A Secure Framework for Remote Healthcare Monitoring using the Internet of Medical Things

Osman Salem and Ahmed Mehaoua
Borelli Research Center, CNRS UMR 9010 - University of Paris, France
{firstname.lastname}@parisdescartes.fr

ICC 2022 - IEEE International Conference on Communications | 978-1-5386-8347-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICC45855.2022.9839025

***Abstract*—In this paper, we propose a secure framework for healthcare monitoring using the Internet of Medical Things (IoMT). In spite of their deployment, these devices still vulnerable to several cyber-attacks, ranging from unauthorized access to private medical data to data modification and injection. These attacks can compromise the privacy of the monitored patient, reduce the reliability of the monitoring system and may harm the life of monitored patient. In this paper, we propose a new framework to detect attacks and secure the communications in IoMT. To prevent eavesdropping and modification attacks, we propose the Ephemeral Elliptic Curves Diffie-Hellman (EECDH) to derive a session key used to provide confidentiality and authenticity. To detect injected measurements, flooding triggered by compromised devices and medical changes in physiological data, we applied the sequential change point detection algorithm Pruned Exact Linear Time (PELT) followed by the boxplot. Our experimental results show that our approach is able to increase the reliability and the accuracy of remote monitoring system, while reducing the false alarms triggered by injected measurements.**

***Index Terms*—Anomaly Detection; PELT; ECC; ECDH; BLE; IoMT; WBANs**

1. Introduction

With the advances in information and communication technologies, the IoMT becomes a promising solution for remote healthcare monitoring, where a set of wearable biosensors are used to collect the physiological data from the monitored patient, and to transmit the acquired measurements to an LPU (SmartPhone or tablet) for processing and alarming the healthcare professionals when an emergency is detected. Such monitoring systems are able to assist the healthcare professionals by analyzing the acquired physiological data in the edge of the network, and raising an alarm when an anomaly is detected by highlighting abnormal changes in monitored parameters.

The use of IoMT devices provides a tool to improve the Quality of Life (QoL) by allowing the monitored patient to continue their Activity of Daily Living (ADL) while being monitored and followed-up. Their fast deployment has an impact on reducing the number of bed occupied by patients kept under-monitoring. The COVID-19 pandemic has driven an exponential rise in IoMT, with quarantine and stay-at-home orders, which dramatically accelerating trends in telemedicine and telehealth.

However, the medical data involves stringent security requirements which are not available in sensors with restricted resources [1]. The collected sensitive medical data are transmitted to the LPU for processing using wireless technology, and an attacker in vicinity can eavesdrop or modify the intercepted data [2] leading to false alarms, or can conduct black hole attack by preventing information from being transmitted to the smartphone, in order to prevent the system from raising alarms. The attacker may also exploit the vulnerabilities [3] in the software of IoMT device to increase the transmission rate and deplete the energy of sensors or to flood the LPU. Therefore, a security framework is required to ensure the integrity of the exchanged data.

Several mechanisms have been proposed and tested in the literature for securing the exchanged data between the sensors and the LPU [4]. The Bluetooth Low Energy (BLE) is widely implemented today in IoMT to transmit data from sensors to the LPU. The object requires a short range communication, low bandwidth, low delay and reduced energy consumption. The BLE secures the communication using the Advanced Encryption Standard (AES) algorithm with a key length of 128 bits. However, when the object does not have I/O capabilities, the BLE "Just Works" pairing mode does not provide any protection against MitM (Man in the Middle) or eavesdropping. As the IoMT device does not have display or keyboard, the default value of pairing code $0x00$ is used as Temporary Key (TK), which in turn is used to derive the Short Term Key (STK) and the Long Term Key (LTK).

In other words, we can connect to any BLE device that uses the "Just Works" pairing mode and access the exchanged medical data. In fact, this pairing mode is deployed in several healthcare devices available in the market. The access to medical data causes a huge violation to the privacy of the monitored patient, and the injection of faulty measurements may threat the life of patient with a decision based on faulty measurements.

In this paper, we implement the EECDH with key renewal process to secure the communications and prevent MitM attacks while using the same security mechanisms in BLE for confidentiality and integrity. We used the Elliptic Curves Cryptography (ECC) with pre-distributed public keys used to derive the encryption key. The ECC has small key size compared to RSA, where a 256 bits key is equivalent to 3072 bits in RSA. Elliptic curve is more convenient for IoMT devices with constraints resources, where their usage is limited to derive a shared key using ECDH. The AES-CCM implemented in the BLE standard is used in our approach to provide encryption and integrity, and to prevent the MitM from conducting eavesdropping or injection attacks.

