A Novel and Low Processing Time ECG Security Method Suitable for Sensor Node Platforms

Jusak Jusak [1], Seedahmed S. Mahmoud[2]

[1] Dept. of Computer Engineering, Institute of Business and Informatics Stikom Surabaya, Surabaya, Indonesia.
[2] Dept. Of Electrical and Electronis Technology, Riyadh Applied Engineering College, Riyadh, Kingdom of Saudi Arabic.

Abstract**:** An anonymisation of electrocardiogram (ECG) signal is essential during the distribution and storage in a public repository. In this paper, we introduce a novel low processing time ECG anonymisation method employing the fast Fourier transform (FFT) method. The proposed framework is suitable for sensor node platforms due to its low processing time. It was developed to address two major inherent limitations in the Internet of Medical Thing (IMedT) environment including most current requirement for securing ECG signal and urgent need for efficient methods to overcome physical limitation of sensor nodes. Ramifications from computer simulation showed that the proposed model was able to obscure both fiducial and non-fiducial features of the ECG signals. Performance evaluation between the original and the reconstructed ECG signals revealed strong cross-correlation implying lossless reconstruction of the original ECG signal. Furthermore, the proposed method achieved a lower processing time security algorithm as compared with the recently proposed wavelet based anonymisation methods. Finally, the proposed framework offered advantages in terms of flexibility in determining the secret key length makes it suitable for various applications.

Keywords**:** anonymisation, electrocardiogram, fast Fourier transform, internet of medical things, internet of things**.**

1. Introduction

Virtual Network Index (VNI) that was released by Cisco in June 2016 awakes imagination about how the Internet will be [1]. According to Cisco's paper, proliferation of global IP traffic and increment the number of devices connected to IP networks will contribute to the exchange of data that reach the order of Zettabyte (ZB) by 2020. Consequently, just about every physical object surrounding us (e.g. healthcare monitoring apparatus, machinery, appliances, autonomous cars and intelligent transportation, etc.) will be connected to the Internet forming the Internet of Things (IoT)[2,3]. In order to handle the countless number and various types of devices as well as linking the existing radio access technologies, a new architecture of the Fifth Generation (5G) networks is currently under consideration [4].

One of the most appealing applications in the era of IoT deployment is health and medical care areas. The IoT that integrating several numbers and various type of sensors together with smart medical devices may serve in, for example, tele-auscultation, medical consultation, remote health monitoring and analysis, remote diagnostics and online treatment as well as elderly care [5-7]. The so-called Internet of Medical Things (IMedT) is expected to reduce operational cost such as consultation and transportation cost. It is also crafted to shrink the gap between those who live in the isolated/remote areas and doctors in the urban areas. Nevertheless, due to small dimension of sensor nodes that construct the IoT and/or IMedT, the sensor nodes inherit particular constrains such as low processing power, limited space of memory and limited battery life. Hence, applications as well as signal processing algorithms that are embedded in the sensor nodes should consider these limitations carefully. For example, in a sensor node that is used for collecting electrocardiogram (ECG) data, selecting signal processing techniques before transmitting the ECG data will be quite a challenge. Complex algorithms will indeed provide high quality of ECG data; however, it will at the same time exhaust the memory and its battery life. Consequently, a low complexity ECG signal processing method is essential in the Internet of Medical Things (IMedT) application due to limited processing resources and capabilities of sensor nodes.

On the other hand, secure ECG signal transmission is highly required as ECG signal contains important health information of a patient. The ECG signal surprisingly inherits uniqueness for each individual over a long period of time [8]. Furthermore, some other works showed that the ECG signal can perform as a biometric identity that contains specific information that belongs to a particular person [9]. These important features of ECG signal make it vulnerable to spoof attack, especially in transmitting the signal from sensor nodes to health care providers via public networks. Based on these facts, hence, an Internet-based e-Health platform that overlooks protection to individual health information is a real threat to patients' privacy. Unfortunately, none of the existing e-Health platforms assign any anonymisation techniques to protect their ECG signal transmission.

An unsecure ECG signal without anonymisation schemes may be subjected to *man in the middle* attack. In the worst case, fraudsters can gain access to a secured service and use the spoofed recorded ECG data to expose private information about patients [10-12]. Fig. 1 presents a scenario of a man in the middle attack in a health information transmission system. The figure displays possible attack points where fraudsters may exploit vulnerability of the system that are including: (i) wireless link between sensor nodes and mobile devices that mostly used to collect health information data from wireless body area networks (WBAN), (ii) wire/wireless link between gateway and the edge router, (iii) wire/wireless link between the edge router and the health care provider router, and finally (iv) in the repository or data center in the health care provider. Therefore, a health care provider needs to comply with certain widely accepted standards in order to minimise such security threat to a system and to protect medical records safely. For example, US Government upheld the Health Insurance Portability and Accountability Act (HIPAA) in 1996 for assuring protection to medical privacy users [13], the European Union ratified the Directive on Data Protection in 1995 [14], the Health Information Privacy Code passed by New Zealand

Government in 1994 established specific rules for agencies in the health sector to ensure protection of individual privacy [15], and the Personally Controlled Electronic Health Record (PCEHR) eHealth system released by the Australian Government in 2012 [16].

In this paper, we introduce a novel ECG anonymisation framework that maintains low processing time attribute driven by the fast Fourier transform (FFT) algorithm. The proposed framework was proposed to address two major constraints in the IMedT environment, i.e., immediate need for securing ECG signal and efficient method for overcoming physical limitation of sensor nodes. We argue although secure transmission channel standards have been long existing in the market, force penetration to the data centre are still possible in many ways. Hence, anonymisation methods are expecting to complement the existing security standards. In contrast to the previous anonymisation techniques in [10, 17], which heavily employ the wavelet packet decomposition, FFT based ECG anonymisation is adopted and aimed to achieve a lower processing time security algorithm for obfuscating the ECG signal. Hence, major modifications of the existing algorithms had been done thoroughly, including: (i) substitution of the wavelet packet algorithm with the FFT algorithm, (ii) major modifications of anonymisation scheme owing the FFT algorithm features, (iii) modification of reversible function as shown in (6), and (iv) pushing out signal reconstruction phase that back-transform frequency domain into time-domain to public server in order to reduce computational complexity of the system. The proposed method is expected to offer minimum computational load that might be suitable for mobile and sensor node platforms [18,19] that form the IMedT system.

