International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 10 | Oct - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Review on Security Mechanisms for Personal and Body Area Networks

Jagdish Panwar[1], Prof. Pankaj Raghuwanshi[2]

Abstract: The processing power and memory availability limitations of the sensors make it difficult to secure body area networks (BANs) or body sensor networks (BSNs). Due to the impracticality of implementing high-end encryption in resource-constrained body sensor networks, heartbeat-based security is preferable. Traditional methods generate random bit sequences (RBS) utilizing biometrics. A common biometric for authentication that makes use of important metrics or attributes is a person's heart rate. The suggested method gives an exhaustive overview of the current biometric security measures for BANs. The hamming distance and entropy have been proven to be the performance evaluation metrics for the traditional method. To guarantee distinctability, one can use the hamming distance metric, while entropy shows the average information associated with the binary data stream. An effective method for securing BANs is anticipated to be aided by the review.

Keywords: Body Area Networks, Physiological Data, Inter Pulse Interval (IPI), Random Bit Stream (RBS), 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.

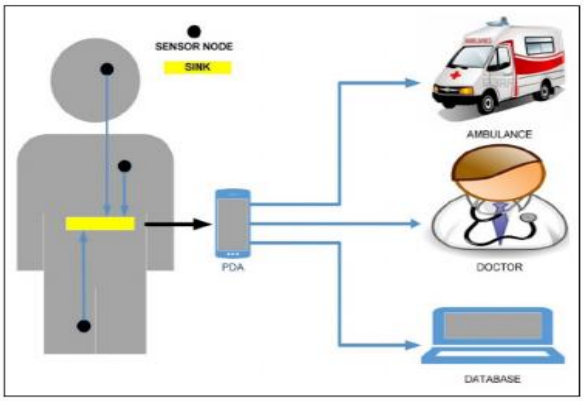

Fig. 1 Typical BAN Architecture for Medical Applications

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. There are some very empirical or basic devices which monitor a persons biomedical parameters such as heartbeat, temperature, calorie consumption and temperature.

Examples are: Fitbit, AliveCor – Personal EKG kit etc. However, most of the devices are in RESEARCH PHASE, and needs FDA (Food and Drug Administration, USA) clearance to be released in the market. With increasing demand in such biomedical monitoring devices which are IoT or internet enabled, a lot of research and testing is going on in this field.

Global Medical Wearable Market is valued at USD 12.788 billion in 2019 and expected to reach USD 37.67 Billion by 2025 with the CAGR of 19.73% over the forecast period.

Some major key players for Global Medical Wearable Market are:

Philips Electronics, Omron Corp., Fitbit Inc , Covidien Plc;, Polar Electro, LifeWatch AG, Garmin, Withings, Jawbone, Everist Genomics, Sotera Wireless, Pebble Technology Corp., Basis Science etc.

(Source: https://www.medgadget.com/2020/04/medical-wearable-market-share-current-trends-and-research-development-report-to-2025.html)

II. AUTHENTICATION MECHANISM

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.

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 2.

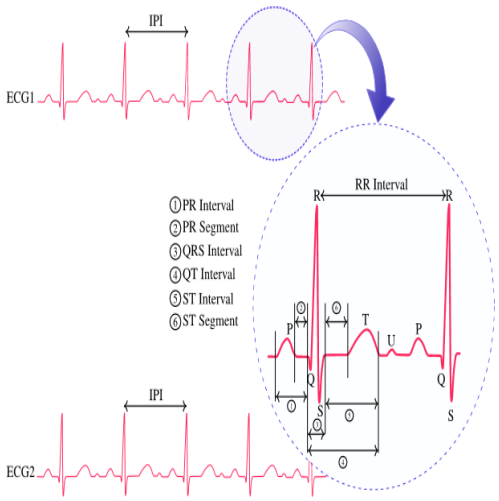

Fig. 2 Physiological Data and its Features

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. PREVIOUS WORK

The discussion of the previous work along with its salient features illustrates the contemporary techniques.

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. The database used for the study is the MIT-BIT library wherein the Electro Cardiogram data is available in the form of .mat files and can be processed for analysis. Moreover, actual monitoring using the ECG monitoring device is also used. The security is based on the authentication provided by a random binary stream (RBS) which is 128 bits in length. 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 significance of the hamming distance lies in the fact that a large hamming distance ensures uniqueness in the data streams of separate individuals thereby making it less likely to match or confuse the receiver of the actual sender's identity. The entropy is significant since it tells us about the average information contained in a random bit stream. Thus high values of both hamming distance and entropy are envisaged.

