Volume 7, Issue 4
August 2018

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

An ECG based secure authentication in wireless body area networks

[1] Abhishek Tiwari, and [2] Durgesh Tripathi

[1,] Research Scholar, Kanpur institute of Technology, Kanpur, Uttar Pradesh, INDIA
[2] Department of Computer Science and Engineering, Kanpur institute of Technology, Kanpur, Uttar Pradesh, INDIA

E-mail: abtics90@gmail.com

ABSTRACT

In the present era, Body area sensor networks (BANs) acts as an effective technology due to its unbeatable features like simple usage, safe, and application in health sector. These are used in number of ways such as in tracking the fitness trackers, in crucial following of emergency response teams, and in the medical implantable devices like heart pacemakers and insulin pumps. These kinds of medical and safety related applications of BAN require a decent class of controlling of access to them and proper and secured data. In this work, we used ECG data as a physiological feature. ECG shows the electrical heart movement and this feature is unique for the particular person at a certain moment. In the preset work, it is shown that both ECG and its beat pattern can be used for online patient identification. Further, poincare plots are drawn for beat pattern and it is shown that using fitted ellipse patient health can be monitored.

Keywords: *ECG, BAN, Poincare*

1. INTRODUCTION

If we look in the recent past years, we will feel that the use of Wireless Sensor Network (WSN) technology has increased quickly. Among a number of applications, an important one is in wireless biomedical sensor network for collecting physiological signals. We can define the Wireless Body Area Network (WBAN) as a wireless network useful for making communication among operating sensor nodes on, in or around the body of an individual with the end purpose to evaluate the important body measurements and functions [1-4]. The above mentioned monitoring signals are after this collected by a personal device, such as PDA or smart phone that works as a data sink for the sensor nodes and transfers them to the specialist for further monitoring,

The development of WBAN is imperative in current scenario of telemedicine and m-health, however the problem of secured data is the problem which is still to be settled. Due to the fact that we expect that nodes of WBAN to be interconnect, a secure communication pathway could be developed by the body that is inaccessible to every single other sort of wireless networks [5-10]. We practically think that in the case of using in a proper way, the framework can normally secure the data transmission within WBAN, where different strategies utilize hardware and software to accomplish a similar reason. At the end of the day, the biometric information gathered from the person can uniquely denote a person, which is not easy to be misused for illegal purpose.

To distinguish data of individual patients EGC based authentication/verification is used. In previous studies it has been found that ECG caries distinctive features and most importantly they are unique in each person [11-12].

In this work we use statistics of the ECG to identify patient. First of all we use complete ECG pattern which is different of each patient, secondly detection of R-R peaks and calculation of heart beat, maximum and minimum heat beat, mean and variance of heart beat, and its pattern is done. We found that these parameters are good enough to distinguish patients, finally encryption of this information is done using cover image, and ECG data can itself embedded on vacant space on ECG image.

2. ECG PEAK DETECTION

The procedural steps for heart beat detection are:

Read ECG data from dat file. Defining ECG signal as $x[n]$

To suppress noise and Q, R, S, and T waves ECG signal pass through a 'high pass' filter with impulse response as $h[n]$, then the output of the filter is $y[n]$ which is defined as $y[n]=h[n]*x[n]$.

To further suppress the un-wanted terms we do $z[n]=(y[n])^m$

Finally, inter-arrival time between consecutive R-R peaks is evacuated, and heart rate is calculated.

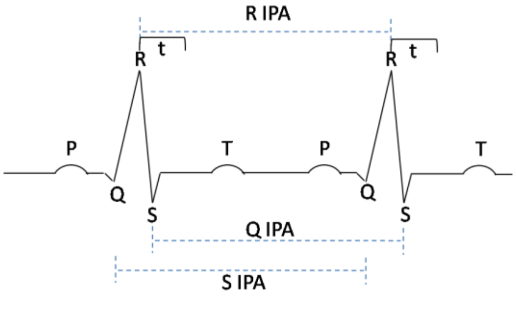

Figure 1: Typical ECG plot

Signal $x(n)$, which in this case is a pure ECG signal. However, the signal that we obtain, $y(n)$, is not a pure ECG signal; it is an ECG signal corrupted with a noise signal, $w(n)$. . In other words, $y(n)= x(n)+ w(n)$, and we are interested in filtering out $w(n)$.

