A Novel Biometrics Method to secure Wireless Body Area Sensor Networks for Telemedicine and M-Health

Article *in* IEEE Communications Magazine · May 2006

DOI: 10.1109/MCOM.2006.1632652 · Source: IEEE Xplore

3 authors, including:

Carmen C. Y. Poon
The Chinese University of Hong Kong
118 PUBLICATIONS **3,930** CITATIONS
SEE PROFILE

Yuan-Ting Zhang
The Chinese University of Hong Kong
422 PUBLICATIONS **10,473** CITATIONS
SEE PROFILE

A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health

Carmen C. Y. Poon and Yuan-Ting Zhang, The Chinese University of Hong Kong
Shu-Di Bao, The Chinese University of Hong Kong and Southeast University

ABSTRACT

The development of the wireless body area sensor network (BASN) is imperative for modern telemedicine and m-health, but security remains a formidable challenge yet to be resolved. As nodes of BASN are expected to be interconnected on or in the human body, the body itself can form an inherently secure communication pathway that is unavailable to all other kinds of wireless networks. This article explores the use of this conduit in the security mechanism of BASN; that is, by a biometrics approach that uses an intrinsic characteristic of the human body as the authentication identity or the means of securing the distribution of a cipher key to secure inter-BASN communications. The method was tested on 99 subjects with 838 segments of simultaneous recordings of electrocardiogram and photoplethysmogram. By using the interpulse interval (IPI) as the biometric trait, the system achieved a minimum half total error rrate of 2.58 percent when the IPIs measured from signals, which were sampled at 1000 Hz, were coded into 128-bit binary sequences. The study opens up a few key issues for future investigation, including compensation schemes for the asynchrony of different channels, coding schemes, and other suitable biometric traits.

INTRODUCTION

When telemedicine was first proposed in the early 1970s, its function was often limited to, for example, patients seeking medical consultation [1]. Nowadays, the implication of the word telemedicine has been broadened to using telecommunication technology to provide medical information and services for a multitude of purposes, such as diagnosis of illness, transfer of medical data and records, monitoring rehabilitation or treatment processes, and even conducting surgical operations. Most recently, another notion has emerged that represents the evolution from traditional desktop telemedicine platforms for simply the practice of medicine to wireless and mobile configurations for delivering medical and healthcare services. This is referred to as mobile health or m-health [2].

The emergence of m-health can be accredited to the development of two Ws: wearable medical devices and wireless communication networks. Wearable medical devices are developed with the aim to collect individuals' medical data unobtrusively and ubiquitously around the clock without disrupting their normal daily lives, when previously only intermittent data could be collected during their irregular visits to clinics or hospitals. On the other hand, advances in wireless communications technology have overcome most of the geographical, temporal, and even organizational barriers to facilitate a completely roaming way of transferring medical data and records [3]. In order to fully utilize wireless technology in telemedicine and m-health, the real challenge lies in the need to develop another type of wireless area network: the body area senor network (BASN).

WIRELESS BODY AREA SENSOR NETWORKS FOR TELEMEDICINE AND M-HEALTH

The development of the BASN is derived from the recent development of the body area network (BAN), which is a system that interconnects devices or sensors *worn on* or *implanted in* the human body in order to share information and resources between the devices. Although the BASN and BAN may appear to be very similar to each other, the description of the BASN is definitely preferred when referring to the type of BAN in telemedicine and m-health where each node comprises a biosensor or a medical device with a sensing unit. In short, BASN is also named body sensor network (BSN).

The BAN was initially proposed to connect personal consumer electronic devices for the

 0163-6804/06/$20.00

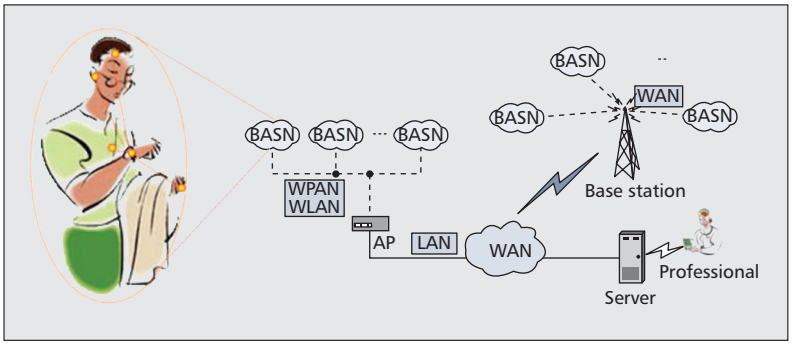

Figure 1. *System architecture and service platform of a BAN for telemedicine and m-health.*

sake of convenience to the user; however, it is found to be practically essential in telemedicine and m-health because several sensors placed at different body parts are often required in the cases of many patients who need long-term and continuous collection of medical data. This gives at least two reasons for setting up a BASN. The first is to optimize the use of resources in order to satisfy the stringent constraints in the terminals. For example, medical data collected from different sensors can be centralized before being passed on to external networks for remote analysis, diagnosis, or treatment. Second, a BASN enhances the control, scheduling, and programming of the overall system such that it is adaptive to body condition and external environment. For example, some nodes of a BASN may have to be reprogrammed from time to time (e.g., a device for drug delivery). In short, the need to develop the BASN is driven by the increase in the number of wearable or implanted biosensors to be placed on users.

