Reliable ECG Signals Based on GMM for Body Area Network

Ahmed Shoeb Al Hasan[1], Md. Hasan Tareque[2]

[1]Department of Computer Science and Engineering, Bangladesh University of Business & Technology, Bangladesh

[2]Department of Computer Science and Engineering, IBAIS University, Bangladesh

Abstract: ***A distinctive and natural trust region for protected data transportations in wireless healthcare systems such as body area networks is provided by the blood flow system in a humanoid body. Regrettably, biometric signal confirmation by biological characteristics in wireless healthcare has not been broadly studied. A data authentication method using electrocardiography (ECG) signal shapes for reducing key exchange overhead is proposed in this paper. Applying stochastic pattern recognition techniques in wireless healthcare is the key impact of this study. The inter-pulse interval (IPI) signal shape at source side is summarized as a biometric authentication key using Gaussian mixture model (GMM), in the suggested method. At the destination point, a light-weight signature authentication scheme is implemented that uses IPI signals gathered locally at the receiver. The suggested authentication scheme has the benefit of high sample misalignment acceptance. The proposed authentication approach achieves a low half total error rate in ECG signals verification.***

Keywords: Body area network, ECG, GMM, inter-pulse interval.

1. Introduction

Before going into the main topics we will recall some preliminary but very important terminology.

1.1 Body Area Network (BAN)

Systems where communication is entirely within, on and in the immediate proximity of a human body [1].

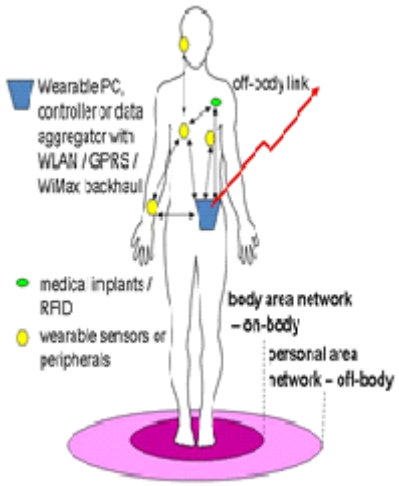

Figure 1: Body Area Network (BAN)

1.2 ECG

The use of the ECG for identity recognition has some key properties:

- The ECG signal attributes are uniquely different from person to person, making it desirable to differentiate incoming data packets from sensors on the same body and the sensors on different human bodies.
- ECG signals are difficult to counterfeit, in supervised conditions.

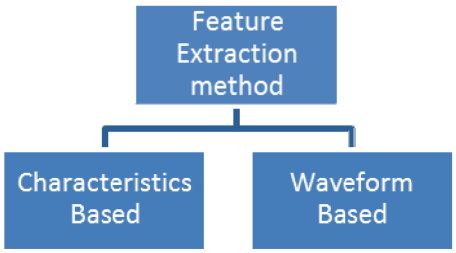

Figure 2: Feature Extraction methods of ECG

1.3 E-HealthCare System

E-Healthcare [2], [3] System is a term for healthcare practice supported by electronic processes and communication.

1.4 Gaussian Mixture Model (GMM)

GMM [4] is a statistical model widely utilized in classification, pattern recognition [5], speed/audio processing [6], user authentication [7], and image watermarking [8]. *o* is defined as *a d-dimensional biometric* authentication sequence (BAS) set including different features.

$$o = \{f1, f2. . . fd\},$$

with a total of *d elements, where fi denotes the* i^{th} *feature to* be modeled.

GMM statistic Eigen value λ, *which includes the weight w, mean* value μ, *and covariance matrix* Σ *of each Gaussian mixture* function $N(\cdot, \mu, \Sigma)$.

