IJMTST | Volume: 2 | Issue: 07 | July 2016 | ISSN: 2455-3778

Security in Medical Devices using Wireless Monitoring and Detection of Anomalies

Pooja S. Band[1] | Archana B. Kanwade[2]

[1]M.E. student, Department of Electronics and Telecomm. Engg, SITS Narhe, Pune, Maharashtra, India,
[2]Asst. Professor, Department of Electronics and Telecomm. Engg, SITS Narhe, Pune, Maharashtra, India

ABSTRACT

`Implantable and medical devices (IMDs) have been advanced with the advancements in engineering and medical science. IMDs are used for applying new therapies to patients, monitoring human body parameters and making diagnosis as per the monitoring result. Increased use of IMDs has enhanced the chances of attacks to them. Therefore, to make use of IMDs for various applications, they need to be secured. A system is developed to achieve the security. The system monitors various human body parameters wirelessly and detects anomaly if unauthorized node participates in communication. The system uses request response protocol in wireless communication. Experiments show that body parameters can be successfully monitored and signal characteristic can be used to detect anomaly.

KEYWORDS: *Attacks, IMDs, monitoring, security, wireless communication*

I. INTRODUCTION

Medical devices, used generally in hospitals, are the articles used in treating health related issues e.g., a disease in humans or in animals with the purpose of curing them from the health problem. These medical devices are needed for modern medicine as they perform many patient monitoring as well as management functions. Such medical device is called implantable if it is partially or totally introduced into the human body or placed on the surface of the body. In recent years, implantable medical devices have been advanced through developments in science and engineering, as well as in microelectronics and biotechnology.

Implantable Medical Devices (IMDs) are mostly used to monitor and help treat medical conditions. These include pacemakers, implantable cardiac defibrillators (ICDs), neuro stimulators and drug delivery systems, which help in managing many diseases [1]. It is expected that the use of IMDs for monitoring will be grown further in the future. Using surgical procedures involving implanted medical devices, patients can improve their lives. In 2005, the number of insulin pump users was nearly 245,000 and the growing rate that is expected for the insulin pump market is 9% from 2009 to 2016 [2]. In [3], as reported by Hanna et al., nearly 25 million patients use wireless IMDs in only the U.S. and every year near about 300,000 more of such devices are implanted. The number of implanted drug-eluting stents in 2004 was above two million [4]. Also, in the year 2000, the number of operations performed for hip replacement was about 152,000, which shows increase of 33% from the number of operations performed in 1990 and also a half of the estimated number of hip replacement operations in 2030 [5].

IMDs are needed to connect to other systems using wireless communication and wireless communication is responsible to cause wireless attacks. Hence, security is very important for IMDs.

To secure IMDs against all wireless attacks, a system is developed. The system is used to monitor the body parameters wirelessly and to detect an anomaly during wireless monitoring. This is achieved by considering signal characteristic and aspects of wireless sensor network.

II. RELATED WORK

Israel and Barold in 2001[6] studied pacemaker systems as implantable cardiac defibrillators. They used a channel between medical devices and

controllers, which was based on radio frequency identification (RFID). But if attacker has a high-gain antenna then it can easily attack the wireless channel. Also, a study done by Fotopoulou and Flynn [7] in 2007 and by Hancke and Centre [8] in 2008 has shown that if attacker is up to ten meters away from IMD, it can access the patient data.

In the study of securing implantable medical devices done by T. Denning, K. Fu, and T. Kohno [9] in 2008, a class of new defensive techniques was developed. These are called Communication Cloacker. These cloackers are to be worn externally. The cloacker coordinates interactions between IMD and the doctor. When the patient is wearing a cloacker, the IMDs become invisible to unauthorized programmers and therefore attackers cannot access the patient's data. In cases, when cloacker is lost or damaged, the emergency practitioner can still access the IMD. Here, since an external device is used for computation, it protects IMDs against battery-draining attacks.

In June 2009, Baldus, Corroy, Fazzi, Klabunde, and Schenk [10] introduced the concept of human-centric connectivity using body coupled communication (BCC). In BCC, human body is used as a transmission medium. To achieve this, a small electric field is induced in human body. A signal is propagated between the devices which are in close proximity of human body or in direct contact with it. Since human body is the communication medium, the communication range is limited only up to the specific distance from human body.

Rasmussen, Castelluccia, Heydt-Benjamin and Capkun introduced an access control scheme for implantable medical devices in November 2009[11]. The scheme is based on ultrasonic distance bounding, which enables the IMDs to have access to its resources only to those devices which are in its close proximity. The scheme uses a message authentication protocol which is based on ultrasonic distance bounding. However, it may be possible that an attacker can approach the patient and even can make physical contact.

