A Secure Transmission Protocol for Wireless Body Sensor Networks

Guangxia Xu
School of Soft Engineering, Chongqing University of Posts and Telecommunications, China
Email: xugx@cqupt.edu.cn

Shuangyan Liu and Yanbing Liu
College of Communication and Information Engineering, Chongqing, China
School of Computer Science, Chongqing University of Posts and Telecommunications, China
Email: {liushuangyan0716 @163.com, liuyb@cqupt.edu.cn}

***Abstract*—A wireless body sensor network (WBSN) is a typically wearable wireless network deployed on a user' body, which consists of biosensors and a local personal wireless hub, which we commonly call wireless body sensor network controller (WBSNC). The sensitive micro data (SMD) of WBSN users is collected by biosensors and forwarded to the WBSNC before it is delivered to the data process center (healthcare terminal or remote server) for further processing. Since SMD involves user's personal privacy, it is important to protect secure transmission of SMD. Therefore it is crucial to admit only legitimate biosensors and WBSNC into the network in a WBSN. Ensuring the safety of data transmission from each biosensor to WBSNC or between WBSNC and the data process center is essential because of the open feature in wireless channel. In this paper, we present a novel kind of cryptography and authentication method to assure a secure network admission and transmission in a WBSN based on ID. The procedures in this system to establish keys for each biosensor and WBSNC must offer high communication validity and as low energy consumption as possible. In addition, we also propose a new way to protect BSN secure access for biosensor and WBSNC in order to block interference from Pseudo Node.**

***Index Terms*—Wireless Body sensor network (WBSN), data cryptography, network security access, WBSN authentication, WBSN security.**

I. Introduction

Recently, with the rapid development in biosensors and wireless communication technologies (e.g., Bluetooth and ZigBee), a wireless body sensor network (WBSN) (we also call wireless body area networks or wireless medical sensor networks) is developing rapidly, which can be defined as using various wireless communication technologies to offer pervasive monitoring of users' sensitive micro data (SMD). A BSN is a typically wearable wireless network deployed on a user' body, which consists of biosensors and a local personal wireless hub, which we commonly call wireless body sensor network controller (WBSNC). The sensitive micro data (SMD) of WBSN users is collected by biosensors and forwarded to the WBSNC before it is delivered to the data process center (healthcare terminal or route server) for further processing. Instead of being diagnosed face-to-face, users' SMD can be monitored remotely, continuously, and in real-time, and then processed and transferred to remote healthcare centers. Due to every biosensor in WBSN transmits and forwards SMD via wireless communication technology, but wireless channel possesses the characteristics of openness, dynamic and uncontrollability, it leads to strict insecurity problems about data transmission. With the rapid development of information technology, it is in badly need of solving the problems that users' information and location privacy in healthcare application, if the BSN system can't take timely measures to meet users' demands for data security , high reliable transmission and location privacy, the development of electronic healthcare and related services will suffer a great obstacles. For instance, an adversary can disguise as one of the sensor nodes in WBSN and inject error messages, launch a denial-of-service (DoS) attack or make a replay attack, moreover, an adversary may eavesdrop the SMD in the wireless channel from a certain distance, so security and privacy are the most crucial problems for data transmission in a WBSN.

Manuscript received September 30, 2013; revised January 16, 2014; accepted January 22, 2014.

This work was supported in part by a grant from National Natural Science Foundation(NSFC61309032), program for Innovation Team Building at Institutions of Higher Education in ChongQing (Grant No. KJTD201310) and The Natural Science Foundation of ChongQing (CSTC2012jjA40053).