A GMM can be uniquely expressed as

$$\lambda = \{wm, \mu m, \Sigma m \mid m = 1, 2, . . . , M\}$$

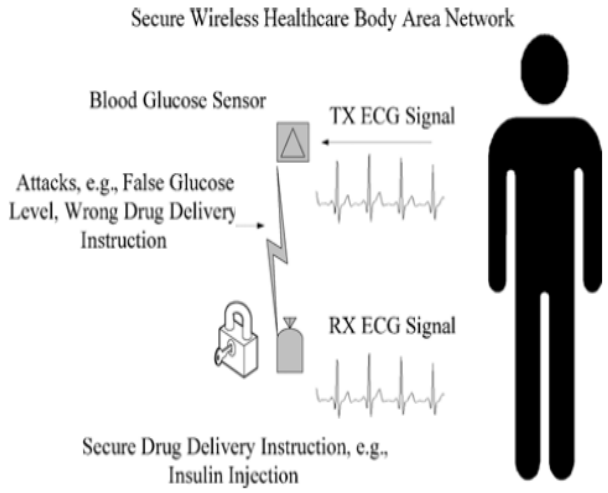

Figure 3: Secure and automatic insulin injection system in a BAN for diabetic patients.

1.5. IPI Signals for GMM-Based Authentication

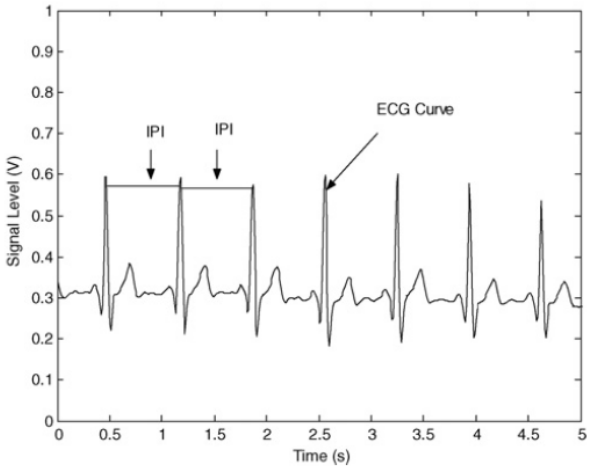

Figure 4: IPI data filtered by a 12th-order digital finite impulse response (FIR) low-pass filter with a cutoff frequency of 25 Hz. An FIR filter is used because the poor impulse response of the infinite impulse response filters may cause distortion.

$J(\lambda)$, a log-based likelihood function [9], [10] is defined as-

$$J(\lambda) = \sum_{i=1}^{n} \ln \sum_{m=1}^{M} w_m N_m(o_i).$$

Table 1: Notations used in this paper

Symbol	*Definition*
D	Message data unit or payload data exchanged among sensors
IPI, IPI'	IPI signals recorded at transmitter and receiver
O, O'	BAS for transmitter and receiver
λ	Stochastic attributes of GMM
$J(\lambda)$, $J'(\lambda)$	Log-likelihood function with λ representing the BAS of O and O
n	No. of sample points in discrete time domain
o, o'	BAS element in O and O
d	Dimension of variable o
M	No. of Gaussian mixture functions
w	Weight of Gaussian function
μ	Mean value of Gaussian function
$\sum$	Covariance matrix of Gaussian function
Θ	GMM signature abstraction process
Θ^{-1}	GMM signature verification process

2. Related Works

a) In 2006, C. Poon, Y. Zhang, and S. Bao,[1] in their paper "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," proposed:
- Secure key exchange scheme for BAN data encryption based on inter-pulse interval (IPI) signal pattern.
- The secret key was committed at the sender side using its own local IPI signals, and de-committed using receiver side IPI signals recorded at the same time.

b) In 1999, A. Juels and M. Wattenberg, in their paper [11] "A fuzzy commitment scheme," applied Fuzzy key commitment scheme to correct the errors in a recovered encryption key due to the slight IPI signal variations in different body locations.