For the purposes of this problem, we consider $w(n) = A\cos(\Omega n)$ for several reasons: this noise signal simulates the actual problem well, and is a real-valued signal

[10]. Now, we know that the cosine function contains two frequencies ±Ω and in order to remove the error signal from y(n), we need to notch out these frequencies. Thus, a notch filter will satisfy the requirements of this problem. Let us flesh out this notch filter, which we will call N.

1. In order to notch out two frequencies, we should consider each frequency separately and notch it out separately. With this in mind, generate the necessary frequency response, N(ω), for the filter N. It should have the form

$$N(\omega)=\frac{(e^{j\omega}-z_1)(e^{j\omega}-z_2)}{(e^{j\omega}-p_1)(e^{j\omega}-p_2)} \qquad (1)$$

Notch filters can be used to remove certain frequency components which are un-desirable by placing zeros at those locations. The radius of the zeros should be equal to unity, while angle of zeros should be at $\Omega_0=\pm\frac{f_0}{f_s}(2\pi)$.

$z_1=e^{j\Omega_0}$ and $z_2=e^{-j\Omega_0}$

$$\Omega_0=2\pi\frac{f_0}{f_s}$$

$$H[z]=\frac{(z-z_1)(z-z_2)}{z^2} \qquad (2)$$

In our case f_s=200 Hz, and f_0=60 Hz, therefore

$$H_N[z]=\frac{z^2-0.618z+1}{z^2} \qquad (3)$$

3. POINCARÉ PLOT

A Poincaré plot, named after Henri Poincaré, is a species of recurrence plot used to quantify self-similarity in processes, usually periodic functions. It is also known as a return map. Poincaré plots can be used to distinguish chaos from randomness by embedding a data set into a higher-dimensional state space [12].

Given a time series of the form x_t, $x_{t+1,}$ x_{t+2} and so on...

a return map in its simplest form first plots (x_t, x_{t+1}), then plots (x_{t+1}, x_{t+2}), then (x_{t+2}, x_{t+3}), and so on.

Applications in electrocardiography

An electrocardiogram (ECG) is a tracing of the voltage changes in the chest generated by the heart, whose contraction in the normal person is triggered by an electrical impulse that originates the sinoatrial node. The ECG normally consists of a series of waves, labeled the P, Q, R, S and T waves. The P wave represents depolarization of the atria, Q-R-S series of waves the depolarization of the ventricles, and T wave the repolarization of the ventricles. The interval between two successive R waves (the RR interval) is a measure of the heart rate. The heart rate normally varies slightly: during a deep breath, it speeds up and during a deep exhalation, it slows down. (The RR interval will shorten when the heart speeds up, and lengthen when it slows.) An RR tachograph is a graph of the numerical value of the RR-interval versus time.

In the context of RR tachography, a Poincaré plot is a graph of RR(*n*) on the *x*-axis versus RR(*n* + 1) (the succeeding RR interval) on the *y*-axis, i.e. one takes a sequence of intervals and plots each interval against the following interval. The recurrence plot is used as a standard visualizing technique to detect the presence of oscillations in non-linear dynamic systems. In the context of electrocardiography, the rate of the healthy heart is normally tightly controlled by the body's regulatory mechanisms (specifically, by the autonomic nervous system).

In Poincare plot more scattering of data represents the good health.

However, scattering along y=x line is comparatively healthier than in any other direction.

Ellipse Generation

The given equation, x^2 / a^2 + y^2 / b^2 = 1, which is the standard equation for an ellipse, is used to represent an ellipse which is centered at the origin. The axes of the ellipse represented by this equation lies along the coordinate axes. For a majority of cases, an ellipse may be centered at any point, or we may have unparallel axes to the coordinate axes. However, this kind of ellipse can simply be acquired by beginning with one in the standard position, and with the application of a rotation and/or a translation. We can include rotations for normal formulation with an angle of 0 (in other words, without any rotation) and translations by the zero vector (without any translation). At that point, we can get each ellipse by making the translation and rotation of an ellipse in the standard position. In this way, the equation could be derived for any ellipse with the application of rotations and translations to the standard equation of an ellipse.

