A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)

Sofia Najwa Ramli[1], Rabiah Ahmad[2], Mohd Faizal Abdollah[3], Eryk Dutkiewicz[4]

[1,2,3]Center for Advanced Computing Technology, Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka, Malaysia

[4]Department of Electrical Engineering, Macquarie University, Australia

sofia_najwa@yahoo.co.uk, rabiah@utem.edu.my, eryk.dutkiewicz@mq.edu.au

Abstract— **The empowerment in wireless communication technologies and sensors have developed the Wireless Body Area Network (WBAN). In the past few years, many researchers have been focusing on building system architecture of health monitoring to improve the technical requirement specifically designed for WBAN. Less research was found in providing the strong security system. As part of communication medium, WBAN faced various security issues such as loss of data, authentication and access control. Implementing high security system leads to inconsistency in computational performance. It is recommended that the security system for WBAN must be implemented with low computational complexity and high power efficiency. None of previous researches successfully identified solution to the above problem. This study explores the use of biometric characteristics in securing data communication within WBAN and reducing computational complexity as well as power efficiency. Hybrid authentication model is used as a conceptual framework for the system. Precisely, the proposed framework requires a unique feature of human body regarded as the authentication identity, while the other techniques use hardware and software to achieve the same purpose. In addition, an authentication process is provided by using this unique feature of the body as a key to develop a security system under the resource-constrained of WBAN sensor challenges.**

Keywords— **Wireless Body Area Network (WBAN), Heart Rate Variability (HRV), biometric, authentication, security**

I. Introduction

Applying Wireless Sensor Network (WSN) technology for various applications has been increased rapidly in the past few years. One of its innovative deployments is in the form of wireless biomedical sensor network for measuring physiological signals. Wireless Body Area Network (WBAN) is a wireless network used for communication among sensor nodes operating on, in or around the human body in order to monitor vital body parameters and movements. These monitoring signals are then gathered by a personal device, like PDA or smart phone that acts as a sink for data of the sensor nodes and transmits them to the healthcare professional for health monitoring.

The progression of WBAN is vital in modern telemedicine and m-health, but security remains a formidable challenge yet to be resolved. As nodes of WBAN are expected to interconnect between each other, the body itself can form an inherently secure communication pathway that is unavailable to all other kinds of wireless networks [1]. It is believed that if it is used properly, the system can naturally secure the information transmission within WBAN, where other techniques use hardware and software to achieve the same purpose. In other words, the biometric information collected from the human body can uniquely represent an individual, which is hard to be deprived by suspicious intruders.

In this work, we proposed a security system to secure medical information communications using biometric features of the body in WBAN. Specifically, the sender's electrocardiogram (ECG) feature is selected as the biometric key for data authentication mechanism within WBAN system. Therefore, patient's records can only be sensed and derived personally by this patient's dedicated WBAN system and will not be mixed with other patients. For accurate authentication, the statistical result is needed to prove the uniqueness of each ECG signals. Besides, an encryption will be included by extracting biometric feature as a secret key for communications within WBAN. But, it is not a major concern in this work.

II. Security Issues in WBAN

At the initial stage, several research groups have contributed the substantial efforts on developing WBAN systems. However, these researchers mainly focused on building system architectures and in lesser extent on evolving network protocols. Besides, it is difficult to discover solutions' providing strong security system for WBAN and security has generally been covered separately.

Extending the scope of technology, there are several security protocols in general sensor networks. Security protocols for Sensor Networks (SPINS) is a set of protocols for achieving security requirements like confidentiality, integrity and authenticity in sensor networks and uses several symmetric keys to encrypt the data as well as compute the Message Authentication Code (MAC) [2][3]. However, SPINS is only considered in general sensor networks, so it is inadequate to be applied in WBAN as it has environmental features like the human body and limited computing resources.

Recently, WBAN security schemes have been introduced progressively using symmetric cryptosystem. They concern with the limited resource issues of WBAN sensors, but have problems like delaying the disclosure of the symmetric keys and providing weak security relatively since it is not resilient against physical compromise [4]. Furthermore, the complexity of sensor node's key managements in WBAN make each component overload. Due to these issues, some researches believe that the sensors have to make use of symmetric cryptographic algorithms to encrypt the data they send to control node and the random number that is used in security protocols can be generated by biometrics [5]. They also believe that biometric is suitable for securing WBAN because its higher security level that can be achieved with less computation and memory requirement, when compared to the generic cryptosystems.

