Hindawi
Security and Communication Networks
Volume 2017, Article ID 3721234, 9 pages
https://doi.org/10.1155/2017/3721234

WILEY | Hindawi

Review Article

A Survey on Secure Wireless Body Area Networks

Shihong Zou,[1,2] Yanhong Xu,[3] Honggang Wang,[4] Zhouzhou Li,[4] Shanzhi Chen,[5] and Bo Hu[6]

[1]*School of CyberSpace Security, Beijing University of Posts and Telecommunications, Beijing, China*
[2]*Nanjing University of Information Science & Technology (NUIST), Nanjing, China*
[3]*Beijing University of Posts and Telecommunications, Beijing, China*
[4]*University of Massachusetts Dartmouth, Dartmouth, MA, USA*
[5]*State Key Laboratory of Wireless Mobile Communications, China Academy of Telecommunications Technology, Beijing, China*
[6]*State Key Laboratory of Networking and Switching, Beijing University of Posts and Telecommunications, Beijing, China*

Correspondence should be addressed to Honggang Wang; hwang1@umassd.edu

Received 30 December 2016; Accepted 16 March 2017; Published 17 May 2017

Academic Editor: Rongxing Lu

Combining tiny sensors and wireless communication technology, wireless body area network (WBAN) is one of the most promising fields. Wearable and implantable sensors are utilized for collecting the physiological data to achieve continuously monitoring of people's physical conditions. However, due to the openness of wireless environment and the significance and privacy of people's physiological data, WBAN is vulnerable to various attacks; thus, strict security mechanisms are required to enable a secure WBAN. In this article, we mainly focus on a survey on the security issues in WBAN, including securing internal communication in WBAN and securing communication between WBAN and external users. For each part, we discuss and identify the security goals to be achieved. Meanwhile, relevant security solutions in existing research on WBAN are presented and their applicability is analyzed.

1. Introduction

Recently, there is an emerging interest in wireless body area networks (WBAN) since it enables real-time and continuous monitoring in various fields including telemedicine, entertainment, sports, and military training, especially benefits for chronic diseases early detection and treatment. WBAN is defined as a kind of ultra-short-range wireless networking technology. Tiny sensors are attached to, implanted in, or implanted around human body, communicating wirelessly among themselves and with processors within two meters to form a body-centered system. With a WBAN-based e-healthcare system, patients medical information can be automatically collected by various sensor nodes and then accessed and processed by the local or remote medical personnel through the network or fixed infrastructure. Consequently, this enables early release of patients from hospital as their conditions can be monitored at home. Medical personnel can also be alerted to provide assistance if the patients condition deteriorates.

Architecture. Based on [1], a general communication architecture of a WBAN-based e-healthcare system is shown in Figure 1. A typical WBAN consists of several sensor/actuator nodes and a body control unit (BCU) (i.e., a PDA or smartphone). Sensor nodes collect the patients physiological signals such as pulse, body temperature, blood pressure, glucose level, and electrocardiogram (ECG). Actuators act according to messages received from the sensors or through interaction with BCU (i.e., an insulin pump). For these two types of nodes, we do not consider them explicitly in the rest of the article to keep the discussion simple. BCU gathers all the physiological data from the nodes and then transmits them to the local/remote medical server together with the patients profile through networks. Timely medical service will be given by medical personnel after accessing and processing the patient-related data. In general, a WBAN has a star topology with the BCU as the central node. Sensors upload data to medical server or personnel via BCU. Medical personnel give orders to sensors via BCU. A more complicated WBAN may have relays sitting between sensors and BCU; they are needed

