A Secure and Robust ECG Signal Transmission System for Cardiac Arrhythmia Identification

1st Kun Hua
Electrical Engineering Department
California Polytechnic State University
San Luis Obispo, California 93407, USA
kuhua@calpoly.edu

2nd Hansong Xu
School of Electronic Information and Electrical Engineering
Shanghai Jiao Tong University
Shanghai 200240, China
hansongxu@sjtu.edu.cn

3rd Tigang Jiang
School of Information and Communication Engineering
University of Electronic Science and Technology of China
Chengdu, Sichuan, 611731 China
jtg@uestc.edu.cn

***Abstract*—This paper proposes a dynamic encryption method for cardiac arrhythmia identification based on electrocardiogram (ECG) signal classification, which is collected from a Wireless Body Area Network (WBAN). We extract five features from collected ECG signals to modify the accuracy of the K Nearest Neighbor (KNN) classifier. KNN gives better performance with the features compared with other classifiers. From our proposed dynamic encryption method in this paper, time-varying encryption keys are provided for the security of consecutive ECG data frames, and Alamouti-based cooperative relays are applied for transmission robustness under noisy transmission channels.**

***Keywords*—Wireless Body Area Network (WBAN), cardiac arrhythmia, electrocardiogram (ECG)**

I. INTRODUCTION

Wireless Body Sensor Network (WBSN) is widely applied for health monitoring. For most health problems, early identification and detection will reduce the probability of health deterioration even death. Cardiac arrhythmia causes most of the sudden cardiac death (SCD) worldwide, according to the American Heart Association [1]. Cardiac arrhythmia can be detected and identified based on ECG signal analysis through WBSN in the following steps. First, many on-body sensors are placed on patients for biomedical monitoring. Second, smart devices (smartphones) are taken as terminals, to receive and transmit biomedical signals from on-body sensors to authorized doctors. Then, the received biomedical signal can be analyzed for cardiac arrhythmia identification. Generally, to monitor ECG signals, high computing rates, security, and robust communication methods are needed for ECG collection and transmission [2].

To identify cardiac arrhythmia, five statistical features, which are R-R interval, P-R interval, QRS complex, Q-T interval, and S-T interval, are extracted from both cardiac arrhythmia ECG and normal ECG signals. Individually, those features are calculated from the peak distance between five individual peaks 'P' 'Q' 'S' 'T' and 'R' peaks in each cardiac cycle of collected time domain ECG [3]. Those statistical features are used as KNN classifier training data sets. Compared with wavelet transform for feature extraction, time domain analysis has less computation duty, plus it provides reasonable contribution for classification as well [4]. In this paper, we modified the KNN classifier for cardiac arrhythmia identification after training from the five features. Meanwhile, the training process, which inputs a set of features and this feature's class, is simple yet effective. Also, KNN has been used for bio-medical signal classification for much research [3] [5], due to its simple process and powerful results. KNN classifies new classes based on the distance between new data points and training cases. The smallest distance may have the best similarity of the according class.

After the collected ECG is identified as cardiac arrhythmia, the patient needs immediate help from the doctor. Then, the complete period of ECG signal should be sent to doctors immediately regardless of the energy cost, its communication duty should be placed as the highest priority, due to the danger of cardiac arrhythmia.

Also, we proposed our dynamic encryption method to improve the security of ECG signal transmission. Since the traditional 'RSA' has the limitation of private keys and public keys selection [6]. While our 'Dynamic RSA' method picks public keys and private keys from time-varying biomedical (ECG) recording key sets. In this way, the public keys and private keys are dynamically changing based on the individual and time-varying biomedical signal. So, it will be even harder for the eavesdroppers to detect and intercept patient's information.

However, somehow, due to the impact of a complex environment (white Gaussian noises, channel fading), the target signals could not be always transmitted with the promised quality. Even the transmission system is not robust enough to handle strong noises, which may lead to medical care accidents. To improve the quality and robustness of the transmission system, we considered cooperative relays with the Alamouti coding scheme for encrypted ECG signal transmission [7]. The Bit Error rate (BER) is derived significantly from our combination cooperative relays.