Rotation counter clockwise about the origin through an angle *α* carries (*x*, *y*) to (*x* cos *α* − *y*sin *α*, *y*cos*α* + *x* sin *α*) .

The equations for a rotation counter-clockwise through an angle *α* can be derived as follows. Express the starting point, (*x*, *y*) in polar coordinates as (*r* cos *θ*, *r* sin *θ*). Now rotating by *α* simply adds that angle to the polar coordinate *θ*, while leaving *r* unchanged. Therefore, the rotated point will be (*u*, *v*), given in polar coordinates by (*r* cos (*θ* + *α*), *r* sin (*θ* + *α*)). To relate these to the original variables, expand the sine and cosine terms using trigonometric identities. Then we will have

$(u, v) = (r\,(\cos\theta\cos\alpha - \sin\theta\sin\alpha),\ r\,(\sin\theta\cos\alpha + \cos\theta\sin\alpha))$

$= (r\cos\theta\cos\alpha - r\sin\theta\sin\alpha,\ r\sin\theta\cos\alpha + r\cos\theta\sin\alpha)$

$= (x\cos\alpha - y\sin\alpha,\ y\cos\alpha + x\sin\alpha)$ (4)

This shows that the equations for *u* and *v* are given by

$u = (\cos\alpha)\,x - (\sin\alpha)\,y$

$v = (\sin\alpha)\,x + (\cos\alpha)\,y.$

These equations are expressed using matrix notation in the following form:

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \qquad (5)$$

We can obtain the inverse operation by rotating through 2π − *α*, and therefore carries (*x*, *y*) to (*x* cos *α* + *y* sin *α*, *y* cos *α* − *x* sin *α*). With the application of the methods of Equation of a Transformed Ellipse now results to the given equation for a standard ellipse which has been rotated through an angle *α*.

$$\frac{\left(x\cos\alpha + y\sin\alpha\right)^2}{a^2} + \frac{\left(x\sin\alpha - y\cos\alpha\right)^2}{b^2} = 1 \qquad (6)$$

Expanding the binomial squares and collecting like terms gives

$$\left(\frac{\cos^2\alpha}{a^2} + \frac{\sin^2\alpha}{b^2}\right)x^2 + 2\cos\alpha\sin\alpha\left(\frac{1}{a^2} - \frac{1}{b^2}\right)xy + \left(\frac{\sin^2\alpha}{a^2} + \frac{\cos^2\alpha}{b^2}\right)y^2 = 1 \qquad (7)$$

As we can see, the above equation is in the form of $Ax^2 + Bxy + Cy^2 = 1$, and the coefficient of the variable *A* and *C* are positive. So, we can conclude that we have a quadratic equation for a rotated ellipse, centered at the origin with a nonzero *xy* term

4. RESULTS

In Figure 2 and 3, both raw and filtered ECG signals are shown for two different ECG signals. On x axis arbitrary time scale is shown, and on y axis amplitude is also shown, again the value of amplitude may differ in different ECGs due to the calibration of different ECG capturing devices. However, depending on requirements value can be re-scaled to different set of values. In this figure, raw ECG is shown; it only contains the noise added during capturing process of ECG signals. The original and filtered ECG signals are well agreement to each other.

In figure 4, both raw ECG and noise free ECG are shown. Here, considered SNR is 10, here slight variation is observed in original and recovered ECG signals. Still they are in well agreement with each other. For clear visualization in Figure 4 single ECG pulse with all the necessary patterns is shown. In this figure two observation can be made easily, first is that the filtered signal is slightly shifted towards left and peak value of R wave reduced, but is not a problem as R wave s the longest peak and can be detected very easily in spite of reduced peak value.