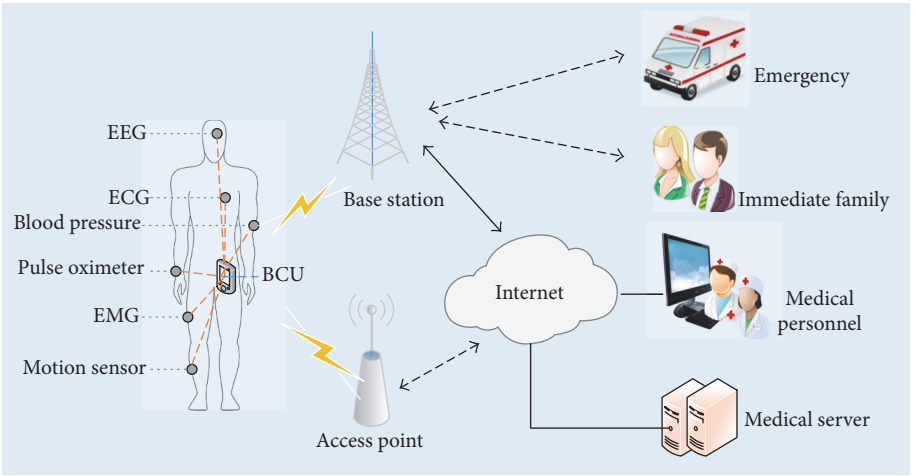

Figure 1: A general communication architecture of a typical WBAN-based healthcare monitoring system.

when a sensor can not reach the BCU due to the human body constitution (e.g., the sensor is deployed at the back while the BCU is placed at the abdomen).

Applications. Based on the WBAN, a wide range of novel medical applications have generated, such as the Cellnovo Type I diabetes management system and LifeStar Ambulatory Cardiac Telemetry (ACT). Cellnovo system is composed of an insulin pump, an activity monitor, and a cellular enabled wireless handset with integrated blood glucose meter. With Cellnovo, the patients body glucose, insulin dose, exercise, and diet information can be automatically recorded by the handset and then delivered to the clinic over web connection. LifeStar ACT can capture and transmit an arrhythmia when it occurs without patients intervention. Upon arrhythmia detection, the system automatically utilizes the integrated phone to transmit the ECG waveform to LifeWatch for further analyzing. The patients doctor will be notified of the arrhythmia based on predetermined notification criteria; thus the system is able to provide assistance for identifying and treating the patient. Also the patient biometrics data can be saved for later offline analysis.

Security Threat. Both the patient-related data and medical messages transmitting in WBAN system are very sensitive and significant. Therefore, WBAN is more likely to be attacked. Malicious attackers may eavesdrop on traffic between the nodes, BCU, and the remote medical personnel and then inject messages, replay old messages, spoof, and ultimately compromise the integrity of device operation. If successful, such behaviors can not only invade a patients privacy but also suppress legitimate data or insert bogus data into the network leading to unwanted actions (drug delivery) or preventing legitimate actions (notifying doctor in case of an emergency) [2]. As reported in Healthcare IT news in February, 2014, hackers accessed a server from a Texas healthcare system, compromising the protected health information of some 405,000 individuals, which was one of the biggest HIPAA security breaches. Even worse, it was demonstrated that implantable cardiac devices can be wirelessly compromised [3] and vulnerabilities also existed in wireless insulin pump systems owing to the low-tech security interface issues [4]. All those above can be a disaster for the patients health and prevent WBAN-based medical applications from being popular. Therefore, strong security measures are essential to reduce the potential risks to the public, as highlighted in [5] issued by the US Food and Drug Administration (FDA), which addressed the need for increasing focus on security in medical devices and hospital networks.

Challenges. Actually, designing security architecture for WBAN can be more challenging than other traditional networks. An ideal security architecture for WBAN has to achieve performance requirements as follows.

(i) *Efficiency*. Limited by their sizes, nodes deployed in WBAN are usually insufficient in power supplies, computation capability, memory space, and communication distance. They are not capable of performing complex and energy-intensive cryptographic operations. Therefore, the security architecture should be designed as fast and lightweight as possible for the purpose of reducing communication overheads and energy consumption.

(ii) *Scalability*. It means plug and play. Taking device compatibility into consideration, it is difficult to preshare any common cryptographic material among different devices. On the other hand, since human body is always in motion, nodes may leave or join the network at any time; therefore cumbersome security operation is inapplicable for WBAN. And we should try to avoid relying on too much prior security context when designing security architecture for WBAN. Scalability does not mean growing size only; the downsizing issues are often ignored. In [6], the authors pointed out the security issues when a node left the network.

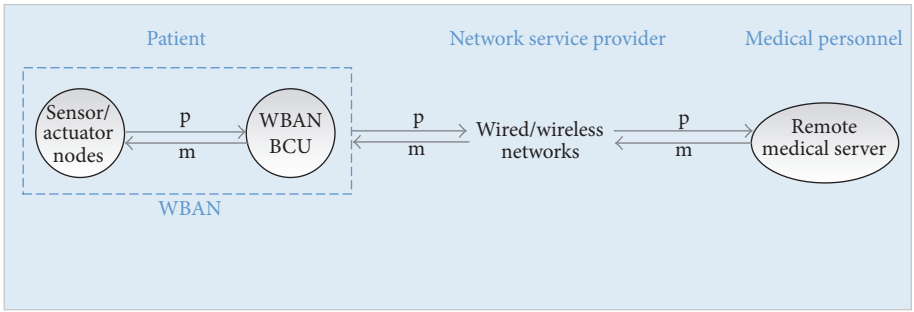

Figure 2: A partition for data transmitting and user involved in a WBAN-based e-healthcare system.