GuangXia Xu is with the College of Soft Engineering, ChongQing University of Posts and Telecommunications, China

ShuangYan Liu is with the College of Communication and Information Engineering, ChongQing University of Posts and Telecommunications, China

YanBing Liu is with the School of Computer Science, ChongQing University of Posts and Telecommunications, China

doi:10.4304/jsw.9.8.2043-2049

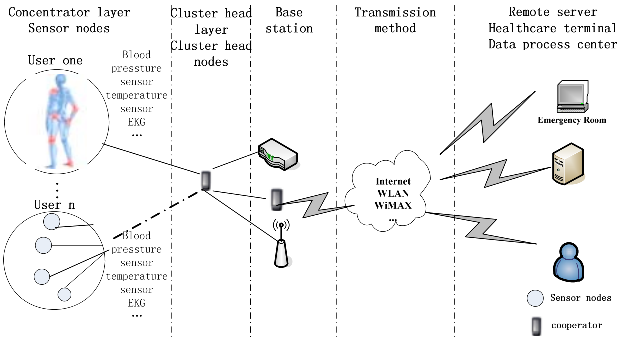


Figure 1. System overview of a general WBSN.

A WBSN ought to have the ability to resist various cyber attacks such as malicious tampering. Failure to get authentic and correct medical information will largely prevent a user from being treated effectively and correctly, what's worse, lead to wrong diagnose. If users' privacy was leaked, their healthcare data may be misused and it is hard for the public to accept WBSN. Therefore, WBSN applications must meet a lot of mandatory security requirements of healthcare alliances such as HITRUST [1] and legal directives, for example those adopted in the U.S. [2] and Europe [3]. Literature [4] offers a kind of security method that an efficient biometric certificateless signature scheme. Ensuring security and privacy in WBSN is essential for all walks of life. For an ordinary user, his or her medical sensor data may have many uses to some parties (e.g., insurance companies). An adversary may profit from user data by selling these obtained through eavesdropping on the WBSN to others. For a person who is very important, such as a company's top administrator, an adversary may aim at hurting him physically by broadcasting wrong information or spoofing his or her medical data, which may lead to a great loss and safety of life. What's more, it is much easier to hack the information transmitted in a wireless WBSN than wired networking. More importantly, physical compromise of a biosensor node is much easier than a BSN server. To solve the above security problems, it is critical to provide proper, secure and effective network access and transmission, as well as lightweight cryptography to encrypt SMD. The following is basic process:

Secure access between sensor node and sensor node: It ensures network access only to eligible SMD and biosensors, they need to make an authentication before starting data transmission among them.

Secure access between sensor node and WBANC: It assures confidential, authenticated, and integrity-protected transmission between each biosensor and WBSNC, which means biosensors and WBSNC also need to make an authentication before starting data transmission.

SMD encryption: It is very important to protect SMD secure transmission in wireless communication channel, data transmitted via wireless channel is much easier to be eavesdropped by an adversary, this paper propose a novel method based on physiological data to encrypt SMD.

However, putting forward a secure network access and lightweight cryptography protocol for a WBSN is not an easy thing. In a word, there are several practical challenging factors:

A. Memory space: a good WBSN should take into account the limited memory space of biosensors extremely, which might effects cryptography algorithm computational complexity and keys mechanism.

B. Computational capability: because of the limited memory and the requirement of low energy consumption of biosensor, biosensors own rather limiter computational capability, which require us to develop lightweight algorithm.

C. Energy consumption: it is a very important factor for biosensor nodes, which are supposed to be minimal since biosensor nodes are powered by very small batteries, so they are required to have lower consumption to operate for a long period of time. As a result, any security mechanism for BSNs should be designed carefully.

D. Minimum delay: a key design criterion in the WBSN security mechanism is able to minimize delays in order to comply with BSN requirements.

E. Communication overhead: by the reason of the limited bandwidth available in a WBSN, low communication overhead is required. For example, secure BSN setup must be carried out in less than 1 s and the maximum allowable time for ECG (electrocardiogram) transmission is 250 ms [5]. Emergency situations in a BSN require the capability for fast medical reaction without disabling security. Cryptographic algorithms used by these nodes must be simple in order to lower algorithms complexity. Moreover, if the message authentication or encryption (decryption) mechanisms are not rather fast, an adversary may launch a DoS attack to exhaust the resources of legal biosensor nodes and make them less capable of carrying out their intended functions. But most commonly used cryptographic techniques are infeasible in BSNs, for example public key cryptosystems. Security research about WBSN is still at an immature stage, especially about authentication and transmission of secure network. Additionally, there is usually not a good practice to use a fixed individual key to secure SMD transmission for a long period of time. First of all, a single encryption key will offer a lot of cipher text for an adversary to crack. Secondly, if the secret key is compromised, all previously transmitted SMD with the same key are also compromised. In the literature, no efficient protocol has been proposed to prevent SMD from being attacked.