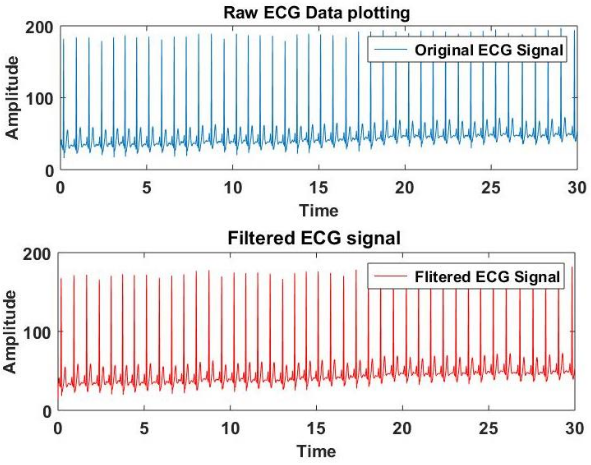

Figure 2: ECG characteristic and types of peaks

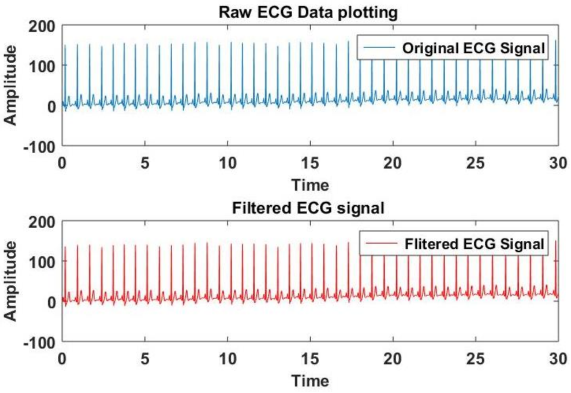

Figure 3: ECG characteristic and types of peaks

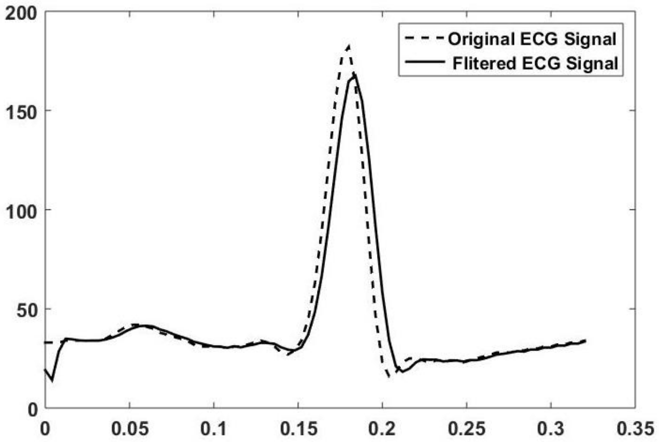

Figure 4: Original and filtered ECG signals (SNR=10)

In the next set of experiment, for ECG signal heart beat pattern is obtained. In the figure base wanderer is seen, and this has to be removed to obtain settled peak. The wanderer removed ECG signal is shown in Figure 5, along with detected peak values.