The development of the BAN/BASN for telemedicine and m-health is only at an early stage. To date, development has been focused on building the system architecture and service platform, as illustrated in Fig. 1.

For example, in the MobiHealth project, Knostantas *et al.* [4] came up with an early BAN prototype by integrating existing technologies. The prototype was tested in nine clinical trials of different healthcare cases, including monitoring patients with cardiac arrhythmia and respiratory insufficiency. Wireless technologies like Bluetooth and Zigbee were used for inter-BAN communications, but for communicating with external networks technologies like General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) were used. The authors concluded that they had already clearly defined every component in the architecture of the service platform they proposed in the article. Nonetheless, they found that if only the current technologies were used, not all problems could be overcome. A typical example is the essential yet arduous challenge relating to the security, integrity and privacy of data transmission.

Another group of leading researchers in this area [5] recently reported the use of off-the-shelf wireless motion sensors to design a prototype of a wireless BAN for computer-assisted physical rehabilitation. The prototype featured a standard ZigBee compliant radio and a common set of physiological, kinetic, and environmental sensors. In their article they also introduced a multitier telemedicine system that can perform real-time analysis of medical data, provide feedback and warning messages to the user, and transfer data to medical servers. Coincidentally, they shared the same view that the security issues of using a BAN for telemedicine remained a formidable challenge yet to be resolved.

Security Challenges and Biometrics

To ensure security of the overall system, BAN/BASN must be protected, for example, against eavesdropping, injection, and modification of packets. Security issues in BANs/BASNs for telemedicine and m-health are particularly important because sensitive medical information must be protected from unauthorized use for personal advantage and fraudulent acts that might be hazardous to a user's life (e.g., alteration of system settings, drug dosages, or treatment procedures). Although the security issues in networks are always considered top priority, studies carried out in this area for BANs/BASNs were few. The very limited work found in this area is not applicable to BASN in telemedicine and m-health because the biosensors in a BASN must operate with extremely stringent constraints, a requirement that was relatively relaxed in generic BANs.

Less threatening than eavesdropping and tampering problems, but as important, is avoidance of interference between BASNs of different individuals, because communications of BASNs could easily cross over to each other when many people have their own BASNs in the future. Therefore, the problem of anti-interference must also be taken care of in the development of a BASN. Even though the two challenges seem to be unrelated to each other, the problems could be converged into one simple question: how can sensors or nodes of a BASN know that they belong to the same individual?

In this article we intend to present and investigate the system performance of a novel biometric solution to this question. Biometrics is a technique commonly known as the automatic identification or verification of an individual by his or her physiological or behavioral characteristics. In order to be a practical biometrics system, it is postulated that the utilized characteristics should be [6]:

- 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: yield a biometric system with good performance; that is, given limited resources in terms of power consumption, computation complexity, and memory stor-

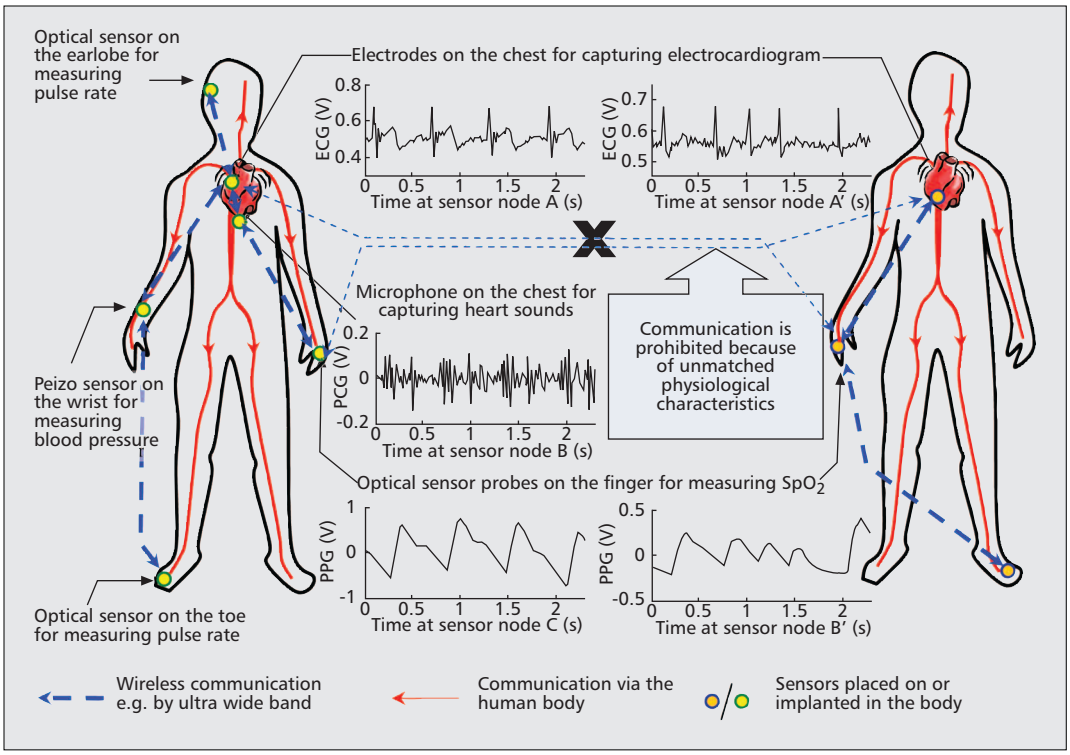

Figure 2. *An illustration of applying the biometrics approach to secure inter-BASN communications.*