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

Overall, our assessment is achieved by the following steps.

(1) On-body sensors collect ECG signals from patients.

(2) Preprocessing and KNN identification for the collected ECG signal on the smartphone.

(3) Cardiac arrhythmia is detected, with 'Dynamic RSA' encryption for collected ECG.

(4). Find a cooperative relay, and transmit encrypted ECG with Alamouti coding, which is shown in Fig 1.

In the remainder of this paper, section II shows the peer work on related topics. Section III analyzes the system model. The simulation results are shown and analyzed based on the proposed methods in section IV. The conclusions are discussed in section V.

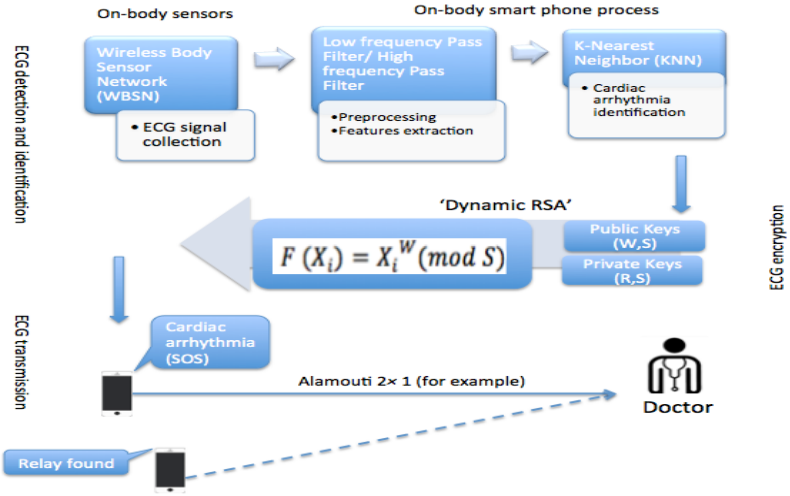

Fig 1. The general process of our system

II. PEER WORK REVIEW

Wireless Body Sensor Networks (WBSN) are widely used for real-time monitoring of ECG signals, emphasizing improvements in security and energy efficiency through the strategic allocation of unequal resources. The ECG signal is partitioned into two blocks, with varying degrees of importance. An unequal distribution of resources, including energy, communication rate, and security levels, is then employed to optimize energy usage while maintaining communication reliability [2].

Given the critical nature of cardiac arrhythmias and their potential fatality, the study underscores the necessity for robust protection and secure transmission of ECG signals. The classification of cardiac arrhythmias leverages statistical features extracted from ECG signals. The statistical features derive from different combinations of RR intervals, heartbeat intervals, and morphology.

Paper [8] studies the Alamouti-based cooperative relays for information transmission. We can assume that cooperative relays as virtual versions of Multi-Input and Multi-Output (MIMO). We are using founded relays (smartphone) as user #2 to cooperatively transmit rather than using multi antennas. Their proposed modified Alamouti-based cooperative scheme gives great BER performance, spatial gains, and diversity gains compared with other communication methods such as Maximum Ratio Combining (MRC), etc. At the same time, the biomedical signal (ECG) transmission should have higher security protection compared to multi-media signals (audio, video, text). So, we induced 'Dynamic RSA' for our ECG encryption.

III. METHODOLOGY

Due to the importance of heart problems, the original ECG signal should be sent out immediately with highly secure and robust encryption and transmission technologies, such as a Wireless Body Area Network (WBAN) to monitor ECG signal and analyze early identification for cardiac arrhythmia. We separate the whole task into three steps: (1) Noise removal and feature extraction of ECG signal; (2) Smartphone-based cardiac classification and encryption (early identification); (3) encoding identified ECG signals.