The IoMT devices are susceptible to various exploits and an attacker can easily change the behavior of compromised devices to increase the transmission rate and flood the LPU. Such change increases the energy consumption of the compromised devices and the LPU, and threats the functioning of the network. There is a need of a suitable system to detect such intrusion and to alert the user. We applied the sequential change point detection algorithm PELT [5] and the box-and-whisker plot on the number of received packets by the LPU to detect such changes and raise a network alert for user.

The rest of this paper is organized as follows. In section 2, we review recent related work. Section 3 presents our proposed approach for securing the communication link between the devices and to detect anomaly in the physiological parameters and in the number of received packets. In section 4, we present our experimental results from the application of our proposed framework on real physiological data. Finally, section 5 concludes the paper and present our future work.

2. Related Work

The IoMT are vulnerable to various attacks as the data is transmitted using BLE wireless technology from the sensor to the LPU [6]. An adversary can modify, eavesdrop or delete the data [7]. The impact of such attacks has been highlighted on insulin pumps with over dosage to kill the patient, and on pacemaker [8] to threat the patient's life.

Aghili *et al.* in [9] proposed a lightweight multi-factor authentication protocol for e-health systems in IoMT. Ayub *et al.* in [10] proposed a secure authenticated key agreement protocol using the concepts of Physically Unclonable Function (PUF). Other research work focused on authentication, encryption, integrity, and intrusion detection to secure the network of IoMT devices [2]. However, most of the proposed solutions have higher computation complexity which prevents their deployment on the constrained resources in IoMT devices.

To overcome these problems, Ahmed *et al.* in [11] proposed an enhanced ECDH for securing the data exchange of IoT applications. Our approach is similar in the spirit to their approach, where we use the Ephemeral ECDH to derive a session key for securing the data exchange of IoMT devices in "Just Works" pairing mode. The use of ephemeral keys allows key renewal every period of time.

In the other hand, the IoMT raises an alarm when a healthcare emergency is detected. Change Point Detection (CPD) algorithms seek to detect abrupt changes in the monitored physiological parameters, such as detecting changes in SpO2 to identify sever hypoxia or patient with COVID-19, or detecting changes in Blood Pressure (BP) to subsequently identify hypertension after vaccine. These changes need to be identified automatically with the large amount of collected data.

Several approaches for identifying changes in monitored data have been proposed in the literature [12]. The most common methods are those based on segmentation. These methods identify one or more points in a dataset where the statistical properties (e.g., mean and variance), change over time, based on the likelihood of the data in the time series. Among the proposed segmentation methods [12], [13], [14], window-based change point detection, Binary Segmentation (BS), and Optimal Partitioning (OP).

BS [14] is a sequential approach with a computational complexity $O(nlogn)$ where n is the number of samples in the segment. The principle of this method is to detect a change point in the time series, and to subdivide it into two parts, the first is before the change and the second is after the change. The operation is repeated on the two resulting parts. BS is fast and seeks to identify the minimum number of change points.

Window-based change point detection is used to perform rapid segmentation of the signal. The algorithm uses two windows that slide along the data stream. The statistical properties of the signals in each window are compared to measure the deviation. Window Segmentation (WS) has low complexity $O(nw)$ where n and w are the number of sample and the size of window respectively. However, it doesn't produce optimal segmentations [13]. The OP method has higher computational complexity $O(n^2)$ when compared to the previous two methods (BS & WS), but is able to find the exact global optimum.

Killick *et al.* in [15] improved the OP by proposing a new approach to search for change points. Their proposed approach is the PELT [5], which is an efficient approximate search method able to detect all change points with respect to the change of the mean or the variance, and regardless of the statistical distribution of the time series. Its basic idea is to divide the time series into several segments where the average of each segment is significantly different from the previous and subsequent segments. The penalty is an adjustable parameter in PELT to control the number of detected change points.