It is believed that if used properly, these systems can be naturally secured conduits for information transmission within a BASN, where other techniques (e.g. by hardware or software programming) must be used in generic wireless networks to achieve the same purpose.

age, the characteristic should be able to be processed at a fast speed with recognized accuracy
- Acceptable: willingness of the general public to use as an identifier
- Invulnerable: relatively difficult to reproduce such that the biometric system would not be easily circumvented by fraudulent acts

Instead of applying biometrics generally in user authentication of common cryptosystems, we intend to develop a technique that would authenticate sensors nodes and/or secure cipher key transmission among them in BASN. As illustrated in Fig. 2, since the human body is physiologically and biologically well-known to consist of its own transmission or transportation systems (e.g., the blood circulation system), we would like to investigate how to make use of these secured communication pathways available specifically in BASN but not other wireless networks. It is believed that if used properly, these systems can be naturally secured conduits for information transmission within a BASN, where other techniques (e.g., hardware or software programming) must be used in generic wireless networks to achieve the same purpose.

The idea is particularly practical in securing BASN with a telemedicine or m-Health application, as nodes of these BASN would already comprise biosensors for collecting medical data, which could be physiological characteristics uniquely representing an individual. If these intrinsic characteristics can be used to verify whether two sensors belong to the same individual, the multiple usages of the recorded physiological signals will certainly save resources while adequate security measures are employed.

The Biometrics Solution

The technique is developed based on a symmetric cryptosystem, which assumes that a robust and secured key distribution scheme is available. In this respect, Cherukuri *et al.* [7] proposed using a group of similar random numbers generated from the properties of the human body at different sites (i.e., a biometric trait) to encrypt and decrypt the symmetric key for secured distribution of it. Since the biometric trait captured at different locations of the body should have slight variations, they employed a fuzzy commitment scheme [8] to ensure that errors in a recovered encryption key can be tolerable to certain degree. At the transmission terminal, the biometric trait (b) was used to commit the key (k), say, using $f_{commit}(k, b) = (hash(k) \,||\, b \oplus k)$, where $\oplus$ is the bitwise XOR operation and $||$ means concatenation. At the receiving terminal, the other biosensor would capture its own copy of the trait, a variant version b (b'), and use it to decommit the key k. If the selected characteristic is unique enough to represent an individual, the encryption key should only be recovered by the trait that is obtained from the same individual. On the other hand, as the biometric trait is used to encrypt the symmetric key, a major concern would be whether its degree of randomness is sufficient for cryptographic purposes. Insufficient randomness would open up the possibility for invaders to guess the coded trait and thus obtain the encryption key for decrypting the confidential medical data. Cherukuri *et al.* [7] suggested using physiological parameters with higher levels of entropy (e.g., blood glucose, blood pressure, and temperature). According to them, heart rate is not a good choice because

If these intrinsic characteristics can be used to verify whether two sensors belong to the same individual, the multiple usages of the recorded physiological signals will certainly save resources while adequate security measures are employed.

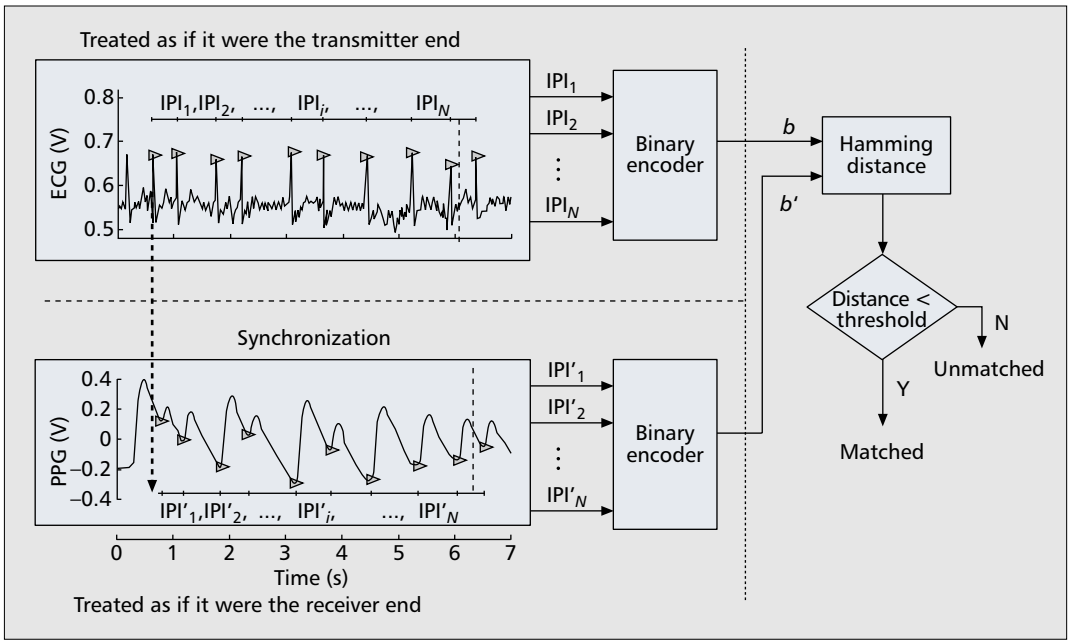

Figure 3. *A block diagram of the experiment protocol.*

its level of entropy is not satisfactory. Unfortunately, details of their work were not found.