(iii) *Usability*. Patients are usually too unskilled to handle with the device operation, which means the security architecture has to be simple enough and easily performed. Complicated professional operations may lead to incorrect configuration on the devices and poor user experience.

To present the security issues we mentioned above more explicitly, we simplify the WBAN communication architecture as shown in Figure 2. Thus our discussion is composed of two aspects; they include securing internal communication in WBAN and securing communication between WBAN and external users. The rest of the paper is organized as follows. In Section 2 we discuss and identify the security goals for internal security issues, followed by the related research survey in Section 3. Security issues existing between WBAN and external users are described in Section 4, and we survey the solution space for this in Section 5. Finally, in Section 6, we summarize the discussion and give some suggested potential research directions.

2. Securing Internal Communication in WBAN

As shown in Figure 1, sensor nodes collect patients' physiological signal through the BCU. Message exchange between them is very sensitive and plays a significant role in ensuring the patients physical conditions. Suppose a scenario like this: Tim is a diabetes patient who has been using a glucose application for monitoring and controlling his glucose level. Unfortunately, due to lacking of strong security mechanism, the system was invaded by malicious attackers (i.e., an insurance). The attackers may eavesdrop and tamper the data transmitted between the sensors and his PDA. Consequently, invalid and inauthentic data may result in Tim being left untreated in time or wrong insulin dose, which is quite undesirable. Therefore, measures for integrity validation, authenticity, replay defense, privacy protection, and confidentiality have to be provided during the WBAN system design to enable secure internal communication. We identify and describe the major security requirements to WBAN in Table 1.

Table 1: Major security requirements for securing internal communication in WBAN.

Security requirements	Description
Data authenticity	Attackers may place malicious nodes in non-line-of-sight (NLOS) places and inject bogus data into the WBAN; thus the communication entities must verify who they claim to be.
Data confidentiality	Due to the openness of WBAN wireless channel, passive attackers can eavesdrop on radio communication between the nodes freely and easily, leading to information disclosure to unauthorized individuals. Therefore data must be encrypted during communication.
Data integrity	Attackers are able to tamper the eavesdropped information and send it back to original receiver to achieve some illegal purpose, which may result in system failure and cause disaster to the patient. Therefore, data must be verified for its integrity.
Data availability	Attackers may launch denial-of-service (Dos) attacks to the medical cloud or BCU, leading to the medical services inaccessible. Therefore, the WBAN must detect and survive from DOS attacks.

3. Solutions for Securing Internal Communication in WBAN

In this section we investigate the solution space for securing internal communication in WBAN. To achieve the goals we summarized above, we lay more emphasis on data confidentiality, authenticity, and integrity. Data availability is not our focus in this article, since Dos attack resistance is very tough and there may not be a good solution for this issue,