To achieve the above security problems, this paper makes two main contributions:

Due to the scale of each BSN is very small, we propose a authentication protocol to develop a secure network access and transmission mechanism in WBSN to provide biosensor nodes authentication in case that an adversary disguise as one of the sensor nodes, at the same time, it will support the establishment of secret keys for each biosensor node and WBSNC and a pre-shared key (*psk*) with another biosensor node and remote server. In addition, to decrease the computation complexity and communication costs, some additional mechanisms such as simple hash function is proposed in the design of the proposed system[6].

An adversary may eavesdrop on the SMD in the wireless channel from a certain distance, so security and privacy are the most crucial problems for data transmission in a WBSN. We also propose a data cryptosystem in a WBSN to achieve the security requirement of a WBSN.

The rest of this paper is structured as follows. In Section II, we present the WBSN network model and analyses security threats, as well as the unique features of WBSNs data. Section III, we describes our proposed solution method. Section IV, we provide theoretical analysis of the security properties of the proposed protocol. Finally, we make a conclusion in Section V.

II. NETWORK MODEL, SECURITY THREATS AND REQUIREMENTS OF WBSNS

A. A WBSN Network Model

A Wireless Body Sensor Network (WBSN) (a.k.a. a Wireless Body Area Network) is a network that consists of wearable and implantable wireless sensors which enables pervasive, long-term, and real-time health management for the host (users). As shown in Fig. 1, a WBSN is a multi-hop wireless network including physiological and environmental monitoring biosensor nodes that are deployed or implanted on a patient or users. We assume that each biosensor does not have any information about their immediate neighboring nodes in advance. A WBSN is handled by the WBSN administrator (e.g., the user himself, the user' relatives, Healthcare service provider, or medical practitioner). The biosensors collect SMD parameters (e.g., electrocardiogram, EKG, blood pressure, activity (e.g., walking, running, and sleeping), and environmental (e.g., ambient temperature, humidity, and presence of allergens, location) from the user's body and its immediate surroundings at regular intervals and forward them to WBSNC, which is a controlling entity called the wireless body sensor networking controller (WBSNC) that collects and processes data for the WBSN. Then, WBSNC transmits the aggregated SMD to the remote server (e.g., healthcare terminal, data process center) over different wireless networks such as cellular, WLAN and WiMAX. A WBSN can even actuate correct treatment (such as drug delivery) based on the data collected. WBSNs can be very useful in assisting medical personnel to make informed decisions about the procedure of the user's treatment by providing them with real-time information about the users' condition and monitoring for other users.

Biosensors form the important foundation of a WBSN and exist in different forms including wrist wearable sensors, implantable sensors, as a part of unfixed devices and biomedical smart clothes. They are different in terms of capabilities and are designed to be unobtrusive to the host. Therefore different sensors in a WBSN have a very limited form factor, power consumption, memory, computation, and communication capabilities compared to generic sensor nodes, thus requiring a WBSN to utilize a lot of nodes in order to collect SMD with a reliable and fault tolerant method. All the biosensors in the WBSN collect SMD to WBSNC at regular intervals via a multi-hop network. WBSNs have numerous diverse practical applications such as sports health monitoring, home-based healthcare for the elderly people, postoperative care and so on.

We suppose that the biosensors communicate with WBSNC wirelessly, because a BSN with wires will make it obtrusive and complicated. The wireless medium is not trust-worthy as its openness. Lack of security may not only lead to leakage of patient privacy, but also harm the users physically through allowing adversaries to injecting forged data or tampering and suppressing legitimate nodes, which can lead to wrong diagnosis and actuation. Therefore, it is very essential to secure SMD security transmission and all sensor communication in a WBSN. In this paper, we aim at securing the network access and transmission within the WBSN.