The structure of the paper is organised according to the following sections. The first section provides general overview of ECG security and its current problem. The last part of the first section emphasizes on the objectives of the paper and prominence of the proposed model in the IMedT environment. Related works will be described in the second section. The third section elaborates the proposed ECG anonymisation approach followed by results and discussions in the fourth section. Conclusions of the paper will be drawn in the last section of the paper.

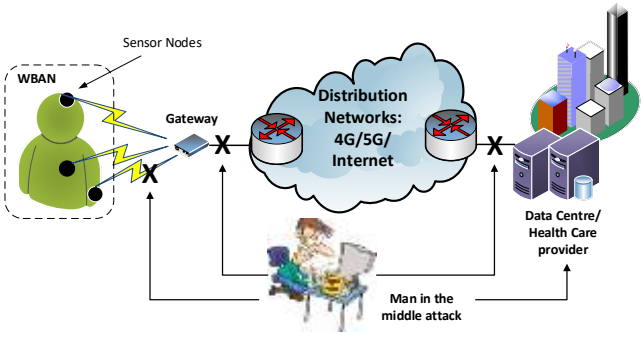

Figure 1. Possible attack points for unsecure ECG signals subjected to man in the middle attack.

2. Related Works

Several studies have been proposed to secure ECG signal by way of anonymisation. In this section, we firstly elaborate two ECG anonymisation approaches used for securing ECG signal transmission. The two algorithms took the advantage of the wavelet packet methods for efficient decomposition of the related ECG signal. The section then followed by an explanation of a light encoding-compression-encryption method focusing on low energy implementation on a mobile phone.

In [10], a wavelet packet-based ECG anonymisation method was proposed to firstly decompose the ECG signal. Subsequently, the low frequency components of the decomposed signal were replaced by zeros in order to distract the time domain structure of the ECG signal. Thirdly, all coefficients including the distracted coefficients and the higher frequency coefficients of the ECG signal were reconstructed for anonymisation. Because of removal of some coefficients in the frequency domain, the structure of the ECG signal becomes different from the original signal. In the distribution process, the distorted ECG signal was purposely transmitted over the networks in order to camouflage the original signal. On the other hand, the removed low frequency signal was sent to an authorised personnel as a secret key. On the receiver part, reconstruction process was done by combining the secret key and the distorted signal in order to recover the original signal. However, we argue that using this method the anonymised ECG signal does not fully conceal the fiducial features since the RR interval (related to heart rate variability, HRV) is present in the signal. Moreover, it was shown that the anonymised signal appeared to be similar to the original ECG signal. Therefore, using this proposed method the anonymised signal can be identified easily by malicious user and used for their purpose. On the other hand, the algorithm showed some advantages. The experiment showed that the size of the secret key attained 5.8% of the original ECG signal size. Secondly, in order to secure the secret key, the algorithm employed compression and encryption techniques before distribution of the secret key.

Algorithm performance of the previous work [10] was improved significantly by a slightly different approach that was introduced in [17]. In this paper a generalized wavelet packet method was utilised to decompose the ECG signal in several sub-bands encompassing low frequency components to high frequency components of the signal. Additionally, the proposed algorithm was equipped with a reversible function and/or operation. In this way, the proposed ECG anonymisation method proved to be able to conceal fiducial and non-fiducial features for both normal and abnormal ECG signals. The same as in [10], the algorithm removed the lower sub-band of ECG signal as a secret key and distributed separately to an authorized person in the medical centre, while the anonymised ECG signal was reconstructed to time domain, transmitted over public networks and stored in a medical database/server. At the receiver end, only an authorized personnel who had a secret key and knew the reversible function would be able to reconstruct the original ECG from the anonymised ECG. Performance of the proposed framework had been examined based on the cross-correlation analysis, power spectral density and percentage residual difference. The paper showed that the reconstructed ECG was highly correlated with the original ECG, which achieved a lossless reconstruction of the ECG data and proved the robustness of the proposed method. It was also found from the performance analysis results that the proposed anonymisation scheme provides high-security protection to ECG data and patient privacy.

In [11], a joint encoding, compression and encryption framework was proposed to secure the ECG transmission. The main idea of this work is to provide light processing power for transmission ECG signal from acquisition devices to mobile phones, and from mobile phones to a medical database. By employing the proposed encoding method, the ECG signal was not only successfully obscured, but also significantly reduced in terms of its file size. It was claimed that the compression ratio reached 3.84. Therefore, the proposed method potentially applies in the small devices such as IoT, which mostly inherits source power limitation. The works were able to increase the security strength by implementing the three phases encoding-compression-encryption schemes on the mobile phone. Using the proposed framework, the new algorithms achieved overall compression ratio up to 20.06 that were greatly expected to reduce the transmission burden over the public networks. A similar method but with different idea was introduced in [20] to secure the ECG signal transmission. In this work, a symmetric cryptography equipped with a lightweight block chipper was implemented in an embedded system aimed to form a secure and energy efficient wireless body area networks (WBAN). The examination results showed that the proposed system attained 0.054 mJ/block energy consumption. It can be interpreted that the system provide low energy consumption but secure transmission during both encryption and description phases.

3. A Proposed Real Time ECG Security Approach

In this part, we will explore the proposed real-time ECG security approach by, firstly providing a general overview of the IMedT system as important building blocks in the Fifth Generation (5G) communication networks. It is then followed by elaboration of the proposed real-time ECG security system and its reconstruction method.

3.1 A general framework of the IMedT system

Internet of Medical Things (IMedT) coordinates myriad of connected mobile medical devices to promote future health care services. Implementation of the IMedT system gives advantage for example for monitoring and tracking not only the state of patients' health but also the medication process and its direct effect to patients. In the health information management point of view, the IMedT could be used to assist logistics of medicine and healthcare apparatus and manage their entire value chain.

IMedT can be considered as an extension of the Internet of Things (IoT) concept. It is the IoT that is envisaged to change the 5G cellular networks perspective. In this context, there will be a shift paradigm from current connected people to connected things concept whereby millions of connected mobile phones and computers will be complemented by billions of devices and sensors yearn for the Internet connection. This increasing number of connected devices pushes direct consequence to the current cellular networks architecture. A number of femto and pico cells in a site that covers certain area with various radio access technologies needed to be linked appropriately to a multitier networks consisting of macrocells. Fig. 2 depicts an imaginary example of a heterogeneous network that connects a number of nodes with several medical sensors to a macrocell base station, a core network and the Internet, subsequently. This heterogeneous network will become one of the important features in the 5G communication networks [21-23]. A healthcare provider resides on the other side of the network.

