements can be gathered in situations when a patient cannot visit a doctor and the implantable medical device has to be reprogrammed immediately.

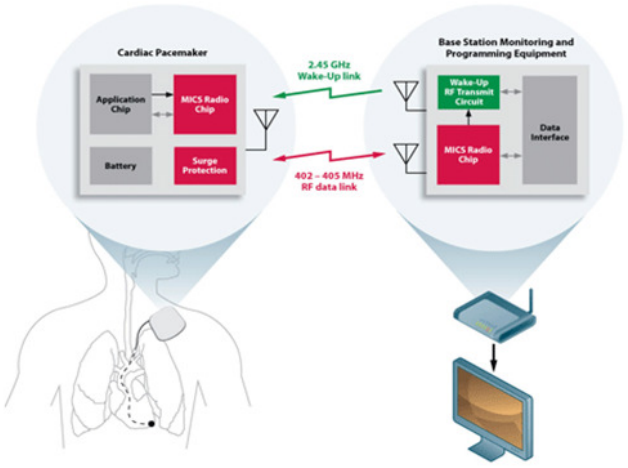

Fig. 1 Cardiac pacemaker

C. Drug disposition

Another application of implantable medical devices is the drug disposition. It is a good solution for patients, who cannot/don't have to stay in hospital, but on the other hand are not able to control taking drugs at home (timing and recommended dose).

D. Implant identification

Sometimes it is necessary to identify whether a patient has any implants and determine the type of these implants. Such functionality is especially useful in emergency situations, when a doctor has to quickly determine all the implanted devices in the patient's body, as well as in many medical examinations which are forbidden for patients with some implants (e.g. magnetic resonance is not allowed for patients with pacemakers).

III. Use Case: Transmission between Cardiac Pacemaker and External Device

Let us consider the following scenario. Our goal is to monitor a patient who has a cardiac pacemaker and program the device using wireless base station. The Zarlink ZL70102 transceiver is integrated with the pacemaker. The base station exchanges data with the pacemaker to gather new measurements. Moreover, from time to time the software installed in the pacemaker has to be updated. To perform any actions the base station has to wake up the transceiver of the pacemaker. It sends wake up signal in 2.45 GHz band and next reprogram the pacemaker or gather measurement data (see Fig. 1).

The medical data are transferred in 402-405 MHz RF data link (MICS specification). In the presented example, all data from the pacemaker have to be transferred to the computer of the doctor. The wireless transmission without any

additional protection and authentication is used. The battery of the pacemaker is also not defended against energy-consuming attacks. Moreover, the privacy of the patient is not secured at all, because each device with functionality similar to the base station can gather data from a pacemaker.

It should be pointed that the common systems with pacemakers do not ensure transmission security and privacy. Therefore, it is currently big challenge to provide secure communication between such device like pacemaker and the base station.

IV. Security in IMD networks

In this section the security aspects in networks formed by IMDs are discussed. We start with short overview of types of attackers and jammers, next we discuss the tradeoff between security, usability and energy consumption. Finally, the security requirements in case of selected IMD devices are discussed.

A. Three classes of adversaries

In computer security, an adversary (attacker) is a malicious entity whose goal is to prevent the user of the security system that provide security requirements like data integrity, confidentiality, authentication and privacy. We can distinguish three main classes of adversaries [3]:

- adversaries with an external device commercially produced for use with IMDs,
- passive adversaries who eavesdrop communication between IMD and an external device,
- active adversaries that can generate extra RF traffic.

In chapter II we presented the possible functionalities of IMDs, i.e., monitoring, controlling, drug disposition, implant identification. Various scenarios of attacks can be realized when consider mentioned functionalities.

The attack with an external device commercially produced for use with IMDs can be easy performed when the objectives of the medical device are monitoring, controlling or drug disposition. If an adversary is able to clone the identifier (id number) of the device it could use such device in the implant identification operation. A passive adversary who eavesdrops on communications between IMD and an external device, in case of not encrypted communication can easy capture measurement data and disturb controlling actions, drug disposition and implant identification. In case of an active adversary that can generate extra RF traffic, the attacker can jam signals from monitoring, controlling and drug disposition. It can also impersonate for another device in order to take part in implant identification.

B. Types of jammers in smart jamming attack

The following types of jammers can be distinguished [13]:

- **Continuous jammer** that produces a continuous signal at a specified power level.
- **Periodic jammer** that produces a periodic pulse of fixed size enough to destroy a packet if hit. The idle interval is the input to this kind of jammer and is based on the jammer budget as well as the desired network throughput.
- **Memoryless jammer** is similar to the periodic jammer. The difference is that the length of the idle period is decided using a memory less distribution, the mean of which is the input parameter for the jammer.
- **Reactive jammer** is channel aware. It jams reactively using the information decoded from the IEEE802.11. Reactive jamming attack has emerged as a great security threat to wireless sensor networks, due to its mass destruction to legitimate sensor communications and difficulty to be disclosed and defended.

