International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 02 | Feb - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Security of Wireless Body Area Networks Based on Markov Chain Enabled Chaotic Networks

Shivam Borban[1], Prof. Pallavi Bagde[2]

Abstract: As BANs have limited processing power and memory availability, securing body area networks or body sensor networks is problematic. Due to the impracticality of implementing high-end encryption in resource-constrained body sensor networks, heartbeat-based security is preferable. To simulate real heartbeats from electrocardiogram (ECG) data, the suggested method uses a deep Markov model to generate random bit sequences (RBS). The interpulse interval (IPI) is defined by the information retrieved from the RR interval, the SS interval, and the QRS complex. The MIT-BIH database (MIT-BIHdb) is the source of the extracted data. Both the entropy and the hamming distance are used to evaluate the performance of the suggested method. Results demonstrate that, in comparison to prior work, the suggested method achieves a greater hamming distance for the amount of bits extracted per IPI. The entropy is somewhat greater than the prior method, fluctuating between 0.95 and 1. The receiving end's ability to accurately and distinguishably detect the received binary sequence for authorization is shown by the rise in hamming distance..

Keywords: Body Sensor Networks, Inter Pulse Interval (IPI), Random Bit Stream (RBS), Markov Discrete Time Markov Chain, Hamming Distance, Entropy.

I. INTRODUCTION

Off late, body area networks and body sensor networks have gained popularity. Hence, their security has become an active area of research. wireless body sensor networks (WBSNs) have emerged as a promising and effective approach for remote healthcare applications due to the rapid development of wearable medical devices and wireless technologies. Since WBSNs are wireless in nature, so secure transmission of medical data becomes one of the essential requirements for its deployment.[1] The Health Insurance Portability and Accountability Act (HIPAA) has stated that security must be applied within WBSNs to restrict the availability of critical data to the unauthorized entities[8]. Additionally, tiny nodes in WBSNs are resource constrained regarding battery, computation capability, and memory. Therefore, it is necessary to provide a balance between medical data security and resource consumption of sensor nodes in WBSNs. In recent times, the objectives of ECG monitoring have gone beyond mere heart rate and rhythm measurement to the analysis of chronic diseases including complex arrhythmias, stress management, and sleep disorders among others. The significance of ECG in clinical applications is because it offers a non-invasive means to evaluate the Autonomic Nervous System (ANS) which can be helpful in diagnoses of cardiac related diseases. Additionally, it has been remarkably explored in several previous studies that ECG signals possess unique characteristics to be utilized for biometric security purposes in WBSNs [9-14]. One of the significant benefits of ECG based security methods is that they are robust against false attacks. Moreover, ECG signal can provide the evidence by signifying that specific application should ensure that the particular person who is posing the biometric security is certainly the same individual who is carrying it [1].

Thus, ECG signal plays an essential role in developing security mechanisms to provide secure communication between patients and physicians in real-time healthcare scenarios. However, the main limitation of WBSNs is that it should be operated under stringent constraints. Thus, to provide a balance between security and resource efficiency a biometric trait such as inter-pulse intervals (IPIs) has been widely considered. IPIs are the time intervals between two successive heartbeats also referred as RR-intervals. In order to initiate communication within sensor nodes of WBSNs, time synchronization is an essential factor.

II. FEATURE EXTRACTION

The regular motion of the human heart is often referred to as the cardiac cycle. The presence of sodium and potassium ions in the blood stream produces very weak electrical signals (voltages) when blood flows in and out of the heart. It has been observed that the ECG signals follow a repetitive or periodic pattern. Based on the trajectory of the ECG curve, certain fundamental features have been identified. The section that follows explains the cardiac cycle. ECG is the graphical representation of the cyclic rhythm of contraction and relaxation activity generated by the heart. An ECG is composed of the P wave, QRS complex, T and U waves.