In general, medical sensors may retrieve all vital sign signals such as body temperature, blood pressure, pulse rate, and respiration rate sensors. However, in this paper we only consider ECG signal due to some reasons. Firstly, ECG is the most commonly recorded signal in the patients monitoring and examination to perceive patient heart failure and cardiovascular disease (CVD) through the Heart Rate (HR) detection and RR Interval calculation. Secondly, ECG signal requires streaming data transmission from patients recorded devices to the healthcare provider, which imposes specific requirement similar to multimedia transmission, i.e. large number of transmitted data and hence, it requires wider bandwidth spectrum, smart storage management and more sophisticated signal processing algorithm to handle the data. Consequently, ECG signal processing involves more challenging methods to securely transmit over communication media.

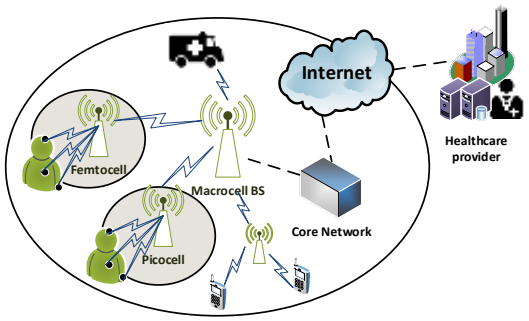

Figure 2. Illustration of multitier heterogeneous networks incorporating medical sensors in 5G communication networks.

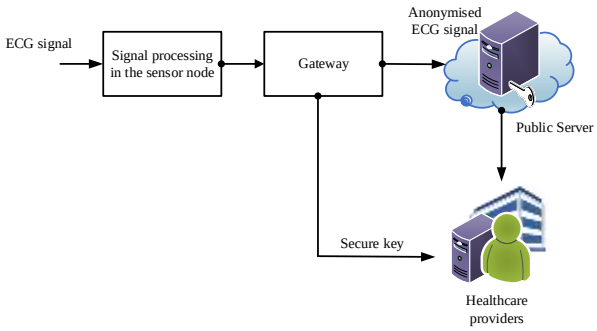

Figure 3. The proposed ECG anonymisation approach

In the IMedT system as shown in Fig. 2, security will be one of the most crucial issues needed to be tackled properly. In fact the security threat jeopardize not only to the ECG data encompassing the path from patients to doctors (resided in the healthcare provider), but also to online pathological reports and feedback traversing public networks from the doctors to the patients. Therefore, securing ECG data in the complete construction of the IMedT system is mandatory.

It is generally known that the IMedT preserves similar characteristics to the IoT system, i.e., low resources in terms of both computation and energy capacity. These limitations are mainly triggered by the small physical size of the sensor nodes that are expected to be attached on the human body comfortably. Consequently, design of the algorithm for

securing the ECG data should be performed by paying specific attention to this particular issue.

3.2. The proposed ECG anonymisation method

The ECG security framework (called as ECG anonymisation) proposed in this paper consist of the following several main processes, i.e. ECG signal transformation from time domain to frequency domain, frequency domain component partition, signal modification in the frequency domain which involves several sub-processes, and ECG signal reconstruction from frequency domain to time domain. Fig. 3 illustrates the ECG anonymisation process, while the detail algorithm in the form of pseudo-code is shown in Algorithm 1.

Step by step process of anonymising the ECG signal sequence is elaborated as follows:

Step 1. Let's assume the ECG signal sequence in the form $\{x[n]: n = 0 \cdots N-1\}$. Apply transformation of the ECG signal sequence using the Discrete Fourier Transform (DFT) to obtain frequency domain signal that is represented by $\{X[k]: k = 0 \cdots N-1\}$, where N is the length of the ECG signal sequence. The DFT of a finite-length ECG sequence of length N is defined by (1) as follows

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-j\left(\frac{2\pi kn}{N}\right)}, \quad k = 0,1,\cdots,N-1. \tag{1}$$

The inverse DFT is provided by the following equation

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k] e^{j\left(\frac{2\pi kn}{N}\right)}, \quad n = 0,1,\cdots,N-1. \tag{2}$$

Theoretically, there are many ways to compute the DFT rule in (1) and (2), however, in this work a FFT algorithm is employed to compute the DFT of an input ECG sequence, $x[n]$. Compared to other methods in calculating the DFT, the FFT produces incredibly more efficient and substantially low computational load algorithm. Given the advantage of the FFT as above, we argue that FFT is sufficient for processing signal in low power mobile devices such as those in sensor nodes. In the proposed method, the ECG sequence length, N is restricted to any positive power of two integer, for example 128, 256, 512, 1024, etc. Two reasons for confining the number for N in that form are: firstly, it is essential to keep the power of two signal length in the digital storage such as in the sensor nodes, and, secondly, it is required by the FFT algorithm to compute the DFT efficiently. Hence, by choosing the length of the ECG signal sequence as a power of two integer, we expect to achieve a near real-time, low power consumption and efficient signal processing for ECG signal anonymisation.

Step 2. Time domain transformation to the frequency domain as in Step 1 is then followed by frequency domain partitioning. The frequency domain partitioning phase is considered the most crucial part in the ECG anonymisation procedures. In this phase, we separate frequency domain signal, $X[k]$ into two sub-bands, i.e., $X_1[k]$ and $X_2[k]$. The first sub-band, $X_1[k]$ represents low frequency components of the signal, while the second one, $X_2[k]$ signifies high frequency components. Partition of the interested signal in frequency domain is shown in (3).

$$X[k] \equiv \left\{ \begin{array}{c} \underbrace{X_1[0 \cdots P]}, \underbrace{X_2[(P+1) \cdots Q]} \\ low-freq. \quad high-freq. \\ component \quad component \end{array} \right\} \tag{3}$$

where P is the expected secret key length and $Q = N-1$.

The length of $X[k]$ represented by Q in the in (3) is determined based on the following assumptions:

a) Variable Q is selected carefully to ensure that the ECG signal samples contain high frequency components up to 250Hz. This assumption is expected to assure all important features extracted from the ECG signal such as QRS complex, P wave and T wave remain unharmed [24,25].

b) The variables Q and P are suggested to obey relation in (4) as

$$0 \equiv Q(\text{mod } P), \tag{4}$$

where mod( ) is a modulus operation. Consequently, applying (4) in the algorithm will guarantee that Q is always positive natural number multiplication of P. Hence, a block of P components of the signal can be repeated to achieve exactly the same length as Q to allow correct modification in *Step 4*.

c) The length of Q is determined by considering algorithm efficiency in the reconstruction process i.e., from frequency domain to time domain of the ECG signal. Therefore, based on this reason, the length of Q should be set to any positive power of two integer.