A. Pre-processing and classification for ECG signal.

ECG signals are detected and collected from the on-body sensors and analyzed at the on-body smartphone. The electrical noise, muscle noise, and unstable DC offset are the main noises that should be filtered out and removed. Since the biomedical signal($10\mu V\ to\ 5mV$) are weak yet sensitive, compared to other natural or artificial noises. We use Low-Frequency Pass Filters (LPF) and High-Frequency Pass Filters (HPF) to remove the effect of the external noises separately [9]. HPF removes DC offset and baseline wonder of ECG signal, and LPF removes the muscle noises.

Five statistic features, (P-R interval, R-R interval, Q-T interval, QRS complex, and S-T interval respectively) are extracted from the filtered ECG signal for estimation of the cardiac arrhythmia [3]. The filtered cardiac arrhythmia signal and five features for both cardiac arrhythmia and normal ECG are shown in Fig 2.

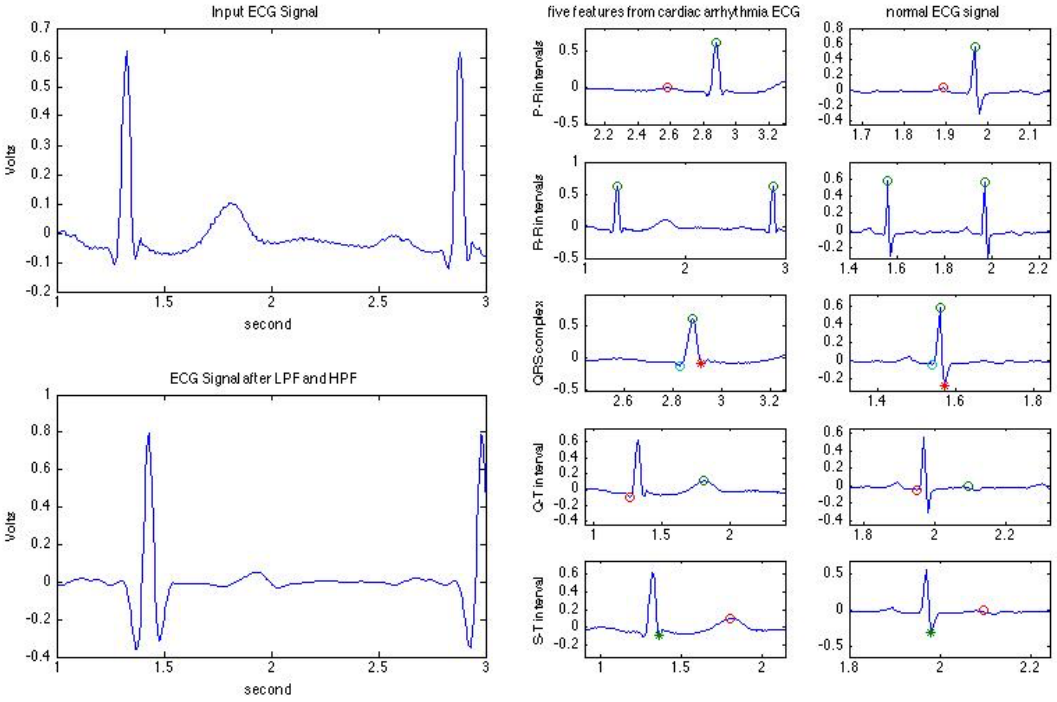

Fig 2. Preprocessing of ECG signal and feature extraction

The left part of Fig 2 shows the collected ECG signal and the results after the LPF and HPF are applied. Those five features are extracted from both cardiac arrhythmia and normal signals, which are shown on the right side of Fig 2. In our paper, the P-R interval is calculated from the peak distance in one cardiac cycle of the P wave and R wave. The R-R interval is calculated from the peak distance of two continuous heartbeats. QRS complex is calculated from the peak distance of Q and S wave containing the R peak in one cardiac cycle. Q-T interval and S-T interval are calculated from the peak distance of Q and S waves to T wave separately.

