Proceedings of the 2005 IEEE
Engineering in Medicine and Biology 27th Annual Conference
Shanghai, China, September 1-4, 2005

Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems

Shu-Di Bao[1,2], Yuan-Ting Zhang[2], Lian-Feng Shen[1]
[1]National Mobile Communications Research Laboratory, Southeast University, Nanjing, China
[2]Joint Research Center for Biomedical Engineering, The Chinese University of Hong Kong, Hong Kong, China

Abstract—**With the evolution of m-Health, an increasing number of biomedical sensors will be worn on or implanted in an individual in the future for the monitoring, diagnosis, and treatment of diseases. For the optimization of resources, it is therefore necessary to investigate how to interconnect these sensors in a wireless body area network, wherein security of private data transmission is always a major concern. This paper proposes a novel solution to tackle the problem of entity authentication in body area sensor network (BASN) for m-Health. Physiological signals detected by biomedical sensors have dual functions: (1) for a specific medical application, and (2) for sensors in the same BASN to recognize each other by biometrics. A feasibility study of proposed entity authentication scheme was carried out on 12 healthy individuals, each with 2 channels of photoplethysmogram (PPG) captured simultaneously at different parts of the body. The beat-to-beat heartbeat interval is used as a biometric characteristic to generate identity of the individual. The results of statistical analysis suggest that it is a possible biometric feature for the entity authentication of BASN.**

Keywords—**Heart rate variability, biometrics, entity authentication, body area sensor network.**

I. Introduction

Great attention has been given recently to information technology and its use for the improvement of health care service delivery. Significant advances in wireless communications and network technologies with parallel advances in wearable/implantable sensors and systems have already made a significant impact on current e-health and tele-medical systems. M-Health, defined as "mobile computing, medical sensor, and communication technologies for health-care" [1], represents the evolution of e-health systems from traditional desktop "telemedicine" platforms to wireless and mobile configurations. A proper integration of medical sensors into m-Health systems would allow physicians to diagnose, monitor, and treat patients remotely without compromising standards of care.

Wireless connectivity of individual intelligent sensors has emerged as the main research trend to facilitate the joint processing of spatially and temporally collected physiological information from different parts of the body and the external communication for mobile health care [1]. Those biomedical sensors within a single human subject are interconnected into a system consisted of a body area network, called Body Area Sensor Network (BASN) [2]. This type of system features extremely low power consumption at the expense of lower communication range and bandwidth.

It is required by law that individual physiological data should be kept in privacy [3]. Hence, the deployment of mobile and wireless technologies in m-Health system should solve the security challenges, i.e. privacy and security of patients' records and transmissions [1]. Since BASNs are the foundational networks for physiological data acquisition and data fusion in m-Health system, as shown in Fig. 1, the secure data transmission in BASNs should be ensured [2,4].

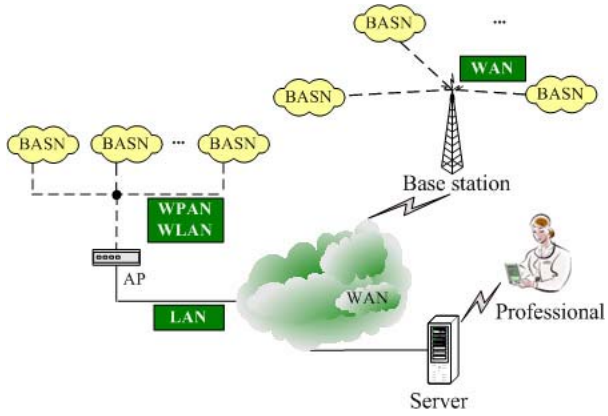

Fig. 1. A BASN combined m-health system model

Because of its super-short communication range, the main security challenges of BASN are eavesdropping, message modification, and communication interference among BASNs. For the eavesdropping and modification challenges, we have proposed a novel and specific symmetric cryptosystem [2,4] for BASN, where physiological signals detected for health monitoring can also be used to generate encryption key as well as key 'witness' to secure the key transmission. Compared with other generic cryptosystems, a higher security level can be achieved with less computation and memory requirement. In this study, a physiological signal based entity authentication scheme is proposed to efficiently achieve secure access control during wireless link setup process.

