DOI 10.29042/2019-4913-4919

Helix Vol. 9 (3): 4913- 4919

Secured Anomalous Detection for Personal Healthcare System

[*1]Dr. Pradeep. B. Mane, [2]Divya Katariya

[1,2] Department of Electronics, All India Shri Shivaji Memorial Society's IOIT, Pune.

Email: pbmane6829@rediffmail.com, divshi04@gmail.com

Received: 24th November 2018, Accepted: 13th February 2019, Published: 30th June 2019

Abstract

Advances and developments in medical systems have prompted a heightening in Implantable and Wearable Medical Devices(IWMD's).IWMD's normally incorporate remote correspondence interface through which they can be associated with Body Area Network(BAN). However, the programmability and remote availability of medicinal gadgets open up open doors for malicious attackers otherwise called anomalies. Therefore, there is a need to detect anomaly which is a vital issue that has been explored inside diverse research zones and applications. In this paper, a non-invasive method or secured framework is used for detection of anomaly that fortify against Radio Frequency attacks that are wirelessly caused on the PHS's(Personal Healthcare System). The proposal is based on a medical security monitor that investigates all the radio-frequency wireless communications to/from medical devices. It identifies malicious transactions using 3 techniques viz, RSSI (Received Signal Strength Indicator), Password and Time Anomaly. Upon detection of an anomalous transaction, it takes suitable response actions such as jamming the commands so that they do not harm the therapeutic gadget. The performance of the system is determined by developing a prototype implementation for monitoring Lung Capacity using Spirometer along with Temperature monitoring using two Radio Peripheral boards i.e. Zigbee. Moving towards the 3rd layer of protection, proves that the system is able to obstruct all kind of attacks resulting in 100 % accuracy showing that it is an effective method to increase the security of BAN.

Keywords

Anomaly Detection, Personal Healthcare System, Security, Wireless Channel Monitoring, Lung Capacity (Spirometer), PHS, BAN.

Introduction

Medicinal advances and in addition developments in ultra-low-control registering, systems administration, and detecting innovations have led to an increase in wireless accessible implantable and wearable medical devices(IWMDs). IWMD's can communicate directly with the server and other devices in the network through remote correspondence interfaces. These remote correspondences include sensors, actuators that are connected to the BAN. A PHS(Personal Healthcare System) can be defined as a network of communicating devices such as sensor or actuators that can provide health information to the user of providing remote health services to the user. The functions performed by the wireless accessible medical devices are sometimes found to be life-critical. So, there is a need to check for any malfunction in their operation. Hence, there is a need for development of system that will allow for the detection of such malfunction/abnormalities or otherwise called Anomalies. Anomaly Detection is defined as detection of abnormalities in the data that do not match with the normal data. Anomaly Detection finds wide range of applications such as detection of fault for cyber security, intrusion detection for health care, fraud detection for credit cards, etc. In this paper, overviews of the attacks are described. To protect the medical devices against any such kind of wireless attacks, three layered Anomaly Detection Technique is described in this paper. The attacker can eavesdrop on the data packets wirelessly send by the remote control. The attacker can try to get the device PIN from the captured or transmitted packets. By changing the settings of the remote control, the attacker can harm the patient by disabling or changing the intended therapy. The false data sent by the attacker can reach the monitor or the controller so that the system provides wrong or unintended therapy to the patient. It is hard to distinguish the assailant's transmissions from the genuine ones. Secured Anomalous Detection for Personal Healthcare System detects wireless attacks using three layered security. It is based on the observation of the physical characteristics of the signal, password/PIN that is embedded in the packet and the time during which the signals are sent. The attacker's password/PIN may match or conform to the communication protocol, they may vary in the physical signal characteristics from the legitimate transmission. The framework utilizes 3 layered peculiarity identification technique to track every single malignant exchange**.** Upon detection of an anomaly or malicious activity, the monitor jams the data sent by the anomaly.

The summary of contribution is as follows:

- In this paper, a non-invasive method or secured framework is used for detection of anomaly that fortify against Radio Frequency attacks that are wirelessly caused on the PHSs.
- The approach is truly non-invasive in nature.
- The effectiveness of the system is demonstrated by developing a hardware implementation for Temperature monitoring, and monitoring of Lung Capacity using Spirometer.

The rest of the paper is organized as follows. Section II presents Related Work with various methods and technologies used. Section III and IV describes Anomaly Detection Techniques and System Design for Lung Capacity Monitoring and

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Temperature Monitoring. Section V presents Tests and Results. Section VI presents performance analysis. Finally, section VII concludes the paper with results.

