Journal of Bioengineering and Biomedical Science

Hartalkar and Bale, J Bioengineer & Biomedical Sci
2018, 8:3
DOI: 10.4172/2155-9538.1000252

Research Article Open Access

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

***Corresponding author:** Sonali Arvind Hartalkar, Department of Electronics and Telecommunication Engineering, M.S.Bidve College of Engineering, Latur, India, Tel: +91-9422641036; E-mail: bestsonali@rediffmail.com

Received Date: July 9, 2018; **Accepted Date:** August 20, 2018; **Published Date:** August 28, 2018

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 a 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.

Keywords: Anomaly; BAN; Lung capacity medical monitoring; Spirometer; WSN

Introduction

As of late, therapeutic advances and developments in ultra low-control figuring, 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).

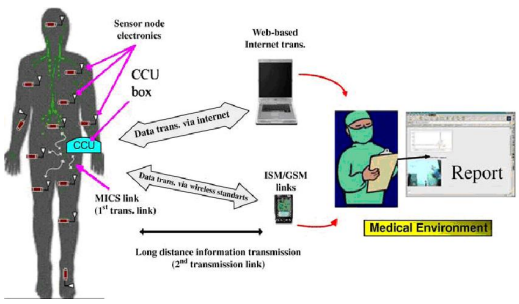

Figure 1: Advanced idea of personal healthcare system.

Figure 1 shows advanced architecture for how IWMDs can be connected to form a PHS. A PHS typically consists of sensors for physiological data collection, actuators for therapy delivery, remote controllers for reconfiguration, and a hub for logging, compressing, and analyzing the raw health data. Since the functions performed by IWMD and PHSs are frequently life-critical, any malfunction in the operation is of utmost concern. An incessant trend in IWMDs has been towards increased functional complexity, software programmability, and network connectivity.

The Federal Communications Commission (FCC) supervises the utilization of people in general Radio Frequency (RF) range inside which RF remote advances work. The 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.

Fuse of remote innovation in restorative gadgets can have numerous advantages, including expanding tolerant portability by dispensing with wires that tie a patient to a medicinal bed, giving social insurance experts the capacity to remotely program gadgets, and giving the capacity of doctors to remotely access and screen understanding information paying little respect to the area of the patient or doctor (clinic, home, office, and so forth…). These advantages can extraordinarily affect quiet results by permitting doctors access to continuous information on patients without the doctor physically being in the healing facility and permitting ongoing alteration of patient treatment. Remote observing can likewise help extraordinary populaces, for example, seniors, through home checking of incessant ailments with the goal that progressions can be distinguished before more genuine outcomes happen.

Information for patients

The utilization of RF remote innovation can mean advances in human services, and patients ought to be educated about the protected and successful utilization of these gadgets over the span of day by day life. Since the aviation routes are shared, the working of your remote restorative gadget might be influenced, (for example, information misfortune or disturbance) by different remote gadgets close you. Likewise with any therapeutic gadget.

Because of the nonappearance of cryptographic assurance, the remote channel has been distinguished as the Achilles' foot sole area of restorative gadgets. Ongoing exhibits of fruitful RF remote assaults on cardiovascular pacemakers and insulin pumps, have put restorative gadget security under incredible investigation. To better see how remote channels can be utilized to trade off medicinal gadgets, we give a short outline of the assault portrayed in on a glucose observing and insulin conveyance framework. This assault misuses the remote channels between the gadget and controller, and between medicinal gadgets. The aggressor initially listens stealthily on the remote parcels sent from a remote control to an insulin pump [1]. From the caught bundles, the assailant figures out the gadget PINs related with the remote control and glucose meter. By mirroring the remote control, the assailant can arrange the insulin pump to handicap or change the expected treatment, stop the insulin infusion, or infuse a significantly higher dosage than permitted. By imitating the glucose meter, the assailant can send fake information to the insulin pump, making the pump alter insulin conveyance in light of the false information. Moreover, the assailant can snoop on the parcels to induce delicate patient information.

The above attack is hard to defend against, especially because it is hard to differentiate the attacker's forged wireless transmissions from legitimate ones. In this paper, we propose a medical security monitor (called MedMon) that detects such wireless attacks and protects PHS integrity and patient safety. MedMon's is based on the observation that although the attacker's transmissions may conform to the communication protocol, they are likely to deviate from legitimate transmissions either in the physical signal characteristics or in the behavior or underlying content. MedMon is an external monitor that tracks all wireless communications to/from medical devices and identifies potentially malicious transactions using multi-layered anomaly detection [2,3].

When anomalies are captured, the monitor can warn the patient and jam the suspicious transmission before it changes the state of the target device. MedMon can be implemented as a dedicated device or built into an existing personal device such as a smartphone. The summary of our contributions is as follows:

1. To design a body area network for patients in ICU.

2. To detect and intercept any anomalous data within the network.

3. To Design and develop a accurate digital spirometer for lung capacity.

The rest of the paper is organized as follows. Section II discusses concept of anomaly. Section III provides an overview of the available defence framework, Section IV evaluates proposed system Finally, Section V concludes the paper result.