TABLE I.

REQUIREMENTS FOR WBSNS

Requirement	Requirement Description
Data confidentiality	It protects data from an unauthorized user
Data Integrity	It assures the correctness of SMD and prevents an adversary from modifying, deleting, creating and replying data, we can use MAC and secret key to guarantee data integrity
Authentication	It is the procedure of identifying the right node
Non-repudiation	It can be used to prevent a bogus node or a device from denying having sent or received data via making evidence
Access control	It protects against unauthorized of network resources.
Availability	It protects against the event impacting the network.
Privacy	It protects the SMD may be derived from the network
Communication flow security	It assures that communication flow only between the authorized end points with no interception from another point.

B. Security Threats of A WBSN

Due to the sensitive characteristic of the SMD biosensors collect and the broadcast feature of the wireless channel biosensors use to communicate, WBSNs potentially face a lot of security threats. These threats derive from two sources: external attacks and internal attacks. External adversaries have the ability to eavesdrop on all traffic within a WBSN, If external adversaries are successful, they not only can invade a user's SMD but also can suppress legitimate information or insert a bogus biosensor node into the WBSN, thus leading to harmful actions or preventing legitimate actions (in case of an emergency). On the other hand, internal attacks, are only able to eavesdrop on the SMD exchanged within the BSN[7]. As follows, we describe the different means of threats in a WBSN[8].

Interception (Eavesdropping): The most serious problem in WBSN is to avoid being eavesdropped everywhere by anonymous attacks. If an attacker can gain the SMD transmitted in a WBSN, it is likely to be used maliciously.

Communication jamming (communication Interruption): Communication interruption results in the destruction of a component of a remote terminal or an element of WBSN. It has an impact on the time of a battery deployed in each WBSN to live, which also reduce the communication rate. It can result in a Dos attack. Under the circumstance of a user's emergency, these threats are likely to kill one's life at the worst.

Tampering with SMD: This occurs when an unauthorized entity inserts, changes, or deletes SMD transmitted by nodes in a WBSN. This is an attack on integrity and can result in a Dos attack or man in the middle attack. For example if the healthcare data of a user is modified, physician may make a wrong diagnosis and end up with a error conclusion, which will bring a serious harm to life of users in a WBSN and hospital or users will suffer a huge loss .

Unauthorized network access: This threat occurs when an attacker gains access to each node in a WBSN by masquerading as a real remote user or a legitimate biosensor. This can result in port scanning and being attacked by a malware. In addition, port scanning of WBSN devices is possible to go through another neighborhood and check every door and window on a personal server in a WBSN. Malware is a short term for malicious software such as a virus or Trojan horse.

Repudiation: This threat occurs when a sender or receiver denies the fact that it have transmitted or received SMD in a WBSN respectively.

In electronic medical, this threat must be removed for a safe treatment in a WBSN.

TABLE II.
TATIONS

Notation	Description
WBSN	*wireless body sensor network*
WBSNC	*wireless body sensor network cooperator*
SMD	*sensitive micro data*
Enc(X,K)	*Encrypting message X with a symmetric key K*
Dec(X,K)	*Decrypting cipher text X with a symmetric K*
,and ||	*Concatenation operator of the two bit streams*
H(·)	*Public one-way collision-resistant hash function*
ECC	*elliptic curve cryptography*
psk	*Pre-shared key*

In order to handle these threats, we must notice that the following trusted model for BSNs: The wireless medium is not trusted. The biosensors do not accept any SMD they receive before they can confirm that the sender is legitimate. The WBSNC is assumed to be completely trustworthy and can measure a variety of SMD. Besides, we assume that adversaries are not in contact with the user's body. Biosensors in the WBSN deployed on the user are assumed to be legitimate and functioning correctly. We do not consider physical compromise of nodes in this paper. It's hard to insert a biosensor node into a human body without the acknowledgement of the user or the user's medical team (which is trusted enough). Even if we can not take into consideration the physical compromise, the issue of security is still worthy of attention to WBSNs due to threats from the wireless channel. This will require us to prevent adversaries from several aspects. For example, joining the WBSN network as a legitimate biosensor node and injecting bogus SMD, encrypting the SMD transmitted in the WBSN network, preventing health data from being reported or modified. Moreover, protecting SMD is a legal requirement as well.