C. Sketch of an attack

Each jamming attack [3] can be divided into two phases: initial phase and a maintenance phase.

- Initial Phase

This phase is a short period compared to the maintenance phase. It is assumed that prior to the start of the initial phase the adversary monitors the traffic to gather some information about WLAN, such as the identifier of each user and data link, traffic demands and current data rates. In the initial phase, the adversary first selects a set of victim links and calculates a target rate for each of them that is no more than the current rate. Then, if the target rate for a victim link is smaller than the current rate, the adversary intensively jams the packets transferred via the victim link to trigger the RAA (Rate Adaptation Algorithm) [12] to decrease the data rate. The jamming in this phase stops when the rate of each victim link reaches the target level. The goal in this phase is to bring down the transmitting rates of the victim links to the target rates.

- Maintenance Phase

After the initial phase, each victim link's rate has already been decreased to the adversary's target rate. However, additional jamming is needed to prevent those links from recovering to their previous higher rates. In this phase, the adversary selectively jams the packets transferred via the victim links so that the RAA does not increase the rates. Compared to the initial phase, the jamming during the maintenance phase is less frequent, but it lasts for a longer period depending on the available energy and the goal of the jammer.

D. Security versus device resources

Strong security mechanisms, such as public key cryptography, can be expensive in terms of both computational time and energy consumption. As with general sensor networks, the use of cryptography can therefore create tension between security and some IMDs' longevity and performance goals. Moreover, increasing resource use for secure communications can amplify the effects of certain malicious DoS attacks, such as repeated attempts to authenticate a device. For security, IMDs might also wish to keep detailed records of all transactions with external devices. These transaction logs could potentially

overflow a device's onboard memory, particularly under DoS attacks or when an adversary explicitly seeks to exhaust a device's memory.

E. Security versus usability

The standard tension between security and usability also applies to IMDs. From an usability perspective, long distance wireless communication between IMDs and external devices offers many advantages, including continuous at-home monitoring and flexibility in clinical settings. However, from a security perspective, wider-range wireless communications increase exposure to both passive and active adversaries. In the Medical Implant Communications Service (MICS) band, an attacker with limited resources might extend the specification's five meter distance using a directional antenna and an inexpensive amplifier. Furthermore, extending of the security mechanisms shouldn't overly complicate user interfaces of the external devices, particularly when healthcare professionals must make quick decisions during emergency care.

F. Security requirements of IMD

Pacemaker and cardioverter defibrillator (ICD) are commonly IMD devices. They are equipped with sealed, battery, sensor-laden pulse generator, wire electrodes that connect the generator to the myocardium (heart muscle) [4], and custom ultralow-power microprocessor, typically with about 128 Kbytes of RAM for telemetry storage. The primary function of these devices is to sense cardiac events, execute therapies, and store measurements such as electrocardiograms. The settings of a pacemaker and ICD are configured based on an external device - a dedicated programmer. Pacemakers and ICDs are often equipped with high capacity lithium-based batteries with lifetime of about five to seven years. Rechargeable batteries are extremely rare due to practical, economic and safety reasons. A lifetime of the device depends on the treatments required. Pacing pulses consume only about 25μJ, each ICD shock consumes 14 to 40J. A single defibrillation can reduce the ICD's lifetime by weeks.

Wireless communication: Previous generations of pacemakers and ICDs transmitted data at low frequencies (near 175 kHz) with a short read range (8 cm) and used low-bandwidth (50 Kbits per second) inductive coupling to relay telemetry and modify therapies. Modern devices use the Medical Implant Communications Service, which operates in the 402- to 405-MHz band and allows for much higher bandwidth (250 Kbps) and longer read range (specified at two to five meters). Currently major pacemaker and ICD manufacturers produce at-home monitors that wirelessly collect data from implanted devices and relay it to a central repository over a dial-up connection. The repository is accessible to medical staff via an SSL-protected Web site.

Reliability: Pacemakers and ICDs sometimes fail. Safety issues involving these devices have received much attention. Since 1990 the US Food and Drug Administration has issued dozens of product advisories affecting hundreds of thousands of pacemakers and ICDs. These statistics show that 41 percent of device recalls were due to malfunctions in firmware (216,533 out of 523,145 devices). These problems underscore potential hazards that come with increasingly sophisticated implantable medical devices. Past abnormalities surfaced under accidental circumstances. The potential for intentionally malicious behavior calls for a deeper investigation into IMD safety from a security [10] and privacy perspective.

