Review Article

A Review on Body Area Networks Security for Healthcare

Guang He Zhang,^{1,2,3,4} Carmen Chung Yan Poon,^{3,5} and Yuan Ting Zhang^{3,4,5}

¹ Institute of Computing Technology, Chinese Academy of Sciences (CAS), Beijing 100190, China

² Graduate University of CAS, Beijing 100049, China

³ CAS/CUHK Research Centre for Biosensors and Medical Instruments, Institute of Biomedical and Health Engineering (IBHE), Shenzhen Institute of Advanced Technology (SIAT), Shenzhen 518055, China

⁴ The Key Laboratory of Health Informatics of CAS, Shenzhen 518055, China

⁵ The Joint Research Centre for Biomedical Engineering, The Chinese University of Hong Kong, Shatin, NT, Hong Kong

Correspondence should be addressed to Carmen Chung Yan Poon, cpoon@ee.cuhk.edu.hk
and Yuan Ting Zhang, ytzhang@ee.cuhk.edu.hk

Received 18 March 2011; Accepted 2 May 2011

Academic Editors: H. Abdel-Wahab, R. Montemanni, and H. M. Sun

Copyright © 2011 Guang He Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Body area networks (BANs) are emerging as one of the main research trends in recent years, particularly in the area of personal health monitoring. Since health data are private and sensitive information, the security of data transmission within a BAN becomes a critical issue that requires immediate attention. In this paper, we attempt to examine possible attacks of the resource-constrained BANs and present state-of-the-art communication protocols, cryptographic methods, and key management schemes that are useful for BANs security. We will also discuss the problems of existing solutions and possible future research directions on security for BANs. A novel biometric method that utilizes the biological channels (biochannels) to assist secure information transmission within a BAN will also be highlighted and discussed.

1. Introduction

Body area networks (BANs) seamlessly connect miniaturized and low-power devices and biosensors that are worn on or implanted in human body. The development of BANs is emerging as one of the main research trends, particularly to collect and jointly process biological data for continuous and long-term monitoring of health conditions [1–4]. Since medical and health data are private and sensitive information that are protected by law in many countries, for example, by the Health Information and Portability Accountability Act (HIPAA) in the USA [5], the European Union Directive 2002/58/EC in Europe [6], and Law of the People's Republic of China on Medical Practitioners in China [7], the security of data transmission within BANs must be addressed in order for them to be widely used in real-life health applications.

Although BANs share some common features with generic wireless sensor networks (WSNs), it is anticipated that the two networks should have very different security schemes. WSNs have many constraints, such as low computation capability, small memory, and limited energy

resources, and the security issues of them have been previously addressed in literatures [8]. SPINS is a suite of security protocols optimized for sensor networks, where the base station accesses nodes using source routing [9]. Differed from SPINS, Undercoffer et al. [10] proposed another protocol that relies upon broadcasts and provides a mechanism for detecting certain types of aberrant behaviours. TinySec is the first fully implemented link layer security architecture for WSNs [11]. It generated secure packets by encrypting data using a group key shared among sensor nodes and calculating a message integrity code (MIC) for the whole packet, including the header.

These security methods that were proposed or implemented for WSNs are not optimal, if not impractical, for BANs, which require a security solution that consumes even less energy and memory space than generic WSNs.

(1) *Energy Consumption.* Unlike generic WSNs, sensors of BANs are placed on or implanted in human body and powering the sensors will at the same time dissipate heat and cause

adverse effects to the human tissues around them. Moreover, small sized battery of biosensors can only carry a limited amount of energy and, in some cases, cannot be recharged conveniently. Meanwhile, both communication and computation operations consume a lot of energy [12]. Broadly speaking, the existing security solutions required a great deal of communication and computation operations and the large amount of energy dedicated for these operations makes them unrealistic for BANs, particularly considering applications that demand real-time data exchange and transmission.

(2) *Memory Occupation.* The size of biosensors and medical devices has to be small enough to avoid disturbing the daily life of the user, and thus the memory of these entities in BANs is extremely limited. For example, in the SmartDust project, TinyOS consumes about 3500 bytes of memory, leaving only 4500 bytes for security and applications, which is insufficient for the current security algorithms [8].