The PELT has several advantageous compared to other methods, specially in terms of linear computational complexity $O(n)$ as it uses dynamic programming and pruning [5]. Several previous work [13], [16] devoted to the search for the most adequate strategy to segment the data, and compare many CPD algorithms. Their results proved that PELT provides the best tradeoff between complexity and detection accuracy, where it has the lower complexity and memory requirements when compared to other methods. This is why we will use PELT in our approach for CPD in the measurements to detect healthcare emergency, and in the number of received packets to detect compromised sensors with high transmission rate, which intend to flood the LPU and deplete the energy.

3. Proposed Approach

Most of IoMT devices do not have I/O capabilities and the "Just works" with the default pin code is used. To secure the communication link between devices and the LPU and to prevent attacks conducted by MitM (as shown in Figure 1), which is able to intercept and alter the data, our proposed approach is based on pre-distributed ECC keys before deployment. These small size pre-distributed keys are used to derive shared session key to encrypt the communication between device and LPU using the AES-CCM deployed in BLE.

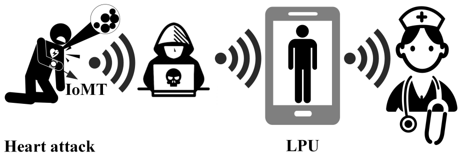

Figure 1. MitM attacks against IoMT

The creation of asymmetric keys is based on modern public key ECC, which is based on mathematical elliptic curves known to produce smaller keys size than RSA, faster operations and reduced processing complexity. Let F be a field with N elements, E is an elliptic curve with a set of points (x, y), and G is the identity or the neutral element of the curve. E is a function known as the Weierstrass Equation (given in Equation 1) defined over the field F:

$$(E)\ :\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

The coefficients $a_1, a_2, a_3, a_4, a_6 \in F$ have real values. A curve of the Weierstrass equation is said to be smooth if the partial derivatives in x and y of the Equation 2 do not cancel each other at the same time instant.

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \quad (2)$$

For their use in cryptography, a simplification of the Equation 1 is given in Equation 3:

$$y^2 = x^3 - ax + b \quad \text{with} \quad 4a^4 + 27b^2 \neq 0 \quad (3)$$

To create an asymmetric key pair (P, K), we used openssl with P-256 (prime256v1) to derive the 256 key pair, with P_i is used denote the public key, which results from ECC point multiplication of G with the private key (η_i):

$$P_i = \eta_i * G \quad (4)$$

The operator "*" is used to denote ECC point multiplication. With a pre-distributed key, the use of ECDH mechanism does not require any exchange between the two devices to derive the shared symmetric encryption key, as shown in Figure 2 and in Equation 5.

$$S_k = \eta_i * P_j \qquad \text{with } i \neq j \quad (5)$$

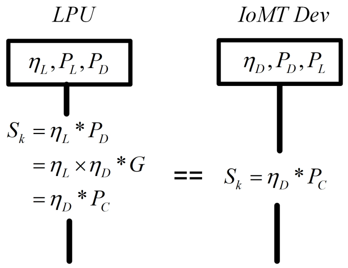

Figure 2. Elliptic Curve Deffie-Hellman (ECDH)

Where S_k is the secret key used to guarantee the security of exchanged data, and P_j is the public key of the other device. However, the derived secret key is always the same. To renew the key in our approach, the LPU starts by deriving an ephemeral ECC key pair $(\eta_E\ ,\ P_E)$ for each IoMT device, and transmits the public key (digitally signed) to the device to derive the same ephemeral secret key (as shown in Figure 3), which will change every period of time T_k.

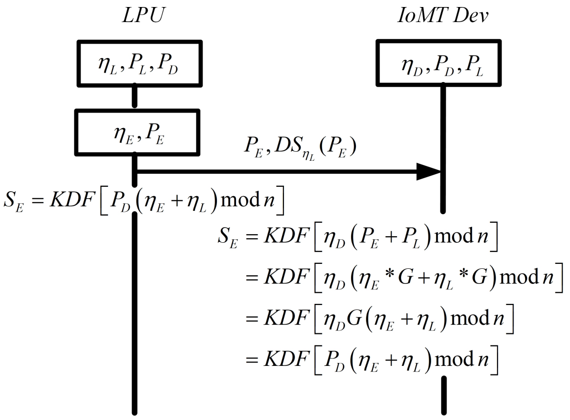
LPU
IoMT Dev
η_L, P_L, P_D
η_D, P_D, P_L
η_E, P_E
$P_E, DS_{\eta_L}(P_E)$
$S_E = KDF\left[P_D(\eta_E + \eta_L) \bmod n\right]$
$S_E = KDF\left[\eta_D(P_E + P_L) \bmod n\right]$
$= KDF\left[\eta_D(\eta_E * G + \eta_L * G) \bmod n\right]$
$= KDF\left[\eta_D G(\eta_E + \eta_L) \bmod n\right]$
$= KDF\left[P_D(\eta_E + \eta_L) \bmod n\right]$

