INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 181-186

DESIGN OF A SECURE ECG BASE BIOMETRIC AUTHENTICATION SYSTEM FOR WIRELESS BODY AREA NETWORK

Vandana Verma[1], Deepak Sharma[2]

[1]M. tech Scholar, Dept. of ECE, LNCT(Bhopal) Indore Campus, Indore (M.P), India.

[2]Assistant Professor, Dept. of ECE, LNCT(Bhopal) Indore Campus, Indore (M.P), India.

ABSTRACT

The increasing use of wireless networks and the constant miniaturization of electrical invasive/non-invasive devices have empowered the development of Wireless Body Area Networks (WBANs). Wireless Body area networks (WBANs) constitute an active field of research and development as it offers the potential of great improvement in the delivery and monitoring of healthcare The RBS is generated from the inter-pulse interval (IPI) extracted from the ECG waveform. The computation parameters considered are the entropy and the hamming distance. The performance evaluation parameters for the proposed technique are the entropy and the hamming distance.

Keywords: Wireless Sensor Network (WSN), Wireless Body Sensor Networks (WBSN), Inter Pulse Interval (IPI), Random Binary Stream (RBS), Hamming Distance, Entropy

1. INTRODUCTION

The need for data transfer in the wireless format has needed for wireless sensor networks. Wireless sensor networks are the connectivity of several sensor modules connected to each other and to a remote control station. With increasing popularity of wireless technology, and ever increasing capabilities inscribed into the nature of wireless sensor networks, BANs became

more and more applicable to sophisticated

application such as medical and defense based applications. The body area network

has the following properties:

1) It is generally characterized by wearable on the body
2) It communicates in the periphery of the body.
3) It has limited resources of processing and memory.

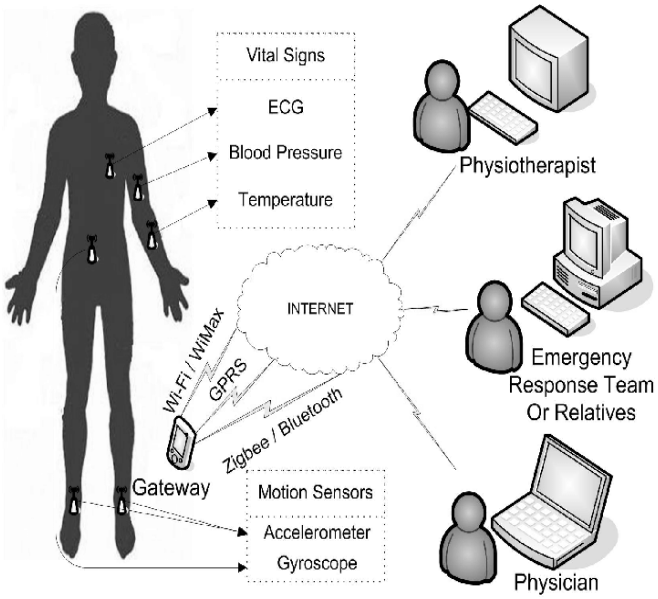

Fig 1. Wireless body area Network

1.1 Wbasn Communication Network:

Wireless body area sensor network has come into existence after the development of wireless sensor network reached some level of maturity. This has become possible due to the tremendous technological advancement leading to easy-to-use wireless wearable technologies and electronic components that are small in size. These sensors, often with own capability of communicating within themselves or with other devices, are developed to gather data and store the recorded data to process further if needed. Such communications could take place via wired as well as wireless mode giving scope to their (i.e. the sensors) increase in number for a particular system or network.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 07, July 2023, pp : 181-186