The KNN classifier is instance-based learning, which brings less computational burden with reasonable classification accuracy, compared with Vector Machine (SVM) and Artificial Neural Networks (ANN) [10]. In this paper, training sets for KNN classification can be represented as a $\{(Xc_1, Xn_1), \cdots, (Xc_T, Xn_T)\}$, in which totally $'n'$ data sets are used for training. Five features from both cardiac arrhythmia and normal ECG are stored at ith training sample $X_T = (Xc_T, Xn_T), T \in [1{:}T]$. $'Y'$ contains the corresponding labels: 'cardiac arrhythmia' and 'normal'. For collected ECG $'X_i'\ i \in [1, M]$, $\{d(X_T, X_i)\}$ shows the distance metric between training sets $'X_T'$ and testing data $'X_i'$, which can be classified to Y labels with following structure.

$$Y = \underset{i}{argmin}\left(\sum d(X_T, X_i)\right) \tag{1}$$

$$d(X_T, X_i), T \in [1{:}T] i \in [1, M] \tag{2}$$

Where $'T'$ and $'M'$ are the training vectors and testing vectors. The distance metric is calculated based on the 'Euclidean distance'.

$$D(i) = d(X_T, X_i) = \sqrt{\sum_{T=1,i=1}^{T,M} (X_T - X_i)^2} \tag{3}$$

Testing vector X_i belongs to the class where $D(i)$ is minimum. Also, we compared the performance of K ranging from 1 to 10, and K was chosen with the optimal accuracy rate. Once the input ECG signal X_i is classified to the 'cardiac arrhythmia' class, it must be sent out to the authorized doctor from the on-body smartphone for further assistance immediately. While, in the real world, the channel condition is always complex and even severe. In this case, encryption and protection methods are necessary to improve transmission security and quality.

B. ECG signal encryption with 'Dynamic RSA'

The protection of ECG signals to avoid interception and detection from eavesdroppers is highly required. First, the 'RSA' has already been widely applied as a standard information security method for many years. Second, it has been successfully applied for secure ECG signal transmission, and it brings reasonable

improvements to security transmission. In this case, we propose a creative 'Dynamic RSA' for ECG signal encryption.

The 'RSA' is a system that has a group of publish keys and private keys. Every user has its own encryption keys and decryption keys. And they make their encryption keys known to the public named 'public keys', while keeping the decryption keys private called 'private keys'. The process is shown as the 'Dynamic RSA' algorithm below. Our private key sets are selected from transmitted ECG features accordingly, which are Shown in Table 1 below.

TABLE 1 PRIVATE KEY SELECTION SETS

$K_0(initial)$	$X_1(PR, RR, QRS, QT, ST)$
$K_1(n)$	$X_2(PR, RR, QRS, QT, ST)$
$K_2(n)$	$X_3(PR, RR, QRS, QT, ST)$
$K_3(n)$	$X_4(PR, RR, QRS, QT, ST)$
⋮	⋮
$K_i(n)$	$X_{i-1}(PR, RR, QRS, QT, ST)$

C. *Encryption Steps*

Input: X_i, $K_i(n)$,

Output: $F(X_i)$

(1) Create a set of private keys from the information of the calculated time domain features in X_i.

$$\left(X_{i-1}(PR, RR, QRS, QT, ST)\right) \rightarrow K_i(n), i \in [1:M].$$

(2) Find two prime numbers $p, q \in K_i(n)$ for $'X_{i-1}'$ data frame, with condition of $S = p \times q, F(s) = (p-1)(q-1)$. The public key can be set as $(W, S), W \in [1, F(S)]$.

(3) The encrypted ECG signal can be expressed as $F(X_i) = {X_i}^W (mod\ S)$. $F(X_i)$ is the target encrypted ECG signal that needs to be transmitted immediately.