In order to satisfy the above requirements, characteristics of BANs should be taken into account when developing the communication protocols as well as the respective security solutions based on these protocols. Regarding the communication protocol, the communication distance of BANs should be less than the height of the human body (about 2.5 meters). Moreover, the positions of biosensors of BANs are relatively stationary, even though their relative positions may change due to body movement. Considering these characteristics will help developing a lightweight communication protocol suitable for BANs.

BANs will also incorporate a smaller quantity of sensors per network compared to generic WSNs, but multiple BANs will have to be set up securely and independently in close proximity. BANs will have access to their own biological and behavioural data as well as biocommunication channels. These resources should be utilised to formulate an optimal solution for BANs. For example, physiological data can be used to generate keys for confidentiality and authentication and the human body can be used as secure channel to distribute keys.

In short, security methods for BANs should not be directly adopted from existing approaches. In this paper, we intend to summarize the efforts made thus far on designing security approaches for BANs. The rest of the paper is organized as follows. Security threats and requirements of BANs are presented in Section 2. We then discussed the security methods of IEEE standard 802.15 communication protocols in Section 3. Public key cryptography (PKC) and symmetric key encryption (SKE) for BANs are, respectively, summarized in Section 4. Key management in BANs, specifically for symmetric keys, is discussed in Section 5. Finally, conclusions are drawn in Section 6.

2. Security Threats and Requirements

For BANs that are used for health applications, they must be protected from impostor nodes or devices that (1) eavesdrop health information (2) access health information without authorisation (3) fabricate identity to verify authentication

(4) deny health information that had been sent or received, and (5) alter health information. To cope with these security threats, the research of security requirements of BANs must include five intertwined areas: confidentiality, authorization, authentication, nonrepudiation, and integrity control [13].

2.1. *Confidentiality.* To prevent any personal health information from being eavesdropped by the attacker, the genuine sensors should not transmit the health information in plain text within a BAN. The confidentiality of health information can be assured by incorporating encryption operations.

2.2. *Authorization.* Authorization mechanism ensures that only authorized entities can be involved in providing information to communicated entities but unauthorized entities cannot. An authorization mechanism can assign the access privileges and limit free access. Without an effective authorization mechanism, the attacker can easily access the health information without any constraints.

2.3. *Authentication.* Authentication, one of the most important security primitives, includes entity authentication and data authentication. Entity authentication is a security mechanism that guarantees that entities are who they claim to be. Data authentication allows a receiver to verify that the data really was sent by the claimed sender and prevents an intruder or unauthorized entity to report false health data or give harmful instructions to the biosensors or medical devices of a BAN, and it can be implemented by digital signature using PKC or by MIC using SKE.

2.4. *Nonrepudiation.* Nonrepudiation assures that an entity cannot deny facts transmitted or receiving any message in BANs. That is to say, all operations of the sender and receiver of health information can be monitored. Furthermore, the attacker can be traced and captured if any nonrepudiation evidence is recorded in communications. Operations of digital signature and digital certificate can provide nonrepudiation for the transmission process of health information in BANs.

2.5. *Integrity Control.* There is a danger that health information will be modified, deleted, and replaced during transmission by a hostile entity or a device error in BANs. Incomplete or wrong health information may result in life-threatening consequences to the owner of BANs. The integrity control is absolutely necessary where any alteration of health information can be detected by communication entities. The calculation of message digest or MIC can check information integrity. Using PKC can also provide integrity protection. However, this often requires out-of-band channels to authenticate the public keys.

3. Security Methods in Existing Communication Protocols

Some of the developers of BANs had already applied three standard communication protocols that sponsored by the

IEEE standards committee for WSN communications [14–16]: IEEE 802.15.1 (Bluetooth) [17], IEEE 802.15.3 (ultra wideband, UWB) [18] and IEEE 802.15.4 (Zigbee) [19], and the draft of communication protocol of IEEE 802.15.6 has been developed specifically for BANs recently. Security issues of these standards are summarized as follows.

3.1. IEEE 802.15.1 (Bluetooth). Four different entities are used for maintaining security at the link layer: a public address which is unique for each user, two secret keys, and a random number which is different for each new transaction. The initialization key is used as the link key during the initialization process when no combination or unit keys have been defined and exchanged or when a link key is lost. The initialization key protects the transfer of initialization parameters. The key is derived from a random number, a personal identification number (PIN) code, or the public address. The PIN can be a fixed number stored in Bluetooth units that do not have a man-machine interface (MMI). Alternatively, the PIN can be selected arbitrarily by the user and entered in units with an MMI.