C. Requirements for WBSNs Security

A WBSN has very stringent constraints of power, memory, and computation capability, especially for those sensors implanted into the body. In this section, we describe the security requirements suitable for every device or communication link [9], which is shown in Table I.

III. Proposed Security Transmission Protocol

Our proposed method consists of two phases. One is the security authentication and association between WBSNC and biosensors, and the other is to assure safety of data transmission. The notations used throughout this paper are listed in Table II.

A. The Security Authentication and Association of a WBSN

We propose a ID-based authentication scheme which is inspired by [10][11]. First of all, WBSNC will generate a private key using a algorithm, which we call pre-shared key(*psk*), at the same time, WBSNC will forward it to all biosensor nodes and remote server via particular bio-channel, that is to say, each node and remote server own a common security key, which can be used to network access authentication and data encryption later. The process is described in Fig. 2.

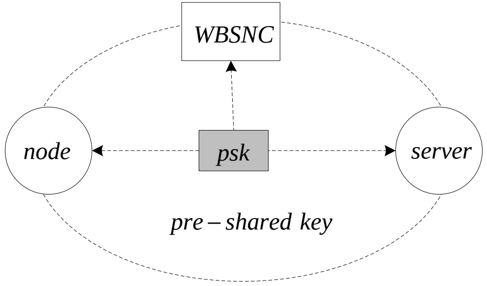


Figure 2. Generation of *psk* (bio-channel).

The association with ID-based key change protocol between WBSNC and biosensors involves two parties: biosensors initiate the communication and WBSNC responds to the initiation. The WBSN is assumed to be administered by WBSNC with each node and remote server owning a common *psk* , in the handshake procedure, the two parties exchange privacy information. Using the pair operation over hash function, the ID-based key change protocol is proposed in this section. WBSNC and biosensors should reach an agreement that owing the same parameters of an ID cryptosystem. The hardware address of biosensors and WBSNC can be considered as the identifier respectively. The ID-based key change protocol is shown in Fig. 3.

Step 1: biosensors build a association request to WBSNC with a K_{node} , K_{node} is from the hash value combined with WBSC'S ID, biosensors' ID and psk. We use the XOR operation to form 8-bit binary code and put it into hash function so that we can get the K_{node}.

Step 2: using the same method, WBSNC can also calculate the K_{WBSNC} via the received biosensors' ID, then WBSNC checks the values whether they are equal or not between K_{node} and K_{WBSNC} .if they are equal, WBSNC sends K_{WBSNC} to biosensors.

Step 3: biosensors also check the values whether they are equal or not via received K_{WBSNC}. If they are equal, biosensors send message authentication code, which we can get through simple hash function.

Step 4: WBSNC calculates the H(K_{WBSNC}) and compares it with K_{node}. If they are equal, the WBSNC establishes a connection with biosensors.

Through the above method, WBSNC and biosensors can build a secure connection, which can prevent an adversary from attacking, it also can hold back the invasion of a forged node.

B. Data Cryptosystem in a WBSN

In this section, we propose a novel data cryptosystem in order to protect security transmission of SMD. We can denote the physiological data collected by biosensors simultaneously as $X_T = \{x_i \subseteq \{0,1\}^n | 1 \le i \le N\}_T$ through sampling, quantizing, and coding, they are binary-coded. In addition, n is the bit length of SMD, T is the period of information collection and N is the number of biosensors in WBSN. Biosensors gather the SMD at regular intervals T.