II. Biometrics

To solve the problem of entity authentication, i.e. node-to-node authentication, between sensors interconnected in

BASN, we introduce the wearable/implantable intelligent sensors that can serve dual functions: (1) the traditional passive function of gathering and transmitting data for processing, and (2) a new function of actively making use of the collected data to recognize the other sensors on the same individual and communicate with them via a secured channel. The proposed technology is intended to apply to telemedicine and related fields, where data collected by the sensors for medical application are now as well used intelligently as a biometric characteristic for the different sensors to recognize each other. The arrangement ensures the optimization of resources for achieving all the necessary purposes efficiently with a single sensor.

The entity authentication in BASN is solved by applying the concept of biometrics, a technique that is commonly defined as the automatic identification or verification of individuals by his or her physiological or behavioral characteristics [5]. Unlike some of the well-known biometric characteristics, such as fingerprint, iris pattern, palmprint, hand geometry and facial pattern [6], which are patterns captured on a specific part of the body surface, the biometric characteristic utilized in BASN is a physiological sign generated by a biological system of an individual, e.g. heart rate variability (HRV).

HRV is a measure of the beat-to-beat alteration in HR, which is readily available in several kinds of physiological signals related to the cardiovascular system, such as ECG and PPG. One of the most common techniques to estimate HR is by estimating the inverse of the time interval between the peaks of adjacent R waves in ECG (as depicted in Fig. 2a). Similarly, PPG is a pulsatile signal that synchronizes with the heartbeat and possesses a waveform close to the arterial blood pressure waveform obtained through direct catheterization. Thus, time interval between the peaks of adjacent pulses in PPG (as depicted in Fig. 2b) can also be used to estimate HR. The difference between successive beat-to-beat HR is a measure of HRV.

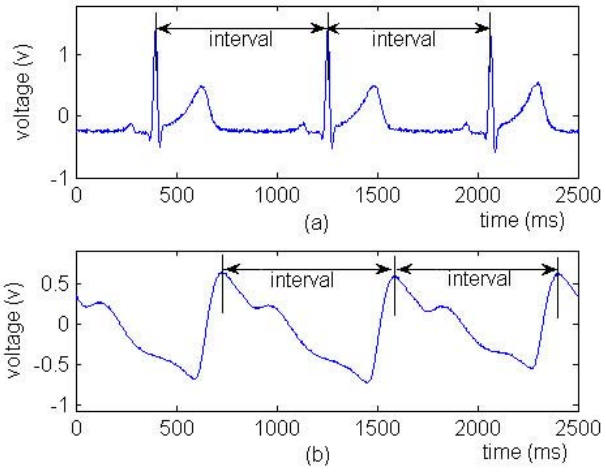

Fig. 2. Examples of ECG signal (a) and PPG signal (b)

HRV and the characteristics of many physiological signals such as ECG [7-8] and PPG [9] have been shown to be unique for different subjects, which satisfy the basic criteria of a biometric characteristic. Moreover, physiological signals can be captured by sensors in/on the human body, so that he or she has full and free motility to work or recreation while the authentication process is carrying out. This will allow a much higher degree of freedom on the users.

Nonetheless, physiological signs such as HRV are time-variant, which make them difficult to be applied in conventional biometric systems, where templates of the biometric characteristic are stored in the system as reference to compare against a copy of the characteristic captured in real-time for identification or authentication purposes. Therefore, we investigated the use of these characteristics in a different way in BASN. Two sensors that are placed at different locations of the same individual, but intended to communicate with one another, will capture their own copy of biometric characteristic independently but simultaneously. Since some of the specific physiological signs collected from different parts of an individual, regardless of the source of measurement, can be identical or highly correlated though possessing a chaotic nature, a match of the signs collected at different nodes is a highly secured indication that the sensors are being on the same individual. If the two sensors were not on the same individual, HRV measured on each of them would be significantly different. Not only that the arrangement avoids potential cross-talk interference between different subjects, it also prevents the system being spoofed by forged characteristics, which is one of the major security concerns of many biometric systems [10].

