This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

An Integrated Biometric-based Security Framework Using Wavelet-Domain HMM in Wireless Body Area Networks (WBAN)

Honggang Wang, Hua Fang, Liudong Xing, Min Chen

***Abstract*— In this paper, an integrated biometric-based security framework is proposed for wireless body area networks, which takes advantage of biometric features shared by body sensors deployed at different positions of a person's body. The data communications among these sensors are secured via the proposed authentication and selective encryption schemes that require low computational power and less resources (e.g., battery and bandwidth). Specifically, a wavelet-domain Hidden Markov Model (HMM) classification method is utilized for accurate authentication based on the non-Gaussian statistics of ECG (electrocardiogram) signals. In addition, the biometric information such as ECG signal is used as the biometric key for the encryption in the framework. Our experimental results demonstrate that the proposed approach can achieve accurate authentication performance without extra requirements of key distribution and strict time synchronization.**

***Index Terms*— Wireless Body Area Networks, Hidden Markov Model, ECG.**

I. Introduction

The healthcare expenditure in the US is expected to increase from $2.9 trillion in 2009 to $4 trillion in 2015. The non-intrusive health monitoring of patients' vital signs over wireless body area networks (WBAN) provides a cost-effective solution to the healthcare system. A WBAN consists of a set of wireless wearable or implanted medical sensors into the human body for vital body signal monitoring. Currently, the WBAN technology is being widely investigated and still in its primitive stage. This technology could lead to the realization of such concepts as telemedicine and mHealth in the future. However, before the WBAN can be widely used in monitoring the health of humans, a critical question has to be answered: *Can the health and medical information provided by the body area networks be trusted?* This problem exists largely due to the lack of security in the operation and communication of resource-limited medical sensor nodes. In this paper, we explore the use of biometric features for the security protection mechanism of WBAN and propose a solution to address this security problem. Specifically, the intrinsic biometric features of a human body are regarded as the authentication identity to secure the distribution of a cipher key in WBAN communications. The biometric circulation system (e.g., blood) in a human body provides "virtual" channels to protect data transmissions in WBAN. The medical data generated from tiny WBAN sensors require secure transmission and limited access. For example, a patient's records are only sensed and derived from this patient's dedicated WBAN system and cannot be mixed with other patients.

In this work, we develop an integrated security system to secure medical information communications using biometric features of the body in WBAN, and apply a time-efficient classification model for data authentication. Specifically, the sender's ECG (electrocardiogram) feature is selected as the biometric key for the authentication since each patient has their unique ECG. A wavelet-domain Hidden Markov Model (HMM) is used to distinguish the biometric feature for the authentication. The use of wavelet-domain HMM avoids key distribution and time synchronization involved in the traditional security systems. Besides the authentication, a low-cost encryption method is proposed to achieve the communication confidentiality over WBAN. The encryption scheme in WBAN must be designed to be secure and accurate with low complexity and high power efficiency. Our proposed framework includes a selective encryption mechanism to protect data confidentiality by using biomedical information (e.g., ECG) as a key. The proposed biometric-based security system for data authentication and encryption is designed under resource constraints (e.g., battery and computation) of biomedical sensors. Our study in this paper is limited to the security protection for data transmissions over body area. The inter-WBAN and WBAN-WLAN (Wireless Local Area Networks) secure communications are beyond the scope of this paper, which can be addressed using traditional authentication or encryption schemes such as those proposed in [1] [2] [3].

II. Literature Review

Considerable efforts such as CodeBlue, MobiHealth, and iSIM [4–6] have been contributed to the development of WBAN in last several years. IEEE organizations such as 802.15.6 and 1073 have also worked on the solution of low power in-body and on-body wireless networks for medical applications. However, the security still remains a formidable challenge yet to be resolved. The security system over WBAN must be implemented with low computational complexity and high power efficiency. As nodes of WBAN are expected to be interconnected on or in the human

Honggang Wang and Liudong Xing are with the Department of Electrical and Computer Engineering at the University of Massachusetts, Dartmouth; Hua Fang is with the Department of Quantitative Health Science at the University of Massachusetts Medical School at Worcester; Min Chen is with Seoul National University.

