ABSTRACT

People with chronic illnesses such as cardiovascular disease, stroke and diabetes can be continuously monitored with the help of Remote Patient Monitoring (RPM) systems. RPM is a form of telehealth that uses small sensor nodes to collect medical data from remote patients and telecommunications to deliver the collected data to healthcare systems. The sensor nodes that are wearable or implanted in a patient's body constitute the medical Body Area Sensor Network (BASN). These sensors transmit the collected data wirelessly to the master node located on the patient's body. The master node forwards the data to a centralized repository, where diagnosis of arrhythmia class is performed and alerts are sent to healthcare providers.

The major concerns in RPM systems developed to monitor cardiac patients are handling of sensitive medical data and identification of the correct arrhythmia class. As per the Health Insurance Portability and Accountability Act (HIPAA), medical applications should guarantee data privacy and security. Complex cryptographic algorithms are not suitable to secure the communication in BASNs due to the low computational capability of sensor nodes. Alerts are sent to healthcare providers based on the condition of the cardiac patients. Hence, accurate identification of the arrhythmia class is very important. Existing arrhythmia classification techniques report low accuracy for a few arrhythmia classes due to class overlap and class imbalance problems.

The proposed work analyzes the suitability of ECG signals for 128-bit cryptographic key generation. The advantage of using ECG signals for key generation is that it eliminates the necessity of an additional random

number generator. The Inter Pulse Intervals (IPI) of ECG signal captured from the patient's body is converted to binary sequence using modular encoding. Based on the number of bits encoded from each IPI, 10-128 IPIs are used to generate a 128 bit binary sequence. The generated 128-bit binary sequence is tested for randomness and distinctiveness. Randomness is tested using the following statistical tests: Frequency test, Block test and Runs test, and the entropy test. The distinctiveness of the generated key is tested using the Hamming distance obtained. The results illustrate that thirty seconds of an ECG signal can generate highly random and distinctive 128-bit cryptographic key.

The generated cryptographic key has to be agreed upon by the communicating sensors in order to achieve secure inter-sensor communication in a BASN environment. Improved fuzzy vault scheme is proposed to minimize the false acceptance rate, false rejection rate and correlation attack. The sender node generates a d^{th} order polynomial in which the generated cryptographic key is embedded on the coefficients of the polynomial (i.e) concatenation of the polynomial coefficients provide the key to be shared. The feature vector of the sender is generated by the concatenation of Fourier transform coefficients and peak index values. Each sender feature is evaluated on the polynomial and a set of valid points is created. A set of chaff points is generated in the same range as that of the valid points and a vault is created. Chaff points are placed such that they are apart from the valid points by an interval value calculated using template. The receiver node tries to compute the actual polynomial from the vault with the help of its own receiver feature set. A minimum of d+1 matching elements should be present between sender and receiver nodes to successfully reconstruct the polynomial. The results demonstrate that a polynomial of order ‘8’ minimizes both False Acceptance Rate (FAR) and False Rejection Rate (FRR).

The possibility of correlation attack by intruders to find the valid points by correlating two or more previously transmitted vaults is prevented in the proposed research work by generating transform vectors using the shared key of the previous communication. Half Total Error Rate (HTER) of the proposed fuzzy vault method is reduced by 25% when compared to the existing methods.

The arrhythmia classification of the ECG signals received from the master node is performed at the aggregation unit. Arrhythmias are classified into five classes, namely: non-ectopic beat (N), supra ventricular ectopic beat (S), ventricular ectopic beat (V), fusion beat (F) and unknown beat (Q) by ANSI / AAMI EC57: 2012standard. The algorithms used for arrhythmia classification incorporate preprocessing, feature extraction, and classification. The noises that degrade the classifier performance are eliminated by preprocessing the recorded ECG signals. The proposed work uses Discrete Wavelet Transform (DWT) for denoising the ECG signal.

Subsequent to denoising, the continuous ECG waveform is segmented into individual heartbeats. Temporal features and morphological features are extracted from segmented ECG recordings. Pre R_R interval, post R_R interval and average R_R interval constitute the temporal features. The coefficients of Fourier transform, Wavelet transform and Stockwell transform comprise the morphological features. Performance evaluation of the extracted feature set illustrates that fusion of temporal features and Daubechies wavelet transform based features provide better results when compared to other feature extraction methods.

Effect of unsupervised Dimensionality Reduction (DR) techniques on reducing the dimension of the feature vector for arrhythmia classification is analysed.Experimental results revealed that the conventional, linear DR technique like PCA is easy to apply, but is not able to capture important information required for class discrimination from low dimensional data representation. Nonlinear techniques are able to capture significant information from the lower dimensional representation itself. At the same time, nonlinear techniques face the important drawback that they require the tuning of parameters. Analysis outcomes show that the mixture of PNN classifier (at spread parameter, $\sigma = 0.4$) and fastICA DR technique with tangential contrast function produce highest F-score of 99.83% with ten dimensions. hNLPCA and KPCA require more computation time for low dimensional mapping. F-score of PPA is around 10% greater than PCA and serves intermediate among linear and nonlinear DR techniques.

A hierarchical classification model is proposed to classify arrhythmias. Classification utilizing KNN classifier is performed at the level 1 of the proposed model and the training of classifier includes samples from all five arrhythmia classes. SVM classifier is used for classification at Level 2 of the proposed model and is trained specifically to classify overlapped classes. The proposed KNN_SVM hierarchical model is used to make decision on arrhythmia class of a test heartbeat. The average sensitivity, specificity, positive predictivity, F-score and accuracy achieved for the proposed hierarchical model is 92.56%, 99.35%, 98.13%, 94.5% and 99.78% respectively.

Classification becomes complicated when class overlap and class imbalance problems occurs together. Non-overlapping features are identified from a set of extracted features using Fisher discriminant ratio based algorithm. The class imbalance problem is handled by using a

Gaussian Mixture Model based anomaly detection technique and sample deletion learning strategy. Multiclass PNN classifier is trained with GMM approved ECG samples. With the help of sample deletion learning strategy, McNN classifier removes redundant training samples. Hence, class imbalance issue is solved by McNN classifier. By reducing the total number of training samples, it is observed that the training time required for the multiclass classifier is reduced. The experimental results demonstrate that the proposed method using PNN classifier produce average sensitivity of 95.37%, average positive predictive value of 98.35% and average F-score of 96.72%. The values of the metrics when McNN is used are 96.7%, 94.15% and 95.29% respectively. The results show an improvement over the previously reported results for automated arrhythmia classification systems.