To summarize, the proposed biometric characteristic is unique, universal, easy to collect and permanence as long as the characteristics are captured simultaneously at both ends while the system has a good performance in terms of cost effectiveness and computational complexity. It is also convenient to users and difficult to circumvent. In other words, it has all the necessary characteristics of a practical biometric system [6], theoretically supporting it to be a feasible solution to the problem of entity authentication between sensors interconnected in BASN.

III. Entity Authentication Scheme

Entity authentication is defined as the process whereby one party is assured of the identity of a second party involved in a protocol. We call the two parties involved prover and verifier. The verifier is requested by the prover to establish a correct relation between a particular identity and the prover. In BASN, we use peer entity authentication scheme to ensure the secure link connection, as shown in Fig. 3.

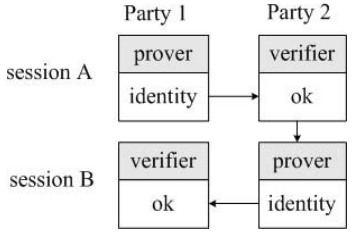

Fig. 3. Peer entity authentication process

In BASN with server-client communication pattern [2,4], the entity authentication process is initiated by the server. As described in Section II, one kind of biometrics can be extracted from physiological signals detected by n nodes in the same BASN, denoted as $I = \{I_0, I_1, \cdots, I_{n-1}\}$, with high similarity. Here, I, unique to individual, is used as identity in our entity authentication. For example, the biomedical sensors within Alice's body area can all be associated with the identity of Alice. Our entity authentication scheme is depicted in Fig. 4, where R_S is a random number generated by the scheme described in [4], E(x) means the encryption of x and D(E(x)) means the decryption of E(x) both using the schemes described in [2,4]. The match process is done by comparing the hamming distance of I_0 and I_i, denoted as H_{0i}, with a special value θ. If $H_{0i} \le \theta$, the match process will be successfully done. Otherwise, the client or the server will drop the authentication challenge or response packet. Since $I_i (i = 0,1,\cdots,n-1)$ generated by different sensors within Alice's body area has high similarity, H_{0i} shall be within the threshold θ, so is the Hamming distance of I_0' and I_i'. It is a special challenge-response entity authentication, which can overcome the weakness of reflection attacks mentioned in [11].

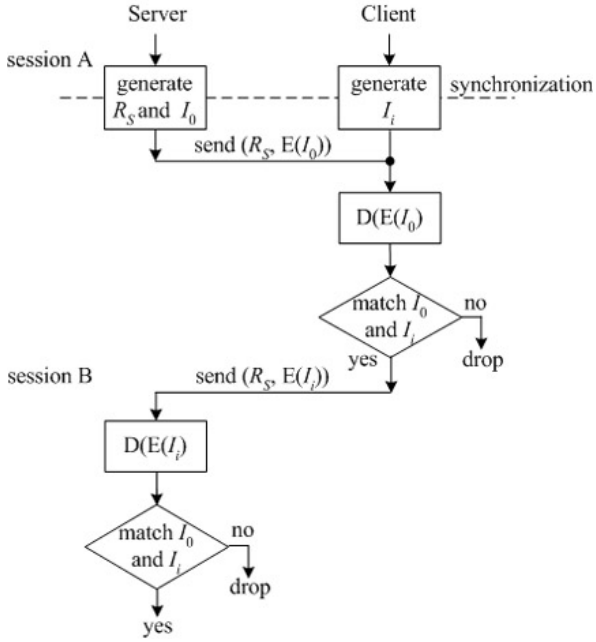

Fig. 4. Entity authentication process

IV. Feasibility Study

The feasibility of generating identity set I from the information of HRV is studied in this section. Because of easy detection, PPG signals are utilized to generate I as an example for the proposed entity authentication scheme.