978-1-61284-233-2/11/$26.00 ©2011 IEEE

body, the body itself can construct an inherently secure communication path that is unique and unavailable to other bodies. The biometric information collected from the human body can uniquely represent an individual and is time varied, which is hard to forfeit by suspicious intruders. These biometric features lay foundations for biometrics-based entity authentication in WBAN. Using these biometric signal can provide strong data security and integrity while eliminating costly key distribution [7]. It may serve as a substitution of public key infrastructure-based authentication, which is too expensive in terms of computation and energy consumption in resource-constrained WBAN. The focus of our study is on the problem of how sensors within a WBAN can utilize the biometric information and differentiate whether they belong to the same person or not. Since the circulation system of a human body naturally form a communication trust channel in which the integrity of data packets coming from the same individual can therefore be protected. Limited research works have been reported in literature regarding secure communications in WBAN utilizing biometric information. In [7], the authors provided a survey of security solutions in pervasive healthcare systems, where biomedical information was utilized for managing access to health information and for securing data collected by medical sensors. Cherukuri et al in [8] proposed a biometrics-based key distribution scheme to secure the inter-sensor communications on the same human body. A symmetric key (pseudo-random number) was generated for the encryption and decryption through error correction code that takes advantages of biomedical features simultaneously from different body locations. They claim that the traditional public key cryptography consumes more resources than the private key system does. The public key approach cannot be directly applied for medical sensors because they are limited in resources and computational capabilities. In [9], the authors proposed a similar symmetric cryptosystem in WBAN using Inter Pulse Interval (IPI) as the biometric feature. In [10], a fuzzy based key scheme was proposed to correct the errors caused by IPI signal variation in the recovered encryption key. Other similar research regarding biometric security in WBAN were found in [11] and [12], where biometric signals were encoded into a 128-bit sequence and the distinctness were measured. However, all of the above research works have focused on secret key distribution issues and require critical time synchronization with extra communication overheads when biometric information of the same human body cannot be available simultaneously. In our proposed approach, we specifically address the low cost authentication and encryption challenges by using biometric information, and propose a statistic HMM based verification scheme that eliminates the overheads caused by time synchronization.

III. HMM Based Authentication and Selective Encryption Approaches

Biometric information has been widely investigated in traditional security systems such as identity verification based on iris [13], fingerprint [14], face [15], handwriting [16]. Unlike traditional biometric cryptosystems in generic networks, the blood circulation system in a human body forms a unique secure communication path specifically available for WBAN [11]. The biometric information utilized in a WBAN should be ubiquitous, easy to collect and distinctive. The distinctiveness of those biometric signals for entity authentication can be effectively identified by statistical methods.

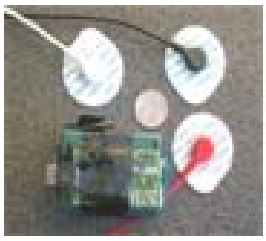

Fig. 1. ECG sensors developed for WBAN [17]

A. Biometric ECG Signals of Medical Sensors

In our previous works [17], we have built up a resource-aware body sensor network architecture to enable real-time ECG healthcare monitoring, especially for secure wireless electrocardiogram data streaming and monitoring. In this architecture, important information (e.g., critical ECG data) is identified, and extra resources are allocated to protect it. Furthermore, WBAN resource factors are exploited to guarantee a strict requirement of real-time performance. In this work, we integrate biomedical information sensing, processing and transmission in a unified platform, where data transmission in a WBAN proceeds with energy efficiency. In order to reduce common mode noises, a right-leg driver amplifier is used in the device to inject the common-mode. Our experiment show that there is very little signal distortion after digital filtering. The signal quality is comparable to that obtained by any existing commercial ECG device. ECG signal is an excellent candidate of biometric information which is desirable for cryptosystems in WBAN. However, the proposed solution is not confined to ECG signals. Other biometric signals can also be easily and smoothly incorporated into the proposed authentication scheme.