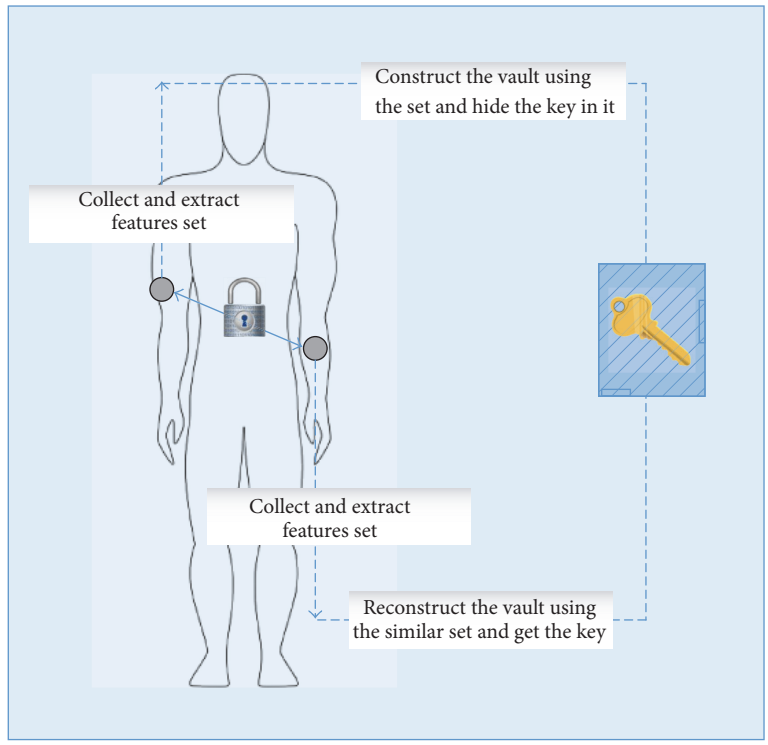

Figure 3: Session key agreement based on Juels and Sudan (JS) algorithm.

so we may only mention it when necessary. Therefore, the section is separated into three subsections and we discuss the existing solution on session key agreement, node, and message authentication.

3.1. Achieving Data Confidentiality in WBAN. In order to prevent the sensitive information from disclosure to unauthorized individuals, the data must be transmitted in encrypted frames. Previously key agreement has been a main focus of many researchers [5]. However, most of them need either preshare key materials or complicated cryptographic calculation, which shows low efficiency and poor flexibility.

Biometric Features-Based Scheme. Since human body itself and WBAN is inextricably linked, several on-going research works have turned to implement securing internal communication based on biometric features. Similar to fingerprint, iris, and facial recognition, physiological signals such as electrocardiograph (ECG/EKG) and photoplethysmogram (PPG) are also distinctive and can be extracted as session keys, since they are long, random, and time-variant.

Hu et al. used Inter-Pulse-Interval (IPI) as session key in [9]. In the proposed scheme, the IPI features generated by each sensor are ordered to form a feature vector and only the sensor collecting the data knows the order of the features; then the sender sends the secret features along with a large number of noisy data to the receiver. Once receiving the packet, the receiver generates a key according to the common features and returns the indexes of the matching features. Finally, the sender identifies the common features in its own feature vector and computes the key accordingly. This scheme is based on Juels and Sudan (JS) algorithm as shown in Figure 3. By using JS algorithm, secret data which the two communication entities want to share can be locked (hidden) in a polynomial (vault) using a set of values A by the sender. If the receiver wants to acquire the secret data, it has to reconstruct the polynomial, which means the receiver should have the same or most values in A. Some other related research [10, 11] has been performed.

The authors in [12] utilized the distinctive ECG signals to encrypt the data transmission between the sender and the receiver based on Improved Juels and Sudan (IJS) algorithm. The sender first extracts features F from the ECG signals to form a session key K, and F is used as the root to build an ECG monic polynomial. Only the receiver with similar features set to F can reconstruct the polynomial and then regenerate K. The idea behind this scheme can be abstracted as follows:

(i) Both sides of the communication channel have a set of similar data, which is derived from the patients biometrics data. Biometrics data is hard to be directly obtained by the NLOS malicious tapping person.

(ii) The data difference between the two sides is minor. Therefore, the data can be used as the encryption key.

(iii) One side only sends few of check symbols of the data rather than the whole data to the other side; this will be enough for the other side to eliminate the data difference and then conclude the key. Because less

data is exchanged, which is subject to exposure, high security and efficiency are achieved. It is hard for the NLOS malicious tapping person to conclude the key from the check symbols.

The IJS algorithm adopted by [12] was used to generate check symbols. One of its shortages must be pointed out here. The check symbols are coefficients of the monic polynomial (the original data is sliced to the roots of the polynomial). Only part of the check symbols are sent to the other side; this depends on how many data difference must be eliminated. The coefficient calculation formulas are shown in the following:

$$b_1 = \sum_i (-a_i),$$
$$b_2 = \sum_{i \neq j} (-a_i) \cdot (-a_j), \ldots, b_n = \prod_i (-a_i), \quad (1)$$

where a_i are roots and b_i are coefficients. b_i usually becomes bigger as i increases. This implies that the coefficients are variable-length; therefore coefficient overflow and separation should be considered.

Figure 4 shows the fault rejection rate (FRR) of the IJS algorithm when it is applied to the MIT-BIH Arrhythmia Database. Ten records (100, 109, 112, 117, 121, 123, 202, 220, 230, 234) are selected from the DB to calculate the FRR. t means how many check symbols are exchanged for the data reconciliation between two data sets. s means how many data items are selected from the data sets.