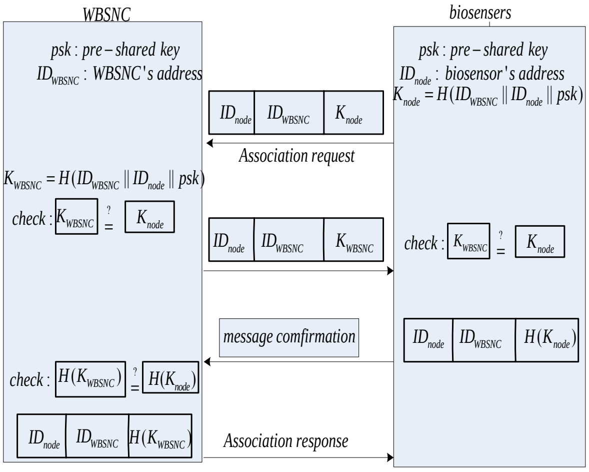

WBSNC
biosensers
psk : pre – shared key
ID_{WBSNC} : WBSNC's address
psk : pre – shared key
ID_{node} : biosensor's address
$K_{node} = H(ID_{WBSNC} \| ID_{node} \| psk)$
ID_{node} ID_{WBSNC} K_{node}
Association request
$K_{WBSNC} = H(ID_{WBSNC} \| ID_{node} \| psk)$
check : $K_{WBSNC} \overset{?}{=} K_{node}$
ID_{node} ID_{WBSNC} K_{WBSNC}
check : $K_{WBSNC} \overset{?}{=} K_{node}$
message comfirmation
ID_{node} ID_{WBSNC} $H(K_{node})$
check : $H(K_{WBSNC}) \overset{?}{=} H(K_{node})$
ID_{node} ID_{WBSNC} $H(K_{WBSNC})$
Association response

Figure 3. Association with ID-based Key Change Protocol.

a. Data encryption phase

In this subsection, there are three kinds of keys, i.e. pre-shared key psk, circulation key K_{cycle} and encryption key K_S. The psk is for encryption and authentication including network association control and establish other secret keys, K_{cycle} is for generating encryption key, K_S is for data protection.

K_{cycle} is generated on the WBSNC's side and distributed with the scheme described in Figure 4, in this process, random number generator is very important in data cryptosystem, the performance of which directly affects the quality of ciphering keys, because the low computation capability and memory constraints, we generate K_{cycle} using a ECC algorithm in WBSNC, which should be a kind of error correcting code, some literatures [12][13][14][15][16] [17]have shown that it is practical to apply Elliptic Curve Cryptography (ECC) to resource constrain environment such as WBANs by using the right selection of algorithms and associated parameters, optimization, and low-power techniques. The study [15] shows the key size comparison between symmetric and asymmetric cryptographic algorithms. As is shown in Table III, ECC is a better alternative if higher security level and flexible association methods are required.

TABLE III.
COMPARABLE KEY SIZE IN EQUIVALENT SECURITY STRENGTH

Security Level (in bits)	**Symmetric** algorithm (key size in bits)	**ECC**-based Algorithm (size of n in bits)	**RSA** (modulus size in bits)
56	56	112	512
80	80	160	1024
112	112	224	2048
128	128	256	3072
192	192	284	7680
256	256	512	15360

Under the protection of psk through XOR operation to encrypt K_{cycle} , WBSNC broadcasts cipher text to all the biosensors and remote server, those devices can recover K_{cycle} with their respective psk. Biosensors are able to generate $nonce_{Ti}$ in a period of time, which means they will produce different kinds of $nonce_{Ti}$ at different times. Biosensors make use of $nonce_{Ti}$ and K_{cycle} to form secret key K_S for protecting data, K_S is different in each cycle T so that data transmission becomes much safer. Finally, biosensors transmit cipher text (binding x_{node} with K_S)to WBSNC and WBSNC can choose to store or forward cipher text to remote server and data process center, which consists of node's ID, WBSNC'ID , cipher text and $nonce_{Ti}$.

b. Data decryption phase

In this phase, remote server and data process center can recovery K_S with $nonce_{Ti}$ and psk, then we can decrypt x_{node} the with K_S .