Device-existence privacy: An unauthorized party should not be able to remotely determine that a patient has one or more IMDs.

Device-type privacy: If a device reveals its existence, the type should still only be disclosed to authorized entities.

Specific-device ID privacy: An adversary should not be able to wirelessly track individual IMDs. This is analogous to the concern about the use of persistent identifiers in RFIDs, Bluetooth and 802.11 media access control (MAC) addresses to compromise an individual's location privacy.

Data integrity: A patient's name, diagnoses, and other stored data should be tamper-proof.

V. PRIVACY RISKS AND IMD FUNCTIONALITY

In the area of implantable medical devices privacy risks are discussed in the context of their applications, i.e., monitoring, controlling, drug disposition and implant identification [9].

Monitoring and privacy risks: During direct readouts from IMDs, only devices in close proximity are able to eavesdrop the transmissions.

We can identify following possible risks: identity theft, hijacking of crucial data and possible infection of the base station (a computer of a doctor). The similar risks can be observed in case of readout from the Internet only instead the risk concerned with not protected computer of a doctor, a gateway can be a weak point in the communication between our IMD and a base station.

Controlling and privacy risks: The transmission during remote control of IMD by the external device can be attacked. It can cause destruction of IMD's software and finally thread to the patient's life.

Drug disposition and privacy risks: Similarly to the controlling functionality, controlling of drug disposition in direct manner or over the Internet is very sensitive to various attacks. The attacker may change the prescribed amounts of drugs taken by the patient in given periods of time. Any unintended changes may affect directly the patient's health.

Implant identification and privacy risks: Quick identification of a type of IMD implanted in a given patient is very important especially in emergency situations when a patient's life is endangered. However, there is a danger that it can be misused to track a patient without his consent. It may result in loss of privacy - an attacker can find out the type of implanted device, and can destroy this IMD attacking again.

VI. Concept of Secure Energy-Efficient Network for Health Monitoring

The concept for health-monitoring supporting energy-efficient security is presented. The focus is on secure, reliable and energy aware communication for health-monitoring.

Let us consider that implantable medical devices consisting of sensors and radio-communication modules are deployed on a human body. The measurements gathered by these devices are transmitted to a base station, located on a patient's belt. In the next step all sensing data collected by the base station are transferred to a mobile device, which plays a role of broker in remote communication between a patient and his doctor.

Figure 2 depicts the possible network formed by IMD devices of various types. I1, I2, I3, I4 are implanted sensors. Let us assume that the aim of I1 device is to monitor patient's pulse, I2 monitors cardiac diseases, I3 monitors the kidney and I4 checks the possibilities of injuries of the knee. S1 represents an external security device located on the patient's body (not implanted). It is responsible for secure transmission between implantable sensors and a base station monitoring.

B1 (base station) is an external device that is responsible for collecting data from all implanted sensors and transmitting further – for example using mobile network communication.

A1 represents an attacker.

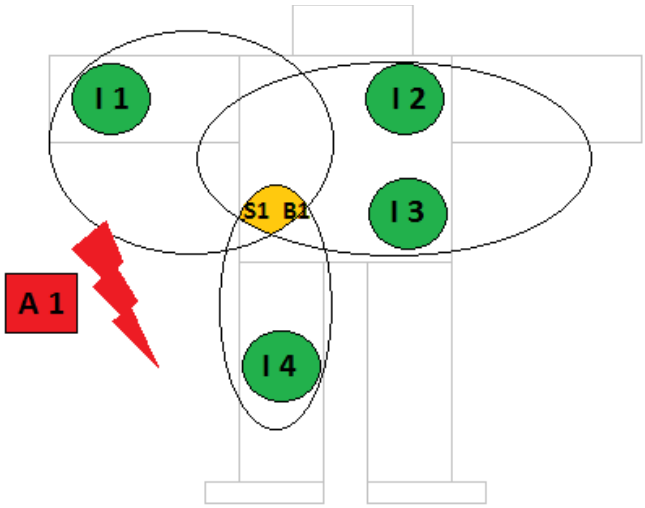

Fig. 2 Communication scheme representing implantable sensors, base station and security node, which jams transmission from attacking node

Various architectures and techniques for protection of discussed IMD network can be designed and developed. A few concepts are briefly described below.

We can apply simple symmetric *key* cryptography for data encryption. We consider the channel in 802.15.4 bandwidth, i.e. 2400-2483.5 MHz. Solution seems to be rather simple, however we assume, that all devices use only correct channel to transmission. We introduce an external device - called security device that is responsible for security and protection against external attacks. Hence, the goal of the *security device* is to monitor communication between sensors and a base station and identify an unusual behavior in the sensor network. Moreover, the functionality of a *security device* should allow to jam strange transmissions in order to save energy consumption in a network.