(4) Receiver can decrypt the received ECG signal by their own private key (R, S), R can be calculated as $R = e^{-1}(mod(p-1)(q-1))$, the decrypted ECG X_i can be calculated as $X_i = F(X_i)^R (mod\ S)$.

According to the above algorithm, private key sets $K_i(n)$, which provided the time varying private key (R, S) and public key (W, S)' features. In this case, the advantage of dynamic time varying of private key sets can be maintained. It will be more difficult for eavesdroppers to detect and intercept. The process of encryption for each data frame can be shown in the equation below.

$$F(X_1) = {X_1}^{K_0(n)} (mod\ S)$$

$$F(X_2) = {X_2}^{K_1(n)} (mod\ S)$$

...

$$F(X_i) = {X_i}^{K_{i-1}(n)} (mod\ S)$$

...

$$F(X_M) = {X_M}^{K_{M-1}(n)} (mod\ S) \quad (4)$$

Fig 4 shows an example of the proposed 'dynamic RSA' encryption scheme for cardiac arrhythmia ECG signals. We can observe that the encrypted code is a time-varying variable during the process of transmission.

D. *ECG signal transmission with Alamouti-coded cooperative relays*

The bio-medical signal is accordingly weak but meaningful. Especially for real-time ECG signal monitoring based on cardiac arrhythmia identification. A secure and robust communication method is required to conquer long-distance distortion and noisy channels. In this paper, we use the virtual Multi-Input Multi-Output (MIMO) technique via relays to improve the quality of transmission (quality of service (QOS)). A case study of Alamouti 2×1 coding is applied in this paper [11]. From the transmitter (U1) to the destination (D), one relay (R1) is added for cooperative transmission. As shown in Fig 3 below.

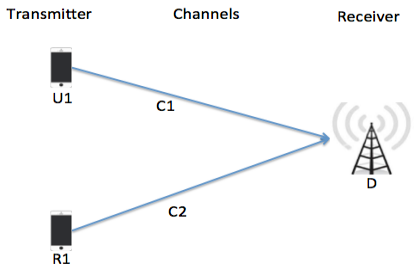

Fig 3. Alamouti 2×1 communication model

We assume that the fading channel (f) and the Gaussian noises (n) are added at the transmission channels C1 and C2. Alamouti code for ECG $K_i(n)$ encryption is listed in Table 2.

TABLE 2 ALAMOUTI CODING TABLE

	U1	R1
T=0	$F(X_1)$	$F(X_2)$
T=0+t	$-F(X_2)^*$	$F(X_1)^*$

The receiver side D received the Alamouti encoded ECG following the equations below with the Gaussian noise n1, n2.

$$D1 = C1(F(X_1)) + C2(-F(X_2)^*) + n1 \quad (5)$$

$$D2 = C1(F(X_2)) + C2(F(X_1)^*) + n2 \quad (6)$$

The signal can be expressed as a matrix below.

$$\begin{bmatrix} D1 \\ D2 \\ D3 \\ \vdots \\ D \end{bmatrix} = \begin{bmatrix} \begin{Bmatrix} F(X_1(j)) \\ -F(X_2(j)) \end{Bmatrix} & -F(X_2(j))^* & F(X_1(j+1)) & -F(X_2(j+1))^* & \begin{matrix} F(X_1(j+n)) \\ \cdots \\ -F(X_2(j+n)) \end{matrix} & -F(X_2(j+n))^* \\ \begin{Bmatrix} F(X_3(j)) \\ -F(X_4(j)) \end{Bmatrix} & -F(X_4(j))^* & F(X_3(j+1)) & -F(X_4(j+1))^* & \begin{matrix} F(X_3(j+n)) \\ \cdots \\ -F(X_4(j+n)) \end{matrix} & -F(X_4(j+n))^* \\ \begin{Bmatrix} F(X_5(j)) \\ -F(X_6(j)) \end{Bmatrix} & -F(X_6(j))^* & F(X_5(j+1)) & -F(X_6(j+1))^* & \begin{matrix} F(X_5(j+n)) \\ \cdots \\ -F(X_6(j+n)) \end{matrix} & -F(X_6(j+n))^* \\ & & \vdots & & & \\ \begin{Bmatrix} F(X_{M-1}(j)) \\ -F(X_M(j)) \end{Bmatrix} & -F(X_M(j))^* & F(X_{M-1}(j+1)) & -F(X_M(j+1))^* & \begin{matrix} F(X_{M-1}(j+n)) \\ \cdots \\ -F(X_M(j+n)) \end{matrix} & -F(X_M(j+n))^* \end{bmatrix} \times \begin{bmatrix} C1 \\ C2 \\ C3 \\ C4 \\ C5 \end{bmatrix} + \begin{bmatrix} n1 \\ n2 \\ n3 \\ n4 \\ n5 \end{bmatrix}$$