In our studies we have, however, demonstrated that using the timing information of heartbeats can in fact be an excellent biometric characteristic for securing the BASN. As shown by Chi-square test and measurement of entropy, it is found that a biometric trait generated from a sequence of interpulse interval (IPI) has a high level of randomness. This finding is also supported by the chaotic nature of heart rate variability reported in literatures [9]. Building on the fuzzy commitment scheme [8] and the secure key transmission scheme in [7], some of us, Bao *et al.* [10], came up with a specific symmetric cryptosystem for BASN, which also considered the generation of the encryption key k from physiological signals and randomness evaluation of k. To this end, binding of the biometric trait with the encryption key can be achieved by some existing algorithms of integrating biometric into cryptosystems [6]. This biometric solution is suitable for securing BASN in telemedicine and m-Health because a higher security level can be achieved with less computation and memory requirement when compared with the generic cryptosystems.

In addition to securing the transmission of the encryption key within the nodes of a BASN, the biometric trait can also be used as an identity for entity authentication (i.e., node-to-node authentication) in a BASN, as proposed by Bao *et al.* in [11]. In that article a possible two-session communication protocol was discussed where the server initiated by sending out b together with a nonce to the client for comparison, and if b matched b', the client responded by sending back the nonce together with b'. A communication pathway would only be established if both the server and client found that the received copy (b'/b) matches the copy it has in hand (b/b').

In this study we further evaluate the performance of this biometrics approach by comparing the error rates of the biometric operating system under different conditions (i.e., when different bit lengths were used or the signals were sampled at different rates).

Experimental Testing and Results

We used data collected previously from two experiments, of which the original purpose was to simultaneously capture electrocardiogram (ECG) and photoplethysmogram (PPG) data for the estimation of blood pressure. In-house circuits were designed for capturing ECG and PPG via stainless steel electrodes and infrared optical sensors. In one experiment 14 healthy subjects were recruited and two PPGs captured from the index fingers of the two hands of each subject, and an ECG captured from three fingers of the subjects were recorded simultaneously for 2–3 min. In another experiment [12], 85 subjects were recruited, and within a 2-month period, ECG and PPG were captured for 2–3 min on 3/4 days. ECG and PPG were both sampled at 1000 Hz. An algorithm was developed to mark the peak of the R-wave of ECG and the foot of the PPG pulse.

We divided the ECG and PPG pairs into segments such that the corresponding ECG segment contained exactly 68 R-waves (resulting in 67 IPIs). A total of 838 data segments were obtained from the 99 subjects. As shown in Fig. 3, IPIs were obtained independent from the different physiological signals, and the sequence of IPIs in one segment was coded into a binary sequence b of 128 bits. Since the Hamming distance was used to evaluate the dissimilarity between two binary sequences b and b', the encoding method was carefully selected such that the Hamming distance of the binary codes corresponding to any two similar IPIs would be

small. Two binary sequences would only be considered "matched" if the Hamming distance was smaller than a threshold. Ideally, b and b' should match only if they were recorded from the same person during the same period of time.

Similar to the generic biometric verification systems, we evaluated the performance of the proposed biometric approach by two types of errors:

- False rejection rate (FRR), the rate of which b and b' measured from the same person during the same period of time were unmatched (i.e., corresponding to a node in the same BASN being rejected by the judging node)
- False acceptance rate (FAR), the rate of which b matched b' measured from a different person or at a different time (i.e., corresponding to a node of another BASN or an impostor being accepted as a legal node)

In addition to the conditions stated above, we investigated the performance of the operating system when the number of IPIs used for each b was reduced from 67 IPIs to 34 IPIs so that b would have 64 bits instead of 128 bits. We also studied the scenario when both ECG and PPG were downsampled from 1000 Hz to 200 Hz. The left and right panels of Fig. 4 show, respectively, the half total error rate (HTER = 1/2(FAR + FRR)) against the distance, and the genuine acceptance rate against the false acceptance rate for the different test conditions. The test conditions and the corresponding minimum HTER are summarized in Table 1.

Discussion

In this study the set of ECG and PPG was divided into segments such that the corresponding ECG segment contained an exact number of R-waves. By doing this, we assume that there is a time synchronization process between the different nodes. Time synchronization of nodes in a wireless network is very important, and state-of-the-art synchronization solutions for wireless sensor networks have already reached a precision of about 100 μs. Although instantaneous synchronization with precision of 1 ms is sufficient for the proposed scheme, the scheme requires the synchronization circuit to interact with the physiological signal detection circuit to record the timestamp upon arrival of the synchronization signal. Due to the physiology of the human circulation system, the generation of the QRS complex in a heart cycle must precede that of the detection of a pulse at the peripheral. Therefore, if the synchronization signal, which indicates the start of the generation of the biometric trait, is emitted by a master node that captures ECG, it is guaranteed that the IPIs captured by other nodes will match the one captured by the master node. Nonetheless, the situation is not straightforward if the synchronization signal is emitted by a node that does not have information about the start of a heart cycle. A possible solution is to examine using a decision scheme that allows one IPI misalignment in two binary sequences.

We select the Hamming distance as the metric for the proposed biometric trait because it works well with the bitwise XOR operation, which is one of the most common operations used in cryptosystems. By using this distance metric, we can be sure that the performance shown in this study reflects the situation where the biometric trait is actually used in securing BASN (e.g., using some of the previously discussed communication protocols for entity authentication or distribution of the cipher key).