Many open issues concerned with assuring the secure transmission with minimal energy usage can be considered. The deployment of IMDs on a patient's body can influence the communication. The idea is to optimize the location of implanted sensors. Optimal distribution of sensor devices may affect the radical reduction of signal strength, i.e. the reduction of energy consumption of implanted sensors.

The intrusion detection system can be implemented in the *security device* (S1) presented in Fig. 2 to protect the system against injections. Intrusion detection system (IDS) can match pre-programmed or learned rules to current transmissions and look for suspicious behaviors. The disadvantage of this solution is that increase of the security results causes higher energy consumption.

Another approach is to provide mechanisms for secure aggregation of sensing data. It allows to conserve the scarce energy resources by eliminating redundant data. Secure data aggregation requires authentication, confidentiality and integrity of data. Various approaches to data aggregation are proposed in literature [11]. It seems that simulation experiments should help to select the best solution that ensure security with minimal energy usage.

Summarizing, the suggested approach to develop a secure and energy-efficient IDM network consists of following steps: 1) optimal deployment of sensors on a patient's body, 2) introducing a security-device with implemented light IDS, 3) development of specialized software for effective transmission monitoring in a network, analyzing traffic patterns and jamming unexpected signals; this software should apply learning techniques, 4) introducing data aggregation inside a base station.

VII. Summary and Conclusion

Many challenges arise from application of networks formed by implanted medical devices. The aim of our work was to point several basic issues that should be solved in the systems that are used in practice. In this paper we provided a brief review of some representative IMDs applications. We distinguished main functionalities of IMDs networks and discussed possible threats that can occur in various types of operations of devices in a network. Finally, we presented a concept of secure and energy-efficient network formed by IMDs. In our future work we plan to implement a network design for monitoring human's body in our laboratory equipped with the Maxfor wireless devices. Our sensors, after distribution on a body will emulate true medical devices. We plan to experimentally check various approaches to network protection and energy aware communication.

ACKNOWLEDGMENT

This work was supported by National Science Centre grant NN514 672940.

REFERENCES

[1] Daniel Halperin and Shane S. Clark and Kevin Fu; "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses", Security and Privacy, 2008. SP 2008. IEEE Symposium on. p. 129 - 142 , 2008

[2] WISP: "Wireless Identification and Sensing Platform", http://seattle.intel-research.net/wisp/; accessed July 2012

[3] MIT news - protecting medical implants from attack http://web.mit.edu/newsoffice/2011/protecting-medical-implants-0613.html; accessed July 2012

[4] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, Kevin Fu; "They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices", ACM SIGCOMM Computer Communication Review - SIGCOMM '11 Volume 41 Issue 4, August 2011 p. 2-13

[5] Panescu D. "Wireless communication systems for implantable medical devices" Emerging Technologies, IEEE Enrgineering in medicine and biology magazine, p. 96-101, March/April 2008

[6] http://www.eetimes.com/design/embedded/4025029/The-challenge-of-designing-in-bodycommunications; accessed July 2012

[7] http://www.secure-medicine.org/publications.php; accessed July 2012

[8] Steven Hanna, Rolf Rolles, Andres Molina-Markham, Pongsin Poosankam, Kevin´ Fu, Dawn Son, "Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices" , 2nd USENIX Workshop on Health Security and Privacy https://www.usenix.org/conference/healthsec11/take-two-software-updates-and-see-me-morning-case-software-security ; accessed July 2012

[9] Kevin Fu, "Software issues for the medical device approval process", a debate "A delicate balance: FDA and the reform of the medical device approval process" 13 th April, 2011 http://www.cs.umass.edu/~kevinfu/papers/fu-senate-comm-aging-med-dev-sw-apr-2011.pdf; accessed July 2012

[10] Tamara Denning, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno, William H. Maisel "Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Device", CHI '10 Proceedings of the 28th international conference on Human factors in computing systems, pages 917-926

[11] T. Denning, K. Fu, and T. Kohno; "Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security"; 3rd USENIX Workshop on Hot Topics in Security (HotSec '08), Article No. 5, July 29,2008

[12] Noubir, Rajaraman, Sheng, Thapa, "On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming", WiSec '11, Proceedings of the fourth ACM conference on Wireless network security, pages 97-108

[13] "Security and Privacy for Implantable Medical Devices" Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, William H. Maisel, Journal IEEE Pervasive Computing archive Volume 7 Issue 1, January 2008. pages 30-39