B. Authentication using HMM-based Classification Approach

Wavelet-domain Hidden Markov Model [19], the integration of wavelet transform and HMM, is a statistical model widely utilized in classification. It has been demonstrated that this approach has flexibility and adaptability, providing an efficient and powerful tool for generalized likelihood ratio testing. In this approach, given a signal observations from two or more classes of signals, we can train HMMs for each class c, and derive parameter θ_m. We use the trained HMM to detect and classify new ECG observation w by which one describes the new ECG observation best. Through computing the likelihood $f(w|\theta_m\}$ of the new

ECG signal observation for each HMM, we decide the class whose HMM provides the maximum likelihood.

$$f_w(w) = \sum_{m=1}^{M} ps(m) fw|s(w|S = m)$$

Wavelet-Domain based HMM structure is built upon the states of the wavelet coefficients and not on the coefficients themselves. The HMM classification approach includes three steps: training; likelihood determination and state determination. As shown in Figure 2, given a set of observed ECG wavelet coefficients $\{w_i\}$, the first step determines the wavelet-domain HMM parameters θ that best characterize the ECG wavelet coefficients.

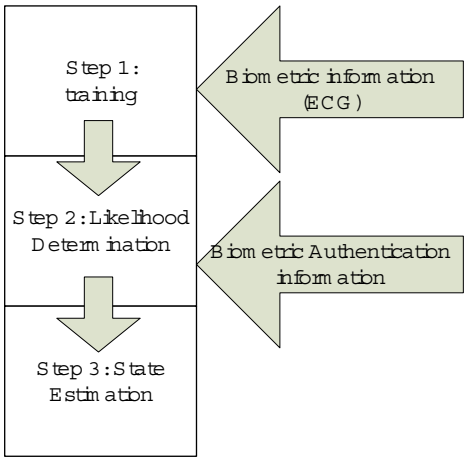

Fig. 2. Authentication using wavelet-domain HMM based classification approach

At Step 2, the likelihood of an observed set of wavelet coefficients $\{w_i\}$ is calculated based on a fixed wavelet-domain HMM with parameters θ. Step 3 determines the most likely sequence of hidden states $\{s_i\}$ for an observed set of wavelet coefficients $\{w_i\}$. To model the biometric information, we need to get the HMM statistics of ECG signal θ. The integration of wavelet transforms and HMM yields a flexible framework for generalized likelihood based classification that matches the inherent structure of real-world signals.

In our study, an integrated biometric-based security system is proposed to secure data communication channel over body area networks. It contains two major components: 1) A HMM-based authentication approach using statistic feature of biometric information; and 2) A selective encryption mechanism using biometric information as a shared key. To model the n-point biometric authentication information such as ECG, we need to find the statistical characteristics θ for HMM to achieve the maximum log-likelihood.

As shown in Figure 3, sensor s1 and s2 share the same biometric information used to secure the communication channel. The message authentication code can be generated with the input of biometric feature and hashes that are calculated based on the original message. At another site, sensor 2 recalculates the hash again based on the message. A HMM likelihood estimation algorithm is used to conduct the authentication process. If the received message matches the signal statistically (i.e., not significantly different), it will be accepted and authenticated. Otherwise, the message is denied and discarded. The key point of this technique is to utilize the statically same biometric information shared at any positions of human body.