$$, (j+n) \in length(X_i) \tag{7}$$

TABLE 3 KNN CLASSIFIER PERFORMANCE AND FEATURE VALUES

Cardiac arrhythmia	P-R interval	QRS complex	Q-T interval	R-R interval	S-T interval	Accuracy rate
Group1	0.62129	0.60525	1.0705	1.6024	0.46525	98.51%
Group2	0.4151	0.31741	1.0246	1.8119	0.70721	99.50%
Group3	0.49709	0.3858	0.87266	1.6573	0.48687	88.56%
Group4	0.48104	0.34027	0.81418	1.6059	0.47391	98.01%
Group5	0.68408	0.78821	1.0594	1.3757	0.27119	97.51%
Group6	0.62129	0.60525	1.0705	1.6024	0.46525	99.50%
Normal1	0.078284	0.038383	0.56993	0.42405	0.53154	99.50%
Normal2	0.080075	0.044552	0.55711	0.41139	0.51256	99.50%
Normal3	0.082363	0.043706	0.56858	0.40998	0.52488	100%
Normal4	0.08495	0.046368	0.5991	0.43356	0.55274	99.50%
Normal5	0.087114	0.049353	0.65333	0.47741	0.60398	99.50%
Normal6	0.078284	0.038383	0.56993	0.42405	0.53154	99.50%

IV. EXPERIMENTAL RESULTS

We evaluate our proposed KNN classifier with the data from the MIT-BIH cardiac arrhythmia database [18]. A total of 6+6 groups of ECG signals (from both cardiac arrhythmia and normal) were used for testing. We can observe from the results that the accuracy rate of our proposed KNN classifier is as high as 99.50% for cardiac arrhythmia, which is much better than NNs (83.5%), although they are using NNs for classification accuracy evaluation after different compression. The best accuracy rate is 97.4% since they have five classes. Also, the accuracy rate is as high as 96% from the SVM. Since we are using the simplest and less computational duty classification method, this proposed classification system is robust for a more stable accuracy rate. Classification results are shown in Table 3, based on the peak distance in Fig 3, Group (1-6) and Normal (1-6) are testing data sets for both cardiac arrhythmia and normal ECG. The result shows that the average accuracy is 96.93% for cardiac arrhythmia with a maximum of 99.50% and a minimum of 88.56%.

To evaluate our proposed 'Dynamic RSA' encryption method, we take two different prime numbers from our biomedical signal key sets. Two groups of public keys and accordingly private keys are used for encryption, which are ((3,33) (7,33)) and ((17,33) (13,33)). Results are shown in Fig 4. To improve the transmission quality of the encrypted ECG signal, we applied cooperative relays. Fig 5 shows that the BER performance can be improved by adding more relays. In Fig 6, by comparing the no relay performance with (2×1) one relay Alamouti coding, we can find the symbol error rate of the relayed system is improved obviously. Fig 7 shows in total $9 + 9$ *groups* of ECG signals are used to measure the classification accuracy under different levels of noise. The upper figure shows that the classification accuracy is below 90% when the BER is equal to or smaller than 6dB. The lower figure shows that when BER is lower than 8dB the classification accuracy is below 90%. To improve the robustness of the cardiac arrhythmia identification system, we considered the Alamouti-based cooperative relays.