Other algorithms may also be used to generate the check symbols, if they are proved to have high efficiency, for example, Reed-Solomon Encoding.

Channel Characteristics-Based Scheme. Data confidentiality can be easily achieved by utilizing physiological features as encryption key since they are long, random, and time-variant. However, since the scheme requires that all sensors participating in the secure initialization progress have the ability to collect the same kind of physiological signals at a similar accuracy, it inevitably requires more advanced hardware and sometimes even causes hardware redundancy. To overcome this challenge, Zhang et al. in [13] found out that the received signal strength indicator (RSSI) values between two sensors can also be extracted as encryption key. During the secure initialization process, the sender and receiver first sample enough RSSI values to generate a feature set F by paired data packet transmission. Based on Improved JS algorithm, the sender will encrypt the sensitive messages collected using F. Once receiving the packet, the receiver needs to first reconstruct the polynomial using F sampled before and then decrypt it and get the session key F.

In [14], the authors enhanced the IJS algorithm for coefficients calculation (encoding) and minor data error recovery (decoding).

In [15], the on-body relatively unstable channels (between the control unit and nonline-of-sight nodes) are exploited to extract secret key from channel characteristics for a secure communication between two on-body devices. The problem

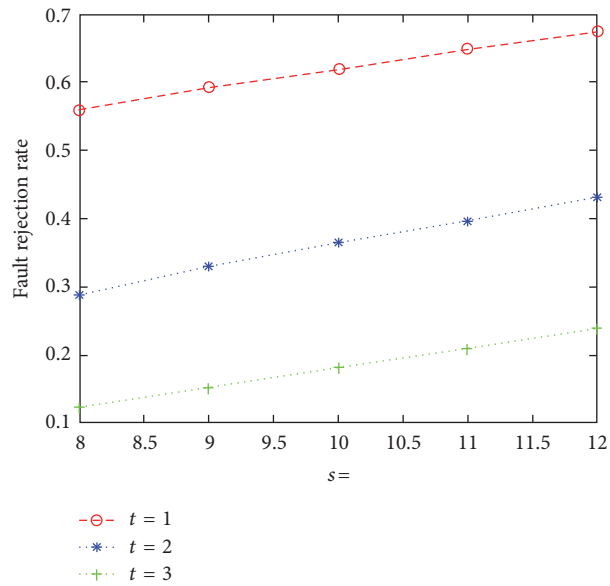

Figure 4: Fault rejection rate of IJS algorithm.

was modeled as a max-flow problem, by solving which, the authors maximized the key generation rate.

In [16], a practical, secure, efficient, communication link characteristic-based, cooperative key generation method was proposed to increase the key generation rate for constrained nodes, which can borrow resources (e.g., energy) from assistant nodes for their key generations.

For Security and Efficiency. The three solutions described in [9, 12–14] are all based on fuzzy vault scheme, without a similar feature set; the attacker cannot unlock the vault to regenerate the key. Moreover, since both physiological signals and RSSI are random and time-variant, the extracted encryption keys are strong enough to resist brute force attack; thus both key security and data confidentiality are satisfied. Compared with conventional solutions, both two schemes show better flexibility without sacrificing the security requirements since they are plug-n-play. It seems that channel characteristics-based scheme is more suitable for securing internal communication in WBAN, for it is more flexible and feasible and has low requirements for hardware. However, since it may need abundant data collecting for improving the authentication efficiency at the primary stage, time cost may lead to extra power consumption. On the other hand, although escaping complex polynomial calculation by using features vectors instead, the security of research in [9] relies on the vault scale and the number of chaff points. Thus trade-off between security and efficiency can still be a challenge.

3.2. Achieving Data Authenticity in WBAN. Achieving authenticity means that data must be sent from legitimate entities and both parties involved are who they claim to be. To ensure data authenticity in WBAN, lightweight and plug-n-play authentication protocol is essential.

PKC-Based Scheme. In conventional cryptography, there have been many available mature algorithms that can be utilized to

identify whether an entity is authorized. Ma et al. proposed zero-knowledge proof- (ZKP-) based authentication scheme for WBAN in [17]. ZKP is mostly applied in situations where the sender attempts to prove that it knows a certain secret without showing it to the receiver. Compared to other public key based identification methods, ZKP was proved to perform better with low computation complexity. However, key materials used to verify the sensors legitimacy have to be preloaded in the sensors before deploying the WBAN; this can lead to poor flexibility and usability.