Step 3. Separate the lowest frequency components of the ECG signal, $X_1[k]$ from $X[k]$ in (3) to obtain an unencrypted and uncompressed key, κ. The key is defined as

$$\kappa[k] = \{X_1[k]: k = 0,\cdots,P\}, \tag{5}$$

where P is the desired secret key length. In this step, removing $X_1[k]$ from $X[k]$ leaves $X_2[k]$ in the frequency domain of the signal sequence. The $X_2[k]$ holds detail information about the ECG signal as it contains high frequency components of the signal.

Step 4. Modify $X_2[k]$ component using a reversible function. We choose multiplication of the $X_2[k]$ component with $\Omega[k]$ defined in (7). Multiplication operation is taken in order to maintain the low complexity characteristics of the algorithm. Modification $X_2[k]$ component can be written mathematically as follows

$$\overline{X_2}[k] = \{X_2[k] * \Omega[k]: k = P+1,\cdots,Q\}. \tag{6}$$

Multiplication of $X_2[k]$ component with the $\Omega[k]$ is an element-wise multiplication, where vector $\Omega[k]$ is defined according to

$$\Omega[k] = \{\kappa[k] + \text{offset}: k = 0, \cdots, P\}, \quad (7)$$

with $\text{offset} = |\min(\kappa)| + \eta$. The element η defined as a constant value to prevent division by zero in the ECG reconstruction process. The $|.|$ represents an absolute operator. It should be clear that element-wise multiplication vector $X_2[k]$ by vector $\Omega[k]$ requires both of them to have the same size, accordingly the block vector $\Omega[k]$ should be repeated until it reaches the same size as $X_2[k]$. Hence, applying (4) in the algorithm as explained in *Step 2* will ensure that vector $X_2[k]$ and repetition of vector $\Omega[k]$ have same size.

Step 5. Establish a security key K and securely distributed the key to authorised healthcare providers. The security key is generated by compressing and encrypting the key, $\kappa[k]$ defined in (5) together with the $\Omega[k]$ represented by the following equation

$$K \leftarrow E(\Delta(\kappa, \Omega)), \quad (8)$$

where operator $\Delta(\ )$ signifies a compression operation and operator $E(\ )$ indicates an encryption operation.

Nonetheless, detail of compression and encryption algorithms is out of scope this paper. In the spirit of maintaining low complexity feature of the system, we suggest to adopt industrial standard that are currently available in the market. For instance, wireless transmission devices equipped with Bluetooth Low energy (BLE) technology has integrated 128-bit AES encryption in the Bluetooth Core Specification version 4.0. Alternatively, Wireless LAN networks that based on the IEEE 802.11i standard currently employ Wi-Fi Protected Access (WPA) security protocols.

Step 6. Upload the modified ECG signal, $\overline{X_2}[k]$ to a secure public server, such as cloud server as a healthcare data repository.

Step 7. Inside the public server, reconstruct the modified $\overline{X_2}[k]$ into time domain utilising the inverse FFT algorithm. The time domain representation, $\overline{x_2}[n]$ is the anonymised ECG signal that conceals part of the original ECG signal.

Algorithm 1 Proposed ECG anonymisation method

// Signal processing in a sensor node
1: Begin
2: $x[n] \leftarrow$ **ECG_signal**
3: Set value for P **and** Q
4: $X[k] \leftarrow$ **Fast Fourier Transform of** $x[n]$
// separate low frequency component
5: $X_1[k] \leftarrow X[0, \cdots, P]$
6: $\kappa \leftarrow X_1[k]$
// compression and encryption
7: $\text{offset} = |\min(\kappa)| + \eta$
8: $\Omega(k) \leftarrow \kappa[0, \cdots, P] + \text{offset}$
9: $K \leftarrow E(\Delta(\kappa, \Omega))$
10: Send K **to healthcare providers as a key**
// separate high frequency component
11: $X_2[k] \leftarrow X[P+1, \cdots, Q]$
// modify high frequency component
12: $\overline{X_2}[k] \leftarrow X_2[k] * \Omega[k]$
13: Upload $\overline{X_2}[k]$ **to public server**

// Signal processing in a public server
// this is the anonymised ECG signal
14: $\overline{x_2}[n] \leftarrow$ **inverse Fast Fourier Transform** $\overline{X_2}[k]$
15: Save $\overline{x_2}[n]$ **with unique ID for a particular individual**
16: End

3.3. The proposed ECG reconstruction method

Reconstruction method is applied to the anonymised ECG signal in order restore the original ECG signal. In our case for example in Fig. 3, an authorised medical personnel in the healthcare provider has to perform ECG reconstruction process in order to interpret the transmitted ECG signal. Without this reconstruction process, a medical personnel can only see noise-like signals. Based on the received information, which consists of the secure key, K, and the anonymised ECG signal, $\overline{x_2}[n]$, the ECG reconstruction method is explained in the following steps, while the detail of the algorithm in the form of pseudo-code is illustrated in Algorithm 2.

Step 1. Firstly, it is necessary to decrypt and decompress the secure key, K to obtain the vector Ω that is mathematically represented by

$$\Omega = \Lambda(D(K)), \quad (9)$$

where operator D and Λ denotes decryption and decompression operation, subsequently. However, the decryption and the decompression operations are beyond the scope of this paper.

Step 2. Transform the anonymised time domain ECG signal, $\overline{x_2}[n]$ in to the frequency domain employing the FFT algorithm to acquire $\overline{X_2}[k]$.

Step 3. Cancel the modification operation in (6) by dividing the vector $\Omega[k]$ into each element in the vector $\overline{X_2}[k]$. As a result, we get $X_2[k]$ as expressed in (10)

$$X_2(k) = \left\{ \frac{\overline{x_2}(k)}{\Omega(k)} : k = P+1, \cdots, Q \right\}, \quad (10)$$

and at the same time retrieve back the key, $\kappa[k]$ according to (11)

$$\kappa(k) = \{\Omega(k) - \text{offset}: k = 0, \cdots, P\}. \quad (11)$$

Step 4. The central part in this reconstruction algorithm is merging the vector $\kappa[k]$ as in (11) into the vector $X_2[k]$ as in (10). The result of this operation is the un-anonymised ECG signal $\tilde{X}[k]$.

Step 5. Convert $\tilde{X}[k]$ into the time domain utilising the inverse FFT algorithm to obtain the lossless ECG signal, $\tilde{x}[n]$. Hereinafter, the lossless ECG signal will be presented to the medical personnel for interpretation and further analysis.