Dodangeh et al in [2] proposed a wireless body area networks (WBANs) security mechanism for medical applications. It is shown that the data of patients is critical and needs to be safeguarded. It also focusses on the tier based mechanism for the Wireless Body Sensor Networks. It is also shown that the electrocardiogram based technique for securing the WBSN architecture is effective and light weight in nature too. Hence it can be employed in several applications. However, it is also very prone to disturbances and noises which need to be removed prior to computation of significant parameters ensuring the security of the data stream.

Arfaoui et al. in [3] presented a stochastic game for adaptive security in constrained wireless body area networks. It can be observed that there are several ways to secure the binary data transmission in the wireless sensor network. Generally a process is said to be random if the events comprising the process do no follow any pattern or governing rule. Moreover, its is necessary that the random binary stream generated for purpose of authentication is significantly random for possible attackers or adversaries yet not extremely complex for the actual receiver or data sink to decode. This necessitates the generation of a randomly varying data stream and which is also distinct enough for each user. The authors have used a stochastic game theory approach to generate the random data stream for the purpose of authentication.

Samanta et al. in [4] proposed a Dynamic Connectivity Establishment and Cooperative Scheduling mechanism for the WBSNs. Moreover, the designed WBSN was also aware of the Quality of Service (QoS) parameters. In the work, it is shown that it is significantly difficult to find the exact morphological features of the physiological signals extracted from the subject. It is often challenging to find the exact peaks in case the ECG is used as the physiological signal due the presence of disturbances. The quality of service (QoS) depends on several parameters such as the throughput

of the system, the bit error rate of the system, the latency of the system, the hamming distance, the entropy and the power consumption. The benefit of a QoS aware body sensor network is the fact that it can adapt to the prevailing conditions in the network and thereby enhance the performance.

Li et al. in [5], presented a 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. It was shown that serious threat of data security attacks due to the fact that data is shared among several sensing modules over free space and hence is not secured via guided transmission. The data thus transferred can be compromised and be attacked to adversaries who can silently either read and extract the data or even manipulate the data. Another chance remains the mechanism of denial of service to an authentic node in the network. The authors proposed a secure authentication mechanism for the sending and receiving ends of the networks.

III. METRICS FOR EVALUATION

The performance evaluation parameters are often taken as hamming distance and entropy. While entropy indicates the average information associated with the binary data stream, hamming distance is metric that ensures distinctability.

While receiving the data, this key is matched at the database and a match guarantees the authenticity of the data. It is extremely challenging for attackers to generate a duplicate of the ECG of the person and hence generation of a fake RBS is almost infeasible in real time applications.

The performance of the system is generally evaluated based on the following parameters:

1) **FMR:** False Match Rate: It is defined as:

$$FMR = \frac{No.of\ False\ Matches}{Total\ No.of\ Matches}$$

2) **GAR**: Genuine Acceptance Rate: It is defined as:

$$GAR = \frac{No.of\ Correct\ Matches}{Total\ No.of\ Matches}$$

3) **Hamming distance (H)**

Given two vectors u, v (bit streams) of length n, the hamming distance between u and v, d(u, v), is the number of places where u and v differ. Mathematically,

$$H = |U| - |V|$$

Hamming distance tells about the randomness of the data. It is necessary to obtain a high hamming distance so that the RBS from different persons are completely different and random. This ensures that data from different persons or attackers is NOT confused at the receiver.

4) **Entropy**

The entropy is computed for the random process as:

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

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.

Entropy tells about the average information content of random bit streams. If the randomness is high, the entropy is high. High randomness requires low probability values. So, the entropy should be as high as possible.

5) **Communication Overhead:** It is the amount of extra bits needed (apart from the original data to secure the transmission). It is defined as:

$$Overhead = \frac{Additional\ Bits}{Actual\ Data\ Size}$$

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 comprehensive survey on securing BANs is provided. The evaluation parameters have been shown as hamming distance and entropy. It is expected that the paper presents with an insight into possible propositions of improvement of the conventional techniques.

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 2021
[2] Peyman Dodangeh, Amir Hossein Jahangir, "A biometric security scheme for wireless body area networks" Elsevier 2020
[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 2019
[4] Amit Samanta, Sudeep Mishra, "Dynamic Connectivity Establishment and Cooperative Scheduling for QoS-Aware Wireless Body Area Networks" IEEE 2018
[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 2017
[6] Z Li, H Wang, M Daneshmand, "Secure and efficient key generation and agreement methods for wireless body area networks", IEEE 2017
[7] AA Omala, KP Kibiwott, F Li, "An efficient remote authentication scheme for wireless body area network", Springer 2017
[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