e-ISSN : 2583-1062

Impact Factor : 5.725

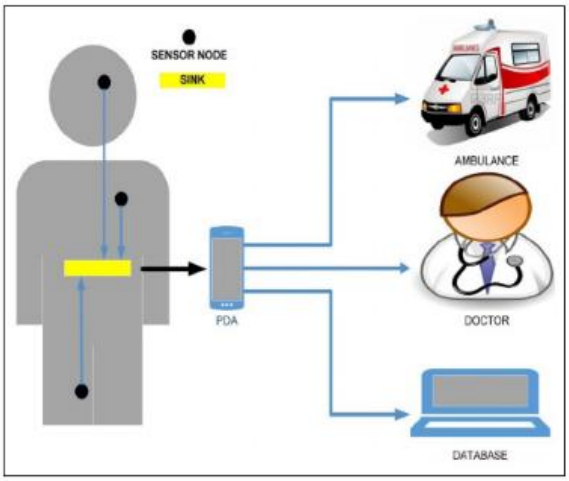

Fig 2. Wireless Body Area Sensor Network in Health Care

1.2 APPLICATIONS OF WBASN:

There are various applications of wireless body sensor networks out of which the two most prominent applications generally are:

1) Medical Applications- Wireless Body Area Networks (WBANs) is one such talented tool that has the impending to appreciably improve health care delivery, investigative monitoring, disease-tracking and related medical procedures. A critical feature of WBANs is their ability to provide highly reliable infrastructure for medical devices, especially those implanted in the human body.
2) Non-Medical Applications - WBASN-based applications pertaining to non-medical applications can be thought of as defense and military, the banking sector, space exploration etc. While commercially available Internet of Things (IoT) is trying to leverage into the Wireless Body Sensor Network architecture, yet a separate segregation of the WBSN for non-medical applications is sought after.

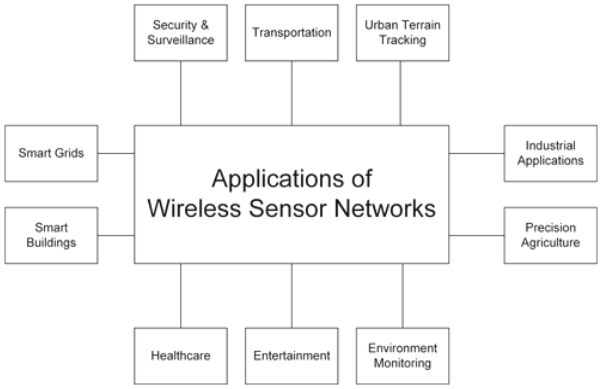

Fig 3. Application Of Wireless Sensor Network

1.3 MOTIVATION

Wireless body sensor networks (WBSNs) are now ubiquitous in several domains. Thus the security also becomes critical. Since high end encryption cannot be employed due to the constraints of memory and processing power, hence its challenging to employ a security paradigm which would be both secure and lightweight in terms of computation. With increasing popularity of wireless technology, and ever increasing capabilities inscribed into the nature of wireless sensor networks, BANs became more and more applicable to sophisticated application such as medical and defense based applications.

1.4 OBJECTIVE

The objective of the proposed work is to enhance the performance of wireless body sensor networks (WBSNs) in terms of security. The objectives can be quantified as:

- Designing a secure authentication mechanism for WBSNs.
- Successfully processing the raw ECG data to remove effects of noise and compute features accurately.

Obtaining high Entropy (ensuring randomness) and high Hamming Distance (ensuring uniqueness or distinctiveness)

Additionally, it is to looked into that the raw data is to be pre-processed before the computation of the critical parameters to authenticate the user in the BSN.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 181-186

e-ISSN : 2583-1062

Impact Factor : 5.725

2. LITERATURE REVIEW

In IEEE 2019, Sandeep Pirbhulal at al. in [1] proposed a heartbeats based random binary sequences (RBSs) generation mechanism for the security and authentication of Wireless Body Sensor Networks.

In ELSEVIER 2018, Peyman Dodangeh et al in [2] proposed awireless body area networks (WBANs) security mechanism for medical applications.

In Elsevier 2017, X Li et al. in [5], presenteda secure key generation technique for WBSNs. The work proposes that it is often infeasible to encrypt and decrypt the dynamic data streams in WBSNs due to the limitations in hardware.