Algorithm 2 Proposed ECG reconstruction method

// Signal processing in a medical personnel device
1: Begin
2: Retrieve the secure key K
// decompression and decryption of K
3: $\Omega \leftarrow \Lambda(D(K))$
4: Retrieve the anonymised ECG signal $\overline{x_2}[n]$ **from public server**
5: $\overline{X_2}[k] \leftarrow$ **Fast Fourier Transform of** $\overline{x_2}[n]$
6: $X_2[k] \leftarrow \overline{X_2}[P+1,\cdots,Q]/\Omega[k]$
7: $\kappa(k) \leftarrow \Omega(k) - \text{offset}$
8: $X_1[k] \leftarrow \kappa(k)$
// merge $X_1[k]$ ***into*** $X_2[k]$
9: $\tilde{X}[k] \leftarrow \left[X_1(0,\cdots,P), X_2[(P+1,\cdots,Q)]\right]$
// this is the reconstructed ECG signal
10: $\tilde{x}[n] \leftarrow$ **inverse Fast Fourier Transform** $\tilde{X}[k]$
11: End

4. Results and Discussions

In this section, we will show performance evaluation of the proposed ECG anonymisation by way of computer simulation. Observation will be emphasized on the ECG signal processing performance evaluation and processing time analysis. In the simulation, we apply two types of ECG signals which consist of normal ECG signals representing healthy subjects and abnormal ECG signals from a patient who suffered arrhythmia. All of the ECG signals in the simulation were retrieved from a publicly available PhysioNet database. The normal ECG signals were obtained from PTB [26] database and the abnormal signal was taken from MIT-BIH database [26].

In this section, performance evaluation based on fiducial and non-fiducial features of the ECG signals will be carried out. The fiducial features will be examined using time domain representation of the signal. On the other hand, the non-fiducial features will be evaluate utilising power spectral density (PSD) representation, cross-correlation of the original and reconstructed ECG signals, percentage residual difference (PRD) of the original and the anonymised ECG signals, and time processing of the proposed framework compared to the wavelet packet-based anonymisation approach [17].

The Percentage Residual Difference (PRD) between the original ECG signal and the anonymised ECG signal that will be used in the performance evaluation is represented by (12) [17]. The PRD is commonly used in many papers to measure the difference between the original ECG signal and the anonymised ECG signal, that is defined according to

$$\text{PRD} = \sqrt{\frac{\sum_{i=1}^{N}\left(x[i]-\overline{x_2}[i]\right)^2}{\sum_{i-1}^{N}x^2[i]}}, \qquad (12)$$

where $x[i]$ denotes the original ECG signal, $\overline{x_2}[i]$ is the anonymised ECG signal and $i = 1,\cdots,N$. N is the total number of samples in the ECG signal.

4.1 Performance evaluation over normal ECG signal

In the first part of performance evaluation for the proposed framework, a normal ECG signal for was taken from PTB database (i.e., patient245, signal s0474). It encompasses signal duration of 10 seconds. According to [26] the normal ECG signal from PTB database was retrieved using sampling frequency, $f_s = 1{,}000\,Hz$. Hence, in overall there were 10,000 points of normal ECG signal. However, there were only 8,192 $\left(2^{13}\right)$ points, which signifies ECG signal duration 8.192 seconds used in the experiment in order to preserve efficient computation of the FFT and the inverse FFT algorithms.

The ECG signal was transformed using FFT algorithm followed by partition of the ECG signal in frequency domain into low and high frequencies. The low frequency acted as a secret key, κ. The length of the secret key was set to $P = 1{,}024$, which is related to frequency 125 Hz. Therefore, frequency components of the ECG signal between 0 and 125 Hz were removed for the secret key. On the other hand, frequency components larger than 125 Hz were operated as ECG anonymisation that will be uploaded to a public server/cloud server after reconstructing it using inverse FFT. In the ECG anonymisation phase, the ECG signal was modified using a constant $\eta = 0.01$.

Time domain representation of normal ECG signal (i.e., patient245, signal s0474) and the anonymised ECG signal are shown in Fig. 4. (a) and (b), respectively. It is clear from Fig. 4 (b) that the proposed ECG anonymisation framework successfully conceals all fiducial features of the original ECG signal in Fig. 4 (a). Frequency domain representation in terms of Welch's power spectral density (PSD) estimation for both the original ECG signal and the anonymised ECG signal are shown in Fig. 5 (a) and (b), respectively. Both diagrams show horizontal axis that has frequency range from DC to one-half the sampling rate. It can be seen in Fig. 5 (b) that the non-fiducial features of the ECG signal have been obscured utterly by anonymisation process of the proposed algorithm.

Examination to both Fig. 4 (a) and (b), as well as Fig. 5 (a) and (b) concludes that the ECG signal of a subject cannot be interpreted by using the anonymised data solely. For example, a man in the middle attack that possibly has access to acquire the anonymised ECG signal can do nothing to decrypt the ECG signal without possessing the key.

One advantage of using the proposed algorithm compared to the previous algorithm, for example in [17], is that its flexibility to choose the secret key length. Fig. 6 (b) depicts the Welch's power spectral density of the anonymised ECG signal with a shorter key length, i.e., $P = 512$ than the one in Fig. 6. A key length $P = 512$ is related to frequency 62.5 Hz. Hence, in Fig. 6 (b) frequency components of the ECG signal between 0 and 125 Hz were removed for the secret key and frequency components larger than 125 Hz were preserved as anonymised ECG. The figure shows that the non-fiducial features of the ECG signal are perfectly concealed by the proposed algorithm utilising a shorter key length.

Fig. 7 (a) illustrates the reconstructed ECG signal after merging vector of the secret key, κ, and vector of the anonymised ECG signal at the medical personnel side. Observe Algorithm 2 for the reconstruction process of the original ECG signal. Comparing Fig. 7 (a) and Fig 4 (a) clearly shows that both figures are identical with high degree of correlation. Moreover, cross-correlation of the original ECG signal and the reconstructed ECG signal that is presented in Fig. 7 (b) reveals that both ECG signals are highly correlated. This strong cross-correlation indicates close similarity between the original and reconstructed ECG signals.