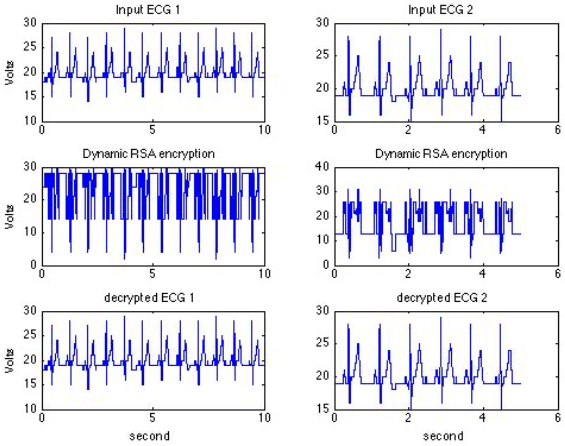

Fig 4. 'Dynamic RSA' encryption and decryption

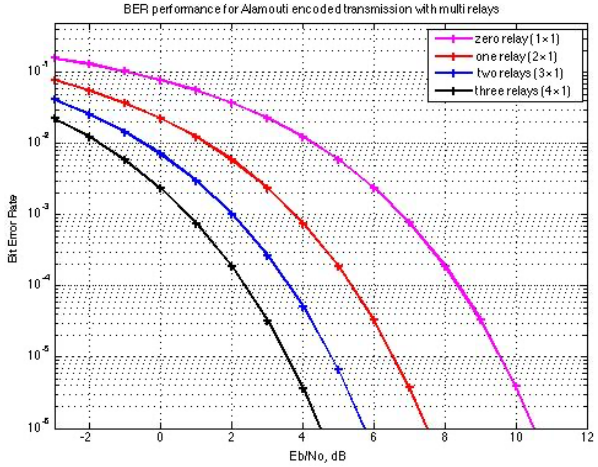

Fig 5. BER performance for multi relays (n×1)

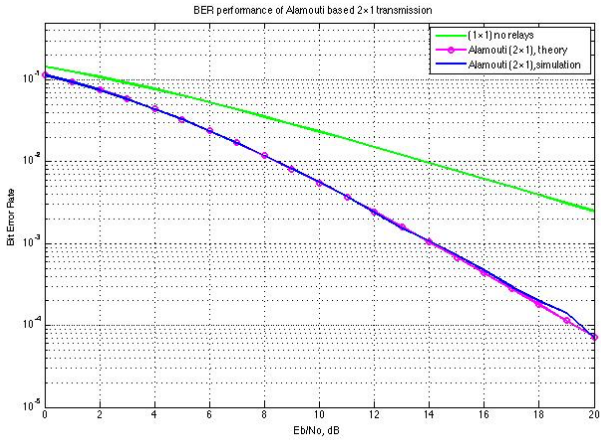

Fig 6. Alamouti-based (2×1) cooperative relay

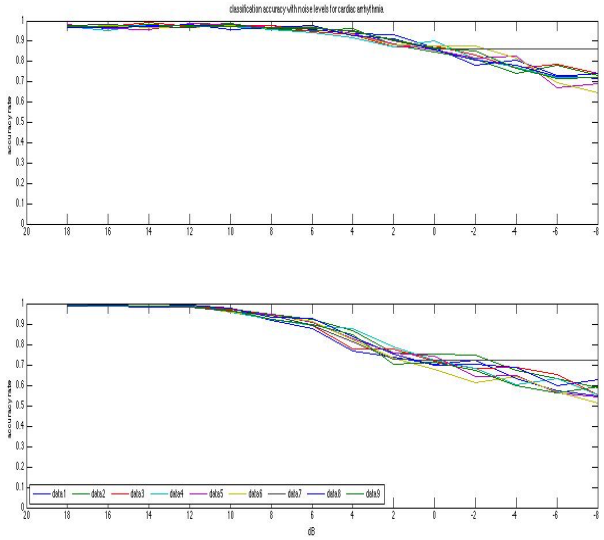

Fig 7. Classification accuracy for cardiac arrhythmia and normal ECG with noise levels of 20 to -6dB