Schechter [12] in 2010 proposed a method of having a key, which will give patient data related to various body parameters. He discovered to print these keys into patient's skin using ultraviolet- ink micropigmentation, beside the point where the device is implanted. Schechter called these ultraviolet- ink micropigmentation as invisible tattoos. The tattoos consist of small, reliable, and inexpensive ultraviolet light emitting diode (UV LED) and for key entry (a keypad or touch-screen), it includes an input mechanism. He discovered that for multiple devices, a single key would be sufficient. But the problem with tattoos is that they can cause skin irritations.

In April 2011, F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li [13] introduced a scheme called IMDGuard for securing medical devices. IMDGuard used a device Guardian. This Guardian is used for implantable cardiac devices like implantable cardioverter-defibrillator, pacemaker etc. It acts as a mediator between the IMD and doctor. IMDGuard basically uses patient's electrocardiography signals to extract keys. In case, if Guardian is lost or not functioning properly then we can easily rekey the IMD since no pre-distributed secret is required to extract the keys. But, if attacker succeeds to have physical contact with patient, he will be able to extract the key.

Gollakota, Hassanieh, Ransford, Katabi, and Fu together discovered an external device called the Shield in August 2011[14]. They called this shield as a personal base station. The shield relays messages between IMDs and external programmer. The shield is responsible for secure communication from IMDs to programmer. The messages sent by IMDs are first encrypted by shield and then sent to programmer. But the programmer's commands which are sent to IMDs by shield are not encrypted, so the confidentiality of commands is not protected.

In 2013, Zhang, Meng, Raghunathan and Jha [15] proposed a new device called medical security monitor (Medmon). The operation of Medmon is based on wireless channel monitoring and anomaly detection. Medmon detects physical anomalies as well as behavioral anomalies. Physical anomalies include three types, out of which, one is received signal strength indicator (RSSI), second is time of arrival (TOA), and the third one is differential time of arrival (DTOA) while behavioral anomalies include command and data anomaly. While Medmon only provides device integrity, it does not protect the confidentiality of the communication channel.

III. SYSTEM IMPLEMENTATION

Figure 1 shows the block diagram of the system. The system is divided into four sub-parts. The most important is the master, which initiates the communication. There are two slave nodes which communicate with master. The system has one more node. This node is an anomaly, which we are going to detect.

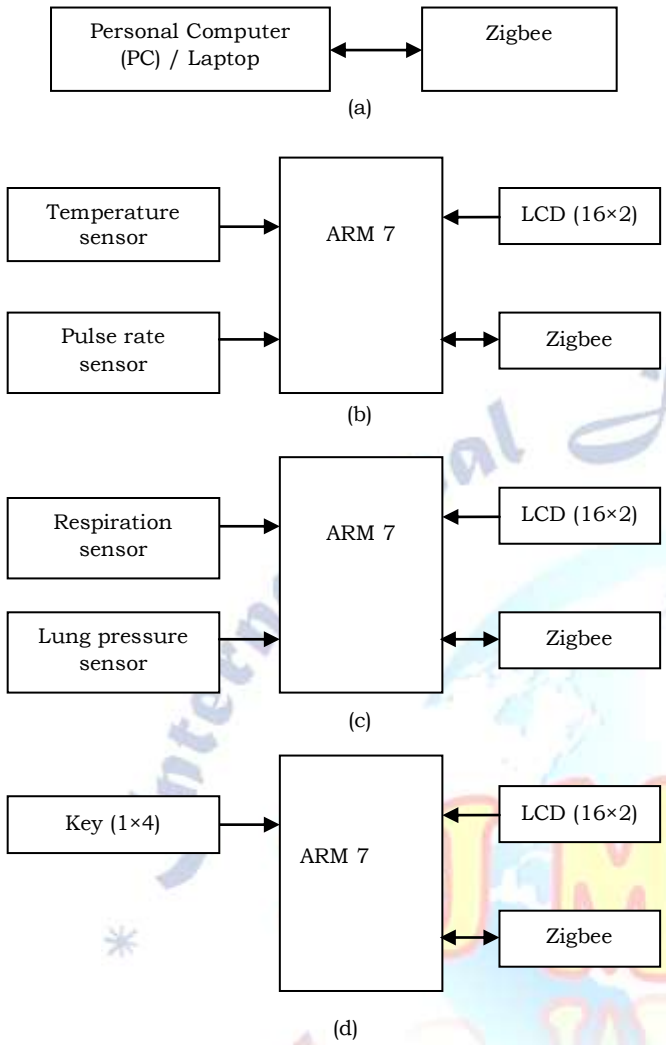

Figure 1: Proposed system
(a) Master (b) Slave 1 (c) Slave2 (d) Anomaly node

For master, we used laptop or personal computer (PC). Microcontrollers are used as other three nodes. To each microcontroller, zigbee is connected for wireless transmission and reception of data. To the two slave nodes shown in figures 1(b) and (c), sensors are connected. These include temperature sensor, pulse rate sensor, respiration sensor and lung pressure sensor. To the anomaly node, a 4×1 keypad is connected.