The limitation of using PIN code to generate the initialization key is that the fixed PIN code is easily attacked by brute force attacking, and entering PIN codes are impractical because nearly all biosensors in a BAN do not have an MMI, especially for the implanted biosensors. Therefore, the security solution in Bluetooth is unsuitable for BANs although how to implement authentication and encryption is described in detail in the specification of Bluetooth.

3.2. 802.15.3 (UWB). UWB supports communications with either no security or strong cryptography. A device operating in no security shall not perform any cryptographic operations on medium access control (MAC) frames, while devices operating in strong security use symmetric key cryptography to protect frames using encryption and integrity. The standard supports the protection of command, beacon and data frames using 128-bit advanced encryption standard (AES) security suite and key management. To prevent replay of old messages, a strictly increasing time token is included in the beacon. A device may reject as invalid a received beacon with a time token less than or equal to the current time token.

The UWB protocol describes no details about authentication, authorization, and nonrepudiation.

3.3. 802.15.4 (Zigbee). The cryptographic mechanism in the standard of [19] is based on symmetric-key cryptography. The requirements of security are data confidentiality, data authenticity, and replay detection. It has 8 security levels, which include encryption and authentication, as well as combined encryption and authentication with different security attributes in MAC sublayer. The security solution of Zigbee does not consider the two most important aspects in symmetric-key cryptography: key generation and distribution. The security level of the standard is therefore unknown, and it strongly relies on which security attribute is selected, the randomness of the key in use, and whether

TABLE 1: The summarization of security methods in these communication protocols.

Protocols	Bluetooth	UWB	Zigbee	TG6
Confidentiality	Yes	Yes	Yes	Yes
Authorization	No	No	No	No
Authentication	Yes	No	Yes	Yes
Nonrepudiation	No	No	No	No
Integrity control	No	Yes	No	Yes

a symmetric key can be distributed securely before the beginning of a communication session.

3.4. 802.15.6. Although the above three communication protocols are currently most frequently used by developers of BANs, they are not optimized solutions as they did not fully consider the constraints and security requirements of BANs. In view of this, IEEE 802.15.6 Task Group 6 (TG6) has been formed with an aim to develop a communication standard optimized for low-power devices and operations on, in, or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer, electronics or personal entertainment [20].

At present, the latest standardization of TG6 draft (IEEE P802.15-10-0245-06-0006) [21] suggests that there are three security levels between nodes and hubs in the secured communication of BANs: unsecured communication, authentication but not encryption, authentication, and encryption. The security service in this draft mainly focused on the key generation, key distribution, and message authentication, the key generation and distribution are based on Diffie-Hellman key exchange method and preshared association, and the MIC is used to authenticate message. The AES has been proposed as cipher function in this draft.

3.5. Summary. To summarize, the security approaches used in existing communication protocols (i.e., Bluetooth, UWB, and Zigbee) are unsuitable for BANs applications given the threats and requirements of BANs security outlined in Section 2. Therefore, researchers of TG6 have already considered some security requirements of BANs and developed the draft of new communication protocol for this purpose. However, the draft did not refer to every security requirement of BANs and thus these threats have not been resolved completely. The security methods in these communication protocols were summarized in Table 1.

4. Key Cryptography in BANs

4.1. Public Key Cryptography in BANs. Selecting an appropriate cryptographic method is crucial because all security services have to be ensured by cryptography. Both PKC and SKE have been proposed for BANs security, and there is no consensus so far which should be used. The state-of-the-art PKC and SKE are summarized in this section and next section, respectively.

PKC is developed based on some mathematical problems where the direct operation is straightforward while the reverse operation is computationally hard. PKC makes use of these problems to generate the public key from the private key but protect the private key from being known when disclosing the public key. Compared with SKE, one of the most attractive features of PKC is that it does not require a secured channel for the initial distribution of keys.

Two most popular mathematic problems used in PKC are the integer factorization problem, from which the well-known RSA cryptosystem [22] is derived, and the discrete logarithm problem, which the more recent elliptic curve cryptography (ECC) [23, 24] is based on. Both RSA and ECC are widely used in traditional network security for authentication and encryption but commonly believed to be impractical for WSNs due to the requirements on computational intensity, code and data size, processing time, and power consumption. Nevertheless, recent studies demonstrated that most operations of RSA and ECC are feasible for WSNs or even BANs after optimizing the expensive large integer operations, especially multiplication, exponentiation, and reduction, for improving the speed of public and private keys generation while reducing the memory occupation and energy consumption.