Channel Characteristic-Based Scheme. The authors in [18] proposed another novel solution BANA to distinguish on-body legitimate nodes and off-body attackers by exploiting the unique characteristics of physical channels in WBAN. In BANA, it is considered that if the user's body stayed in a smoothly moving state, the received signal strength (RSS) variation among on-body channels is more stable compared to it between on-body and off-body communication channels. Thus the off-body attackers can be distinguished by the BCU based on clustering analysis after collecting abundant RSS variation values. Meanwhile, the BCU can be verified in a similar way.

For Security and Efficiency. For BANA, the attacker is able to launch strategic attacks to the authentication process. For example, the attacker may deploy a large number of malicious nodes to deviate classification result. But it is expensive and easily detected. Moreover, the attacker cannot statistically predict the communication channel between on-body sensors and BCU since channel is dynamic with short coherence time and both BCU and on-body sensors are more than half wave length away from off-body attackers. The experiments were conducted in several different scenarios, and the results indicated that the solution was able to successfully authenticate six sensors in 12 s with zero false negative rates and very low false positive rates. However, the average authentication time (six nodes in 12 s) is much more than it in [17] (18 nodes in 2.26 s); thus we may need to improve the clustering efficiency to make it faster.

3.3. Achieving Data Integrity in WBAN. To authenticate the data integrity, MAC (Message Authentication Code) or hashed MAC is a common method to protect messages from malicious manipulation in WBAN. As in [12, 13], the sender sends the encrypted message, IJS coefficients together with the hashed MAC to the receiver. The receiver needs first to reconstruct the polynomial to unlock the key before decrypting the ciphertext and then recalculates the MAC using the same algorithm; thus malicious tampering on data cannot escape being detected. Signature can also be utilized for data integrity validation in [7, 8]. However, it may not be so suitable for WBAN, since pubic key algorithms are often complex and energy-intensive.

In [19], the authors proposed a distributed prediction-based secure and reliable routing framework (PSR) for WBAN. They demonstrated that PSR can significantly increase routing reliability and effectively resist data injection attacks.

Table 2: Major security requirements for securing communication between WBAN and external users.

Security requirements	Description
Data confidentiality, authenticity, integrity, and availability	Data must be transmitted in encrypted frames and measures have to be provided against message modification, privacy disclosure, and Dos attack.
Access control	Besides identifying attackers, differences in professional knowledge among the patient, doctor, and nurses may have influence on the patients treatment; thus fine-grained access control policy has to be enforced to define the users access privileges.
Nonrepudiation	The origin of data (i.e., patient or medical personnel) cannot be denied for having sent or received the messages.

4. Securing Communication between WBAN and External User

In a WBAN-based healthcare system, users attempting to communicate with WBAN can be various types, as shown in Figure 2. They include the self-monitoring patients, network service provider for data transmission and application support, and local/remote personnel who offer medical service. Considering the privacy and significance of patient-related data and medical messages, WBAN may suffer threats such as message modification and unauthorized access. It is desirable that proper security mechanism should be considered for securing the communication between WBAN and external users, where each user must prove their authenticity and then access the data according to their privileges. We identify and describe the major security requirements for securing communication between WBAN and external users in Table 2.

5. Solutions for Securing Communication between WBAN and External Users

In this section we investigate the solution space for securing communication between WBAN and external users. We do not pay much attention on solutions to data authenticity, confidentiality, integrity, and availability since such problems have been discussed enough in traditional communication networks. Considering the user diversity, we mainly focus our attention on access control. The section is separated into two parts, first we introduce a few existing research on access control, discuss their implementation mechanism, and give an analysis for security and efficiency. Then a brief introduction to a novel end-to-end security protocol for WBAN-based healthcare system followed.