PPG signals of twelve healthy subjects were detected and recorded by two PPG sensors. Throughout the signal recording period, the subjects were asked to remain quiet. For each subject, the 1st derivatives of PPG signals were simultaneously obtained from two channels at the left and right index fingers. The results of the typical PPG signals are shown in Fig. 5. Using a specific and efficient coding method, $I_i (i = 0,1)$ were generated with the bit-length of 128 from peak intervals of those PPG signals. It should be noticed that I_0 and I_1 were identities of two PPG sensors on the same subject, which means they were used by those two PPG sensors to recognize each other. Because of the chaotic feature of physiological signals I shall have good randomness performance and thus averagely it will need 2^{127} times to guess the right value for attackers.

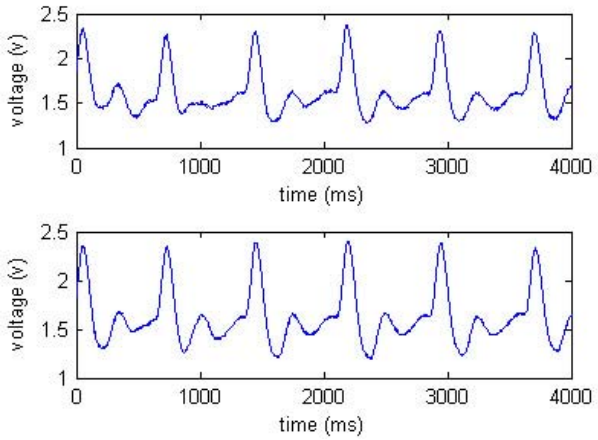

Fig. 5. Example of 2-channel 1st derivatives of PPG signals

In total, six pairs of I_0 and I_1 with 128-bit length were generated from each subject. We statistically analyzed the similarity of I_0 and I_1 using hamming distance. Fig. 6 depicts the distribution of hamming distance of I_0 and I_1 over 12 subjects. All the hamming distance of I_0 and I_1 is within 22, showing good similarity between identities generated by the biomedical sensors in the same BASN.

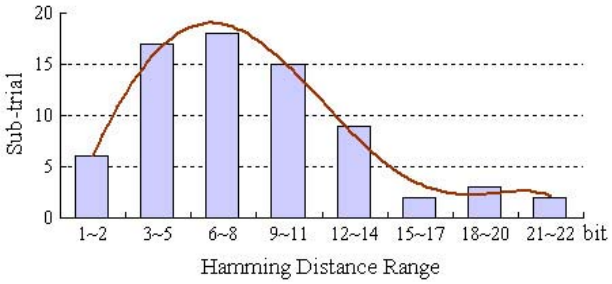

Fig. 6. Hamming distance distribution of I_0 and I_1

We also analyzed the hamming distance of I_0 and $\overline{I_0}$, where I_0 and $\overline{I_0}$ were identities of two sensors on different subjects. The results of data analysis show that there is great difference between these two identities, which means identity set of one BASN is quite different from those of other BASNs. Fig. 7 depicts an example of hamming distance of I_0 and $\overline{I_0}$, where $s_1 \sim x$ ($x = s_2, \cdots, s_{12}$) means the

two identities, wherein one is from subject s_1 and the others are from subject x ($x = s_2, \cdots, s_{12}$). The identity of each sub-trial is with 128 bit-length. As we can see, the hamming distance of I_0 and $\overline{I_0}$ is quite large. Therefore, the results suggest that HRV is a possible biometric characteristic to be used in the proposed entity authentication scheme for BASN.