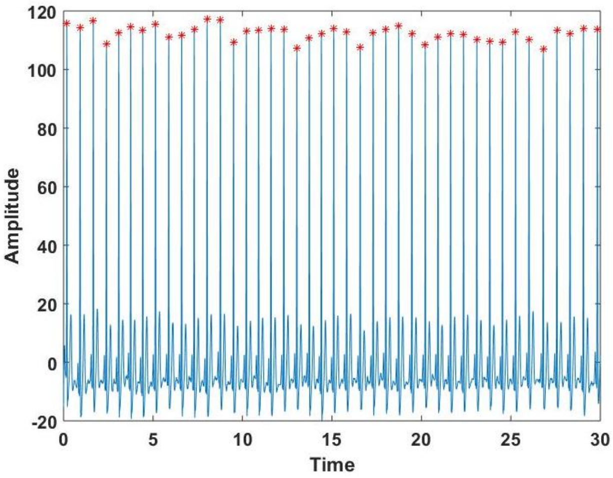

Figure 5: Peak detected ECG signal

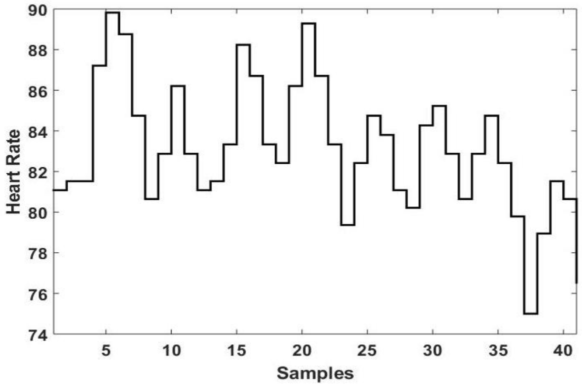

Figure 6: Beat pattern for sample ECG 1

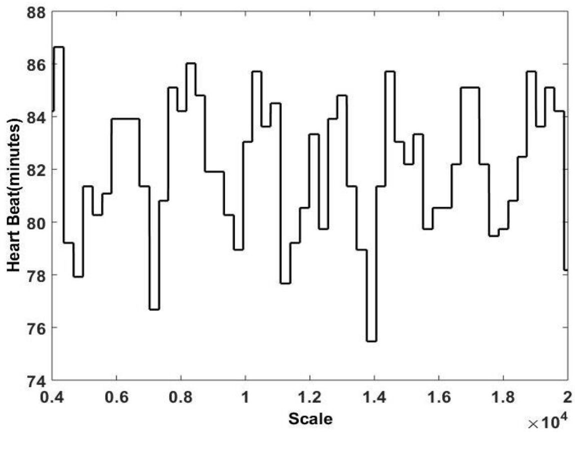

Figure 7: Beat pattern for sample ECG 2

The obtained beats per minute for various sample sizes are shown in Figure 6. The sample sizes are in 1000 scale. However, it should be noted that generally beat pattern can be obtained for any range of sample values, therefore x scale becomes arbitrary, as beat pattern depends on time interval between R-R waves. The beat pattern for other ECG is shown in Figure 7. After comparing two beat patterns, it can be concluded that the beat pattern for two different ECG is also different. Therefore for patient identification, both ECG and its beat pattern can be used.

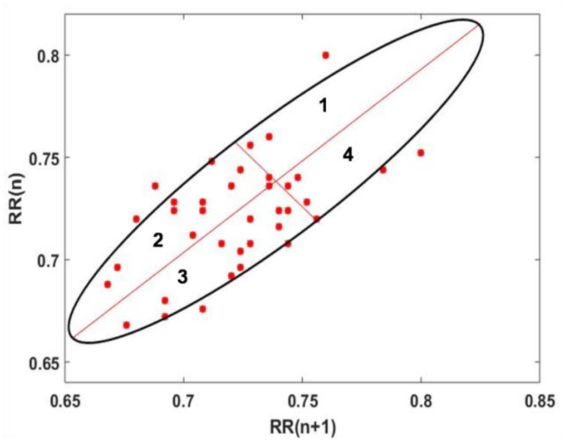

Figure 8: Poincare Plot and fitted ellipse for ECG-1

In Poincare plot current plot is shown in Figure 8. Here, values are scatted over the plot therefore this ECG is for a healthy person. For ellipse generation a Matlab code is written, which on the basis of data points decide angle of rotation, centre, length of major and minor axis, for the current set of results, the obtained parameters for ellipse are

Center = 0.7389, 0.7383

Length of major axis = 0.2298

Length of minor axis = 0.0517

In Figure 9, Poincare plot for ECG-2 signal is plotted, here again variability is observed but it is not in y=x direction, therefore it can be concluded that this person is healthier but he/she is lesser healthier than person in ECG -1.