Figure 3. Ephemeral ECDH

The confidentiality and integrity of the exchanged data are provided by AES-CCM to avoid the MitM from accessing the content or modifying the values of measurements. To prevent data suppression by the MitM, the transmission is reliable and must be acknowledged (ACK) in both directions to avoid black hole attack. In the case where the IoMT device does not receive an ACK after 3 retransmissions for k consecutive packets, it raises a local alert (light or sound) to notify user with network or security problem.

To detect anomaly in acquired vital signs, we start by preprocessing the data over a window of measurements. Let $y_{1:n}$ represents the sequence of measurements during the period of time T, where $y_{1:n} = (y_1, \ldots, y_n)$ is a set of n physiological measurements with real values. The CPD algorithm is able to identify m changes along with their positions $t_{1:m} = (t_1, \ldots, t_m)$. The position of the change point is an integer between 1 and n. The time series is supposed to be piecewise stationary, which means that some characteristics of the process suddenly change at unknown time instants $t_1 < t_2 < \ldots < t_m$. The data are normalized, and their values are between 0 and 1.

To detect change points, we applied the PELT method that aims to identify the instants of change in $y_{1:n}$. It is based on the OP and pruning method. The OP method aims to minimize cost:

$$\sum_{i=1}^{m+1} \left\{ C(y_{(t_{i-1}+1)}, \ldots, y_{t_i}) + \beta \right\} \tag{6}$$

Where C is a cost function for the i^{th} segment, and β is a penalty to prevent over-fitting. Subsequently, PELT uses pruning to increase the efficiency of the OP method while ensuring that the method finds an overall minimum of the cost function. The optimal segmentation is $F(n)$:

$$F(n) = \min_{t} \left\{ \sum_{i=1}^{m+1} \left[C\left(y_{(t_{i-1}+1)}, \ldots, y_t + \beta \right) \right] \right\} \tag{7}$$

The main idea behind the pruning is to remove these values of t which can never be minima of the minimization performed in each iteration. The OP method applies recursive conditioning by starting with a first conditioning on the last change point and calculating the optimal segmentation of the data up to the change point:

$$F(n) = \min_{t} \left\{ \begin{array}{c} \min\limits_{t|t_m} \sum\limits_{i=1}^{m} \left[C(y_{(t_{i-1}+1)}, \ldots, y_{t_i}) + \beta \right] \\ + C(y_{(t_m+1)}, \ldots, y_n) \end{array} \right\} \tag{8}$$

Using Equation 6 to simplify the previous equation, the internal minimization is equal to $F(t_m)$ and the Equation 8 can be re-written as:

$$F(n) = \min_{t_m} \left\{ F(t_m) + C(y_{(t_m+1)}, \ldots, y_n) \right\} \tag{9}$$

We applied the PELT on the received measurements and on the number of received packets. The CPD in the received measurements allows to detect emergency and to raise alarm for healthcare professionals, while the CPD in the total number of packets allows to detect compromised sensors with an increased transmission rate. However, the PELT method is sensitive to changes and identify all the change points with several false alarms. To increase the reliability of the system by reducing the False Alarm Rate (FAR), we apply the box-and-whiskers (boxplot) by comparing each identified change point by PELT with robust statistical parameters derived from a window of previous w values in order to confirm its deviation.

Let $Y_i^w = \{y_{t-w,i}, \ldots, y_{t,i}\}$ represents the sliding window of the last w values ($[DPC - w, DPC]$) for the i^{th} monitored attribute. The first quartile Q_1 and the third quartile Q_3 of Y_i^w are used to derive the interquartile range $\hat{\sigma} = IQR = Q_3 - Q_1$. A measurement is considered as abnormal (as shown in Figure 4) if the following condition is satisfied:

$$y_{t,i} \leq Q_1 - 1.5.(Q_3 - Q_1) \vee y_{t,i} \geq Q_3 + 1.5.(Q_3 - Q_1) \tag{10}$$

A medical alarm is raised if the deviation is detected only in the monitored biometrics parameters and not in the number of received packets.