The experiment results show that our proposed method for cardiac arrhythmia identification will achieve the optimal accuracy rate. Meanwhile, our 'Dynamic RSA' makes the transmission more secure through biomedical (ECG) signal encryption and the Alamouti-based cooperative relay methods improved the robustness of the transmission system as well.

V. Conclusion

This paper introduced the KNN-based approach of cardiac arrhythmia identification through Wireless Body Sensor Networks and analyzed feature extraction and selection for the KNN classifier. Our proposed scheme can achieve an average 96.93% classification accuracy for cardiac arrhythmia, which is reasonable and optimal, compared to NNs and SVM. Besides, we proposed the 'Dynamic RSA' encryption method, which offers public keys and private key sets from time-varying biomedical information. The robustness and security of ECG signal communication are improved through cooperative relays and Alamouti coding.

References

[1] Flores-Calero, M. and Almeida, C., 2023. Sudden Cardiac Death detection by using a hybrid method based on TWA and dictionary learning: A data experimentation. IEEE Access.

[2] Hartmann, M., Hashmi, U.S. and Imran, A., 2022. Edge computing in smart health care systems: Review, challenges, and research directions. Transactions on Emerging Telecommunications Technologies, 33(3), p.e3710.

[3] Wang, B., Chen, G., Rong, L., Liu, Y., Yu, A., He, X., Wen, T., Zhang, Y. and Hu, B., 2022. Arrhythmia Disease Diagnosis Based on ECG Time–Frequency Domain Fusion and Convolutional Neural Network. IEEE Journal of Translational Engineering in Health and Medicine, 11, pp.116-125.

[4] Brusa, E., Delprete, C., Gargiuli, S. and Giorio, L., 2022. Screening of Discrete Wavelet Transform Parameters for the Denoising of Rolling Bearing Signals in Presence of Localised Defects. Sensors, 23(1), p.8.

[5] Swapna, M., Viswanadhula, U.M., Aluvalu, R., Vardharajan, V. and Kotecha, K., 2022. Bio-signals in medical applications and challenges using artificial intelligence. Journal of Sensor and Actuator Networks, 11(1), p.17.

[6] Zhao, J., 2023, January. DES-Co-RSA: A Hybrid Encryption Algorithm Based on DES and RSA. In 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA) (pp. 846-850). IEEE.

[7] Ma, S.C., Alkhaleefah, M., Chang, Y.L., Chuah, J.H., Chang, W.Y., Ku, C.S., Wu, M.C. and Chang, L., 2022. Inter-Multilevel Super-Orthogonal Space–Time Coding Scheme for Reliable ZigBee-Based IoMT Communications. Sensors, 22(7), p.2695.

[8] Kun Hua, Honggang Wang, and Wei Wang "Alamouti Based Cooperative Wireless Networks for Multiplexing-Diversity Balanced Multimedia Transmission" Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, 27-31 Aug. 2012, PP 803 - 807

[9] Zhang, G., Garrett, D.R. and Luck, S.J., 2023. Optimal Filters for ERP Research I: A General Approach for Selecting Filter Settings. bioRxiv.

[10] Latif, G., Ben Brahim, G., Iskandar, D.A., Bashar, A. and Alghazo, J., 2022. Glioma Tumors' classification using deep-neural-network-based features with SVM classifier. Diagnostics, 12(4), p.1018.

[11] Zhai, C., Li, Y., Wang, X., Zheng, L. and Li, C., 2023. Wireless Powered Cooperative NOMA With Alamouti Coding and Selection Relaying. IEEE Transactions on Mobile Computing.