C. Selective Encryption using Biometric Information

Authentication, by itself, can protect the integrity and authenticity of medical data. But other techniques such as encryption are still required to protect the confidentiality of messages in WBAN. Encryption approaches in WBAN must be designed to protect data transmission with low cost. In the proposed framework, we incorporate a low complexity and energy-efficient selective encryption mechanism in the biometric-based security system. Specifically, we propose a selective encryption scheme that provides an efficient security solution for data transmission over WBAN. As discussed in our previous work [18][20], the encryption overhead is related to how many bits to be encrypted, the unit-block encryption time, and the encryption block size. Therefore, the principle of the proposed selective encryption is to only encrypt the major components of biomedical data rather than all biomedical information. Compared with traditional full encryption approaches, the selective encryption can significantly reduce the computational overheads, which is suitable for the resource-limited medical sensor. In addition, the key distribution and management are difficult and challenging in resource limited sensor nodes, especially in biomedical sensor nodes. The intrinsic characteristics of the human body potentially share the biometric information that can be a cipher key for the sensor nodes in WBAN. The proposed selective encryption approach can remove the need for key distribution in WBAN based on biometric information. In this scheme, the biomedical signals containing major information are chosen to be encrypted by using statistic ECG biometric feature as a key. For example, in the proposed approach, we can extract clinically meaningful metrics such as the QRS axis, QT-interval, ST-level, and T-wave abnormalities as the most important information of ECG medical data. These ECG statistics will be regarded as the secret key shared only over body area networks.

IV. Performance Evaluation

In our experiment, we choose ECG signals as the biometric authentication identity that can be characterized as the HMMs parameters θ. In the performance evaluation, HMM modeling and likelihood comparison processes are performed to check the authentication accuracy. In our study, the statistical characteristics of ECG signals are extracted in the proposed scheme without any synchronization requirements. In fact, the statistics of ECG signals are very similar within a short period of time on the same human body. These similarities are desirably extracted by the proposed HMM based authentication scheme with a high level of misalignment tolerance. Because the proposed approach does require time synchronization it can significantly reduce

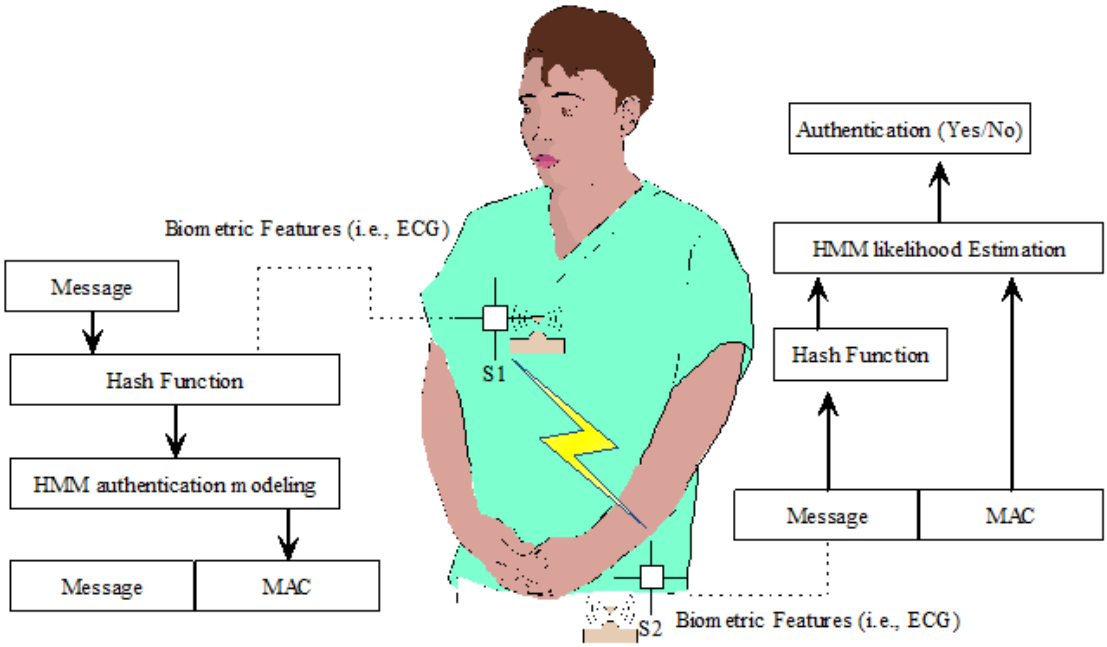

Fig. 3. An Integrated Biometric-based Security System using HMM

the additional communication and computational overheads. In our case study, two persons' ECG signals are collected. The proposed HMM authentication process firstly train the signal from Person I and acquired HMM parameters θ. These parameters are the input of HMM authentication process to classify Person II's ECG signal.