A. Temperature sensor

Temperature sensor is used for measuring the temperature of patient. It measures the body temperature. Temperature sensor gives output as analog voltage. The voltage is corresponding to the temperature measured. This analog voltage is given to microcontroller. As microcontroller works only on digital value, analog voltage needs to be converted to digital. This task is performed by 12 bit analog-to-digital converter (ADC) embedded in microcontroller. The digital temperature obtained from microcontroller is converted back into analog by digital-to-analog converter (DAC) in microcontroller and displayed on LCD which is a 16×2.

B. Pulse rate sensor

To determine the pulse rate of the patient, pulse rate sensor is used. This sensor determines the number of pulses of patient per minute. The output of the pulse rate sensor is analog. This analog output is given to microcontroller which coverts it first into digital and then processes. If the patient has disorder in his lungs, the pulse rate of the patient is different from the normal value.

C. Respiration sensor

The respiration rate of the patient is monitored using a respiration sensor. This sensor measures the number of breaths per minute of the patient. Respiration rate sensor is designed using IR sensor.

D. Lung pressure sensor

The functioning of lungs of a patient is determined using a pressure sensor attached at one end of pipe. Patient has to exhale air from other end of pipe. The pressure sensor gives analog voltage at its output which is given to microcontroller. ADC in microcontroller converts the analog voltage into digital. This digital voltage will be processed by microcontroller. Digital-to-analog converter (DAC) will convert it back into analog which is displayed on PC.

Here, the maximum pressure that can be applied by lungs is determined.

E. Zigbee

Zigbee is the most important part of the system. For wireless transmission of signals, zigbee is used. Zigbee is connected to the two slaves, an anomaly node as well as to the master i.e., PC.

F. Microcontroller

The system uses ARM7 microcontroller. The two slaves and an anomaly node includes microcontroller. All the sensors are connected to the microcontroller. One slave includes two sensors, temperature and pulse rate connected to the microcontroller while the other slave has respiration and lung pressure sensor connected to other microcontroller. Within the microcontroller, there is 10 bit ADC (Analog-to-digital converter) to convert analog input received from sensors to digital value and a DAC (Digital-to-analog converter) which is transmitted wirelessly to PC and displayed on it.

G. Liquid Crystal Display (LCD)

Here, a 16×2 LCD is used to display the anomaly on the two slaves.

IV. DESIGN METHODOLOGY

The system uses request response protocol in wireless communication. Zigbee plays the most

important part in wireless communication.

Two cases are considered. Communication starts with master, that is, PC/laptop sending request for data from the slaves for patient data which includes temperature, pulse rate, respiration rate and lung pressure. Slave 1 gives temperature and pulse rate of patient while slave 2 gives respiration rate and lung pressure. Some time is allocated for slave 1 response and next interval of time is allocated for slave 2 response.

Two types of anomalies are detected at master and at slaves.

1) TOA (Time of Arrival):

Case I: Anomaly behaving as master:

At slaves, the time required for reception of request is fixed. If the request does not come within the time interval, it is detected as time anomaly.

If an unauthorized node in the communication network sends request for data to slaves, it is detected if it does not send the request within the time period.

Case II: Anomaly behaving as slave:

At master, time required for reception of response is fixed. If the data does not come within the time interval, it is detected as time anomaly.

When an unauthorized node responds to the master at other than the desired time, it is detected as an anomaly at master.

2) Password anomaly:

Case I: Anomaly behaving as master:

At slaves, the time required for reception of request is fixed. If the request comes within the time interval, its password is checked. If password is incorrect, it is detected as password anomaly.

If an unauthorized node in the communication network sends request for data to slaves within the specified time but with incorrect password, it is detected as password anomaly at slaves.

Case II: Anomaly behaving as slave:

At master, the time required for reception of response is fixed. If the data comes within the time interval, its password is checked. If password is incorrect, it is detected as password anomaly.

When an unauthorized node responds to the master within time and the frame received has wrong password, it is detected at master.

Request from master consists of the frame id indicating the slave for which request is been sent.

The time of response for the slaves is fixed since PC sends requests consecutively for the two slaves.

V. RESULTS

Figure 2 shows the experimental setup. It includes the two slaves, master and an anomaly to be detected.