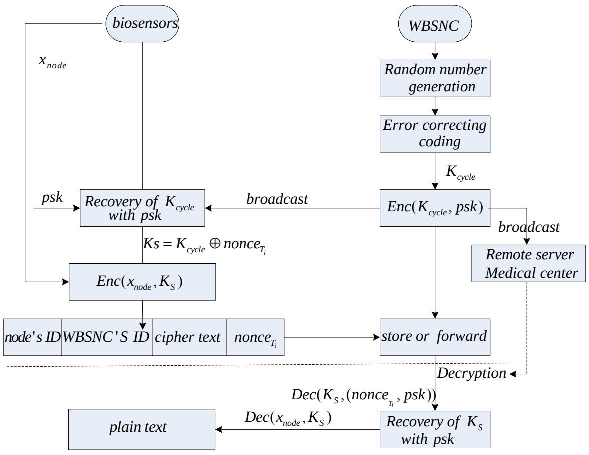


Figure 4. The procedure of data encryption and decryption in a WBSN.

IV. Security Analysis Of The Proposed Protocol

A. The Security Analysis of Authentication and Association of a WBSN

One-way hash function is easy to compute but difficult to inverse, its conception is described as follow:

mapping f : for all of $x \in X$, $f(x)$ is easy to compute, but for arbitrary $y \in f(x) = Y$,it is difficult to find $x \in X$ that makes $f(x) = Y$ on calculation. Due to the property of one-way in hash function, under the circumstance of unknown *psk*, it is difficult to find the same output from two different messages. So the forged biosensors can not establish security association without *psk* and identifier of biosensor and WBSNC. For another thing, K_{node} or K_{WBSNC} can be used as the message authentication code through hash function, which decreases the memory requirement of key Storage.

B. The Security Analysis of Data Cryptosystem in a WBSN

we generate K_{cycle} using a ECC algorithm in WBSNC, in this paper, there is no need to decrypt the K_{cycle}. Because of the security of ECC algorithm, it is not possible for the adversary to again the K_{cycle} , Table IV indicates that ECC is more feasible than RSA for WBANs from the perspective of energy.

TABLE IV.
ENERGY CONSUMPTION OF KEY EXCHANGE COMPUTATIONS

Algorithm	key Exchange Protocol	
	BIOSENSORS[mJ]	**WBSNC**[mJ]
RSA-1024	15.4	304
RSA-2048	57.2	2302.7
ECC-224	128	60.4
ECC-160	22.3	22.3

We can conclude that K_{cycle} is security, furthermore, pre-shared key *psk* offers the protection for K_{cycle} while biosensors broadcast messages. The encryption K_S is also difficult to be attacked Since K_{cycle} is security, so it is safe to encrypt x_T via K_s , this method realizes the data in the process of transmission with lower energy consumption.

Legal biosensors can decrypt the messages via *psk* deployed on themselves and pseudo nodes can not gain the *psk*.

Security authentication and association for a WBSN ensure network access only to eligible SMD and biosensors, it is necessary to make an authentication before starting data transmission among them, which assures confidential, authenticated, and integrity-protected transmission between each biosensor and WBSNC. Additionally, an adversary not only can invade a user's SMD but also can suppress legitimate information, thus leading to harmful actions or preventing legitimate actions (In case of an emergency).

On the other hand, internal attacks are able to eavesdrop on the SMD exchanged within the BSN, so it is critical to protect SMD secure transmission in wireless communication channel, this paper proposes a novel method based on symmetrical key to encrypt SMD. By the system, we can achieve secure network admission and transmission.

V. Conclusion

In this paper, we have described the WBSN frame and have introduced the potential security threats. To examine the security threats, we have presented a novel secure and lightweight network admission and transmission protocol. A ID-based security framework is proposed for data authentication within WBSN and a lightweight encryption algorithm is described to secure data of WBSN users.