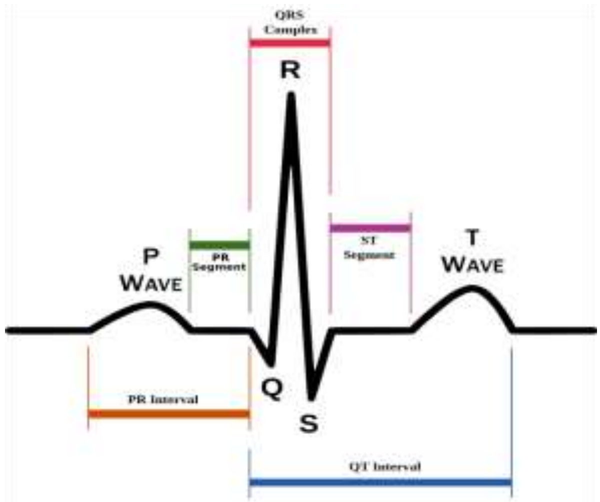

Fig 1 ECG signal showing P, Q, R, S, T and U waves.

They are denoted by the capital letters P, Q,R,S, and T and U. The P wave is the contraction of the atria, while the QRS complex is associated with the contraction of the ventricles. The T wave is due to the relaxation of the ventricles. The P, Q, R, S, T and U waves of the ECG signal contain all the important features that characterize the activity in the heart. A typical ECG signal waveform of a normal heart beat is shown in figure 1. The ECG signal is measured through a number of electrodes that are normally attached to a patient's body. ECG recordings usually contain high and low frequency noise. Amplitudes within beats vary from person to person.

a) Data Pre-Processing prior to Feature Extraction

Prior to the feature extraction stage, proper pre processing stage in very crucial for the correct extraction of features. In some ECG signals the noise level is very high and it is not possible to recognize it by single recording, it is important to gain a good understanding of the noise processes involved before one attempt to filter or preprocess a signal. The ECG signal is very sensitive in nature, and even if small noise mixed with original signal the characteristics of the signal changes. The most difficult problem faced by an automatic ECG analysis is the large variation in the morphologies of ECG waveforms, it happens not only for different patients or patient groups but also within the same patient. Since the ECG signal is the most affected by 50-60 Hz power line noise also called baseline drift, therefore we need to employ high pass filtering for its removal.

b) Extraction of Morphological Features

This stage consists of extraction of salient features which can give conclusive results for different heartbeat cases.. The heartbeat detection module attempts to locate all heartbeats .The feature extraction module forms a feature vector from each heartbeat. The feature extraction modules are required, because greater classification performance is often achieved if a smaller number of discriminating features are first extracted from the ECG.[7].[9] The Feature Extraction Parameters:

- RR interval evaluation.
- SS interval evaluation.
- QQ interval evaluation.
- QRS complex evaluation.

ECG Feature Extraction plays a significant role in diagnosing most of the cardiac diseases. One cardiac cycle in an ECG signal consists of the P-QRS-T waves. This feature extraction scheme determines the amplitudes and intervals in the ECG signal for subsequent analysis. The amplitudes and intervals value of P-QRS-T segment determines the functioning of heart of every human.

III. RANDOM BIT GENERATION

The random bit generation has been implemented using the Markov process. A Markov process is a random process indexed by time, and with the property that the future is independent of the past, given the present. Markov processes, named for Andrei Markov, are among the most important of all random processes. In a sense, they are the stochastic analogs of differential equations and recurrence relations, which are of course, among the most important deterministic processes. The complexity of the theory of Markov processes depends greatly on whether the time space **T** is **N** (discrete time) or [0,∞] (continuous time) and whether the state space is discrete (countable, with all subsets measurable) or a more general topological space.

$$\textbf{When } T = [0, \infty] \qquad (1)$$

or when the state space is a general space, continuity assumptions usually need to be imposed in order to rule out various types of weird behaviour that would otherwise complicate the theory. When the state space is discrete, Markov processes are known as Markov chains. The general theory of Markov chains is mathematically rich and relatively simple. Any process is a Markov Process if:

$$P(X_{s+t} \epsilon A | F_s) = P(X_{s+t} \epsilon A | X_s) \nabla s, T \in U \qquad (2)$$