c) K. Venkatasubramanian, A. Banerjee, and S. Gupta, in their paper [12] "Plethysmogrambased secure inter-sensor communication in body area networks," proposed :
- A photoplethysmogram (PPG)-based key agreement scheme to enable symmetric key-based secure inter-sensor communication by means of unique PPG.
- In that approach, a fuzzy vault was created using a secret key and the transmitter side PPG signals, and the receiver side PPG signals were used to unlock the vault to reconstruct the secret key.

d) S. Kaur, O. Farooq, R. Singhal, and B. S. Ahuja, in their [13] paper "Digital watermarking of ECG data for secure wireless commuication," proposed :
- a watermarking-based ECG signal tempering identification approach.
- A low frequency 15-digit chirp code is embedded in wirelessly transmitted ECG signal.
- That scheme can also completely remove chirp code watermarks from reconstructed ECG signal to minimize ECG visualization distortion.

e) M. Li and S. Narayanan, in their [14] paper "Robust ECG biometrics by fusing temporal and cepstral information," proposed :
- A robust ECG biometric approach for personal healthcare security.
- In this approach, temporal intra-heartbeat patterns of different individuals were modeled by Hermite polynomial expansion and support vector machine.
- In the frequency domain, spectral feature extraction was applied in conjunction with GMM to model short-time

ECG characteristics.

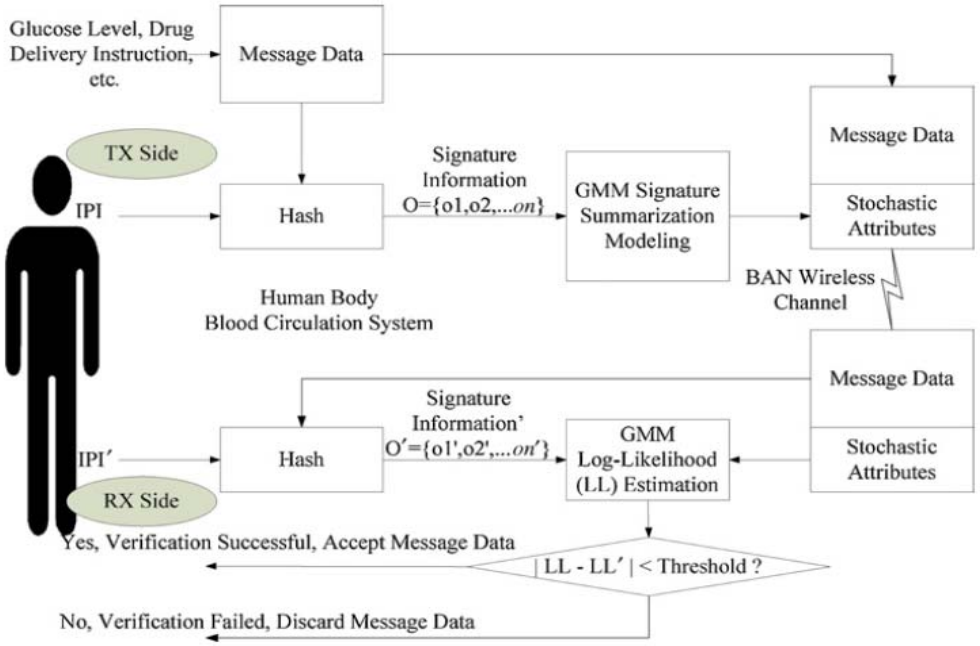

Figure 5: Proposed System Architecture

3. Proposed System

Two Steps:

- Signature Abstraction
- Signature Verification

3.1 Signature Abstraction

To create authentication signatures based on biometric IPI signals, we need to consider how to acquire the optimal stochastic [17] attributes *λ for GMM that maximizes the log likelihood J (λ), given the BAS O from IPI signals.*

Each *d × d-dimensional covariance matrix of the BAS is* expressed as a single unknown parameter *σ2 as follows:*

$$\Sigma_m = \sigma^2 \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & \\ \cdots & 0 & \cdots & 0 & \cdots \\ \cdots & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