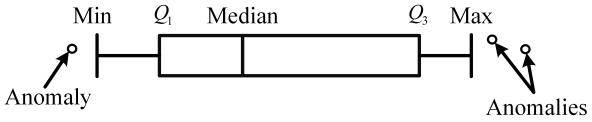

Figure 4. box and whiskers

4. Experimental Results

To conduct experiment and analyze the performance of our proposed approach, we used real physiological data collected from a patient with cardiovascular disease. The monitored patient have 68 years old, 1.75 meter living independently in his apartment and kept under monitoring. The used dataset is private and collected using other prototype and stored inside a CSV file. We focus only on chunk with changes in our experiments.

Five vital signs are available in the dataset: BP, Heart Rate (HR), Pulse, SpO2 and Respiration Rate (RR). The measurement units are: mmHg for BP, beat per minute (bpm) for HR and Pulse, respiration per minute (rpm) for RR and % for SpO2. To simulate real life scenario in Figure 1, we used two Raspberry Pi 4B, with 8 GB of RAM and BLE as IoMT devices that read data from the CSV file and transmit records to the LPU (Android tablet) for processing. The first device transmits SpO2 and Pulse, while the second is used to transmit BP, HR and RR.

We start our experiments by using AdaFruit USB stick as BLE sniffer and Wireshark to prove the ability of MitM to access the data in the BLE pairing mode. We refer to [17] and several tutorial available online to conduct such attack using kali Linux [18].

To prevent security attacks and leakage of sensitive data, we start by implementing our approach for ephemeral key derivation from ECDH, which is used to encrypt the data. We also configure the two devices to renew the key every 10 minutes to prevent off-line password guessing. The anomaly detection is implemented in the LPU and aimed to identify changes in physiological and total number of received packets. The received data on the LPU from the two Raspberry devices are decrypted before processing.

The variations of BP measurements are presented in Figure 5 where the heavy change is visible around the time instant 18000 sec and lasts until the end. Similarly, the variations of the HR and PULSE are shown in Figures 6 and 7 where correlated changes occur at the same instant as the BP. The variations of the RR and SpO2 are presented in Figure 8 and 9 respectively. The SpO2 falls down and becomes lower than 90% (asphexia) at the same time instant 18000 sec, and this explains the simultaneous increase in the number of RR and in the measurements of BP, HR and PULSE. The patient tries to get more oxygen by increasing his respiration and making more effort. In fact, the patient needs oxygen assistant in this chunk of data.

The variations of whole physiological parameters are presented in Figure 10, where we can identify a correlated change points around 18000 sec for approximately whole