For example, Gura et al. [25] implemented ECC and RSA on two 8-bit microcontrollers (Atmel ATmega128 at 8 MHz) by a new algorithm that reduces the number of memory accesses to accelerate multiple-precision multiplication. On an Atmel ATmega128 at 8 MHz without hardware acceleration, they were able to perform an RSA-1024 operation with exponent $e = 2^{16} + 1$ in 0.43 second using 542 bytes of data memory and 1,073 bytes of code and a 160-bit ECC point multiplication in 0.81 second using 282 bytes of data memory and 3,682 bytes of code. Malan et al. [26] implemented ECC for a WSN on a 8-bit, 7.3828-MHz MICA2 mote by optimizing the algorithms for addition and multiplication of points, conversion of integers to nonadjacent form, and generation of pseudorandom numbers. Public and private keys are generated within 34.2 seconds and 0.23 second, respectively, and occupied just over 1 KB of SRAM and 34 KB of ROM.

Wander et al. [27] reduced the amount of data exchanged in a typical Internet-based secure sockets layer (SSL) handshake to conserve energy. By doing so, they were able to implement authentication and key exchange protocols of PKC on an Atmel ATmega128 L low-power microcontroller. The energy cost of their key exchange protocol of RSA-1024 is 15.4 mJ in client and 304 mJ in server, while the one by elliptic curve digital signature algorithm with 160-bit keys (ECDSA-160) is 22.3 mJ either client or server.

A hybrid multiplication method [28] has been proposed by Wang et al. for accelerating exponentiation in RSA and ECC by reducing the number of memory accesses in conventional multiprecision multiplication. On MICAz motes with 4 KB RAM, the method used 15,832 byte for code and 3,224 byte for data to perform 1024-bit RSA public and private key operation in 0.79 s and 21.5 s, respectively. The

method also completed a 160-bit ECC signature generation and verification in 1.3 s and 2.8 s on MICAz motes, respectively, and in 1.60 s and 3.30 s on TelosB motes.

Uhsadel et al. [29] observed that over three quarters of the processing time for elliptic curve operations were spent on modular multiplication. Therefore, they presented an optimized arithmetic algorithm that can complete a modular multiplication for a 160-bit standard compliant elliptic curve (secp160r1) on 8-bit microcontrollers in 0.37 ms and thereby significantly reduced the processing time and lowered the energy consumption of ECC in sensor networks. This brings the vision of implementing PKC for BANs with all its benefits for key distribution and authentication a step closer to reality.

Other researchers proposed integrating ECC into the security protocols of WSNs or BANs. For instance, TinyECC, a configurable library for ECC operations in WSNs, is implemented [30], and its flexibility allowed it to be integrated into sensor network applications by developers. Tan et al. [31] developed protocols using ECC based on identity-based encryption-Lite (IBE-Lite) for BANs.

In conclusion, the speed of the public and private key generation or signature generation and verification have been significantly reduced; however, the memory and power requirement of these operations are still found to be unaffordable to biosensors of BANs. Moreover, RSA and ECC are also considerably slow for encrypting and decrypting large volumes of health data in practice.

4.2. Symmetric Key Cryptography in BANs. In contrary, using SKE for BANs security is preferred because it needs fewer resources (e.g., in terms of memory and computation capacities). Different from using public key for encryption and private key for decryption in PKC, encryption key and decryption key are the same in SKE. In this section, we will introduce several symmetric cryptographic algorithms that can be used for BANs.

Rivest cipher 4 (RC4) was designed by Ronald Linn Rivest. It generates a pseudorandom stream of bits (a keystream) and combines these bits with the plaintext using bitwise exclusive-or for encryption and decryption. Rivest cipher 5 (RC5) is a block cipher notable for being more secure than RC4 but at an expense of speed, simplicity, and efficiency. In order for using RC5 in sensor networks, the RC5 system architecture has been recently investigated for developing a high-performance design in terms of encryption throughput [32]. The architecture, designed with a pipeline technique, was able to increase the encryption throughput by over 80% when compared to related work.