Methods

Concept of anomaly and causes of anomaly in wireless sensor network

Concept: Anomalies are unusual measurements that may be obtained from sensors in a wireless sensor network for various reasons e.g. faulty sensors , actual events i.e. a change in some monitored property of the variable, obstructed or even faulty communication system among sensors , etc. They represent values, which appear to be different from others obtained from similar ambient conditions in such a way that one is fairly convinced they must be from a different distribution. Anomalies are also called outliers [4,5].

Causes

I. Faulty sensors or motes: Broken sensor, dead batteries, non-deliberate obstruction of wireless sensor communication, faulty motes, etc., all qualify as anomalies caused by faulty sensors or equipment. This is especially true if the anomalies disappear once the faults are fixed, if not, sabotage will be the more likely cause.

II. Sabotage: For this, an enemy that seeks to water down, or aggravate measurements with an aim to mislead decision makers causes the anomalies deliberately. This usually may take several forms. This has led to the research in the area of security in wireless sensor networks, with different already developed.

III. Errors: Errors may be due to changes in sensor intrinsic characteristics. An example is the changes in measurements by a sensor at different temperatures. Errors may also occur when the sensors communicate non-steady state measurements.

IV. Events: Events are the actual anomalies that the wireless sensor network designer wishes to have to deal with. They represent the actual information. For whatever application, events are the changes that need to be monitored and should affect decision-making processes that take place based on measurements from wireless sensor networks.

Available technics for monitoring and anomaly detection

Rediofrequency identification: Pacemaker systems were considered as implantable cardiac defibrillators [6,7]. In this study, they assumed a channel between medical devices and controllers. This channel was based on radio frequency identification (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. The 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 staff 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. The devices which are very near to the human body play important role in BCC.

Signal propagates between these devices only. Thus, range of the communication is limited very close to the human body.

Ultrasonic distance bounding: This scheme used a message authentication protocol. The 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. There are chances that an attacker can make the physical contact with patient by approaching him. Parameters-The key has to be printed into patient's skin with the help of ultraviolet- ink micropigmentation. The key is placed near the point of IMD implantation. The ultraviolet-ink micropigmentation were called invisible tattoos. The 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 defibrillator 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].

Shild: Shield as a personal base station. Patients have to wear this shield on the body near the IMD. Messages were coordinated between programmer and IMDs using shield. Shield provides secured communication of IMDs with programmer. Shield encrypts the messages sent by IMDs and sends them to the programmer. Considering the reverse case, the commands from the programmer to be send to IMDs by the shield are not encrypted. Therefore, commands do not remain confidential [17].

Medmon: Medmon, meaning medical security monitor. Medmon provides security by two ways. First is through wireless monitoring and second is through anomaly detection. Anomalies include physical and behavioral. Physical anomalies are of three types. These are time of arrival (TOA), differential time of arrival (DTOA) and received signal strength indicator (RSSI). Behavioral anomalies consist of the two, i.e., data anomaly and command anomaly [18]. Medmon keeps a record of previous data and commands. If new data or command arrives, it is compared with the previous record to decide if new data or command is a behavioral anomaly or not. Medmon performs all its functions without being affected by changes in its environment, but has a drawback that data being communicated through the channel does not remain confidential.

Proposed system

Disadvantages of existing system

1. The body area networks are susceptible to any attacks from within as well as outside the network.

2. The Body area network have no security against data which is being transmitted by other slaves form different network.

3. The existing body area networks are expensive to install and require regular maintenance.To avoid the above drawback we propose a system having:

Objectives

1. To design a body area network for patients in ICU.

2. To detect and intercept any anomalous data within the network.

3. To Design and develop a accurate digital spirometer for lung capacity.

We propose a general framework for securing medical devices based on wireless channel monitoring and anomaly detection. Our proposal is based 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 identify potentially malicious transactions [19].

Upon detection of a malicious transaction, Med Mon takes appropriate response actions, which could range from passive (notifying the user). A key benefit of Med Mon is that it is applicable to existing medical devices that are in use by patients, with no hardware or software modifications to them.

In our paper we are showing that the Slave is acting as Master as well as slave configuration to cause anomaly in the network. As slave it receives the data from master and sends false reading to master which can cause Issues since the master diagnosis will be inaccurate since false data is being fed to the Master via Anomalous Node.

Request and response protocol: Master send a request for data to slaves at particulat interval of time

- Time anomaly: If a transmission is scheduled to occur at specific points in time, the occurrence of the transmission at a non-scheduled time reveals an anomaly.

- Password anomaly: After receiving the frame the master/Slave will check for the security password. If the password is correct then only slave will respond to master request.

Results

Lung capacity and respiratory rate are noted at particular time interval (Table 1, Figures 2 and 3).