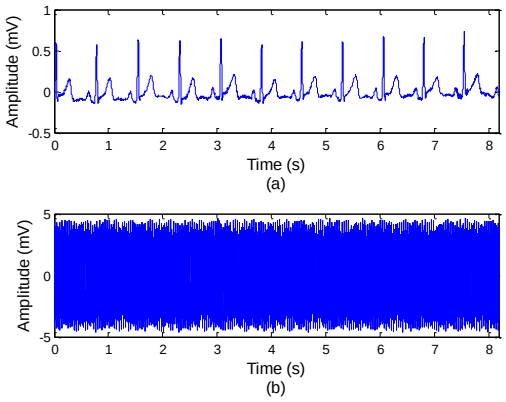

Figure 4. Time domain representation of normal ECG signal: (a) original ECG signal, (b) anonymised ECG signal for $P = 1{,}024$.

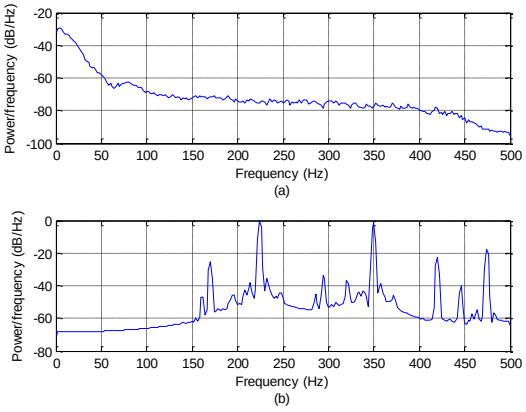

Figure 5. Power spectral density representation of normal ECG signal: (a) original ECG signal, (b) anonymised ECG signal for $P = 1{,}024$.

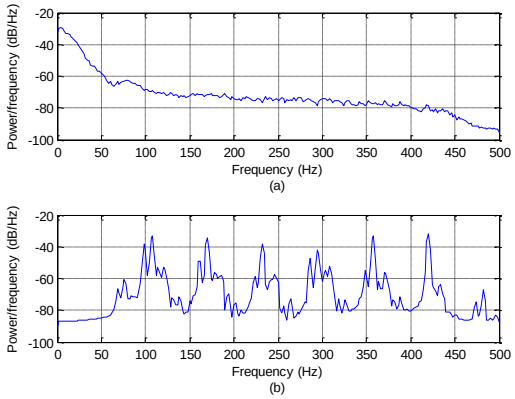

Figure 6. Power spectral density representation of normal ECG signal: (a) original ECG signal, (b) anonymised ECG signal for $P = 512$.

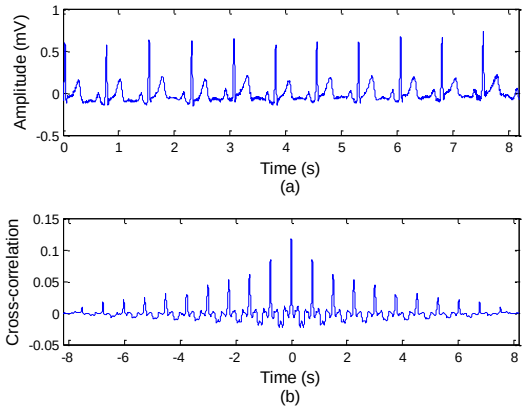

Figure 7. (a) Time domain representation of reconstructed ECG signal, (b) cross correlation between original normal ECG signal and the reconstructed ECG signal.

Furthermore, performance evaluation of the PRD as shown in (12) for the secret key length $P = 1{,}024$ gives $\mathrm{PRD} = 18.76\%$, which shows there is significant different between the original ECG signal and the anonymised ECG signal.

4.2 Performance evaluation over abnormal ECG signal

In the second study, an abnormal ECG signal was taken from MIT-BIH arrhythmia database (i.e., signal 105m) with 10 seconds signal duration. An arrhythmia syndrome reveals an abnormal heart beat pattern. This is mainly caused by problems in the heart's electrical system. This abnormality is commonly classified into two basic patterns, i.e., slower electrical impulses than normal ECG signal called bradycardia (heart rate is less than 60 beats per minute) and faster electrical impulses than normal ECG signal called tachycardia (heart rate is more than 100 beats per minute)[27, 28]. The abnormal tachycardia syndrome ECG signal was taken using sampling frequency, $f_s = 360Hz$. There were 3,600 points of the abnormal ECG signal, however, there were only 2,048 $\left(2^{11}\right)$ points, which signifies ECG signal duration 5.7 seconds used in the experiment to maintain efficient computation of the FFT and the inverse FFT algorithms.

The length of the secret key was set to $P = 256$, which is related to frequency 45 Hz. Therefore, frequency components

of the ECG signal between 0 and 45 Hz were removed for the secret key, κ, and frequency components larger than 45 Hz were used for ECG anonymisation. The ECG signal was modified using a constant value, $\eta = 0.01$.

Fig. 8 (a) and (b) depicts the original abnormal ECG signal for a subject that suffered from a tachycardia syndrome (i.e., signal 105m) and the anonymised abnormal ECG signal, respectively. The figures show that all fiducial features of the ECG signal can be completely concealed by the proposed algorithm. On the other hand, performance evaluation in terms of non-fiducial features of the ECG is illustrated in Fig. 9 (a) and (b). The figures reveal that Welch's power spectral density of original abnormal ECG signal and the anonymised signal are clearly dissimilar. In other words, the proposed algorithm had successfully hidden the original ECG signal details from the eavesdroppers.

Additionally, Fig. 10 (a) shows that the proposed reconstruction algorithm had been able to retrieve back the original abnormal ECG signal. Examination on the cross-correlation between the original abnormal ECG signal and the reconstructed abnormal ECG signal verifies that both ECG signals are highly correlated as seen in Fig. 10 (b).

Examination based on the PRD shows that residual difference between the original abnormal ECG signal and the anonymised signal results in $\mathrm{PRD} = 1.33\%$ for secret key length $P = 256$. Comparison between PRDs of the normal ECG signal with $f_s = 1{,}000\,Hz$ and the abnormal ECG signal with $f_s = 360\,Hz$ confirm the previous result in [17] that the PRD values depend on the sampling frequency.

4.3 Performance evaluation over algorithm processing time

An algorithm with low processing time is ultimately important to conserve energy in mobile and sensor node platforms. Consequently, one criterion in mind in designing an ECG anonymisation algorithm is that the running algorithm embedded in the devices should preserve low computational of the overall IMedT system. In this sub-section, ECG anonymisation processing time of the proposed algorithm for different values of secret key length is examined as opposed to the wavelet packet-based anonymisation technique in [17].