In IEEE 2016, Hussein Moosavi et al. in [10] the authors proposeda Delay-Aware Optimization of Physical Layer Security mechanism for Multi-Hop WBANs

3. PROBLEM IDENTIFICATION

3.1 Data-Pre Processing:

The IPI based RBS generation is often challenging due to the following facts:

- It is very difficult to remove the noise effects and residual noise effects can make the computation of the ECG based features inaccurate.
- It is difficult to maintain both randomness and uniqueness of the RBS.
- Randomness makes it difficult to attackers to detect the RBS
- Uniqueness or distinctiveness is necessary to ensure that different individuals will generate different RBS.

Some common forms of disturbances are depicted in the following figure

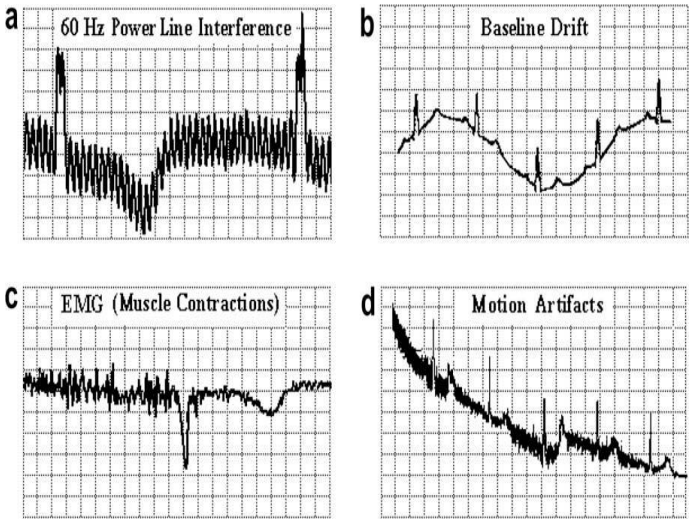

Figure 4

Motion Artifacts

Possible Noise and Disturbances in Calculation of IPI

The most common types of noise and disturbance encountered in using the ECG signal as the physiological signal are the following:

1) Power Line Interference
2) Baseline Drift
3) EMG (muscle contraction)

Generally the noise affecting ECG data is the low frequency noise which can be filtered out using high pass filtering.A high pass filter allows only high frequencies and hence would stop low frequency noise present in the ECG signal. The filtering retains the critical information in the ECG signal while only removing the disturbances in the signal which tend to corrupt the signal.

The proposed work needs the high pass filter in order to remove the low frequency noise and artifacts intertwined with the signal under interest. The frequency response of the high pass filter is shown in the subsequently.

4. PROPOSED METHODOLOGY:

4.1 The Typical ECG Signal and IPI Computation

The typical ECG waveform can be used an effective metric for the authentication purpose. The property to be used is the repetitive pattern of the ECG shown below.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 181-186

e-ISSN : 2583-1062

Impact Factor : 5.725

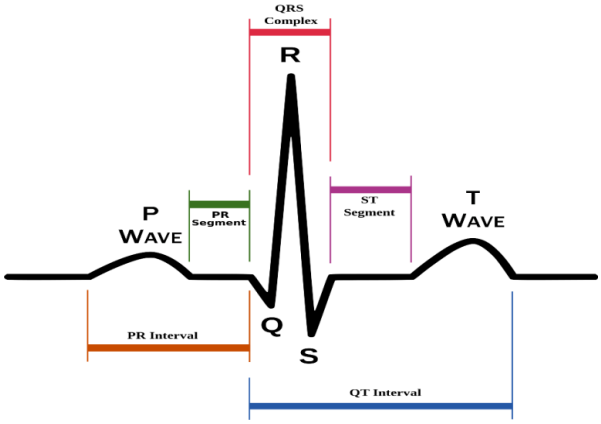

Figure 5

the ECG wave comprises of the following sections:

1) P Wave
2) Q Wave
3) R Wave
4) S Wave
5) T Wave
6) PR Interval
7) QT Interval
8) PR Segment
9) ST Segment
10) QRS Complex

The pulse repeats itself and hence inter-pulse intervals (IPI) are designated as:

1) PP Interval
2) QQ Interval
3) RR Interval
4) SS Interval
5) TT Interval

Based on the inter-pulse intervals computed, the random binary stream is to be generated.