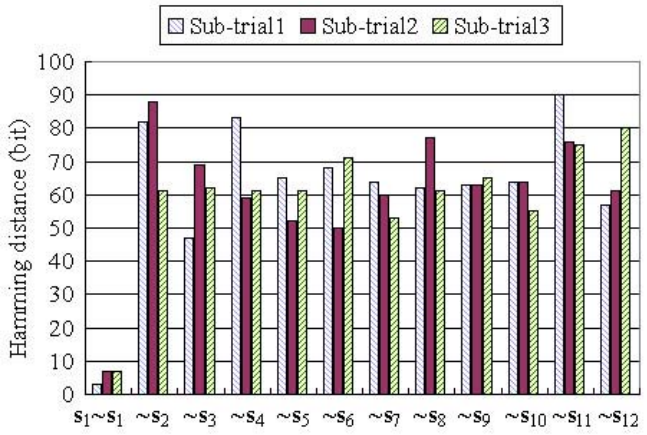

Fig. 7. Example of hamming distance of I_0 and $\overline{I_0}$

IV. Conclusion

BASN which is formed by miniature biomedical sensors will become a basic component in the future m-Health systems for long-range continuous health monitoring. Because of the importance of secure physiological data transmission we focus on the security issues of BASN, through which physiological data are transferred to a remote server for further process. Compared with generic sensor networks, BASN has its own characteristics, of which the most significant one is that it is physiological signal that the nodes of BASN detect, process, and collect. Specially, we utilize these two characteristics of physiological signals to achieve secure entity authentication process: (1) good variability; and (2) high similarity of the information extracted from physiological signals simultaneously detected by nodes in the same BASN.

Consequently, we introduced a novel physiological signal based entity authentication scheme specific to BASN. The information extracted from physiological signals is used to generate identity information for mutual authentication. All the nodes in the same BASN have the same identity set of the human subject. Our entity authentication scheme adopts challenge-response protocols, which are widely used for identity verification over insecure channels. Moreover, by using biometrics to generate unique identity set for each individual, our scheme avoids the possibility of reflection attacks in challenge-response protocols.

For the feasibility study, HRV is used as a biometric feature to generate the identity information of individuals. 12 healthy subjects were included in the experiment, and 2 channels of PPG signals were simultaneously captured from each subject. The statistical analysis suggests that it is a possible biometric characteristic to be used in the proposed entity authentication scheme for BASN.

With random number generation scheme and secure key transmission scheme described in [2,4], the proposed entity authentication scheme will allow the secure identity verification during wireless link setup process. The utilization of chaotic nature of the human subject for secure communications is deemed to have a promising future. Further research work incorporating synchronization process should be carried out in order to practically deploy the proposed scheme.

Acknowledgment

This work was supported in part by Hong Kong Innovation and Technology Fund. We also are grateful to Standard Telecommunication Ltd., IDT Technology Ltd., and Jetfly Technology Ltd. for their support given to the ITF project.

References

[1] R. S. H. Istepanian, E. Jovanov, and Y. T. Zhang, "Introduction to the special section on m-health: beyond seamless mobility and global wireless health-care connectivity", *IEEE Trans. Info. Tech. Biomed.* vol. 8, no. 4, pp. 405–414, Dec. 2004.

[2] S. D. Bao, Y. T. Zhang, and L. F. Shen, "A new symmetric cryptosystem of body area sensor networks for telemedicine", in *Proc. 6th Asian-Pacific Conference on Medical and Biological Engineering*, Apr. 2005.

[3] Health Insurance Portability Accountability Act (HIPAA).

[4] S. D. Bao, L. F. Shen, and Y. T. Zhang, "A novel key distribution of body area networks for telemedicine", in *Proc. IEEE International Workshop on Biomedical Circuits and Systems*, pp. S2.1 17–20, Dec. 2004.

[5] A. Jain, R. Bolle, and S. Pankanti (Eds), "Biometrics: Personal Identification in Networked Society", *Kluwer Academic*, Boston, 1999.

[6] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, issue 1, pp. 4–20, 2004

[7] L. Biel, O. Pettersson, L. Philipson and P. Wide, "ECG Analysis: A New Approach in Human Identification," *IEEE Trans. on Instrumentation and Measurement*, vol. 50, pp. 808–812, June 2001.

[8] T.W. Shen, W.J. Tompkins, and Y.H. Hu, "One-lead ECG for identity verification," in *IEEE Proc. of the Second Joint EMBS/BMES Conference, 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society*, vol. 1, pp. 62–63, 2002.

[9] Y.Y. Gu, Y. Zhang and Y.T. Zhang, "A novel biometric approach in human verification by photoplethysmographic signals", in *Proc. of 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine*, pp. 13–14, 2003.

[10] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," *Proc. SPIE*, vol. 4677, pp. 275–289, 2002.

[11] "Limitations of challenge-response entity authentication", *IEE Electronics letters*, vol. 25, no. 17, pp. 1195–1196, Aug. 1989.