Here,
X represents a state
s is the time metric
t is a delayed metric
P is the probability space
A is the state space
Xs is a previously existent state
U is the universal state of spaces

IV. PROPOSED ALGORITHM

The data is extracted from MIT-BIH db. Then the ECG signal is displayed. The signal is then passed through a high pass filter the output of which is displayed again. The baseline drift is seen to be removed from the ECG signal due to filtering.
Let y(t) denote the output of the filter, x(t) denote the raw ECG signal and h(t) denote the impulse response of the filter. Then:

$$y(t) = x(t) * h(t) \quad (3)$$

where * denotes convolution in the time domain.
It should be noted that the sampling frequency of the filter should follow the Nyquist criteria i.e.

$$f_s \geq 2f_m \quad (4)$$

Where Fs denotes the sampling frequency and fm denotes maximum frequency of the signal. Subsequently squaring the signal is done to accurately detect R peaks as R peaks are much larger in amplitude compared to other peaks.

$$Sqr_{sig} = [y(t)]^2 \quad (5)$$

Where Sqr_sig denotes square of the filtered signal.
It should be noted that squaring is done only for detection of R peaks as other peaks cannot be discriminated after squaring and may introduce errors.
Peaks are detected after setting a threshold which varies adaptively with the concerned peak and signal under consideration. Peaks are detected using the difference operation that a sample is a peak if it is greater in magnitude compared to previous and subsequent values i.e.

$$S_{k-1} < S_k > S_{k+1} \quad (6)$$

Then 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. Subsequently generate the random bit stream based on the Discrete Markov Chain given by:

$$X = [X_1, X_2 \dots\dots\dots\dots\dots\dots X_n] \quad (7)$$

Subsequently, compute the hamming distance (H) and Entropy (E)
Given two vectors u, v ∈ F n, the hamming distance between u and v, d(u, v), to be the number of places where u and v differ. Mathematically,

$$H = |U| - |V| \quad (8)$$

The entropy is computed for the random process as:

$$H(X) \triangleq -\sum_{x \in X} P_x(x) log[P_x(x)] \quad (10)$$

Here,
H is the entropy
X is the random variable
x is any value that the random variable can attain
P is the probability
log represents the logarithm to the base 2.

V. RESULTS:

The results obtained are enunciated subsequently.