Data Preparation

The data in the form of ECG is to be processed in the following manner.

Let

y(t) represents the output of the high pass filter,

x(t) represents the input to the filter

h(t) represents the impulse response of the filter.

Then:

$$\mathbf{y(t) = x(t) * h(t)} \qquad \textbf{(4.1)}$$

here * denotes convolution operation

Shannon's sampling theorem has to be invariably followed in the sampling of the ECG data i.e.

$$\mathbf{f_s \geq 2f_m} \qquad \textbf{(4.2)}$$

Here,

Fs is the sampling frequency

Fm is the maximum frequency of the ECG data

The squaring operation is performed subsequently so as to remove any kind of ambiguity among the R peak and other neighboring peaks

$$\mathbf{Sqr_{sig} = [y(t)]^2} \qquad \textbf{(4.3)}$$

It is a challenge none the less to devise a mathematical condition to find the peaks among the multitude of samples in the signal. A peak would exist at a given discrete sample location if the following condition is satisfied.

$$\mathbf{S_{k-1} < S_k > S_{k+1}}$$

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 181-186

e-ISSN : 2583-1062

Impact Factor : 5.725

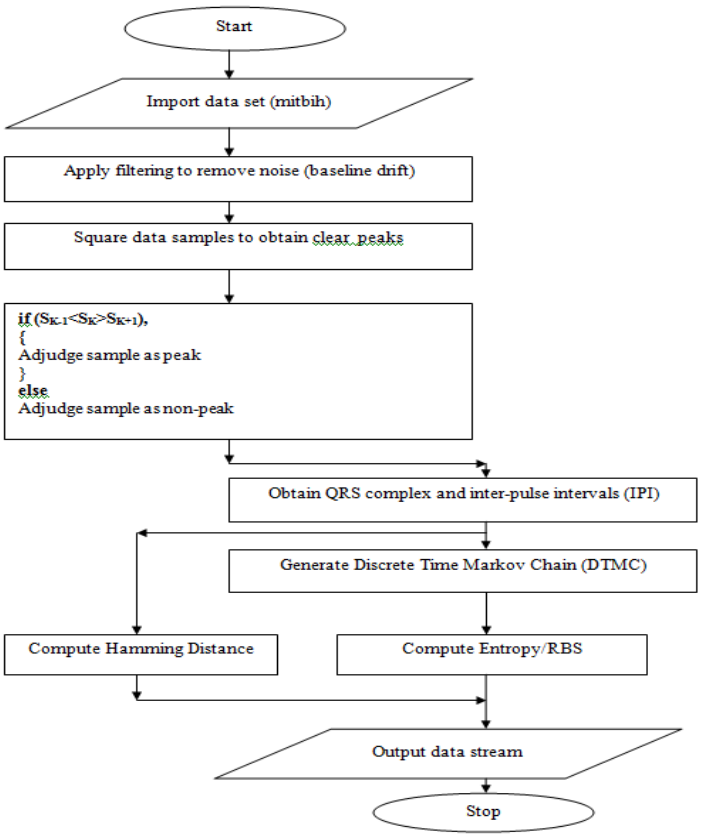

Figure 6 - Flowchart of Proposed System

RBS Generation

The locations of the peaks are stored and through subsequent differences, the features are extracted. The inter-pulse interval (IPI) is computed from the features using either R-R interval or QRS complex interval.

