Bioengineering 2017 Secured and Efficient Data Sensing for Medical Based Body Area Network

Sonali Arvind Hartalkar* and Bale VS

Department of Electronics and Telecommunication Engineering, M.S.Bidve College of Engineering, Latur, India

Abstract

We propose a general framework for securing medical devices supported wireless channel observation and anomaly detection. Our proposal is predicated on a medical security monitor (Med Mon) that investigate on all the radio-frequency wireless communications to/from medical devices and uses multi-layered anomaly detection to spot probably malicious transactions. Upon detection of malicious dealings, Med Mon takes applicable response actions. A key good thing about Med Mon is that it's applicable to existing medical devices that area unit in use by patients, with no hardware or computer code modifications to them.

In this paper we need to indicate that the Slave is acting as Master furthermore as slave configuration to cause anomaly within the network. As slave it receives knowledge |the info |the information} from master and sends false reading to master which may cause problems since the master diagnosing are going to be inaccurate since false data is being fed to the Master via abnormal Node. We conjointly designed one digital spirometer

Introduction

DAs of late, therapeutic advances and developments in ultra lowcontrol figurLng, systems administration, and detecting advances have prompted a blast in implantable and wearable restorative gadgets (IWMDs). IWMDs are right now used to perform cardiovascular pacing, defibrillation, breath action, insulin conveyance, profound cerebrum incitement, intrathecal sedate imbuement, and numerous other demonstrative, checking, capacities.

IWMDs usually incorporate remote correspondence interfaces through which they can be associated with outer demonstrative or programming gear, or to body zone systems (BANs) to frame individual social insurance frameworks (PHSs). He Federal Communications Commission (FCC) supervises the utilization of people in general Radio Frequency (RF) range inside which RF remote advances work. He FDA's approaches on remote restorative gadgets are composed with the FCC and furnish medicinal gadget producers with greater consistency and a superior comprehension of administrative necessities for therapeutic gadgets that use these advances.

Rediofrequency Identification

Pacemaker systems were considered as implantable cardiac defibrLllators [6,7]. In this study, they assumed a channel between medical devices and controllers. HLs channel was based on radio frequency LdentLficatLon (RFID). But here the drawback was if antenna of the attacker is of high gain then there were chances that wireless channel can be easily attacked. And attacker can easily access the patient data, if it is within ten meters of distance from IMD [8,9].

Communication clocker

Communication Clockers. Patients have to worn these clockers externally. He interactions taking place between IMDs and the doctor are coordinated by clockers. When the patient wears the clocker, unauthorized programmers are not able to see the IMDs. So, patient's data cannot be accessed by an attacker. In emergency, medical staو can access the IMD by removing the clocker. But, if patient is not wearing the clocker, it is lost or damaged, external programmer can access the IMD [10]

Body coupled communication:

A new concept of human-centric connectivity, they used body coupled communication (BCC) technology where human body is used as a transmission medium [11]. For BCC, a small electric field is induced in human body. He devices which are very near to the human body play important role in BCC. Signal propagates between these devices only. Hus, range of the communication is limited very close to the human body.

Ultrasonic distance bounding:

HLs scheme used a message authentication protocol. He protocol used the concept of ultrasonic distance bounding. In this protocol, messages are encrypted beyond the distance measured by the IMD i.e., distance near to the IMD. By this concept, IMDs are accessible to the devices which are very closer to them. Here are chances that an attacker can make the physical contact with patient by approaching him. 3arameters-He key has to be printed into patient's skin with the help of ultraviolet-ink micropigmentation. He key is placed near the point of IMD implantation. He ultraviolet-ink micropigmentation were called invisible tattoos. He devices which are used for communication with IMDs consist of a reliable, inexpensive and a small ultraviolet light emitting diode (UV LED) and to enter the key, it has a device like a keypad or any other mechanism. Multiple

devices may use the single key. No daily effort is required for UV micropigmentation except the use of sunscreen [12,13].

IMD guard:

IMDGuard is used for implantable cardiac devices like pacemaker, implantable cardioverter defibrLllator etc [14]. It uses a Guardian, a wearable device which plays a role of mediator between doctor and IMD. In this case, to extract the key, electrocardiography (ECG) signals of the patient are used. When Guardian is lost by the patient or it does not function properly, it can be easily rekeyed as nothing is required except ECG signal of patient. In case, if attacker could make physical contact with patient, he can extract the key [15,16].

Reference

- Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, et al. (2008) Pacemakers and implantable cardiac defibrLllators6oiware radio attacks and zero-power defenses. IEEE Symposium on Security and Privacy.
- Review on security of medical devices (2016) International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.
- Park GE, Webster TJ (2005) A review of nanotechnology for the development of better orthopedic implants. J Biomed Nanotechnol 1:18-29.
- Zhang M, Raghunathan A, Jha NK (2013) MedMon: Securing medicaldevices through wireless monitoring and anomaly detection. IEEE Transactions on Biomedical Circuits and Systems 7: 871-881.

Note : This work is partly presented at 5th International summit on Medical Biology & Bioengineering (September 27-28, 2017 Chicago, USA)