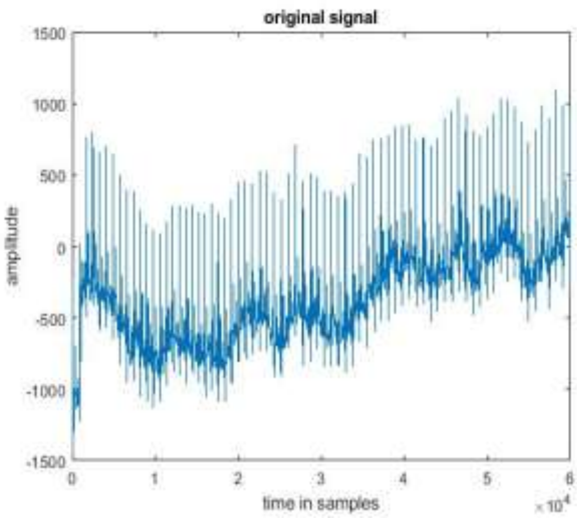

Fig.2 Original Data Sample

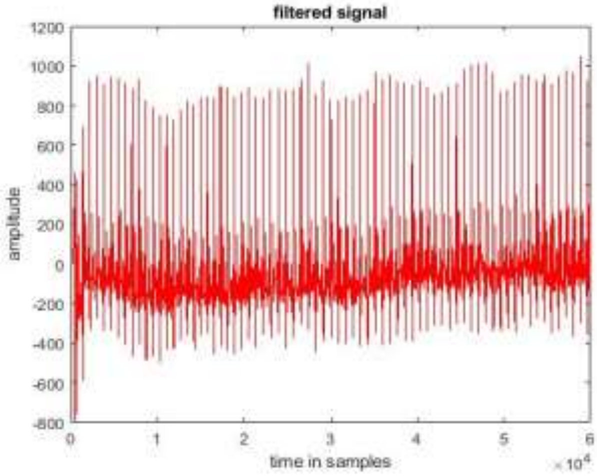

Fig.3 Filtered Data Sample

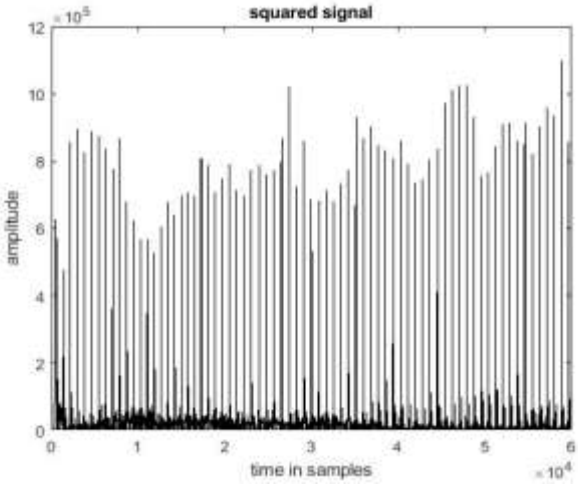

Fig.4 Squared Data Sample

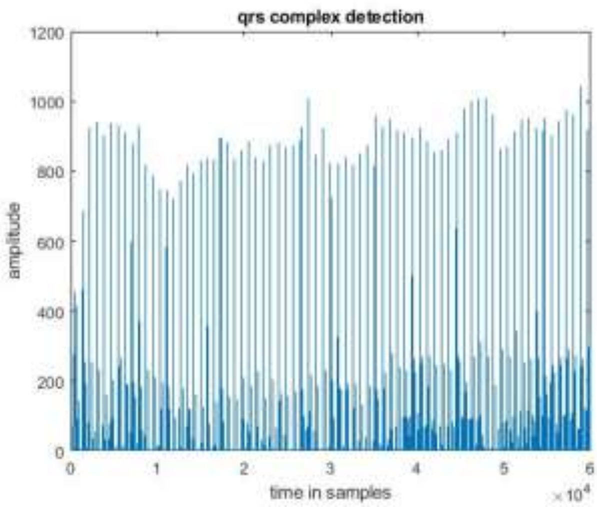

Fig.5 QRS Complex Detection

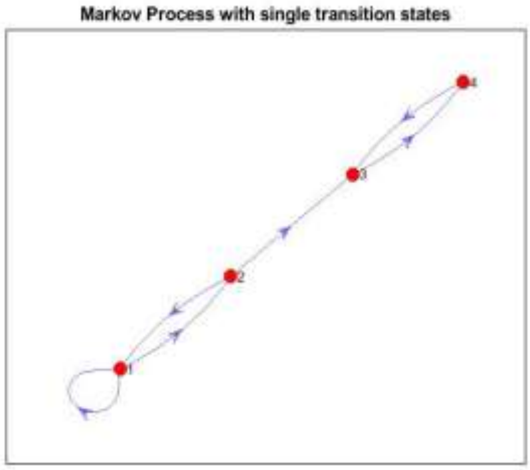

Fig.6 Single Transition Markov Chain

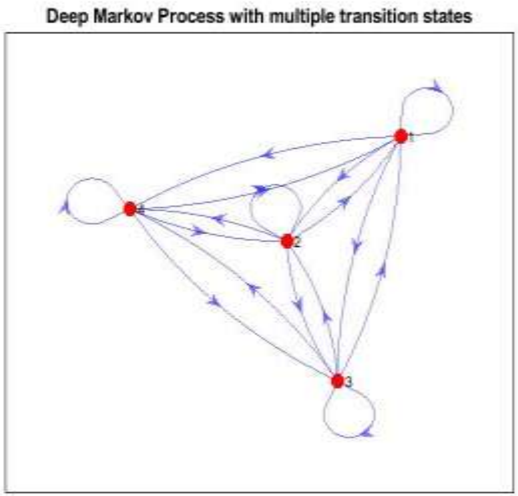

Fig.7 Multiple Transition Deep Markov Chain

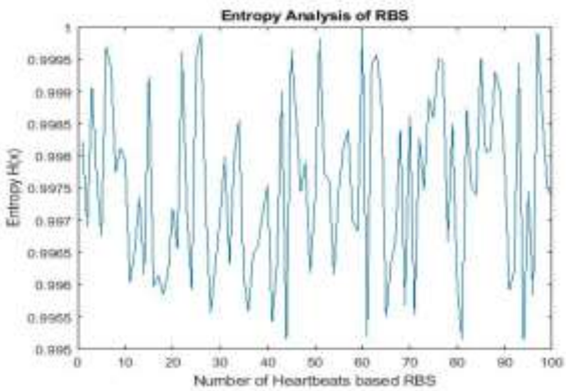

Fig.8 Variation of Entropy w.r.t. RBS

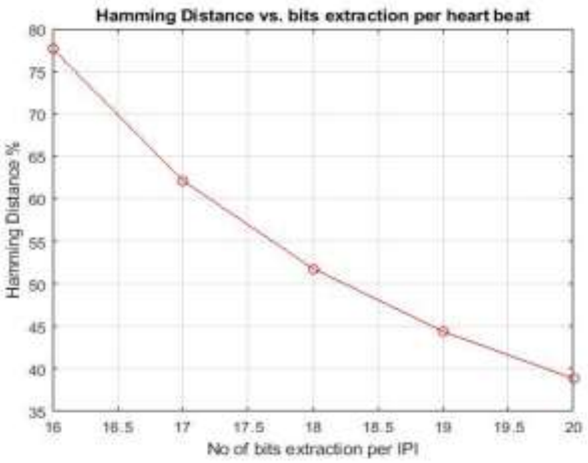

Fig.9 Variation of Hamming Distance w.r.t. No. of extracted bits/IPI

Comparison with Previous Work:

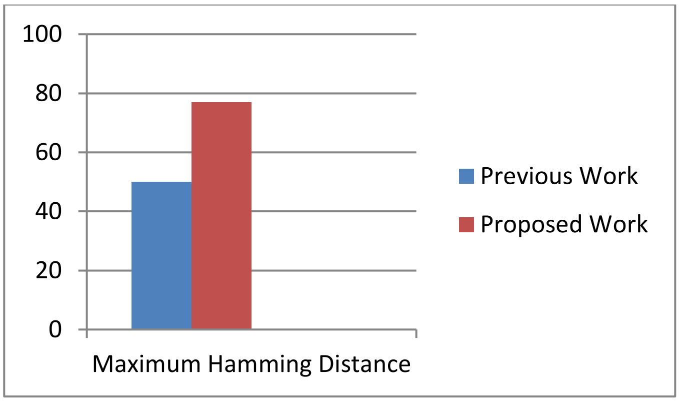

Figure.10 Comparative Hamming Distance Analysis

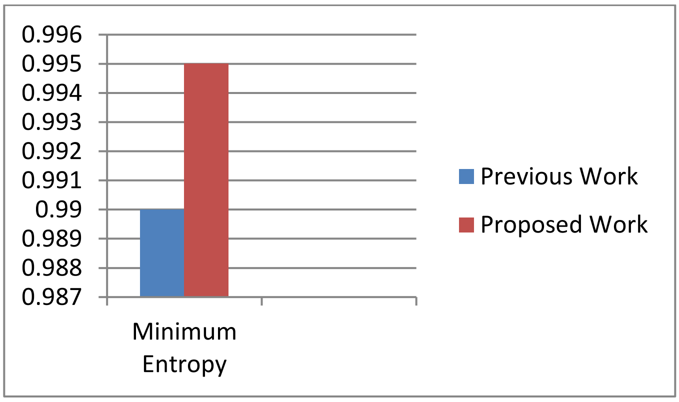

Figure.11 Comparative Entropy Analysis

Conclusion: It can be concluded from previous discussions that body area networks and body sensor networks have gained popularity. Hence, their security has become an active area of research. Wireless body sensor networks (WBSNs) have emerged as a promising and effective approach for remote healthcare applications due to the rapid development of wearable medical devices and wireless technologies. Since WBSNs are wireless in nature, so secure transmission of medical data becomes one of the essential requirements for its deployment. In this paper, a secure heartbeat based random bit sequence generation mechanism has been proposed using the Markov Process. It has been shown that the proposed technique achieves better results in terms of hamming distance and entropy compared to previous work. In crease in Hamming distance ensures higher chances of accurate detection and reliability at the receiving end. Higher entropy ensures higher information content of the bit stream.