Date	Time	Lung Capacity	Respiratory rate
20-05-2018	16:28:27	0	0000
20-05-2018	16:28:57	0	0000
20-05-2018	16:29:30	0	0000
20-05-2018	16:29:57	0	0000
20-05-2018	16:30:27	0.94	0072
20-05-2018	16:30:57	0.94	0095
20-05-2018	16:31:27	0.94	0095
20-05-2018	16:31:57	0.94	0095

Table 1: Results of lung capacity and respiratory rate at particular time interval.

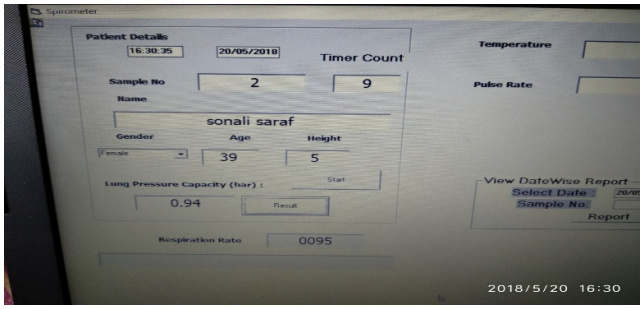

Figure 2: Patient details.

Figure 3: Respiratory rate.

Discussion and Conclusion

Advantages of proposed system

1) The proposed Body area network is equipped with a security mechanism which blocks any attacks or anomalous readings from other slaves.

2) The BAN designed is inexpensive and can very well cover today's hospital rooms.

3) Efficient design to detect and block anomalies.

4) Less time delays.

5) Quick response time.

6) Fully automate system.

7) Robust system, low power requirement.

Disadvantages of proposed system

1) Initial set up Cost is high.

2) Maintenance is high.

Application of paper

1) Hospitals.

2) Nursing homes.

3) Old age homes.

Future scope

Add other methods of anomaly such as RSSI.

Use more advances encryption and decryption.

References

1. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, et al. (2008) Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. IEEE Symposium on Security and Privacy.
2. Review on security of medical devices (2016) International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.
3. Park GE, Webster TJ (2005) A review of nanotechnology for the development of better orthopedic implants. J Biomed Nanotechnol 1: 18-29.
4. Zhang M, Raghunathan A, Jha NK (2013) MedMon: Securing medical devices through wireless monitoring and anomaly detection. IEEE Transactions on Biomedical Circuits and Systems 7: 871-881.
5. Insulin pumps-global pipeline analysis, opportunity assessment and market forecasts to 2016. Global Data (2010).
6. Hanna K (2001) Innovation and invention in medical devices: workshop summary. National Academies Press.
7. Israel CW, Barold SS (2001) Pacemaker systems as implantable cardiac rhythm monitors. Am J Cardiol 88: 442-445.
8. Fotopoulou K, Flynn B (2007) Optimum antenna coil structure for inductive powering of passive RFID tags. IEEE International Conference on Identification, pp: 71-77.
9. Hancke GP, Centre SC (2008) Eavesdropping attacks on high-frequency RFID tokens. In Proc. Workshop Radio Frequency Identification Security, pp: 100-113.
10. Denning T, Fu K, Kohno T (2008) Absence makes the heart grow fonder: New directions for implantable medical device security. In Proc. Conf. Hot Topics in Security, pp: 1-7.
11. Baldus H, Corroy S, Fazzi A, Klabunde K, SchenkT (2009) Humancentric connectivity enabled by body-coupled communications. IEEE Communications Magazine 47: 172-178.
12. Rasmussen KB, Castelluccia C, Heydt-Benjamin TS, Capkun S (2009) Proximity-based access control for implantable medical devices. In Proc. ACM Conf. Computer and Communications Security, pp: 410-419.
13. Schechter S (2010) Security that is meant to be skin deep: using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices. Microsoft Research, Tech Rep.
14. Xu F, Qin Z, Tan C, Wang B, Li Q (2011) IMDGuard: Securing implantable medical devices with the external wearable guardian. In Proc. IEEE Int. Conf. Computer Communications, pp: 1862-1870.
15. Gultepe E, Nagesha D, Sridhar S, Amiji M (2010) Nanoporous inorganic membranes or coatings for sustained drug delivery in implantable devices. Adv Drug Deliv Rev 62: 305-315.
16. Fu K (2009) Inside risks: Reducing risks of implantable medical devices. Communications of the ACM 52: 25-27.
17. Maisel WH, Kohno T (2010) Improving the security and privacy of implantable medical devices. N Engl J Med 362: 1164-1166.
18. Li C, Raghunathan A, Jha NK (2011) Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. IEEE 13th International Conference on e-Health Networking, Applications and Services, pp: 150-156.
19. Gollakota S, Hassanieh H, Ransford B, Katabi D, Fu K (2011) They can hear your: Non-invasive security for implantable medical devices. In Proc. ACM Conf. Special Interest Group on Data Communication.