5.1. Achieving Fine-Grained Access Control between WBAN and External Users. Access control is the primary concern

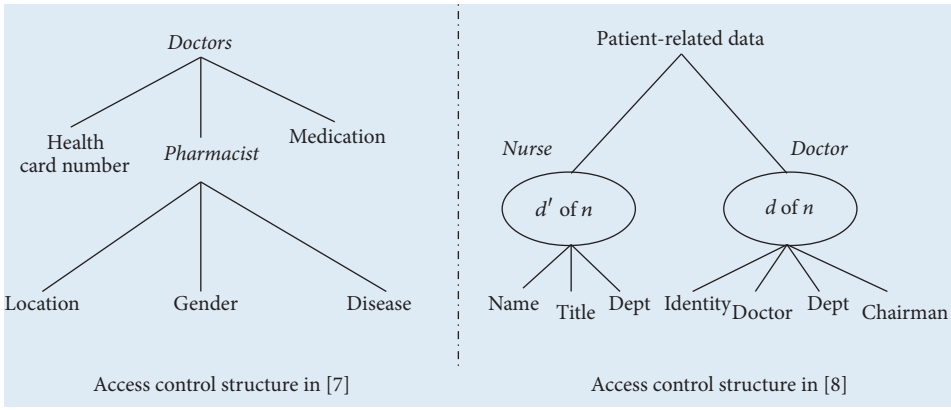

Figure 5: Access control structure-based ABE in [7, 8].

in all multiuser systems. Taking both privacy and safety for patients into account, fine-grained access control policies must be enforced among different users based on their legitimacy and roles. External attackers should be prevented from accessing the patient-related data. Patients access privileges on device operation should be least since they are unprofessional. For medical personnel including patients, primary doctors, nurses, interns, and pharmacist, their privileges should also be differentiated, since differences in professional level may lead to inaccurate medical commands.

ABE-Based Scheme. As a one-to-many encryption method, ABE is an effective primitive to achieve fine-grained access control, where the ciphertext is meant to be readable only by a group of users that satisfy a certain access policy (AP). Its expressiveness on the AP makes it a good candidate for fine-grained data access control in WBAN [20]. The authors in [7] utilized CP-ABE (ciphertext-policy attribute-based encryption) for controlling the external access to patient-related data. In the proposed solution, an access tree is created based on different roles (nonleaf nodes of the tree) of the external users, as shown in Figure 5. Moreover, the patient-related data is divided into different attribute sets (leaf nodes of the tree) to the external users based on their relation to the patient. The external users have to provide corresponding attributes to acquire the secret key and thereafter he can use the secret key to decrypt the ciphertext. The research in [8] made a proper tradeoff between security and elasticity for WBAN user access control. In the proposed solution, user identity is assumed to be composed of n attributes, as shown in Figure 5, too. Besides, the authors enforce a lower bound on the number of common attributes between a users identity and the access rights specified for the sensitive data. Then if the user has at least d out of n attributes possessed by the data, he will have authority to obtain the data from the WBAN. This solution allows external legitimate medical personnel to access critical information stored in a WBAN even if they do not have enough credentials, thus ensuring that the patient can get timely treatment in emergent situations where the patient cannot reach his primary doctor.

For Security and Efficiency. Both solutions in [7, 8] can tolerate collusion attack; that is, any set of colluding users will not be able to derive any key belonging to other users. Meanwhile, nonreputation is also achieved based on digital signature. However, the security of both of them is based on Bilinear Diffie-Hellman (BDH) problems. Since the bilinear paring operation on elliptic curve is complicated and energy-intensive, it may not be so suitable for resource-constrained WBAN.

5.2. An End-to-End Security Protocol for WBAN-Based Healthcare System. To minimize the user involvement, the research in [21] intended to establish an end-to-end communication channel between WBAN nodes and the back-end medical cloud. The solution is designed based on JS algorithm we described previously; thus it works as follows. The sending sensors first extract features set from physiological signals, which are used to construct the vault for locking the session key. Since medical cloud here is not privy to the physiological signals like sensors, the scheme uses a generative model of the physiological signals at the cloud for vault reconstructing. The generative model output synthetic signals that are diagnostically equivalent to the original physiological signals can be used to generate features that are common enough with the sender for opening the vault. Therefore, after receiving the vault from sensors, the cloud tries to open it with physiological features from synthesized physiological time-series obtained using the generative model, decrypt it, and acquire the session key; thus the key establishment is fulfilled.

Despite the transparency and usability for session key distribution, the solutions security relies on the computational complexity of the vault, which may not be suitable for resource-constraint sensor nodes, although it is quite lightweight for medical cloud with massive computation capability.