Figure 2: Experimental setup

Figure 3 shows snapshot on master which is the result of wireless monitoring of human body parameters like temperature, pulse rate, respiration and lung pressure. Here, as data is transmitted within time and password of frame is matched, no anomaly is detected.

Figure 3: Wireless monitoring

For a lung patient, value of lung pressure is very less than the normal. Doctor gives him treatment as per this value. If master receives incorrect value (from anomaly), patient will be wrongly treated. This may affect patient's health.

When anomaly is behaving as master, it is detected at slaves as shown in figure 4(a) and (b).

(a) (b)

Figure 4: (a) Password anomaly at slave (b)Time anomaly at slave

Figure 5 shows anomaly at master.

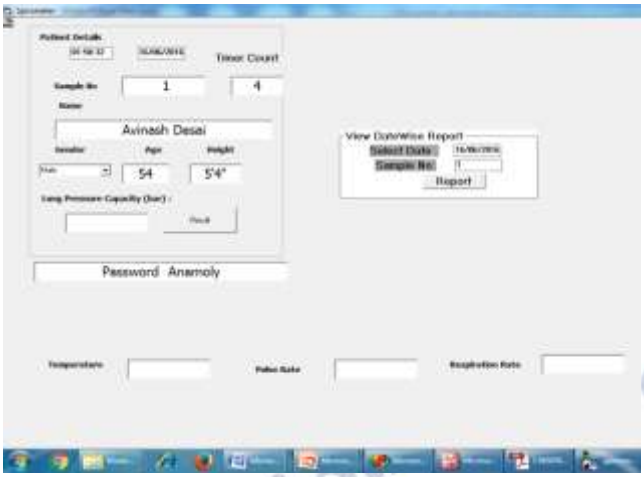

Figure 5: Anomaly at master

VI. CONCLUSION

The system provided wireless monitoring of human body parameters. If attacker tries to harm patient by sending request to slaves or by sending response to master, it is detected. This has been achieved by two ways. At slaves, the time for request frame is checked. If time is incorrect, it is anomaly. In a similar way, anomaly is detected at master if response is received other than specified time. In case if time of request or response frame is correct, it is checked for password. Incorrect password shows anomaly. Thus, implantable medical devices are secured by wireless monitoring and anomaly detection.

REFERENCES

[1] Halperin, Daniel, et al. "Pacemakers and implantable cardiac defibril-lators: Software radio attacks and zero-power defenses", *IEEE Symposium on Security and Privacy,* 2008.

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

[3] Hanna, K. Innovation and invention in medical devices: workshop summary. National Academies Press (2001).

[4] Park GE, Webster TJ A review of nanotechnology for the development of better orthopedic implants. J Biomed Nanotechnol 1:18–29 (2005).

[5] Gultepe E, Nagesha D, Sridhar S, Amiji M Nanoporous inorganic membranes or coatings for sustained drug delivery in implantable devices. Adv Drug Deliv Rev 62:305–315 (2010).

[6] Israel and S. Barold, "Pacemaker systems as implantable cardiac rhythm monitors," Amer. J. Cardiol., vol. 88, no. 4, pp. 442–445, Aug. 2001.

[7] K. Fotopoulou and B. Flynn, "Optimum antenna coil structure for inductive powering of passive RFID tags," in *Proc. IEEE Int. Conf. Radio Frequency Identification,* Mar. 2007, pp. 71–77.

[8] G. P. Hancke and S. C. Centre, "Eavesdropping attacks on high-frequency RFID tokens," *in Proc. Workshop Radio Frequency Identification Security,* Jul. 2008, pp. 100–113.

[9] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," *in Proc. Conf. Hot Topics in Security,* Jul. 2008, pp. 1–7.

[10] H. Baldus, S. Corroy, A. Fazzi, K. Klabunde, and T. Schenk, "Human centric connectivity enabled by body-coupled communications," *IEEE Commun. Mag.*, vol. 47, pp. 172–178, Jun. 2009.

[11] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. ACM Conf. Computer and Communications Security,* Nov. 2009, pp. 410–419.

[12] S. Schechter, Security That is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices, Microsoft Research, Tech. Rep. MSR-TR-2010-33, Apr. 2010.

[13] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE Int. Conf. Computer Communications,* Apr. 2011, pp. 1862–1870.

[14] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM Conf. Special Interest Group on Data Communication,* Aug. 2011.

[15] Zhang, Meng, Anand Raghunathan, and Niraj K. Jha. "MedMon: Securing medical devices through wireless monitoring and anomaly detection." Biomedical Circuits and Systems, *IEEE Transactions on* 7.6(2013): 871-881.