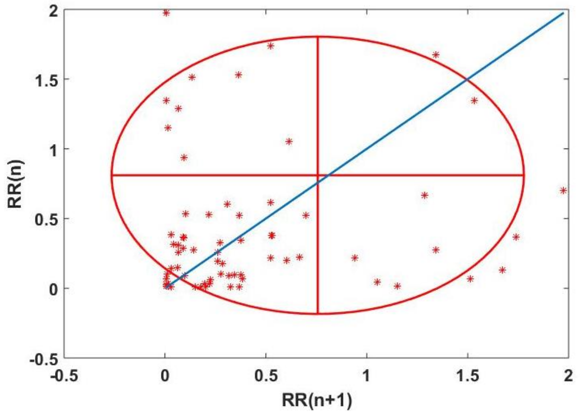

Figure 9: Poincare Plot and fitted ellipse ECG-2

Center = 0.7569, 0.81

Length of major axis = 2.0430

Length of minor axis = 1.9884

ECG BASED AUTHETICATION GUIDELINES

Step 1: Record Patients ECGs and send one copy in remote database, obtain heart rate pattern for each ECG and record it.
Step 2: Send secondary copy recorded on some other day to database for authentication/verification.
Step 3: Obtain heart rate pattern for send ECGs.

Step 4: Check similarity among ECGs and Heart rate pattern and record scores
Step 5: If score obtained for both the process is more than 0.5, authenticate the patient otherwise reject it**.**

We tested 67 ECG images, 35 of healthy people, 25 for ill people and 7 for critically ill people. We are able to identify 66 people from their respective ECGs, one of the critically ill person cannot be identified due to very distorted ECG.

5. CONCLUSIONS

In this chapter discusses the various concepts related to ECG based authentication. First of all ECG filtration process is detailed and it has been found that using notch filter unwanted noise can be suppressed significantly. ECG processing is detailed, and its peaks are detected, from these detected peaks ECG heart rate pattern is obtained, and it has been found that both ECG and its heart rate pattern is unique foe each individual. To judge the level of similarity cross correlation is performed among different ECGs and beat pattern, and finally guidelines are set for ECG based authentication on the basis of obtained scores.

REFRENCES

1. Cao, H.; Leung, V.; Chow, C.; and Chan, H., (2009). Enabling technologies for wireless body area networks: A survey and outlook. *IEEE Communications Magazine*, *47*(12).
2. Ullah, S.; Higgins, H.; Braem, B.; Latre, B.; Blondia, C.; Moerman, I.; Saleem, S.; Rahman, Z.; and Kwak, K.S., (2012). A comprehensive survey of wireless body area networks. *Journal of medical systems*, *36*(3), pp.1065-1094.
3. Kumar, P.; and Lee, H.J., (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, *12*(1), pp.55-91.
4. Sametinger, J.; Rozenblit, J.; Lysecky, R.; and Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM*, *58*(4), pp.74-82.
5. Gold, R.D., (2014). Safety and reliability considerations. *VLSI in Medicine: VLSI Electronics Microstructure Science*, *17*, p.247.
6. Rushanan, M.; Rubin, A.D.; Kune, D.F.; and Swanson, C.M., (2014), May. SoK: Security and privacy in implantable medical devices and body area networks. In *Security and Privacy (SP), 2014 IEEE Symposium on* (pp. 524-539). IEEE.
7. Da He, D.; Winokur, E.S.; and Sodini, C.G., (2011). A continuous, wearable, and wireless heart monitor using head ballistocardiogram (BCG) and head electrocardiogram (ECG). In *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE* (pp. 4729-4732). IEEE.
8. Al Taradeh, N.; Bastaki, N.; Saadat, I.; and Al Ahmad, M., (2015). Non-invasive piezoelectric detection of heartbeat rate and blood pressure. *Electronics Letters*, *51*(6), pp.452-454.
9. Shu, Y.; Li, C.; Wang, Z.; Mi, W.; Li, Y.; and Ren, T.L., (2015). A Pressure sensing system for heart rate monitoring with polymer-based pressure sensors and an anti-interference post processing circuit. *Sensors*, *15*(2), pp.3224-3235.
10. Venkatasubramanian, K.K.; Banerjee, A.; and Gupta, S.K.S., (2010). PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, *14*(1), pp.60-68.
11. Zhang, Z.; Wang, H.; Vasilakos, A.V.; and Fang, H., (2012). ECG-cryptography and authentication in body area networks. *IEEE Transactions on Information Technology in Biomedicine*, *16*(6), pp.1070-1078.
12. Yao, L.; Liu, B.; Yao, K.; Wu, G.; and Wang, J. (2010), October. An ecg-based signal key establishment protocol in body area networks. In *Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2010 7th International Conference on* (pp. 233-238). IEEE.