The AES, which has been proposed to be used in IEEE standard 802.15.3, is a new encryption standard adopted by the US government to replace the previous data encryption standard (DES). The AES comprises three block ciphers, AES-128, AES-192, and AES-256. The AES algorithm has been recently implemented in a BAN node [33].

Noticing that traditional symmetric cryptographic algorithms such as RC5 and Skipjack are not designed for the 8-bit computing devices used in sensor networks; a new cryptographic algorithm HIGHT has been proposed and

TABLE 2: The summarization of cryptographic algorithms.

Algorithms	Description
RC4	Stream cipher, simple.
RC5	Block cipher, a variable block size (32, 64, or 128 bits), more secure than RC4.
AES	Block cipher, a 128-bit block size, the encryption standard adopted by the USA
HIGHT	Block cipher, block size (64 or 128 bits)
KATAN	Block cipher, block size (32, 48, or 64 bits)

evaluated [34]. HIGHT is designed with a 64-bit block length and 128-bit key length, which are suitable for low-cost, low-power, and ultralight implementation. It uses a 32-round iterative structure, which is a variant of the generalized Feistel network. When implemented on MICA2, HIGHT is found to consume less power than RC5 on TinySec while operate at a similar speed and take up a reasonable memory size.

KATAN/KTANTAN is a new family of very efficient hardware-oriented block ciphers [35]. KATAN is composed of three block ciphers, with 32-, 48-, or 64-bit block size, and KTANTAN contains the other three ciphers with the same block sizes. It has better performance than other lightweight algorithms in [36, 37].

The feasibility of various cryptographic algorithms (e.g., RC4, RC5, MD5, IDEA), including key setup time, memory occupation, encryption and decryption time, and so forth, has also been investigated for sensor networks on an Atmel Atmega128 L 8-bit, 7.3728 MHz microprocessor [38]. The 128-bit key setup time of RC4 is only 5.09 milliseconds while RC5 is 17.39 milliseconds. The data memory of RC4 and RC5 is 0 bytes while the program memory of RC4 and RC5 is 428 bytes and 5,808 bytes, respectively. For a 128-byte plaintext, the encryption time of RC4 and RC5 is about 10 milliseconds and 60 milliseconds, while the decryption time of them is about 5 milliseconds and 40 milliseconds. Amongst different algorithms, the RC4 showed the best cryptographic processing time and power dissipation. Therefore, Zhang et al. [39] presented a simple, lightweight, and robust protocol based on RC4 and achieved data confidentiality, authentication, integrity with low overhead and simple operations. The protocol is considered to be suitable for BANs security.

These cryptographic algorithms can be summarized in Table 2.

5. Symmetric Key Management in BANs

Key management is the hardest part of cryptography in reality. The two most important aspects of key management are key generation and distribution. As aforementioned, asymmetric key generation in PKC is based on some hard mathematical problems and does not require a secured channel for key distribution. On the other hand, key generation algorithms of SKE are less computation expensive, but the distribution of the symmetric key requires a secured channel or method. In this section, we will review key generation and distribution for SKE in BANs.

5.1. General and Biometric-Based Symmetric Key Generation. Symmetric keys for data encryption or entity authentication are random binary sequences (BSs). In theory, hardware random number generators based on some physical process with inherent randomness should be used as a seed to generate a true random BS; however, the process of the truly random BS generation using this method is rather complicated and slow. Two most commonly used methods for generating random and pseudorandom BSs are to convert from random source signals and to calculate by mathematical algorithms (e.g., linear congruential generator), respectively.

For example, error of the received bits, which is randomly distributed and uncorrelated from one sensor to another, has been proposed to be used to generate cryptographic pseudorandom numbers for nodes of WSNs [40]. Latif et al. [41] also presented a method for generating BSs for sensor networks by converting from a digital received signal strength indicator (RSSI) of a communication packet, and the RSSI is the measurement of the power present in a received radio signal. The benefit of these methods is that they have low communication operating costs and do not require additional hardware; however, the randomness of the resulted BSs that are generated from the error of the received bits depends on the quality and frequency of communication. If RSSI is to be used, all nodes except the base station must change their positions from time to time such that different RSSI are read to generate random BSs. Neither methods are suitable for BANs since the error of the received bits in BANs is uncertain and the position of nodes in BANs is relatively stationary.