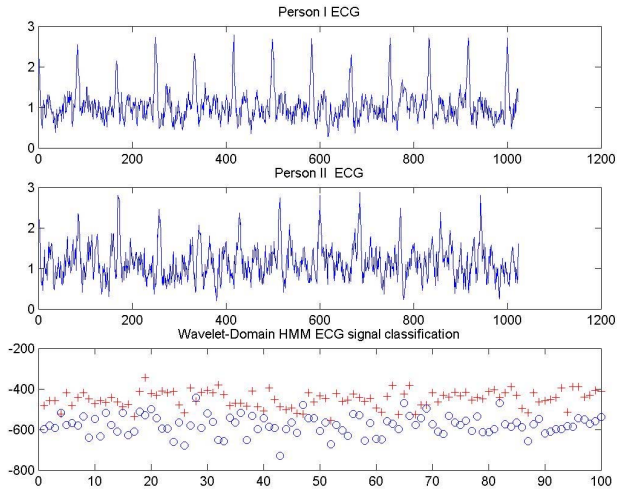

Fig. 4. ECG Classification using HMM

Figure 4 (a) and (b) show the ECG signal from Person I and from Person II respectively. Figure 4 (c) shows the authentication accuracy, which is achieved by the wavelet-domain HMM ECG signal classification. As shown in Figure 4(c), Person I's identity (marked by "+") and person II's identity (marked by "circle") are classified accurately. This result shows the HMM is an efficient approach to distinct the ECG identities for the authentication.

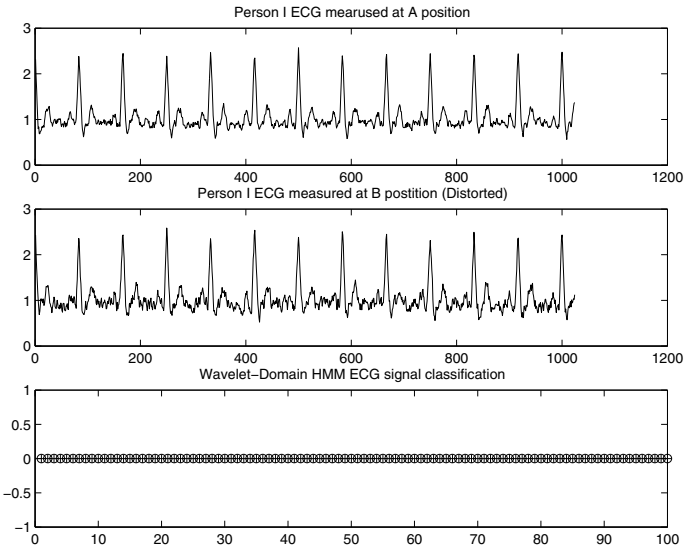

Fig. 5. Biometric (ECG) based Authentication using HMM

Figure 5 (a) and (b) shows the ECG measurement at A position and the measurement at B position of the body. Because the ECG signal could be distorted due to many factors of medical sensors, the ECG signal from B position has been distorted compared with the measurement at A position. However, our approach can tolerate the signal distortion, verifying the message and authenticating signal statistically. These results demonstrate that our proposed approach can achieve high authentication performance.

V. Conclusions

In this paper, we have studied a security framework that can secure the body sensor communication with lower overheads by utilizing body biometric information. To authenticate the data message, we proposed a wavelet-domain statistic approach that can model distinct biometric information (e.g., ECG) and authenticate message signatures among body sensors with high accuracy. The proposed framework opens a new vista of integrating biometric information into the security in wireless body area networks (WBANs).