References

[1] Sandeep Pirbhulal, Heye Zhang, Wanqing Wu, Subhas Chandra Mukhopadhyay, “Heart-Beats Based Biometric Random Binary Sequences Generation to Secure Wireless Body Sensor Networks”, IEEE 2024

[2] Peyman Dodangeh, Amir Hossein Jahangir, “A biometric security scheme for wireless body area networks” Elsevier 2023

[3] AmelArfaoui, Asma ben Letaifa, Ali Kribeche, Sidi Mohammed Senouci, Mohamed Hamdi, “A Stochastic Game for Adaptive Security in Constrained Wireless Body Area Networks” IEEE 2022

[4] Amit Samanta, Sudeep Mishra, “Dynamic Connectivity Establishment and Cooperative Scheduling for QoS-Aware Wireless Body Area Networks” IEEE 2021

[5] X Li, MH Ibrahim, S Kumari, AK Sangaiah, V Gupta, “Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks”, Elsevier 2020

[6] Z Li, H Wang, M Daneshmand, “Secure and efficient key generation and agreement methods for wireless body area networks”, IEEE 2019

[7] AA Omala, KP Kibiwott, F Li, “An efficient remote authentication scheme for wireless body area network”, Springer 2018

[8] N Yessad, S Bouchelaghem, FS Ouada “Secure and reliable patient body motion based authentication approach for medical body area networks”, Elsevier 2017

[9] D He, S Zeadally, N Kumar, JH Lee, "Anonymous authentication for wireless body area networks with provable security" IEEE 2016

[10] H Moosavi, FM Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks", IEEE 2016 [11] C Hu, H Li, Y Huo, T Xiang, "Secure and efficient data communication protocol for wireless body area networks" IEEE 2016

[12] MH Ibrahim, S Kumari, AK Das, M Wazid, "Secure anonymous mutual authentication for star two-tier wireless body area networks", Elsevier 2016.

[13] D He, S Zeadally, L Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks" IEEE 2015

[14] J Shen, H Tan, S Moh, I Chung, Q Liu, "Enhanced secure sensor association and key management in wireless body area networks", IEEE 2015

[15] H Xiong, Z Qin, "Revocable and scalable certificate-less remote authentication protocol with anonymity for wireless body area networks", IEEE 2015

[16] C Wang, Y Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing", Springer 2015

[17] M Rushanan, AD Rubin, DF Kune, "Sok: Security and privacy in implantable medical devices and body area networks", IEEE 2014

[18] M Zhang, A Raghunathan, NK Jha, "Trustworthiness of medical devices and body area networks", IEEE 2014

[19] AFA Rahman, R Ahmad, "Forensics readiness for wireless body area network (WBAN) system", IEEE 2014

[20] R Dautov, GR Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography", IEEE 2014

[21] SN Ramli, R Ahmad, MF Abdollah, "A biometric-based security for data authentication in wireless body area network (wban)", IEEE 2013

[22] SS Javadi, MA Razzaque, "Security and privacy in wireless body area networks for health care applications", Springer 2013

[23] C Hu, N Zhang, H Li, X Cheng, "Body area network security: a fuzzy attribute-based signcryption scheme" IEEE 2013

[24] D He, S Chan, Y Zhang, H Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks" IEEE 2013

[25] M Al Ameen, J Liu, K Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications" Springer 2012

[26] Z Zhang, H Wang, AV Vasilakos, "ECG-cryptography and authentication in body area networks", IEEE 2012