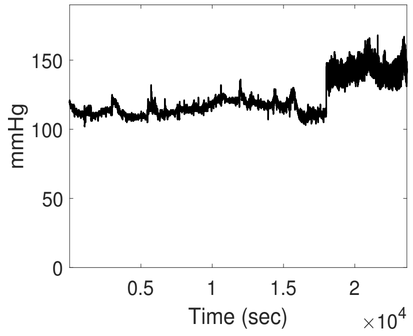

Figure 5. Blood Pressure

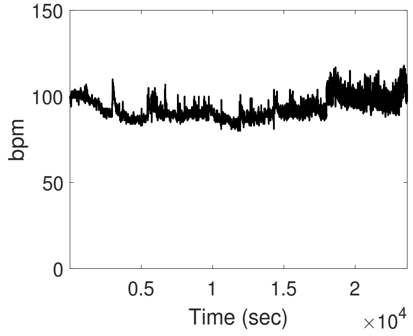

Figure 6. Heart Rate

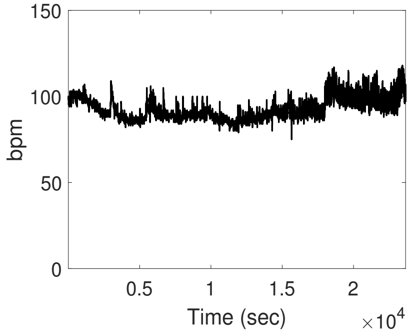

Figure 7. PULSE

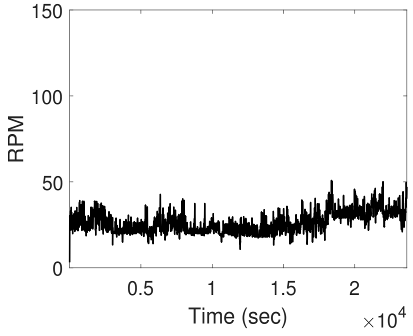

Figure 8. Respiration rate

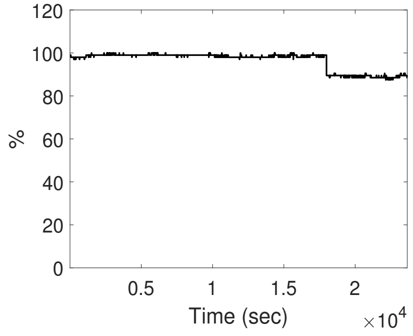

Figure 9. SpO2

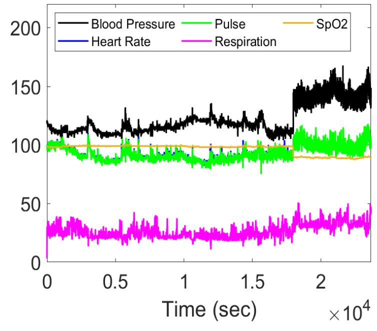

Figure 10. All parameters

parameters. The HR and PULSE superpose as they measure the same information.

In the second set of experiments, we test the security of our approach by assuming the worst case scenario to simulate MitM attack, where an attacker succeed to compromise both IoMT devices by exploiting software vulnerability. We start by increasing the transmission rate and the value of measurements for only one device in the beginning, followed by simultaneous increase in the rate of the second device (as shown in Figure 11) to deplete the energy of compromised sensors, and to flood the LPU with packets containing modified values. The measurements of HR in the beginning of attack can be distinguished from the Pulse as shown variations located inside the ellipse in Figure 12.

The average of received measurements in each second was derived and used in Figure 12. Our approach detects a change in the number of received packet for these variations and raises a local alert for user as network connection alert. The raised medical alert is represented by vertical red line in Figure 12 and triggered only if there is no change point in the number of received packets.

In the third set of experiments, we conduct performance analysis using he Receiver Operating Characteristic (ROC) to study the impact of the threshold on the accuracy of the system in terms of True Positive Rate (TPR) and False Alarm Rate (FAR). We also conduct performance comparison with existing works [19] which are based on the difference between predicted and measured values to identify change in time series. The prediction of the current measurement were achieved using Long Short-Term Memory (LSTM), AutoRegressive Integrated Moving Average $ARIMA(p, d, q)$ and Auto Regressive $AR(p)$, with $p = 4$, $d = 1$ and $q = 2$.

The obtained ROC is presented in Figure 13 where for a TPR of 99%, our approach has a FAR of 6%, followed by LSTM with 8%, AIRMA with 9% and AR with 12%. In fact, the use of our approach slightly outperforms the LSTM in term of FAR. In the other hand, even if the four methods have a linear computational complexity $O(n)$, our method has less execution time for processing one record than LSTM, where the decision delay of our method is 25.56 sec while the delay for LSTM is 39.63 sec, followed by ARIMA with 20.61 sec and AR with 18.48 sec.

5. Conclusion

In this paper, we proposed a framework to secure the exchange of medical data in IoMT and to detect anomaly in the number of received packets and in the acquired vital signs from monitored patient. We used the EECDH to exchange the session key in "Just Works" pairing mode, while keeping the same mechanisms used in BLE to ensure confidentiality and integrity. To detect healthcare emergency, we applied the PELT algorithm followed by boxplot to detect change in the monitored physiological parameters with reduced FAR. Furthermore, to detect attacks aimed to deplete the energy of sensors or to flood LPU, we applied the same CPD algorithm on the number of received packets