On the other hand, biological data are potentially random source signals. It has been observed that the last binary digit of biological data often fluctuate with certain degree of randomness and therefore has been proposed to be used to generate seeds for calculating pseudorandom numbers for cryptography [42]. Features extracted from the frequency domain of physiological signals such as electrocardiogram (ECG) and photoplethysmogram (PPG) [43, 44] and those from static biological features such as fingerprint images [45] have also been evaluated for the generation of authentication or encryption keys for BANs.

The greatest advantage of generating random keys from biological and physiological signals for BANs with a health-care application is that these data are already available to the BANs and by making use of them, addition costs required for key generation can be minimised. In addition, compared to password-based authentication or encryption, using keys that are generated from static biometric features also have the advantage of being impossible to be forgotten or lost, and using keys that are generated from dynamic biometric features have advantage of time variant.

5.2. Symmetric Key Distribution. Key distribution is central to symmetric cryptography. Predistribution of symmetric secret keys is possibly a practical approach to protect BANs communications. Another practical method is the deterministic pairwise key predistribution scheme (DPKPS) that has been implemented on the MICAz sensor platform. The

scheme only consumes an extremely small amount of energy, 17.23 μAh , and memory space, about 2 KB flash memory and 69 bytes RAM, to compute and exchange a pairwise key between two sensor nodes [46]. Key predistribution is however relatively inflexible as the biosensors will have to dispatch keys in advance. Adding new biosensor to an existing network thus becomes difficult.

A method of using asymmetric keys to protect the distribution of symmetric key has been presented for mobile ad hoc networks [47]. Although the idea can be adopted for BANs, the additional cost is high.

5.3. Key Distribution via Biochannels. Since nodes of BANs are placed in or on the human body, they are inherently linked by pathways which we named biological channels (biochannels) [48]. Biochannels are commonly referred to the voltage-gated channels that allow the exchange of selected ions across the otherwise impermeable cell membrane. In this context, we use bio-channel to denote any biological conduit that is part of the human body and enables the transfer of exogenous or endogenous information. Information can be transmitted by methods such as volume conduction on the human body.

Another challenging research direction that makes use of biochannels to implement SKE in BANs is to simultaneously generate symmetric random keys from dynamic biometric features obtained at multiple nodes of a BAN so as to bypass the problem of key distribution. There are features (e.g., interpulse intervals, IPIs) common to multiple physiological signals such as ECG and PPG [48]. These features have been recently studied for the generation of random keys in BANs, and the performance of these keys is perfect but the costs are quite low. At present, it is still difficult to obtain exactly the same random BS from two signals. Therefore, fuzzy commitment (FC) [49] has been proposed to match the pair of similar but inexact BSs. Considering the limitations of bit strings and order invariance of FC, Juels et al. [50] proposed fuzzy vault (FV) to be used on datasets of an arbitrarily order. Since FC cannot handle vectors that do not have the same number of features or vectors with features that are not aligned in the same order, FV has been used to develop a symmetric key distribution method in BANs [44]. Nevertheless, the computation of generating a number of random chaff points by the sender and calculating the secret key by the receiver for FV require a large amount of energy and memory space. Implementation of the method on the resource-constrained BANs is technically challenging.

Since not every sensor node in a BAN can collect the same signal or be composed of some common features, more work have to be carried out in this area to develop a low-cost and reliable method for distributing keys to all sensors in order to use SKE for securing BANs.

6. Conclusions

In conclusion, BANs need a security mechanism that combined their characteristics and security requirements to deal with the potential attackers. The draft of communication

protocol of IEEE 802.15.6 has proposed some strategies for security of BANs. Both PKC and SKE have their pros and cons for BANs security. However, the SKE is more preferable because of resource constraints of BANs. Key management is one of the most important aspects in BANs security yet there has not been a perfect method for key distribution.

BANs are anticipated to have significant impact on current personal healthcare monitoring systems by changing the way how patients are diagnosed and treated. Although the development of the BANs for health applications is only at an early stage, securing the collection and transmission of data collected by the biosensors or medical devices of BANs must be addressed without delay. Future directions of development of BANs should carefully consider the unique characteristics of and resources already available to this kind of network for deriving an optimal solution, including the communication protocol and the respective security scheme they used.

Acknowledgments

This work was supported in part by the Hong Kong Innovation and Technology Fund (ITF), the 973 Project Fund (2010CB732606), and the Guangdong Innovation Team Fund in China. The authors are grateful to Standard Tel-ecommunication Ltd., Jetfly Technology Ltd., Golden Meditech Company Ltd., Bird International Ltd. Bright Steps Corporation, and PCCW for their supports to the ITF projects.