This is necessary to render reliability to the system with highest amplitude. The QRS complex is the easiest waveform peak needed for reliable detection. Subsequently generate the random bit stream based on the Discrete Markov Chain given by:

$$\mathbf{X} = [\mathbf{X_1}, \mathbf{X_2} \dots \dots \dots \dots \dots \dots \mathbf{X_n}]$$

The random binary stream generated in the proposed work is done using the Random Markov Process. Markov processes are often seen as finite state transition systems in which the present outcomes do not depend on the previous outcomes thereby rendering randomness to the process. The Markov processes are generally classified as the continuous time Markov Process and the Discrete Time Markov Process also called the Discrete Time Markov Chain (DTMC)

5. RESULTS

Obtained Results- The dataset used in the work is the MIT-BIH db. The ECG data has been extracted in the form of .mat files. A subsequent evaluation of the obtained results follows. FiF

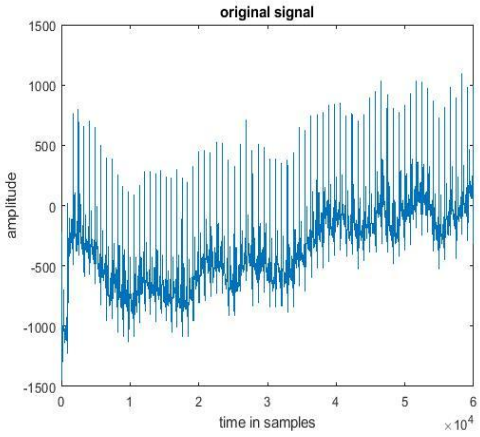

Figure 7 : Original ECG Data Sample

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 181-186

e-ISSN : 2583-1062

Impact Factor : 5.725

The figure above depicts the original ECG data sample. It can be seen that there exists baseline drift and low frequency noise in the data.

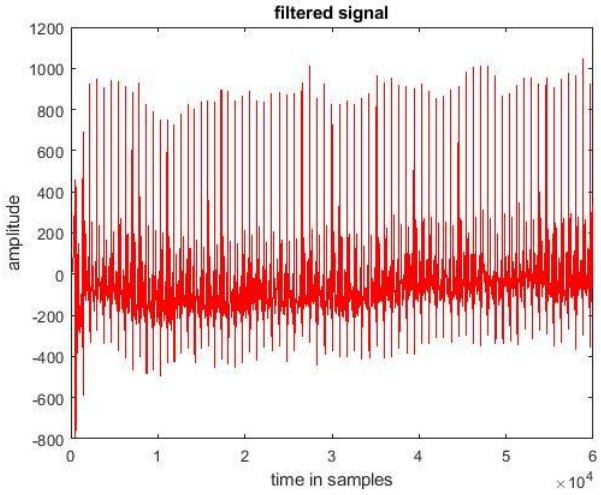

Fig 8. Filtered Data Sample

The figure above shows that the high pass filtering is competent to remove the baseline drift and associated low frequency noise effects. It can be seen that he vertical wandering of the signal with respect to the x-axis is absent indicating the removal of the major part of the noise and only the existence of the traces.

6. CONCLUSION

It can be concluded from previous discussions that a very useful category of wireless sensor networks is the Wireless Body Sensor Networks (WBSNs).

The proposed technique incorporates the deep Markov model for random bit sequence (RBS) generation from the ECG based data which has been used as the counterpart for the actual heart beats.

The features which have been extracted for the inter pulse interval (IPI) are RR interval, SS Interval and QRS complex. It has been shown that the proposed technique achieves better results in terms of hamming distance and entropy compared to previous work and proposed work attains higher value of hamming distance and entropy compared to the previously existing techniques.

7. FUTURE SCOPE

Future scope of enhancement of the proposed system can be thought of as:

- Increasing the Entropy and hamming distance of the system by implementing chaos.
- Trying out different filtering techniques such as the median or mode filter to compute features more accurately.

8. REFERENCES

[1] Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., ... & Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. Journal of medical systems, 36(3), 1065-1094.

[2] Tobon, D. P., Falk, T. H., & Maier, M. (2013). Context awareness in WBANs: a survey on medical and non-medical applications. Wireless Communications, IEEE, 20(4), 30-37.

[3] Boulemtafes, A., & Badache, N. (2016). Design of Wearable Health Monitoring Systems: An Overview of Techniques and Technologies. In mHealth Ecosystems and Social Networks in Healthcare (pp. 79-94). Springer International Publishing.