From the experiment, minimum HTER is found to be 2.58 percent for 99 subjects (FRR = 3.99 percent). For the 14 healthy subjects, minimum HTER is almost 0 percent. It is found that the increase in error rates is not simply because of the larger sample size. In fact, when the examination was limited to only the 85 subjects, two-thirds of whom were aged 50 years old or above and were suffering from one or more chronic diseases at the time of the experiment, the minimum HTER is even higher (4.26 percent). We found that the major reason for the increase in error rate in the 85 subjects is due to the asynchrony of IPIs obtained from the ECG and PPG. It is noticed that the signals captured from the 85 subjects are noisier than those obtained from the 14 healthy subjects, and the automated detection algorithm was unable to identify the same number of R waves in ECG and pulses in PPG for some of the data segments. This could be due to motion artifacts or their health conditions (e.g., an R wave in ECG does not result in a corresponding pulse in PPG). Missing a characteristic point in either ECG or PPG will result in a mismatch in the series of IPIs obtained thereafter. Since our coding scheme did not take care of this situation, the Hamming distance obtained between two asynchronous series of IPIs is large. This can justify why FARs, which contributed mostly to the right part of HTER curves in Fig. 4a, do not show significant difference for the different subject groups, but the FRRs (left part of the HTER curves) do.

On the other hand, the bit-length of each sequence mainly affects the FAR (Fig. 4c). The minimum HTER is increased from 4.26 percent to 6.98 percent when the number of IPIs used for coding reduced from 67 to 34. We found that the current coding scheme may not be optimal for achieving a high performance system. For a person with an average heart rate of 60 beats per minute, the system would require over 1 minute for acquiring enough information for 1 binary sequence. In future, it is important to investigate other coding schemes, e.g. to use multiple IPIs instead of individual IPI, in order to maximize the performance with a minimal number of heartbeats required.

Lastly, it is found that reducing the sampling rate from 1000 Hz to 200 Hz does not have a significant effect on the performance of the system. Operating at a lower sampling rate saves resources and is therefore desirable. Nonetheless, it is anticipated that further reducing the sampling rate might degrade the performance, for the spectra of ECG and PPG would be distorted if the sampling rate went below 100 Hz.

The reason IPI can possibly be used to secure BASNs can be understood from the common security requirements laid down for generic biometric systems. Indeed, IPI fulfils most of the uni-

The situation will not be straightforward if the synchronization signal is emitted by a node that does not have information about the start of a heart cycle. A possible solution will be to examine using a decision scheme that allows one IPI misalignment in two binary sequences.

As mentioned before, an important limitation of BASN is it must be operated with extremely stringent constraints. For using the proposed approach, the increase in complexity of individual sensors would be minimal if a common biometric trait, e.g., IPI is readily available in all sensors.

# of subjects	# of data segments	Sampling rate (Hz)	# of IPIs used/ binary sequence	Coding bits	Minimum HTER (%)	FRR (%)	FAR (%)
14	49	1000	67	128	0.01	0.00	0.03
85	789	1000	67	128	4.26	6.46	2.06
99	838	1000	67	128	2.58	3.99	1.18
85	1599	1000	34	64	6.98	9.51	4.46
85	789	200	67	128	4.65	6.95	2.35

Table 1. *Test conditions, the resultant minimum HTER and the corresponding FAR and FRR.*

versally accepted requirements of a good trait as presented by Jain *et al.* [6]. It is not difficult to find that IPI is a trait that is universal, collectable, effective, and acceptable. IPI is a vital sign that can be collected from any living human being. More important, it can be obtained with different types of sensors and from several kinds of physiological signals that are related to the cardiovascular system (e.g., ECG, PPG, and heart sounds). These physiological signals, which are typically one-dimensional low-frequency signals, can be collected by medical equipment at a reasonably low cost. As its dimensions are few and its resolution is low, processing them and obtaining the trait from them are likely to be computationally inexpensive. Therefore, such a trait is effective and could yield good performance. In addition, these physiological signals are often the basic physiological signals that will be collected in a telemedicine or m-health application for clinical purposes. This ensures that their acceptability is not an issue and that calculating IPI from them for securing data transmission will hardly increase the resources required from the terminals. This last characteristic is important to the application of BASNs in telemedicine and m-health, which must operate in an environment with extremely stringent constraints.

Perhaps the most distinctive feature of using this biometrics in BASNs compared to its usage in conventional biometric systems is that the trait to be used in BASNs should be random in nature. This is contrary to the requirement of a trait for a conventional biometric system, where templates of the trait are stored in the system as a reference to compare against a copy of the trait captured in real time for identification or authentication purposes. Due to the way the conventional system operates, the trait must be time-invariant; otherwise, it is futile to compare newly captured traits with those available in the database. Unlike conventional biometric systems, the biometric trait in a BASN is captured independently but simultaneously. Therefore, there is no need for the trait to be permanent. In fact, the level of security is enhanced when the trait changes with time and possesses a chaotic nature, since this would make it very difficult for an invader to guess the trait, which can be the authentication identity or the means to secure the cipher key. Furthermore, if the signal changes with time, the system may even reassign a new key once a while, and thus further enhance the level of security. Therefore, the criteria for requiring the trait to be distinctive, permanent, and invulnerable should be modified in the case of applying it in BASNs as follows:

- Distinctive: The characteristic should be sufficiently different on any two individuals when copies of it are captured simultaneously, even if the copies are captured by different types of biosensors and at different locations of the body.
- Time-variant but invulnerable: The characteristic should change with time and have a high level of randomness so that biometric traits captured at different times would not match even if they are obtained from the same individual. This ensures a much higher level of security.