References

- [1] L. Bos, K. Wac, V. Jones et al., "Mobile patient monitoring: the MobiHealth system," *Journal on Information Technology in Healthcare*, vol. 2, no. 5, pp. 365–373, 2004.
- [2] 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 Transactions on Information Technology in Biomedicine*, vol. 8, no. 4, pp. 405–414, 2004.
- [3] M. R. Yuce, S. W. Ng, N. L. Myo, J. Y. Khan, and W. Liu, "Wireless body sensor network using medical implant band," *Journal of Medical Systems*, vol. 31, no. 6, pp. 467–474, 2007.
- [4] C. Poon and Y. T. Zhang, "Perspectives on high technologies for low-cost healthcare," *IEEE Engineering in Medicine and Biology Magazine*, vol. 27, no. 5, pp. 42–47, 2008.
- [5] J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg, "An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule," *National Institute of Standards and Technology*, pp. 800–866, 2005.
- [6] Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002.
- [7] "Law of the people's Republic of China on medical practitioners," 1996, <http://www.moh.gov.cn/publicfiles/business/htmlfiles/mohzcfgs/s3576/200804/18250.htm>.
- [8] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

- [9] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.
- [10] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in *Proceedings of the CADIP Research Symposium*, 2002.
- [11] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pp. 162–175, Baltimore, Md, USA, November 2004.
- [12] J. Hill, S. Hollar, K. S. J. Pister, D. Culler, R. Szewczyk, and A. Woo, "System architecture directions for networked sensors," *SIGPLAN Notices*, vol. 35, no. 11, pp. 93–104, 2000.
- [13] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 80–88, 2010.
- [14] E. M. Staderini, "UWB radars in medicine," *IEEE Aerospace and Electronic Systems Magazine*, vol. 17, no. 1, pp. 13–18, 2002.
- [15] X. Zhao, D. Y. Fei, C. R. Doarn, B. Harnett, and R. C. Merrell, "A Telemedicine System for Wireless Home Healthcare Based on Bluetooth (TM) and the Internet," *Telemedicine Journal and e-Health*, vol. 10, no. 2, pp. S110–S116, 2004.
- [16] A. Wheeler, "Commercial applications of wireless sensor networks using ZigBee," *IEEE Communications Magazine*, vol. 45, no. 4, pp. 70–77, 2007.
- [17] "IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements part 15.1: wireless medium access control(MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)," IEEE Std 802.15.1™, 2005.
- [18] "IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements part 15.3: wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs) amendment 1: MAC sublayer," IEEE Std 802.15.3b, 2006.
- [19] "IEEE Standard for Information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)," IEEE Std 802.15.4™, 2006.
- [20] IEEE-SA IEEE 802.15 WPAN™ Task Group 6 (TG6) Body Area Networks <http://www.ieee802.org/15/pub/TG6.html>.
- [21] <https://mentor.ieee.org/802.15/documents>.
- [22] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [23] Koblitz N., "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.
- [24] V. S. Miller, "Use of elliptic curves in cryptography," in *Proceedings of the Advances in Cryptology (CRYPTO '86)*, pp. 417–426, 1986.
- [25] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 925–943, Boston, Mass, USA, 2004.
- [26] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in *Proceedings of the 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON '04)*, pp. 71–80, October 2004.
- [27] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom '05)*, pp. 324–328, Kauai, Hawaii, 2005.
- [28] H. Wang and Q. Li, "Efficient implementation of public key cryptosystems on mote sensors," in *Proceedings of the International Conference on Information and Communication Security (ICICS '06)*, pp. 519–528, 2006.
- [29] L. Uhsadel, A. Poschmann, and C. Paar, "An efficient general purpose elliptic curve cryptography module for ubiquitous sensor networks," in *Proceedings of the the Software Performance Enhancement for Encryption and Decryption (SPEED '07)*, 2007.
- [30] A. Liu and P. Ning, "TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks," in *Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN '08)*, pp. 245–256, St. Louis, Mo, USA, April 2008.
- [31] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in *Proceedings of the 1st ACM Conference on Wireless Network Security*, pp. 148–153, Alexandria, Va, USA, April 2008.
- [32] O. Elkeelany and A. Olabisi, "Case study: integrated design of RC5 encryption," in *Proceedings of the IEEE Southeast Conference (SoutheastCon '07)*, pp. 69–72, Richmond, Va, USA, March 2007.
- [33] B. Wang, S. J. Lin, Y. T. Zhang et al., "A body sensor networks development platform for pervasive healthcare," in *Proceedings of the 3rd International Conference on Bioinformatics and Biomedical Engineering, (ICBBE '09)*, pp. 1–4, Beijing, China, June 2009.
- [34] K. Woo Kwon, L. Hwaseong, K. Yong Ho, and L. Dong Hoon, "Implementation and analysis of new lightweight cryptographic algorithm suitable for wireless sensor networks," in *Proceedings of the 2nd International Conference on Information Security and Assurance (ISA '08)*, pp. 73–76, Busan, Korea, April 2008.
- [35] C. Clavier, K. Gaj, C. De Cannière, O. Dunkelman, and M. Knežević, "KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers," in *Proceedings of the Cryptographic Hardware and Embedded Systems (CHES '09)*, pp. 272–288, Springer, Berlin, Germany, 2009.
- [36] P. Paillier et al., "PRESENT: an ultra-lightweight block cipher," in *Proceedings of the Cryptographic Hardware and Embedded Systems (CHES '07)*, pp. 450–466, Springer, Berlin, Germany, 2007.
- [37] J. Song, T. Kwon, M. Yung, C. Lim, and T. Korkishko, "mCrypton—a lightweight block cipher for security of low-cost RFID tags and sensors," in *Information Security Applications*, pp. 243–258, Springer, Berlin, Germany, 2006.
- [38] K. J. Choi and J. I. Song, "Investigation of feasible cryptographic algorithms for wireless sensor network," in *Proceedings of the 8th International Conference on Advanced Communication Technology (ICACT '06)*, pp. U1379–U1381, Seoul, Korea, 2006.