The title of the paper is centered 17.
Then the GMM stochastic attributes *λ,* which need to be estimated, become:

$$\lambda = \left\{ w_1, \mu_1, \sigma_1^2, \cdots, w_M, \mu_M, \sigma_M^2 \right\}$$

Expectation-maximization (EM) algorithm is proposed to approximate the optimal parameters of the GMM which represents the BAS *O and transmitter side IPI signals.* A new posterior probability *βj (oi) is defined* [4],[7]-[9],[15] to simplify the BAS modeling EM algorithm.

$$\beta_j(o_i) = \frac{w_j N_j(o_i)}{\sum_{m=1}^{M} w_m N_m(o_i)}$$

βj (oi) denotes the probability that the *ith BAS point oi is created by* the *jth Gaussian mixture function.* First-order derivative of mean and covariance of each Gaussian mixture function be zero, in order to acquire the maximum value of the BAS likelihood *J (λ).*

Mean value, the covariance value, and the weight of each Gaussian mixture function in modeling the transmitter side BAS and IPI can be expressed as follows:

$$\mu_j = \frac{\sum_{i=1}^{n} \beta_j(o_i)\, o_i}{\sum_{i=1}^{n} \beta_j(o_i)}$$

$$\sigma_j^2 = \frac{\sum_{i=1}^{n} \beta_j(o_i)\,(o_i - \mu_j)'\,(o_i - \mu_j)}{d \sum_{i=1}^{n} \beta_j(o_i)}$$

$$w_j = \frac{\sum_{i=1}^{n} \beta_j(o_i)}{n}.$$

3.2 Signature Verification

The BAS at the receiver side is created using and the received data payload. The log-likelihood value at the receiver side *can be calculated as:*

$$J'(\lambda) = \sum_{i=1}^{n} \ln \sum_{m=1}^{M} w_m N_m(o_i')$$

The signature is efficiently verified if the dissimilarity Of J (**λ**) and J' (**λ**) is below a predetermined threshold value *T, such that*

$$\left| \frac{J'(\lambda) - J(\lambda)}{n} \right| \leq T.$$

4. Complexity Analysis

Suggested signing and verification processes effectively avoid extra communication expenses by removing the key exchange process. Rigorous sample synchronization requirement has been removed by the proposed process. There are four parameters important for determining the complexity cost of the proposed algorithm, i.e., *i, d, n, and M.*

The total amount of calculations for this algorithm is at an order of $O\ (iMnd^2)$.The major constraint for the complexity is the number of samples n. The complexity can be reduced significantly by decreasing the number of samples.

5. Limitations and Future Scope

The proposed system in this paper has intra-BAN secure communication. The inter-BAN and BAN to wireless local area network secure communications can be introduced.

6. Conclusion

A new reliable ECG signal security scheme is proposed to secure the communications inside a BAN. A GMM-based stochastic authentication scheme was developed utilizing the locally captured ECG-IPI signal to avoid key exchange overhead. A low-cost signature abstraction scheme based on EM algorithm was proposed to train the GMM with specific ECG signal patterns. A simple signature verification scheme was also developed to match the signature with receiver side ECG signal patterns. The proposed authentication scheme has a low authentication HTER even with low sample resolutions and small number of Gaussian mixtures under poor sample synchronization conditions. The proposed system has a deficiency that it only works for intra-BAN communication.