With these principles established, the use of biometrics in BASNs for telemedicine and m-health can be extended to using other physiological signals or parameters as traits, as long as they satisfy the criteria discussed above. However, IPI is selected for research because of its unique characteristics. IPI can be obtained with different types of sensors and from different physiological signals (e.g., ECG, PPG, heart sounds, blood pressure wave, and blood flow) so that it is available to a multitude of biosensors that serve different functions in BASNs. IPI also has the advantage that the variation of it is usually acceptable even if it is measured at different body parts (e.g., from the chest, fingertips, or a lower limb). Unlike body temperature, which varies if the sensors are implanted in the body or placed on the body surface, IPI can be measured without much variation using sensors implanted in the body (e.g., intra-arterial catheter) or placed on the body surface (e.g., using electrodes to capture ECG).

As mentioned before, an important limitation of a BASN is that it must operate under extremely stringent constraints. For using the proposed approach, the increase in complexity of individual sensors would be minimal if a common biometric trait (e.g., IPI) is readily available in all sensors. We illustrate an example (Fig. 2) with a list of practical biosensor which capture physiological signals that embed IPI information. For signals that embed the biometric trait, the increase in complexity of sensors, in terms of both computation and memory requirement, would be minimal.

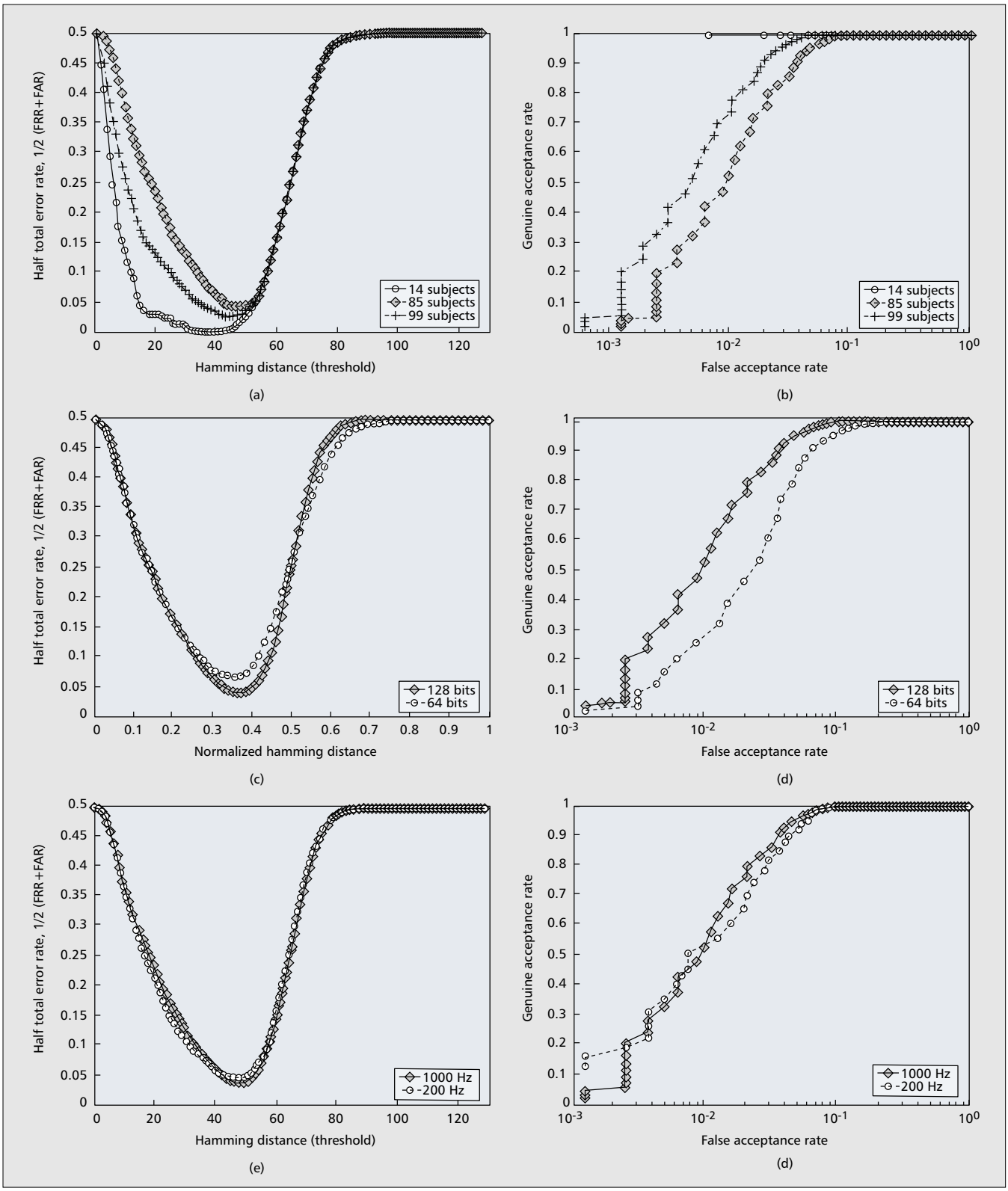

Figure 4. *The performance of the biometrics system operating under different conditions: a) and b) with different numbers of subjects; c) and d) using different numbers of coding bits; e) and f) at different sampling rates.*