ECG anonymisation processing time as a function of ECG signal length, Q, is shown in Fig. 11. A normal ECG signal (i.e., patient245, signal s0474) taken from PTB database with sampling frequency $f_s = 1{,}000\,Hz$ was used for evaluation, The signal covers 2 (two) minutes duration. However, in order to provide efficient calculation of the FFT in the proposed algorithm, a power of two integer ECG signal length was chosen for each simulation. In this simulation, ECG signal lengths, Qs, were set to $2^{12} = 4{,}096$ points up to $2^{16} = 65{,}536$ points signifying time duration between 4,096 seconds and 65,536 seconds. The processing time computation for each data point in Fig. 11 was run over 100 simulations.

It can be seen in Fig. 11 that ECG anonymisation processing time produced by our proposed algorithm for several values secret key lengths outperforms the preceding wavelet packet-based algorithm. The figure shows that the proposed framework is approximately 5 times faster than the wavelet packet based. For instance, the proposed framework took only approximately 6 milliseconds to anonymise the ECG signal for signal length $Q = 2^{14} = 16{,}384$ points. On the contrary, the existing wavelet packet based algorithm spent longer processing time, which is approximately 33 milliseconds.

Fig. 11 also reveals that the processing time of the proposed framework is comparable for several runs of anonymisation processes with variations of the secret key length. Therefore, it can be interpreted that the proposed framework offers flexibility for the applications to designate the secret key length in the ECG anonymisation and reconstruction processes. Comparing to the previous wavelet packet-based approach, the preceding algorithm can only provide the key size that was regulated by a factor of $\frac{N}{2^j}$, where N represents the ECG signal length and j is the decomposition level.

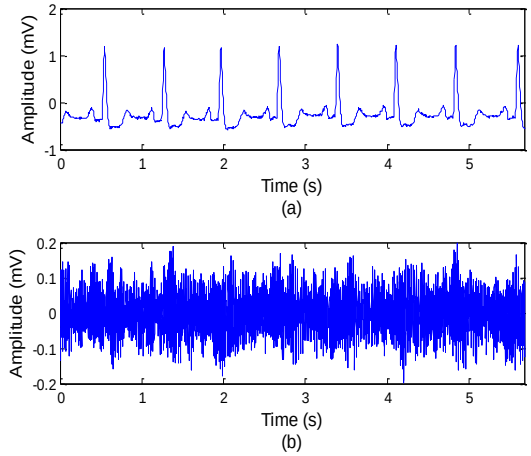

Figure 8. Time domain representation of abnormal ECG signal – tachycardia: (a) original ECG signal, (b) anonymised ECG signal for $P = 256$.

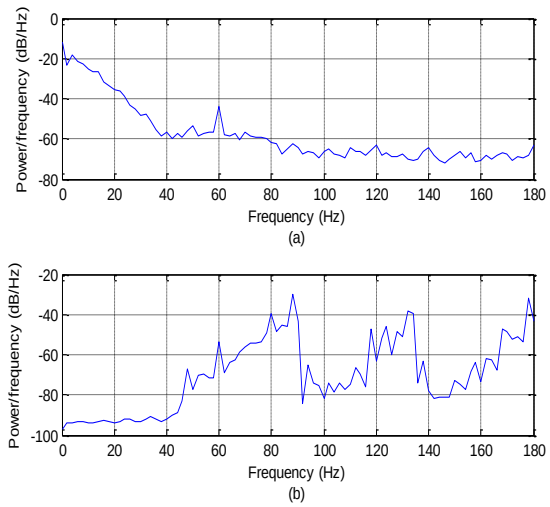

Figure 9. Power spectral density representation of abnormal ECG signal – tachycardia: (a) original ECG signal, (b) anonymised ECG signal for $P = 256$.

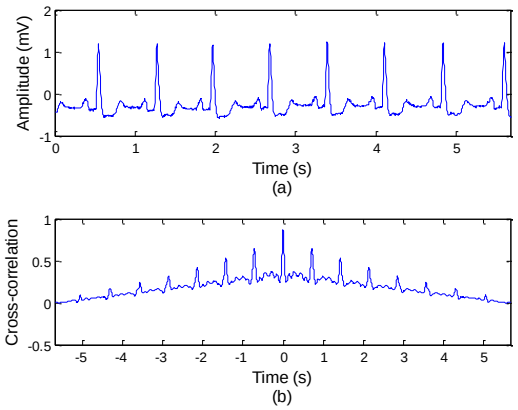

Figure 10. (a) Time domain representation of reconstructed ECG signal, (b) cross correlation between original abnormal ECG signal and the reconstructed ECG signal.

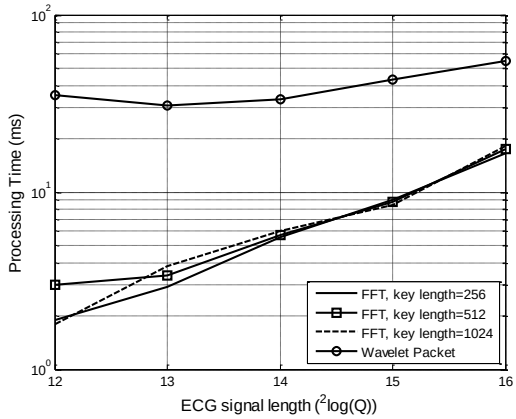

Figure 11. Processing time of ECG signal anonymisation using the proposed algorithm for different key lengths compared to the wavelet packet anonymisation technique.

5. Conclusions

Applications of the IoT in health and medical care areas are envisioned to be the one that can fully benefit from the IoT deployment. Henceforth, the term of Internet of Medical Things (IMedT) is commonly referred to such emerging technology. Nevertheless, due to small dimension of medical sensor nodes that construct the IMedT, the sensor nodes hold physical limitation in terms of low processing power, space of memory and battery life. Furthermore, transmitting ECG signal from sensor nodes to health care provider through public networks requires rigid security frameworks to protect patient's privacy. In this paper, a novel ECG anonymisation and reconstruction model have been proposed to address two major constraints in the IMedT environment, i.e., firstly, to accommodate the most current need for securing ECG signal transmission and secondly, to create an efficient method for overcoming power source limitation of sensor nodes.

Performance evaluation examined using computer simulation over normal and abnormal ECG signals concluded the following results: (i) the proposed framework has ability to conceal both fiducial and non-fiducial features of the ECG signals in the anonymisation phase and correctly retrieved the original signal after successful reconstruction process, (ii) evaluation based on PRD showed that there is significant different between the original ECG signal and the anonymised ECG signal, (iii) on the contrary, strong cross-correlation indicated close similarity between the original and the reconstructed ECG signals implying the proposed algorithm achieves lossless reconstruction of the original ECG signal, (iv) examination over processing time showed that the proposed algorithm consumed lower processing time compared to the existing wavelet packet-based algorithm, (v) finally, processing time of the proposed framework is comparable for several simulations with variations of the secret key lengths that makes it suitable for various applications.