References

[1] N. Potlapally, S. Ravi, A. Raghunathan, N. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Trans. Mobile Computing,* vol.5, no. 2, pp. 128-143, Feb. 2006.

[2] J. Chen, Y. Wang, "Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience," *IEEE Commun. Mag.,* vol.43, no.12, pp.26-32, Dec. 2005.

[3] V. Coskun, E. Cayirci, A. Levi, S. Sancak, "Quarantine region scheme to mitigate spam attacks in wireless-sensor networks," *IEEE Trans. Mobile Computing,* vol.5, no.8, pp.1074-1086, Aug.2006.

[4] http://fiji.eecs.harvard.edu/CodeBlue

[5] http://www.mobihealth.org .

[6] http://www.cs.uoregon.edu/research/wearables/index.html

[7] K. Venkatasubramanian, S.Gupta, *Security Solutions for Pervasive Healthcare, Security in distributed, grid, mobile, and pervasive computing,* Auerbach Publications, CRC Press, pp 443-464, 2007.

[8] S. Cherukuri, K. Venkatasubramanian, 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 Processing Workshops,* pp.432-439, 2003.

[9] C. Poon,Y. Zhang, S. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag,* pp.73-81, Apr. 2006.

[10] A. Juels, M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6^{th} ACM Conf. Comp. and Commun. Sec.,* pp.28-36, Nov. 1999.

[11] S. Bao, Y. Zhang, L. Shen, "Physiological signal based entity authentication for body area sensor networks ad mobile healthcare systems," in *Proc. IEEE Engineering in Medicine and Biology,* pp.2455-2458, 2005.

[12] S. Bao, Y. Zhang, "A design proposal of security architecture for medical body sensor networks," in *Proc. IEEE International Workshop on Wearable and Implantable Body Sensor Networks,* 4pp, 2006.

[13] U. Uludag, S. Pankanti, S. Prabhakar, A. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE,* vol.92, no.6, pp.948-960, 2004.

[14] K. Chan, Y. Moon, P. Cheng, "Fast fingerprint verification using subregions of fingerprint images," *IEEE Trans. Circuits and Systems for Video Technology,* vol.14, no.1, pp.95-101, 2004.

[15] S. Ben-Yacoub, Y. Abdeljaoued, E. Mayoraz, "Fusion of face and speech data for person identity verification," *IEEE Trans. Neural Networks,* vol.10, no.5, pp.1065-1074, 1999.

[16] D. Muramatsu, M. Kondo, M. Sasaki, S. Tachibana, T. Matsumoto, "A Markov chain Monte Carlo algorithm for bayesian dynamic signature verification," *IEEE Trans. Information Forensics and Security,* vol.1, no.1, pp.22-34, 2006.

[17] H. Wang, D. Peng, W. Wang, H. Sharif, H.H. Chen, A. Khoynezhad, "Resource-aware Secure ECG Healthcare Monitoring through Body Sensor Networks," *IEEE Wireless Communication Magazine,* vol. 17, no. 1, pp.12-19, 2010.

[18] W. Wang, D. Peng, H. Wang, H. Sharif, "An Adaptive Approach for Image Encryption and Secure Transmission over Multirate Wireless Sensor Networks," *Wireless Communications and Mobile Computing Journal,* John Wiley & Sons, 2007.

[19] M.S. Crouse, R.G. Baraniuk, R.D. Nowak, "Hidden Markov models for wavelet-based signal processing," Signals, Systems and Computers, *the Thirtieth Asilomar Conference,* pp.1029-1035 vol.2, 3-6, 1996.

[20] H. Wang, M. Hempel, D. Peng, W. Wang, H. Sharif, H.H. Chen, "Index-Based Selective Audio Encryption for Wireless Multimedia Sensor Networks" *IEEE Transactions on Multimedia,* vol. 12, no. 3, pp. 215-223, Apr. 2010.