- [39] C. N. Zhang, X. Huang, Q. S. Yu, and C. Yang, "An RC4-based lightweight security protocol for resource-constrained communications," in *Proceedings of the 11th IEEE International Conference on Computational Science and Engineering (CSE Workshops '08)*, pp. 133–140, July 2008.
- [40] A. Francillon and C. Castelluccia, "TinyRNG: a cryptographic random number generator for wireless sensors network nodes," in *Proceedings of the 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops (WiOpt '07)*, pp. 1–7, Limassol, Cyprus, 2007.
- [41] R. Latif and M. Hussain, "Hardware-based random number generation in Wireless Sensor Networks(WSNs)," in *Proceedings of the 3rd International Conference and Workshops on Advances in Information Security and Assurance (IAWSN '09)*, pp. 732–740, Seoul, Korea, 2009.
- [42] J. Szczepanski, E. Wajnryb, J. M. Amigo, M. V. Sanchez-Vives, and M. Slater, "Biometric random number generators," *Computers and Security*, vol. 23, no. 1, pp. 77–84, 2004.
- [43] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proceedings of the 27th Conference on Computer Communications (IEEE INFOCOM Workshops '08)*, pp. 1–6, Phoenix, Ariz, USA, 2008.
- [44] K. K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proceedings of the IEEE Military Communications Conference (MILCOM '08)*, pp. 1–7, San Diego, Calif, USA, November 2008.
- [45] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A biometrics based security solution for encryption and authentication in tele-healthcare systems," in *Proceedings of the 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '09)*, pp. 1–4, Bratislava, Slovakia, November 2009.
- [46] O. G. Morchon, H. Baldus, and D. S. Sanchez, "Resource-efficient security for medical body sensor networks," in *Proceedings of the 3rd International Workshop on Wearable and Implantable Body Sensor Networks (BSN '06)*, pp. 80–83, Cambridge, Mass, USA, 2006.
- [47] A. Boukerche and Ren Y., "The Design of a secure key management system for mobile Ad-hoc networks," in *Proceedings of the 33rd IEEE Conference on Local Computer Networks (LCN '08)*, pp. 320–327, Quebec, Canada, 2008.
- [48] C. C. Y. Poon, Y. T. Zhang, and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for tel-medicine and M-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.
- [49] A. Juels and M. Wattenberg, "Fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pp. 28–36, Lion City, Singapore, November 1999.
- [50] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes, and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.