Related work

This section presents several existing techniques and methodologies used against wireless attacks and discusses their merits and limitations.

Earlier work surveys[1] the security measures and research in WBAN. It uses a technology that provides remote mechanism to monitor and collect patients health record data using wearable sensors [2],[3].Cryptography is the best approach for ensuring the remote correspondence or remote channel and forestalling unapproved access.

IMD Guardian [2] is a cryptographic scheme for implantable cardiac devices. In this the Electrocardiography signals of patients are utilized for extraction of key so that no pre-appropriated mysteries are required and rekeying is simple. However, assailants or attackers might have the capacity to extricate the key through physical contact with the patient.

Salem et.al [3] proposed a framework for detection of anomaly in WBAN.

Lee et.al [4] proposed encryption using Elliptic Curve Cryptography (ECC).It is based on management Secure Key in healthcare systems. Three steps are used in the scheme i.e Registration of key, Verification of key and key exchange.

Barau et.al [5] suggested patient centric control scheme to access personal health information efficiently and securely by establishing diverse access privilege and attributes sets dependent upon who requested for the data.

Mana et.al [7] proposed a biometric approach from the heartbeat, an intrinsic characteristics of the individual's body. It uses techniques or processes to guarantee privacy in the location of WBAN.

Attacks that again and again request communication with the IWMD like denial-of-service attacks cannot be defended or resisted by the Cryptographic methods.

A new mechanism based on ultra-sonic distance bounding enables an IWMD to grant access to those devices that are in close proximity. In this scheme, a token is used for emergency mode of operation [8].

On the other side, an outer gadget called the "Shield," is presented in [9]. The shield acts as an arbitrator between the IWMD and the outer programmer. The shield can guard only against short proximity remote assaults.

The paper discusses about the security of the system. The system directly communicates with the IWMD without any mediator. It monitors the communication and only interferes when an anomaly is detected. Unlike other systems, it is suitable for both short and long range distances. It is truly non-invasive and totally secured as it does not allow the attacker to eavesdrop on the communication channel among the components of the PHS.

Anomaly Detection Techniques

The anomalies and its types along with the detection techniques are described in this section.

Anomalies are change in data that do not match with a normal behavior.

For example, if the data is expected to be 0000 whereas the received data is 0100 it reveals anomaly.

*	*	*	*

Expected Data

The design in data patterns that do not match with the expected data patterns is shown below.

*	0	*	*

0	*	$	*

Anomaly

Figure 1: Different Data Patterns Reflecting Anomaly.

Anomalies might be induced in the data for a variety of reasons, such as malicious activity, for example, credit card fraud, cyber-intrusion, terrorist activity or breakdown of a system, but all of the reasons have the common characteristic that they are interesting to the analyst. The interestingness or real life relevance of anomalies is a key feature of anomaly detection.

Anomaly Detection refers to the issue of discovering sequence/sample that don't match to expected conduct. These nonconforming examples are regularly alluded to as inconsistencies, anomalies, conflicting perceptions, exemptions, deviations, amazements, or contaminants in various application spaces. Inconsistency identification strategies are normally utilized as a part of different domains, but have not been investigated with regards to therapeutic gadgets. In this paper, the system infers the legitimacy of a packet using a sequence of checks. Transmission is allowed only if it passes these checks. The system checks for the three layers of protection before taking any therapeutic action.

i) RSSI (Received Signal Strength Indicator): The 1st level of security is to obtain the signal strength through RSSI i.e Zig-bee. The monitor will verify the legitimacy of the transmitter by knowing this characteristic. In this, the distance between the monitor or the Central Monitoring Unit and the IWMD is fixed whereas the distance between the Anomaly and the monitor will vary. Since, the distance between the monitor and the IWMD is fixed and expected to remain consistent, the signal strength sent by the attacker can report to be a peculiarity. If the signal strength of the IWMD and the anomaly are found to be in the same range then the monitor will check for the 2nd and the 3rd layer of protection. If the

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

signal sent by the Anomaly is found out of range, the monitor will jam the signals send by the Anomaly. After the training, the set point of RSSI is decided to be -200 db.