Nonetheless, IPI has its own limitations, and obviously, no matter how commonly it can be found in physiological signals, not every biosensor captures signals with IPI information. Typical examples are motion sensors placed on knees or in shoes. For these nodes, an extra sensor may be needed to implement the proposed approach. It has been pointed out that having a biosensor just for the sake of securing inter-BASN communication may result in bulkier sensors and consequently limit its acceptance. Despite this fact, the increased complexity is

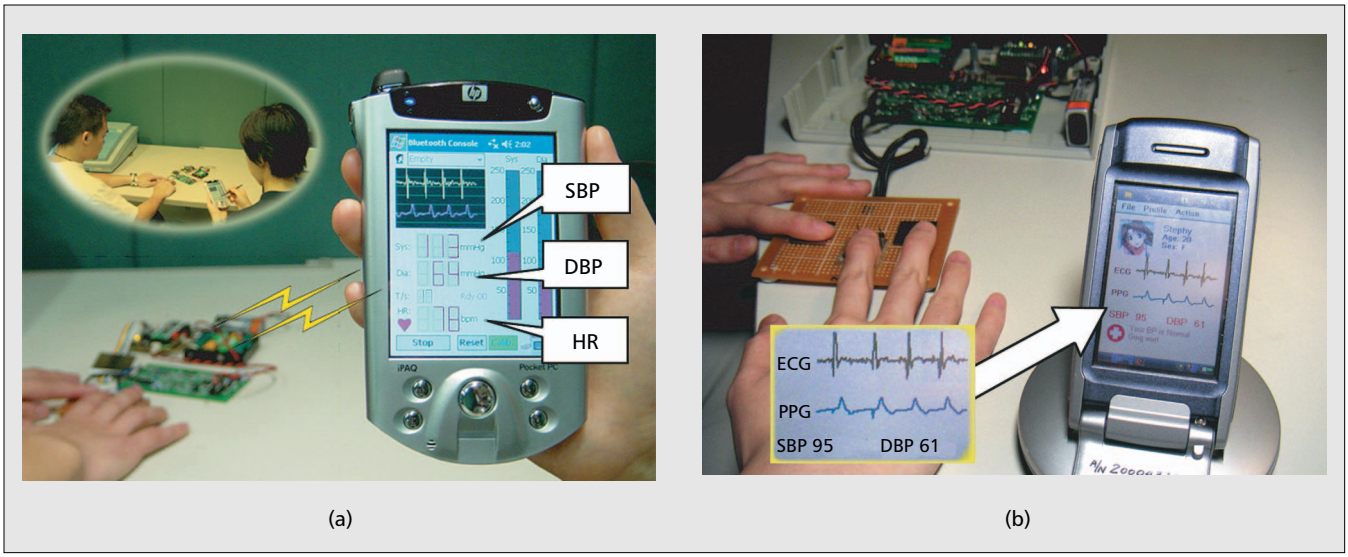

Figure 5. *Wireless and cuffless blood pressure meters: a) PDA-based; b) mobile-phone-based.*

worthwhile in view of the increased security it can bring about, particularly when compared to that required by existing technology to achieve a similar level of security. The increased complexity could be minimized by careful selection of the type of sensors. It is also important to explore other usages of the extra sensor (e.g., by investigating data fusion methods to fully exploit the new information). Concerning sensors placed on body parts where capturing IPI information is difficult, the situation will be more difficult and may require a node that has less resource restriction to act as a bridge for distributing the cipher key to the sensors by other methods.

Lastly, it has also been pointed out that a developing technology (ultra wideband, UWB, radar [13]) for remote capturing of heart rate could post security threats on the proposed technology. Although current UWB radar technology may not be mature enough to perform this fraudulent act, it indeed opens up such a future possibility. In this respect further studies must be carried out to investigate how to enhance the proposed technology to prevent this kind of attack.

Concluding Remarks and Application Scenario

This article introduces a novel biometrics approach to secure wireless BASNs for telemedicine and m-health, and illustrates the concept by using IPI as an example. Evaluating the method on 838 datasets collected from 99 subjects, it is found that the minimum HTER is 2.58 percent (FAR = 1.18 percent and FRR = 3.99 percent) when the signals are sampled at 1000 Hz and the trait is coded into a 128-bit binary sequence. The study has opened up a few key issues for future investigation, including compensation schemes for the asynchrony of different channels (due to diseases, physiological phenomena, motion artifacts, diction errors, etc.), coding schemes, and other suitable biometric traits.

The findings of this study complement the major research work of our research center in the development of wearable intelligent sensors and systems (WISS) for telemedicine and m-health applications [3, 12]. WISS can be nodes of BASNs; examples include a wireless and cuffless blood pressure measurement device that is developed based on a PDA and mobile phone [12]. Figure 5 illustrates the prototypes of this device, where a sensing module is used to collect physiological signals from the user, and a personal base station (a PDA or mobile phone) is used to receive the physiological parameters such as heart rate, blood pressure, and their variabilities. At present, signals are conveyed via Bluetooth transmission. In the foreseeable future we shall be actively looking into integrating a biosensor onto this kind of personal base station to turn it into a master node of a BASN so that all other sensing modules worn on or implanted in the body can be connected to it. The biometrics system discussed in this article can be employed to ensure the authenticity, confidentiality, and integrity of the data transmission between the master node and all the other sensory nodes. Just as the development of the two Ws has broadened the scope of telemedicine and brought about the notion of m-Health, the use of biometrics for securing wireless BASNs can be a key opening up a new era for telemedicine and m-health.