On the contrary, some researches utilize the asymmetric cryptosystem in mobile and ad hoc networks and also try to examine the unique characteristics of WBAN [6][7]. One concern about the asymmetric cryptosystem is a resource constraint problem but recent work has shown that performing ECC consumes a lot less of memory and computing power [5][[7]. These researches deal with a scope of limited WBAN but they exclude the implanted sensor networks. The objective of WBAN is also the implementation of body area network that can contact with everywhere in, on, and out the human body.

By comparison, each approaches has several issues to be considered in terms of the security services in WBAN. Further, there is a trade-off between performance and security. Related to these, another research group has proposed these two heterogeneous cryptosystems in their research, which provides security and privacy to WBAN. In [2] , they believe that these two cryptosystems can be applied in the authentication of WBAN depleting each weak point of them at once. So their focus is on the method on how two cryptosystems can be utilized appropriately and partly in WBAN. However, all the above research works have focused on secret key distribution issues and require time synchronization when biometric information of the same human body cannot be available simultaneously.

Consequently, in [1], they introduce a biometric-based security framework using wavelet-domain Hidden Markov Model. The aim is to achieve accurate authentication performance among body sensors without extra requirements of key distribution and strict time synchronization. In this proposed approach, low cost authentication challenges is addressed by extracting statistically biometric information from patient's data and authenticate message signatures among WBAN communications with high accuracy. Thus, it will certainly save resources while adequate security measures are employed.

III. BIOMETRIC-BASED SECURITY APPROACHES FOR DATA AUTHENTICATION

Biometric is a technique commonly known as the automatic identification or verification of an individual by his or her physiological or behavioural characteristics. Biometric approach uses an intrinsic characteristic of the human body as the authentication identity to secure the distribution of a cipher key within WBAN communications. Because of the data that are detected, collected and transmitted in WBAN is comparatively sensitive, an ideal biometric trait should present 100% reliability, user friendly, fast operation and low cost. Besides, it is postulated that the utilized biometric should satisfy the following properties indicated in TABLE 1[5].

TABLE 1. BIOMETRIC PROPERTIES

Properties	Description
Universal	Possessed by the majority, if not the entire population.
Distinctive	Sufficiently different in any two individuals.
Permanent	Sufficiently invariant, with respect to the matching criterion, over a reasonable period of time.
Collectable	Easily collected and measured quantitatively.
Effective	Sufficiently invariant, with respect to the matching criterion, over a reasonable period of time.
Acceptable	Yield a biometric system with good performance that is given limited resources in terms of power consumption, computation complexity and memory storage, the characteristic should be able to be processed at a fast speed with recognized accuracy.
Invulnerable	Relatively difficult to reproduce such that the biometric system would not be easily circumvented by fraudulent acts.

A. Heart Rate Variability (HRV)

As discussed previously elsewhere by [5][8][9][10], it is claimed that heart rate variability (HRV) signals have unique characteristics and chaotic nature, which put up random characteristics and thus can be utilized in secure communications. Additionally, unlike traditional biometric cryptosystems in generic networks such as fingerprint, iris pattern, palm print, hand geometry and facial pattern, the blood circulation system in a human body forms a unique secure communication path specifically available for WBAN.

HRV is a physiological phenomenon where the time interval between heartbeats varies. The measurement of HRV provides a non-invasive measurement of the autonomic nervous system (ANS) activity, which comprises two basic components: the sympathetic and parasympathetic. The heart rate may be increased by acting sympathetic activity or decreased by acting parasympathetic activity. Changes in the balance of sympathetic/parasympathetic control of heart rate will result in measurable changes in HRV. The analysis has been applied widely to many clinical studies including sudden death, cardiovascular diseases, hypertension and diabetes [11].

HRV can be obtained using the variations of heartbeat-to-heartbeat intervals that can be measured by any cardiac related signal. However, the current, ECG is preferred compared traditional biometric. It is because of the following reasons [10]:

- Universality: ECG is inherent and natural, and can be collected from any living human subject.
- Permanen*ce*: ECG is stable over a large period of time. Even though certain localized characteristics of the pulses might get distorted, the overall diacritical waves are still observable.
- Uniqueness: The inter-individual variability of ECG is a result of several parameters that control the waveforms.
- Robustness: Because of the uniqueness and the person's own characteristics, it is extremely difficult to steal and use someone's ECG, and it is equally difficult for an individual to mimic someone else's heart signals as they are the outcome of a combination of several sympathetic and parasympathetic factors of the human body.
- Liveness detection: Unlike other biometric technologies, ECG is collected from the living legitimate subject without requiring extra computational effort.

HRV can be analyzed by using two major techniques [11]. One is statistically analyzing a sequence of RR intervals of ECG in time domain. The other one is analyzing the spectrum of the same RR intervals of ECG data in frequency domain. In this study, HRV will be analyzed in time domain since ECG signals are recorded in time series. Therefore, it can reduce computational complexity and save more resources.