ii) Password Based Anomaly : The physical characteristics of the signals i.e RSS(Received signal strength) are analyzed first. If the transmitted signal is able to pass the 1st layer of security, the monitor checks for the information send by the devices. The signals basic information related to the password and time will be checked by the monitor to find the abnormalities in the information. If the information sent by the device is correct and no abnormality is found, the monitor grants access to the object device to send the actual data. If the abnormality is found the monitor will straight away jam all the data send by that device. There is a possibility that PIN of the IWMD gets hacked and is known by the other devices and the signal is professedly transmitted from that device to the monitor. In that case, the monitor will check for the registered PIN. If the PIN is sent by the unregistered device and is found to be correct, the monitor will grant access to that device. Although the device is allowed to send the data, the monitor will check for the 3rd layer of security i.e Time Anomaly. If the PIN is incorrect, the monitor will jam all the data sent by that device.

iii)**TOA (Time Of Arrival):** RSSI i.e the 1st layer of security cannot guarantee that all attacks will be detected. So there is a need to check for password that is associated with each device. In case if the attacker anyhow tries to hack the password it will check for the time. In this event the transmission is booked to happen at particular focuses in time (0-10sec), the event of the transmission at an irregular interval of time (10-15sec) reports an anomaly.

System Design

The prototype implementation for Lung Capacity monitoring using Spirometer and Temperature monitoring is described in this section.

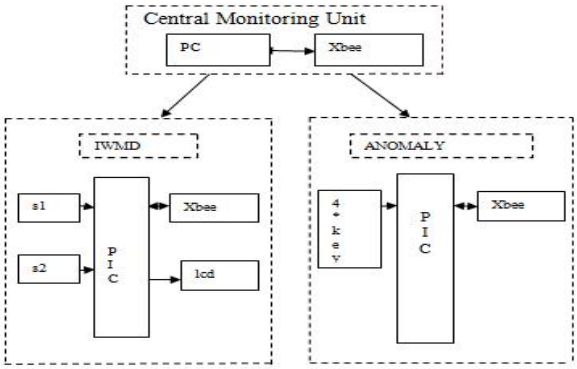


Figure 2: Block Diagram

Where R:-Request

S1 :- Spirometer,

S2 :- Temperature Sensor

The above block diagram works on Request and Response Protocol. The Central monitoring unit is the actual monitor that requests for the data to both the IWMD and the Anomaly. The data of both the devices is transmitted wirelessly to the monitor through Zig-bee. It consists of the following components: Lung Capacity sensor (Spirometer): A *Spirometer* is an apparatus for measuring the amount of air inhaled and exhaled by the lungs. It shows the capacity of the lungs with how much pressure the air is exhaled out. A manual key is provided to the patient for applying pressure. As the patient applies pressure, the lung pressure capacity will be determined by the spirometer. In the experiment, one board is used to perform as actual transmission and another to simulate the attacker. Both the boards have transmit paths that can be used independently to transmit the data to the monitor.

Test and Results

Experiment 1: In this, the distance between the monitor and the IWMD is set to 30 cm whereas the distance is varied between the monitor and the malicious programmer i.e. anomaly. The malicious programmer is varied between 30-300 cm away from the monitor. After 50 trials, the set point of the transmitted signal strength is set to -200 db. This is 15 db higher than the strength of the IWMD whereas it is 15 db lower for Anomaly's signal strength. A command is initiated by the monitor for the signal strengths of both the IWMD and the malicious programmer. Since the anomaly is transmitting the signal from various distances, its signal strength also varies. It is observed that, as the anomaly moves away from the monitor its signal strength decreases. Since the signal strength is lower than the expected, the monitor will jam the data sent by the Anomaly. However, sometimes it happens that the anomaly being at a distance away from the monitor sends wrong signal strength showing in range with the IWMD. In that case, performance analysis is done as discussed in section V. It is possible that the Anomaly comes in close proximity to the IWMD and tries to send false data. In that case, there is a need for the second and the third layer of protection. The observation table for 50 readings is shown below.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Actual Values(dbm)	Predicted Values(dbm)
-219 (In Range)	-180 (Out of Range)
-214 (IR)	-176(OR)
-203(IR)	-182(OR)
-217(IR)	-196(OR)
-219(IR)	-202 (IR)
-202 (IR)	-214(IR)
-215(IR)	-206(IR)
-208(IR)	- 212(IR)
-203(IR)	-215(IR)
-201(IR)	-208(IR)
-206(IR)	-211(IR)
-211(IR)	-170(OR)
-216(IR)	-219(IR)
-212(IR)	-203(IR)
-208	-211
-216	-202
-222	-215
-209	-208
-220	-201
-204	-204
-208	-222
-201	-216
-215	-211
-209	-220
-205	-216
-219	-218
-221	-202
-219	-205
-216	-211
-201	-203
-218	-215
-207	-208
-212	-219
-216	-225
-215	-204
-192	-201
-187	-207
-173	-196
-160	-198
-185	-206
-196	-212
-179	-217
-181	-203
-192	-200
-198	-201
-174	-219
-183	-208
-160	-211
-102	-222
-188	-205