References

[1] C. Poon, Y. Zhang, and S. Bao, “A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health,” IEEE Commun. Mag., vol. 44, no. 4, pp. 73–81, Apr. 2006.
[2] K. Venkatasubramanian and S. Gupta, “Security solutions for pervasive healthcare,” in Security in Distributed, Grid, Mobile, and Pervasive Computing. Boca Raton, FL: CRC Press, 2007, pp. 443–464.
[3] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, “Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body,” in Proc. IEEE Int. Conf. Parallel Process. Workshops, Oct. 2003, pp. 432–439.
[4] J. Jang, “Gaussian mixture model,” in Data Clustering and Pattern Recognition [Online]. Available: http://mirlab.org/jang/books/dcpr.
[5] Bilik, J. Tabrikian, and A. Cohen, “GMM-based target classification for ground surveillance Doppler radar,” IEEE Trans. Aerospace Electron. Syst., vol. 42, no. 1, pp. 267–278, Jan. 2006.
[6] R. Huang and J. Hansen, “Unsupervised discriminative training with application to dialect classification,” IEEE Trans. Audio, Speech Language Process., vol. 15, no. 8, pp. 2444–2453, Nov. 2007.
[7] F. Cardinaux, C. Sanderson, and S. Bengio, “User authentication via adapted statistical models of face images,” IEEE Trans. Signal Process, vol. 54, no. 1, pp. 361–373, Jan. 2006.
[8] H. Yuan and X. Zhang, “Multiscale fragile watermarking based on the Gaussian mixture model,” IEEE Trans. Image Process., vol. 15, no. 10, pp. 3189–3200, Oct. 2006.
[9] J. Gauvain and C. Lee, “Maximum a posteriori estimation for multivariate Gaussian mixture observations of Markov chains,” IEEE Trans.Speech Audio Process., vol. 2, no. 2, pp. 291–298, Apr. 1994.
[10] D. Reynolds, T. Quatieri, and R. Dunn, “Speaker verification using adapted Gaussian mixture models,” Dig. Signal Process, vol. 10, nos. 1–3, pp. 19–41, Jan. 2000.
[11] Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proc. 6th ACM Conf. Comput. Commun. Sec., Nov. 1999, pp. 28–36.
[12] K. Venkatasubramanian, A. Banerjee, and S. Gupta, “Plethysmogram based secure inter-sensor communication in body area networks,” in Proc. IEEE MILCOM, Nov. 2008, pp. 1–8.
[13] S. Kaur, O. Farooq, R. Singhal, and B. S. Ahuja, “Digital watermarking of ECG data for secure wireless communication,” in Proc. Int. Conf. Recent Trends ITC, Mar. 2010, pp. 140–144.
[14] M. Li and S. Narayanan, “Robust ECG biometrics by fusing temporal and cepstral information,” in Proc. IEEE ICPR, Aug. 2010, pp. 1326–1329.
[15] M. Shi and A. Bermak, “An efficient digital VLSI implementation of Gaussian mixture models-based classifier,” IEEE Trans. Very Large Scale Integr. Syst., vol. 14, no. 9, pp. 962–974, Sep. 2006.
[16] W. Wang, K. Hua, M. Hempel, D. Peng, H. Sharif, and H. H. Chen, “A stochastic biometric authentication scheme using uniformed GMM in wireless body area sensor networks,” in Proc. IEEE Int. Symp. PIMRC, Sep. 2010, pp. 1620–1624.
[17] W. Wang, H. Wang, M. Hempel, D. Peng, H. Shareef, H. Chen, “Secure Stochastic ECG Signals Based on Gaussian Mixture Model for e-Healthcare Systems” in IEEE SYSTEMS JOURNAL, VOL. 5, NO. 4, DECEMBER 2011

Author Profile

Ahmed Shoeb Al Hasan is currently working as Lecturer in the Department of Computer Science & Engineering at Bangladesh University of Business & Technology (BUBT). He received B.Sc in CSE from Military Institute of Science & Technology (MIST), Bangladesh in 2010. Now he is pursuing M.Sc in CSE from Bangladesh University of Engineering & Technology (BUET). His research interest includes Network Security, Wireless & Mobile Communication Networks, Signal Processing, and Image Processing.

Md. Hasan Tareque received the B. Engg. degree from Bangladesh University of Professionals in 2010 and currently pursuing the M. SC degree with Bangladesh University of Engineering and Technology (BUET) in Computer Science & Engineering. He is currently a senior lecturer in CSE/CSIT department at IBAIS University. His current research interests include image processing, automated biometric technologies, artificial intelligence, wireless sensor networks, Algorithms, Robotics.