Time domain measures of HRV based on the data of the intervals between adjacent normal QRS complex have two major approaches. One is derived from direct measurements of normal beat to normal beat, NN intervals, which consist primarily of SDNN, the standard deviation of NN intervals. The standard deviation reflects all the cyclic components responsible for variability in the period of recording [12]. It can be calculated for 24 hours long-term recordings or for short term, five minutes recordings. In most heart rhythms, NN interval is equivalent to the R-R interval. Another is derived from the difference between NN intervals and most commonly used measures include RMSSD and pNN50. The RMSSD is the square root of the mean squared differences of successive difference NN intervals [11]. The pNN50 represents the proportion of interval differences of successive normal-beat-to-normal-beat intervals greater than 50 milliseconds [11].

B. R-Peak Detection

In order to avoid erroneous conclusions, it will be better if only sinus rhythms are present in the tacho gram. Therefore, pre-processing of the RR interval time series is very necessary. A normal ECG trace consists of a P wave, a QRS complex and a T wave. The P wave is the electrical signature of the current that causes atrial contraction, the QRS complex corresponds to the current that causes contraction of the left and right ventricles, and the T wave represents the repolarization of the ventricles.

The QRS complex is the most characteristic waveform of the signal with higher amplitudes. The R peaks have the largest amplitudes among all the waves making them easiest to detect. However, QRS detection is difficult. It is not only because of the physiological variability of the QRS complex, but also because of the various types of noise that can be present in the ECG signal [13]. Noise sources include muscle noise, artefacts due to electrode motion, power-line interference, baseline wander, and T-waves with high frequency characteristics similar to QRS complex. Figure 1 shows a noisy ECG signal (the upper part) and the output of QRS detection after pre-processing (the lower part). The peak amplitudes show the R peaks of ECG signal.

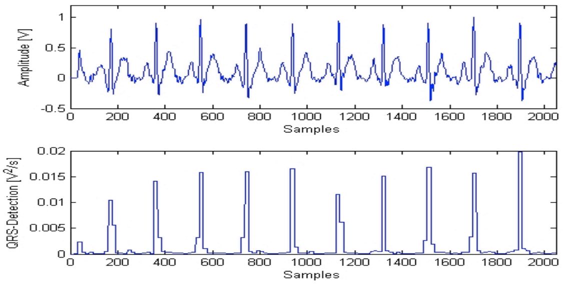

Figure 1. Before and After the Pre-processing

C. Data Authentication Model

In the proposed model, the message authentication code (MAC) can be generated with the input of biometric feature and hashes that are calculated based on the original message as shown in Figure 2. Then, the message will be sent to the destination. At the destination point, if the received signal matches statistically, it will be accepted and authenticated. Otherwise, the message is denied and discarded. The key point of this technique is to utilize the statistically same biometric information at both ends without any synchronization to secure data distribution within WBAN. Figure 3 shows the proposed biometric-based security for data authentication in WBAN.