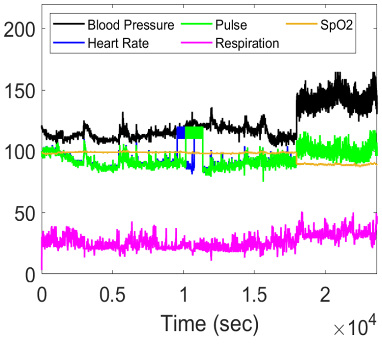

Figure 11. Injected values

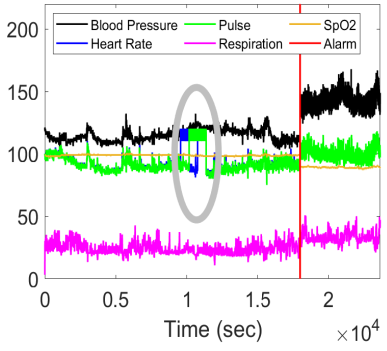

Figure 12. Normal & Alarm

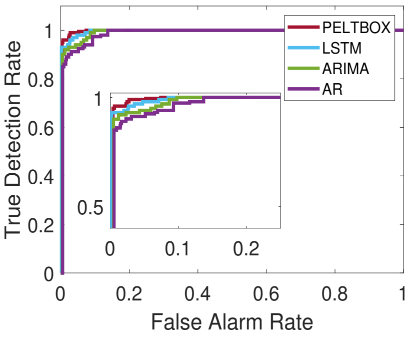

Figure 13. ROC

in LPU to raise network alarm. Our experimental results on real physiological data showed that our approach is effective and able to achieve a good detection accuracy with a FAR of 6%. Our future work will focus on anomaly detection in energy consumed by compromised IoMT device.

References

[1] J. Fiaidhi and S. Mohammed, "Security and Vulnerability of Extreme Automation Systems: The IoMT and IoA Case Studies," *IT Professional*, vol. 21, no. 4, pp. 48–55, 2019.

[2] G. Thamilarasu, A. Odesile, and A. Hoang, "An Intrusion Detection System for Internet of Medical Things," *IEEE Access*, vol. 8, pp. 181 560–181 576, 2020.

[3] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (iomt)," in *15th Int. Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019, pp. 457–464.

[4] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT Communications: A Survey," *Sensors*, vol. 20, no. 17, 2020.

[5] R. Killick and I. Eckley, "changepoint: An r package for changepoint analysis," *Journal of statistical software*, vol. 58, no. 3, pp. 1–19, 2014.

[6] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical internet of things: a review," *Security and Communication Networks*, vol. 2018, 2018.

[7] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices – a review," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019.

[8] H. A. M. Puat and N. A. Abd Rahman, "IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy," in *Journal of Physics: Conference Series*, vol. 1712, no. 1, 2020, p. 012009.

[9] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT," *future generation computer systems*, vol. 96, pp. 410–424, 2019.

[10] M. F. Ayub, M. A. Saleem, I. Altaf, K. Mahmood, and S. Kumari, "Fuzzy extraction and PUF based three party authentication protocol using USB as mass storage device," *Journal of Information Security and Applications*, vol. 55, p. 102585, 2020.

[11] M. I. Ahmed and G. Kannan, "Secure end to end communications and data analytics in iot integrated application using ibm watson iot platform," *Wireless Personal Communications*, pp. 1–16, 2021.

[12] C. Truong, L. Oudre, and N. Vayatis, "Selective review of offline change point detection methods," *Signal Processing*, vol. 167, p. 107299, 2020.

[13] G. J. van den Burg and C. K. Williams, "An evaluation of change point detection algorithms," *arXiv*, vol. abs/2003.06222, 2020.

[14] S. Kovács, H. Li, P. Bühlmann, and A. Munk, "Seeded binary segmentation: A general methodology for fast and optimal change point detection," *arXiv preprint arXiv:2002.06633*, 2020.

[15] R. Killick, P. Fearnhead, and I. A. Eckley, "Optimal detection of changepoints with a linear computational cost," *Journal of the American Statistical Association*, vol. 107, no. 500, pp. 1590–1598, 2012.

[16] C. Truong, L. Oudre, and N. Vayatis, "Selective review of offline change point detection methods," *Signal Processing*, vol. 167, p. 107299, 2020.

[17] A. Lahmadi, A. Duque, N. Heraief, and J. Francq, "MitM Attack Detection in BLE Networks using Reconstruction and Classification Machine Learning Techniques," in *2nd Workshop on Machine Learning for Cybersecurity (MLCS'20)*, 2020, pp. 1–16.

[18] B. Hills, "Machine in the Middle (MitM) BLE Attack," https://www.blackhillsinfosec.com/machine-in-the-middle-mitm-ble-attack/, 2020.

[19] A. Khamparia, R. H. Mondal, P. Podder, B. Bhushan, V. H. C. de Albuquerque, and S. Kumar, *Computational Intelligence for Managing Pandemics*. Walter de Gruyter GmbH & Co KG, 2021, vol. 5.