Table 1: Observation of 50 Trials

Experiment 2: In this, the process gets reversed i.e the Anomaly is moved towards the monitor to come in close proximity of the IWMD. There comes a point where signal strengths of both the IWMD and the Anomaly are found to be in range. The monitor can now accept the data sent by the malicious programmer considering it as a true data. So, there is a need for executing the 2nd layer of protection i.e password based anomaly. For this, the monitor requests for the password/PIN. The anomaly is caught if it sends the wrong PIN and the monitor jams the data sent by the anomaly. The

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

actual Frame format is shown in fig 3.below. The password is embedded in the middle of the packet. So, the monitor gets enough time to decide whether to jam after receiving half of the packet. Over 50 transmissions, it is found that the monitor jammed all the command packets sent by the anomaly resulting in 100% detection rate, since the false PIN sent by the Anomaly does not match with the stored PIN of the IWMD.

S O F	Source ID	Router ID	PIN/ password	Destination Id	E O F

Figure 3: Frame Format

Experiment 3: There is a need for 3rd layer of protection only if the adversary somehow manages to hack the password of the IWMD. If the Anomaly sends correct PIN to the monitor, the monitor will check for the time within which the password is sent. The predefined time for the IWMD to send the data is 0-10 sec. The data sent by the anomaly will be jammed if it tries to send the data after 10 secs.

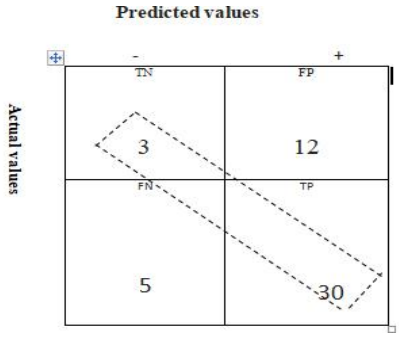
Performance Analysis

In this paper, Confusion Matrix is used to evaluate the performance of the classification model. A Confusion Matrix is a table used to describe the performance based on a set of test data for which the true values are known. The accuracy is calculated for each type of anomaly using the confusion matrix.

Case I:- To calculate accuracy for 1st level of security i.e RSSI.

There are two possible predicted classes: "True" and "False". In this paper, True is considered as Positive instance and False is considered as Negative instance. Positive instance means that the actual and the predicted values must be In Range whereas Negative instance means that the actual and the predicted values must be Out of Range. However, for 35 Positive instances 30 values are found to be In Range and 5 are found to be Out of Range i.e 30 TP and 5 FN. Similar is the case for 15 Negative instance 12 values are found to be Out of Range and 3 values are found to be In Range. The actual and the predicted values for Positive as well as Negative instance is shown in table above.

The Confusion Matrix for the above case is shown below.



From the observation table, it is clear that out of 35 positive instances, 30 trials were true and 5 were false. For negative instances, 3 were true and 12 were false. The Accuracy can be calculated as follows:

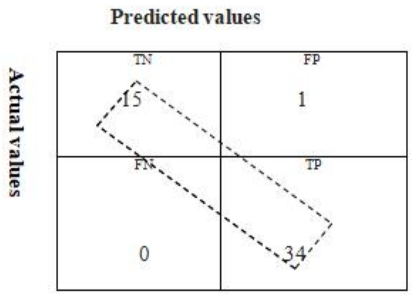
Accuracy = TP+TN / Total no. of trials

= 30+3/50

= 66%

Case II:- To calculate accuracy for 2nd level of security i.e Password Anomaly. In this case, Positive instance is denoted by R and Negative instance is denoted by W.

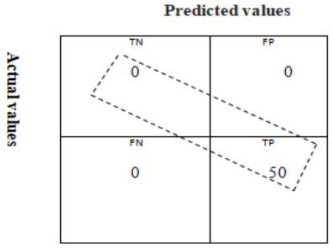
R stands for the Right PIN whereas W stands for the Wrong PIN. Since, the length of the PIN is 4 bit, total 16 combinations are possible. These 16 combinations are considered as 16 negative instances. Out of these 16 instances, it is possible that only once the PIN will be correct. As 16 combinations are considered as Negative instances, the remaining 34 out of 50 trials are considered as Positive trials. The confusion matrix for Password Anomaly is given as:



  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Accuracy = 34+15/50
=0.98
= 98%

Case III:- To calculate Accuracy for 3rd level of security i.e Time Anomaly.
As per experiment 3 described in Section III, the time interval (0-10 s) is predefined for the IWMD to send data to the monitor. In this case, the Positive instance is denoted by T and Negative instance is denoted by OT.
T stands for the time interval within which the data will be sent. And OT stands for Out of Time i.e if the anomaly tries to send the data after 10 sec it will be considered as OT. There is a possibility that the anomaly may hack the PIN and try to send the data within the predefined time. But, there is a condition that the anomaly is allowed to enter the PIN only 3 times. If the accuracy is calculated based on this condition it is the same as accuracy of the password anomaly. However, in real time it is not possible for the anomaly to send the correct PIN within the stipulated time i.e. 10 sec. Out of 50 trials, it is found that the anomaly was unable to send the correct PIN within 10 sec. So, the Confusion Matrix for the above condition is given as follow:



$$\frac{50+0}{50}$$

Accuracy =50+0/50
=100% **Error! Bookmark not defined. Error! Bookmark not defined.**

Conclusion
In this paper, a non-invasive method or secured framework is used for detection of anomaly that fortify against Radio Frequency attacks that are wirelessly caused on the PHSs. This secured framework solution aims at increasing the reliability of the system and thereby increasing the patient's integrity and data confidentiality. Using 3 layered anomaly detection technique; it detects all the wireless communication caused to the medical devices/from the medical devices identifying potentially malicious transactions. This system is able to detect 66% of attacks using1st layer of security i.e RSSI. The 1st layer is not 100% reliable and hence there is a need for 2nd and the 3rd layer of security. It is possible that a skeptical attacker may evade the 1st layer of security by knowing the physical characteristics of the signals, the other types of attacks can be caught by switching to Password/PIN anomaly. The 2nd layer of anomaly is 98% reliable stating that it is however better than the 1st layer of security. Moving towards the 3rd layer of security i.e Time Anomaly, the system is able to detect all attacks resulting in 100 % accuracy.

References
1. D. Arney, K. Venkatasubramanian, O. Sokolsky, and I.Lee, "Biomedical devices and systems security," in Proc. IEEE Int. Conf. Engineering in Medicine and BiologySoc.pp.2376–2379, (2011).
2. F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "IMD Guard: Securing implantable medical devices with the external wearable guardian," in Proc. IEEE Int. Conf. Computer Communications, pp. 1862–1870,(2011).
3. Osman Salem , Alexey Guerassimov , Ahmed Mehaoua,"Anomaly detection in medical wireless sensor networks using SVM and linear regression models", International Journal of E-Health and Medical Communications, Volume 5 Issue 1, (2014).
4. Young Sil Lee, E. Alasaarela and Hoon Jae Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," The International Conference on Information Networking 2014 (ICOIN2014), Phuket, pp. 453-457, (2014).
5. M. Barua, X. Liang, R. Lu and X. Shen, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, pp 970-975,(2011).
6. Dasgupta,D. and Majumdar, N, "Anomaly detection in multi dimensional data using negative selection algorithm," in Proceedings of the IEEE Conference on Evolutionary Computation. 1039– 1044, (2002).

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

7. Mohammed Mana , Mohammed Feham , and Boucif Amar Bensaber; “Trust Key Management Scheme for Wireless Body Area NetworksI,”International Journal of Network Security, Vol. 12, No. 2, PP. 75–83, (2011).
8. F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, “IMD Guard: Securing implantable medical devices with the external wearable guardian,” in Proc. IEEE Int. Conf. Computer Communications, pp1862–1870,Apr. (2011).
9. 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).
10. M. Rushanan, A. D. Rubin, D. F. Kune and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," 2014 IEEE Symposium on Security and Privacy, San Jose, CA,(2014).
11. Forrest, S., Esponda, F., and Helman, P, “A formal framework for positive and negative detection schemes,” in IEEE Trans. Syst. Man Cybernetics, Part B. IEEE, 357–373,(2004).
12. LEE, W.AND XIANG, D. 2001,“Information-theoretic measures for anomaly detection,” in Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society, 130,(2001).
13. 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).
14. S. Schechter, “Security That is Meant to be Skin Deep: U sing Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices, Microsoft Research,” Tech. Rep. MSR-TR-2010-33, Apr. (2010).
15. C. Li, A. Raghunathan, and N. K. Jha, “Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system,” in Proc. IEEE Int. Conf. e-Health Networking, Applications and Services, Jun. (2011).

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495