Acknowledgment

The authors wish to thank the anonymous reviewers for their critical suggestions that greatly improved the quality of this paper. This work was supported in part by a grant from National Natural Science Foundation(No.61309032), Chongqing Innovative Team Fund for College Development Project (No. KJTD201310) and the Natural Science Foundation of Chongqing (cstc2012jjA40053), the Chongqing medical research project(No.2013-1-049).

References

[1] The health Information Trust Alliance (HITRUST). [Online].Available:http://www.hitrustalliance.org

[2] The US Congress. (1996). Health Insurance Portability and Accountability Act. Washington, DC.[Online]. Available:http://www.hhs.gov/ocr/ privacy/I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in *Magnetism*, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] The European Parliament and the Council of the European Union, Directive 95/46/EC [Online]. Available: http://eur-lex.europa.eu/
LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:
HTML

[4] Ming Luo, Donghua Huang and Jun Hu. "An Efficient Biometric Certificateless Signcryption Scheme," Journal of computers, vol. 8, No7, July 2013.

[5] C. Cordeiro and M. Patel, "Body area networking standardization: Present and future directions," in Proc. BodyNets, 2007.

[6] G.H.Zhang, Carmen C.Y.Poon and Y.T.Zhang. "A biometrics based security solution for encryption and authentication in Tele-Healthcare systems."in Proc, ISABEL 2009.

[7] M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.

[8] Shahnaz Saleem, Sana Ullah and Kyung Sup Kwak, "Towards security issues and solutions in wireless body area networks," in Proc.INC, 2010.

[9] Chol-soon Jang, Deok-Gyu Lee and Jong-wook Han, "A proposal of security framework for wireless body area network," International conference on security technology, 2008.

[10] Jingwei Liu, Kyung Sup Kwak. "Hybrid security mechanisms for wireless body area networks," in Proc, CUFN,2010.

[11] Shu-Di Bao, Yuan-Ting Zhang and Lian-Feng Shen. "A design proposal of security architecture for medical body sensor networks," in Proc.International workshop on wearable and implantable body sensor networks, 2006

[12] A. Liu and P. Ning, "TinyECC: Elliptic Curve Cryptography for sensor networks (version 0.1)," Sept. 2005, available at http://discovery.csc.ncsu.edu/software/TinyECC/.

[13] D. J. Malan, M. Welsh, and M. D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS based on Elliptic Curve Cryptography," Proceeding of the 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, Oct. 2004.

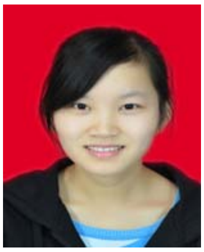
[14] A. S. Wander et al., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," Proceeding of PerCom'05, Mar. 2005.

[15] Elliptic Curve Cryptography, SECG Std. SEC1, 2000, available at www.secg.org/collateral/sec1.pdf.

[16] Ya-li Liu, Xiao-lin Qin, Chao Wang et al., "A Lightweight RFID Authentication Protocol based on Elliptic Curve Cryptography," Journal of computers, vol. 8, No11, November 2013.

[17] Xiaoqiang Zhang, GuiliangZhu, Weiping Wang et al., "New Public-Key Cryptosystem Based on Two-Dimension DLP," Journal of computers, vol. 7, No1, January 2012.

Guangxia Xu earned her Ph.D. degree at Chongqing University in 2011. She is an associate professor of the School of Software Engineering at Chongqing University of Posts and Telecommunications. Her current research interests include dependable computing, distributed systems, security of wireless network and flash memory.



Shuangyan Liu earned her bachelor's degree in North university of China in 2012,a Graduate student of Chongqing University of Posts and Telecommunications now. Her research interests include security of wireless network, internet of things and body sensor network.

Yanbing Liu earned PhD degree at University of Electronic Science and Technology of China in 2007. He is a professor of the School of Computer Science at Chongqing University of Posts and Telecommunications. His current research interests include traffic analysis of wireless, traffic modeling, resource assignment and resource allocation.