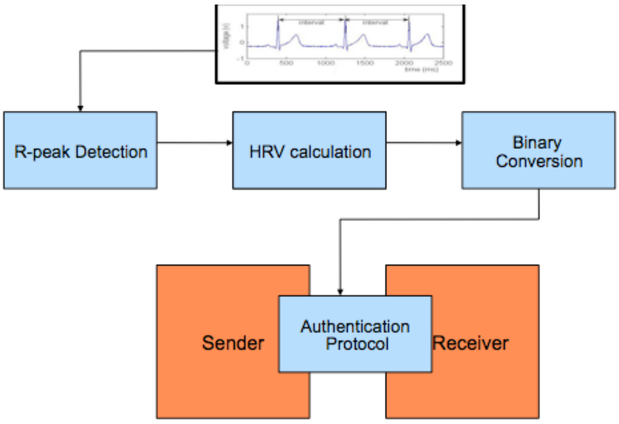

Figure 2. Biometric Feature Used to Calculate MAC

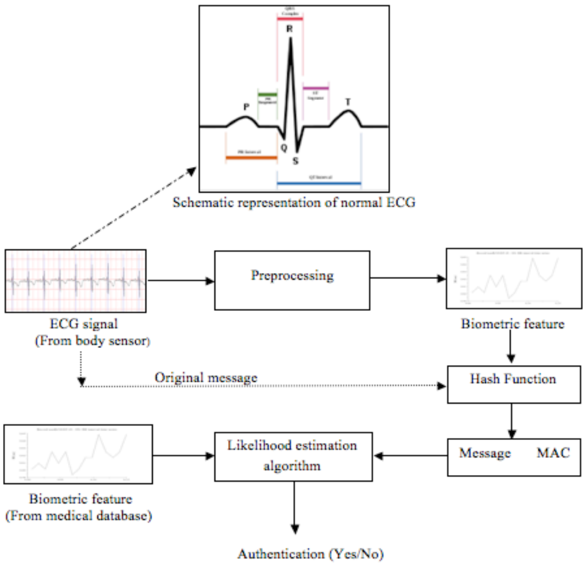

Figure 3. Proposed Biometric-based Security for Data Authentication

Authentication, itself, is used to simultaneously verify both the data integrity and the authenticity of a message. Nevertheless, encryption is also needed to protect data in transit especially for data being transferred via networks. Therefore, encryption approaches in WBAN must be designed with low cost. However, the key distribution and management are difficult and challenging in resource limited sensor nodes, especially in biomedical sensor nodes. In this work, the biomedical signals are encrypted by using biometric feature as a cipher key to remove the need for key distribution in WBAN.

IV. CONCLUSIONS

In this paper, a biometric-based security framework is proposed for data authentication within WBAN. Specifically, the sender's electrocardiogram (ECG) feature is selected as the biometric key for data authentication mechanism within WBAN system. Therefore, patient's records can only be sensed and derived personally from this patient's dedicated WBAN system and cannot be mixed with other patients. The security system in WBAN must be implemented with low computational complexity and high power efficiency. In this proposed approach, low cost authentication challenges is addressed specifically by using biometric information instead of cryptographic key distribution. Thus, it will certainly save resources while adequate security measures are employed. The future work is to build experiment based on the proposed system and to improve the system if needed.

ACKNOWLEDGMENT

The authors would like to thank all the reviewers for their helpful comments. This research is currently supported by the Exploratory Research Grant Scheme (ERGS) funding by the Ministry of Higher Education Malaysia and MyBrain 15 (MyPhD) scholarship program for the academic year of 2011-2014.

REFERENCES

[1] H. Wang, H. Fang, L. Xing, and M. Chen, “An Integrated Biometric-Based Security Framework Using Wavelet-Domain HMM in Wireless Body Area Networks (WBAN),” *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, Jun. 2011.

[2] C. S. Jang, D. G. Lee, J.-W. Han, and J. H. Park, “Hybrid security protocol for wireless body area networks,” *Wireless Communications and Mobile Computing*, no. April 2010, pp. 277–288, 2011.

[3] J. Liu and K. S. Kwak, “Towards Security Issues and Solutions in Wireless Body Area Networks,” *Networked Computing INC 2010 6th International Conference on*. pp. 1–4, 2010.

[4] C. William, C. C. Tan, and H. Wang, “Body Sensor Network Security : An Identity-Based Cryptography Approach,” *Security*, pp. 148–153, 2008.

[5] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, “A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health,” *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[6] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, “Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring,” *2010 IEEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing*, pp. 327–332, 2010.

[7] K. M. Sharmilee, R. Mukesh, A. Damodaram, and V. Subbiah Bharathi, “Secure WBAN Using Rule-Based IDS With Biometrics And MAC Authentication,” *2008 10TH IEEE INTERNATIONAL CONFERENCE ON EHEALTH NETWORKING APPLICATIONS AND SERVICES*, pp. 102–107, 2008.

[8] S.-D. Bao, L.-F. Shen, and Y.-T. Zhang, “A novel key distribution of body area networks for telemedicine,” in *2004 IEEE International Workshop on Biomedical Circuits Systems*, 2004, pp. 2–5.

[9] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, “Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems.,” *Conference proceedings : ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference*, vol. 3, pp. 2455–8, Jan. 2005.

[10] L. Yao, B. Liu, K. Yao, G. Wu, and J. Wang, “An ECG-Based Signal Key Establishment Protocol in Body Area Networks,” *2010 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing*, pp. 233–238, Oct. 2010.

[11] G. H. Lin and K. P. Lin, “Comparison of Heart Rate Variability Measured by ECG in Different Signal Lengths,” vol. 25, no. 2, pp. 67–71, 2005.

[12] A. Jovic and N. Bogunovic, “Feature set extension for heart rate variability analysis by using non-linear, statistical and geometric measures,” *Proceedings of the ITI 2009 31st International Conference on Information Technology Interfaces*, pp. 35–40, Jun. 2009.

[13] W. J. Pan J., Tompkins, “A Real-Time QRS Detection Algorithm,” *IEEE Transactions on Biomedical Engineering*, vol. BME-32, no. 3, pp. pp.230–236, 1985.