Acknowledgment

This work was supported in part by Hong Kong Innovation and Technology Fund. We are grateful to Standard Telecommunication Ltd., IDT Technology Ltd., Jetfly Technology Ltd., Golden Meditech Company Ltd. and Bird International Ltd. for their supports given to the ITF projects. We are also thankful to the reviewers for their valuable comments and suggestions.

References

[1] R. L. Bashshur, T. G. Reardon, and G. W. Shannon, "Telemedicine: a New Health Care Delivery System," *Ann. Rev. Public Health*, vol. 21, 2000, pp. 613–17.

[2] R. S. H. Istepanian, E. Jovanov, and Y. T. Zhang, "Guest Editorial 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, 2004, pp. 405–14.
[3] K. Hung and Y. T. Zhang, "Implementation of a WAP-Based Telemedicine System for Patient Monitoring," *IEEE Trans. Info. Tech. Biomed.*, vol. 7, no. 2, June 2003, pp. 101–07.
[4] D. Konstantas *et al.*, "Mobile Patient Monitoring: The MobiHealth System," *Proc. Int'l. Cong. Med. and Care Compunetics*, Hague, The Netherlands, 2–4 June 2004.
[5] E. Jovanov *et al.*, "A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation," *J. NeuroEng. and Rehab.*, vol. 2, no. 11, Mar. 2005, p. 6.
[6] U. Uludag *et al.*, "Biometric Cryptosystems: Issues and Challenges," *Proc. IEEE*, vol. 92, no. 6, June 2004, pp. 948–60.
[7] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A Biometric based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body," *Proc. IEEE Int'l. Conf. Parallel Processing Wksp.*, 6–9 Oct. 2003, pp. 432–39.
[8] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," *Proc. 6th ACM Conf. Comp. and Commun. Sec.*, G. Tsudik, Ed., 1999, pp. 28–36.
[9] I. Radojicic, D. Mandic, and D. Vulic, "On the Presence of Deterministic Chaos in HRV Signals," *Proc. Comp. in Cardiology*, Sept. 2001, pp. 465–68.
[10] S. D. Bao, Y. T. Zhang, and L. F. Shen, "A New Symmetric Cryptosystem of Body Area Sensor Networks for Telemedicine," *Proc. 6th Asian-Pacific Conf. Med. and Bio. Eng.*, Japan, Apr. 2005.
[11] S. D. Bao, Y. T. Zhang, and L. F. Shen, "Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems," *Proc. 27th IEEE Int'l. Conf. Eng. Med. and Bio. Soc.*, Shanghai, China, Sept. 2005.
[12] C. C. Y. Poon and Y. T. Zhang, "Cuffless and Noninvasive Measurements of Arterial Blood Pressure by Pulse Transit Time," *Proc. 27th IEEE Int'l. Conf. Eng. Med. and Bio. Soc.*, Shanghai, China, Sept. 2005.
[13] E. M. Staderini, "UWB Radars in Medicine," *IEEE AESS Sys.*, Jan. 2002, pp. 13–18.

BIOGRAPHIES

CARMEN C. Y. POON (cpoon@ee.cuhk.edu.hk) received her B.A.Sc. in engineering science (biomedical option) and her M.A.Sc. in biomedical engineering at the University of Toronto, Canada. She is currently a Ph.D. student at the Chinese University of Hong Kong (CUHK). Her research interests include biosignal processing and biosystem modeling, and development of wearable medical devices for telemedicine and m-health. She was awarded first prize, the IFMBE Outstanding Chinese Student Award, at the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society in 2005.

YUAN-TING ZHANG (ytzhang@ee.cuhk.edu.hk) received his Ph.D. from the University of New Brunswick, Canada, in 1990. He joined CUHK as a lecturer in 1994, became an associate professor in 1996, and a professor in 2002. He serves currently as director of the Joint Research Centre for Biomedical Engineering, Head of the Division of Biomedical Engineering at CUHK, and chairman (adjunct) of the Department of Biomedical Engineering at Sun Yat-sen University, China. He was the Vice-President of IEEE Engineering in Medicine and Biology Society (EMBS) in 2000 and 2001. His research focuses on wearable medical devices, body sensor networks, and bio-model-based signal processing for telemedicine and mobile healthcare.

SHU-DI BAO received her B.S. degree from Ningbo University, China, in 1999, and her M.S. degree from Southeast University, Nanjing, China, in 2003. She is currently a Ph.D. candidate in electronic engineering at Southeast University and a research assistant at CUHK. She won the Young Investigator Award (YIA) and YIA Best Presentation Award at the 6th Asian-Pacific Conference on Medical and Biological Engineering held in Japan in 2005. Her current research interests include information retrieval, security and fault tolerance, and efficient communications for body sensor networks and telemedicine systems.

Just as the development of the two Ws has broadened the scope of telemedicine and brought about the notion of m-Health, the use of biometrics for securing wireless BASN can be a key in opening up a new era for telemedicine and m-Health.