6. Conclusions and Future Work

The popularity of wearable devices is leading a revolution in traditional medical models. WBAN can not only free

people from traditional hospitals and clinics but also reduce the burden of disease management for those with chronic diseases such as diabetes and hypertension especially. In this article, we mainly focus on the security issues in WBAN, solutions for securing internal communication, and securing communication between WBAN and external users which are surveyed and analyzed. For internal communication security, channel characteristic-based scheme seems to be a better solution. Meanwhile, being extensible, collusion-resistant, and fine-grained, ABE-based scheme is very suitable for ensuring user security. Future solutions need to make a tradeoff among security, efficiency, flexibility, and usability.

As a future trend, medical sensors tend be smaller and smarter with the development of microsensor technology, embedded technology, and low-power wireless communication technology. For nanoscale or implanted nodes, the resource-constraint issues may be tougher. Moreover, we envision such a situation that people can wear sensors like clothes and buy sensors from stores or using 3D printing; this may require higher compatibility and flexibility when designing security protocols for them. Consequently, there still remains many challenges towards achieving a safe, unobtrusive, and user-friendly WBAN system. This article could provide a reference for researchers aiming at a secure WBAN, promoting WBAN medical application for being widely used in people's daily life.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Key Research and Development Program of China (2016YFF0204001) and the CICAEET fund and National High-Technology Program (863) of China (no. 2014AA01A701).

References

[1] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: a survey," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 171–193, 2011.

[2] D. Arney, K. K. Venkatasubramanian, O. Sokolsky, and I. Lee, "Biomedical devices and systems security," in *Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS'11*, pp. 2376–2379, USA, September 2011.

[3] S. Gollakota, H. Hassanieh, B. Ransford et al., "They can hear your heartbeats: non-invasive security for implantable medical devices," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 2–13, 2011.

[4] N. Paul and T. Kohno, "Security risks, low-tech user interfaces, and implantable medical devices: a case study with insulin pump infusion systems," in *Proceedings of the 3rd USENIX conference on Health Security and Privacy*, p. 8, USENIX Association, 2012.

[5] U.S. Food and Drug Administration, "Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff." September 25, 2013.

[6] R. Sun, Z. Shi, R. Lu, J. Qiao, and X. Shen, "A lightweight key management scheme for 60 GHz WPAN," in *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP'12)*, pp. 1–6, 2012.

[7] M. Barua, X. Liang, R. Lu et al., "Peace: an efficient and secure patient-centric access control scheme for ehealth care system," in *Proceedings of the Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference*, pp. 970–975, 2011.

[8] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 37–46, 2013.

[9] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proceedings of the 32nd IEEE Conference on Computer Communications, IEEE INFOCOM 2013*, pp. 2274–2282, Italy, April 2013.

[10] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 9, pp. 2546–2559, 2015.

[11] X. Chengsheng Yuan, Sun. X, and Lv. Rui, "Fingerprint liveness detection based on multi-scale LPQ and PCA," *China Communications*, vol. 13, no. 7, pp. 60–65, 2016.

[12] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070–1078, 2012.

[13] Z. Zhang, H. Wang, A. V. Vasilakos et al., "Channel information based cryptography and authentication in wireless body area networks," in *Proceedings of the 8th International Conference on Body Area Networks*, pp. 132–135, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013.

[14] Z. Li and H. Wang, "A key agreement method for wireless body area networks," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 690–695, 2016.

[15] L. Shi, J. Yuan, S. Yu, and M. Li, "Mask-ban: movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 52–62, 2015.

[16] Z. Li, H. Wang, M. Daneshmand, and H. Fang, "Secure and efficient key generation and agreement methods for wireless body area networks," in *IEEE International Conference on Communications, (ICC'17)*, 2017.

[17] L. Ma, Y. Ge, and Y. Zhu, "TinyZKP: a lightweight authentication scheme based on zero-knowledge proof for wireless body area networks," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1077–1090, 2014.

[18] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," in *Proceedings of the 5th ACM conference on Security and Privacy in Wireless and Mobile Networks (WiSec'12)*, pp. 27–38, 2012.

[19] X. Liang, X. Li, Q. Shen et al., "Exploiting prediction to enable secure and reliable routing in wireless body area networks," *IEEE Proc. INFOCOM*, pp. 388–396, 2012.

[20] M. Li, W. J. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.

[21] A. Banerjee, S. K. Gupta, and K. K. Venkatasubramanian, "PEES: physiology-based end-to-end security for mHealth," in *Wireless Health*, p. 2, 2013.