References

[1] Cisco VNI, "The zettabyte era: trends and analysis," Cisco and/or its affiliate, June 2017. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html. Accessed on 21 July 2017.

[2] L. Atzori, A. Iera, and G. Morabito, "Internet of Things: a survey," Computer Networks, Vol. 54, No. 15, pp. 2787-2805, Oct. 2010.

[3] A.U. Rehman, S.U. Rehman, I.K. Khan, M. Moiz, and S. Hasan, "Security and privacy issues in IoT," International Journal of Communication Networks and Information Security, Vol. 8, No. 3. pp. 147-157, Dec. 2016.

[4] J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, and A.C.K. Soong, J.C. Zhang, "What will 5G be?," IEEE Journal of Selected Areas in Communications, Vol. 32, No. 6, pp. 1065-1082, June. 2014.

[5] S.M.R. Islam, D. Kwak, M.D.H. Kabir, M. Hossain, K.S. Kwak, "Internet of Things for health care: a comprehensive survey," *IEEE Access*, Vol. 3, pp. 678-708, Jun. 2015.

[6] J. Jusak and I. Puspasari, "Wireless tele-auscultation for phonocardiograph signal recording through the zigbee networks," IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob), Bandung, Indonesia, pp. 95-100, 27-29 Aug. 2015.

[7] J. Jusak, H. Pratikno, and V.H. Putra, "Internet of Medical Things for cardiac monitoring: paving the way to 5G mobile networks," IEEE Int. Conference on Communication, Networks and Satellite (COMNETSAT 2016), Surabaya, Indonesia, pp. 75-79, Dec. 2016.

[8] L. Biel, O. Petersson, L. Philipson, and P. Wide, "ECG analysis: a new approach in human identification," IEEE Transactions on Instrumentation and Measurement, Vol. 50, No. 3, pp. 808–812, Jun. 2001.

[9] I. Odinaka, P. Lai, A.D. Kaplan, J.A. O'Sullivan, E.J. Sirevaag, J.W. Rohrbaugh, "ECG biometric recognition: a comparative analysis," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, pp. 1812–1824, Aug. 2012.

[10] F. Sufi, S.S. Mahmoud, and I. Khalil, "A novel wavelet packet-based anti-spoofing technique to secure ECG data," International Journal of Biometrics, Vol.1, No. 2, pp. 191–208, Aug. 2008.

[11] F. Sufi and I. Khalil, "Enforcing secured ECG transmission for realtime monitoring: a joint encoding, compression and encryption mechanism," Security and Communication Networks, Vol. 1, No. 5, pp. 389-405, Oct. 2008.

[12] T. Oluvan, C.E.A. Chambell, S. Hole, K. Radhakrishnan, and A. Sedigh, "Mitigating external threats in wireless local area networks," International Journal of Communication Networks and Information Security, Vol. 6, No. 3. pp. 200-216, Dec. 2014.

[13] Department of Health & Human Services USA, "Security 101 for covered entities HIPAA Security Series (2)," Department of Health & Human Services, USA, pp. 1-11, 2007.

[14] European Parliament and of the Council, "Directive 95/46/EC of the European Parliament and of the Council: on the protection of individuals with regards to the processing of personal data and on the free movement of such data," Official Journal of European Communities (1), No. 281, pp. 31-50, Oct. 1995.

[15] Privacy Commisioner, *Health information privacy code 1994 Ed. 2008*, Auckland, New Zealand: KB Printed Ltd., 2008.

[16] C. Pearce and M. Bainbridge, "A personally controlled electronic health record for Australia," Journal of the American Medical Informatics Association, Vol. 21, No. 4, pp. 707-713, Mar. 2014.

[17] S.S. Mahmmoud, "A generalized wavelet packet-based anonymisation approach for ECG security application," Security and Communication Networks, Vol. 9, No. 18, pp. 6137-6147, Dec. 2016.

[18] F. Hu, S. Lakdawala, Q. Hao, and M. Qiu, "Low-power, intelligent sensor hardware interface for medical data pre-processing," IEEE Transactions on Information Technology in Biomedicine, Vol. 13, No. 4, pp. 656-663, May 2009.

[19] A. Sa-ngasoongsong, J. Kunthong, V. Sarangan, X. Cai, and S.T.S. Bukkapatnam, "A low-cost, portable, high-throughput wireless sensor system for phonocardiography applications," Sensors, Vol. 12, No. 8, pp. 10851-10870, Aug. 2012.

[20] T. Narmadha, M. Kalaiarasi, and M. Meenakshi, "Lightweight secure ECG transmission in wireless body area networks – PRESENT chipper based implementation," International Conference on Communications and Signal Processing, pp. 1066-1070, India, Apr. 2017.

[21] N. Bhushan et al., "Network densification: the dominant theme for wireless evolution into 5G," IEEE Communications Magazine, Vol. 52, No. 2, pp. 82-89, Feb. 2014.

[22] E. Hossain and M. Hasan, "5G Cellular: key enabling technologies and research challenges," IEEE Instrumentation and Measurement Magazine, Vol. 18, No. 3, pp. 11-21, May 2015.

[23] I.F. Akyildiz et al., "5G roadmap: 10 keys enabling technologies," Computer Networks, Vol. 106, pp. 17-48, Sept. 2016.

[24] V.K. Murthy and T.M. Grove, "Clinical usefulness of ECG frequency spectrum analysis," Annual Symposium on Computer Applications in Medical Care, 9 Nov. 1978.

[25] L. Sornmo and P. Laguna, "Electrocardiogram (ECG) signal processing," in Wiley Encyclopedia of Biomedical Engineering, John Wiley & Sons, Inc., 2006.

[26] The PTB Diagnostic ECG Database (Physionet). [Online]. Available: http://www.physionet.org/ physiobank/database/ptbdb. Accessed June 2017.

[27] MIT-BIH Arrhythmia Database (Physionet). [Online]. Available: http://physionet.org/ physiobank/database/svdb. Accessed June 2017.

[28] B.M. Kaplan, R. Langendorf, M. Lev and A. Pick, "Tachycardia-bradycardia syndrome (so-called: sick sinus syndrome): pathology, mechanisms and treatment," American Journal of Cardiology, Vol. 31, pp. 497-508, Apr. 1973.