Efficient Certificateless Access Control for Wireless Body Area Networks

Fagen Li, *Member, IEEE*, and Jiaojiao Hong

***Abstract*— Wireless body area networks (WBANs) are expected to act as an important role in monitoring the health information and creating a highly reliable ubiquitous healthcare system. Since the data collected by the WBANs are used to diagnose and treat, only authorized users can access these data. Therefore, it is important to design an access control scheme that can authorize, authenticate, and revoke a user to access the WBANs. In this paper, we first give an efficient certificateless signcryption scheme and then design an access control scheme for the WBANs using the given signcryption. Our scheme achieves confidentiality, integrity, authentication, non-repudiation, public verifiability, and ciphertext authenticity. Compared with existing three access control schemes using signcryption, our scheme has the least computational cost and energy consumption for the controller. In addition, our scheme has neither key escrow nor public key certificates, since it is based on certificateless cryptography.**

***Index Terms*— Wireless body area networks, security, access control, signcryption, certificateless cryptography.**

I. Introduction

With the rapid progress in wireless communication and medical sensors, wireless body area networks (WBANs) [1], [2] are under rapid research and development. A typical WBAN is composed of a number of implantable [3], [4] or wearable sensor nodes and a controller [5]. The sensor nodes are responsible for monitoring a patient's vital signs (e.g. electrocardiogram, heart rate, breathing rate and blood pressure) and environmental parameter (e.g. temperature, humidity and light). The sensor nodes communicate with the controller and the controller acts as a gateway that sends the collected health data to the healthcare staffs and network servers. The WBANs increase the efficiency of healthcare since a patient is no longer required to visit the hospital frequently. The clinical diagnosis and some emergency medical response can also be realized by the WBANs. Therefore, the WBANs act as an important role in creating a highly reliable ubiquitous healthcare system. A good survey about the current state-of-art of WBANs is given by Movassaghi *et al.* [6].

Since collected data by the WBANs act as a vital role in the medical diagnosis and treatment, only authorized users can access these data [7]. Therefore, it is important to design an efficient access control scheme that is capable of authorizing, authenticating and revoking a user to access the WBANs. Without this access control, the health data may be abused, which may result in a catastrophic consequence. However, it is not an easy thing to design an efficient access control scheme for the WBANs because the resource of the sensor nodes is very limited.

A. Related Work

Security issues in the WBANs must be solved before real development [7]. Some secure schemes for the WBANs have been proposed for different security goals. In 2013, Hu *et al.* [8] discussed how to protect the communication between external users and the WBANs. Their solution is attribute-based encryption (ABE) [9]. However, the ABE may not be a good choice since it requires some costly cryptographic operations. These costly operations are a heavy burden for resource-limited sensor nodes [7]. Lu *et al.* [10] proposed a privacy preserving opportunistic method for the WBANs. This method can obtain reliable data process and transmission with minimal privacy disclosure. Zhao *et al.* [11] discussed the key management problem of the WBANs. In order to reduce the energy consumption, they used energy-based multihop-route-choice method and biometrics synchronization mechanism. He *et al.* [12] discussed how to provide a secure communication channel in the WBANs. They used the lightweight one-way hash chain to establish session keys. Tan *et al.* [13] designed an efficient identity-based encryption (IBE) scheme named IBE-Lite for the WBANs. Compared with the traditional public key infrastructure (PKI) that employs a digital certificate to bind an identity and an public key, the identity-based cryptography (IBC) [14] does not require digital certificates. A user's public key is computed from its identity information, such as identification numbers, e-mail addresses and IP addresses. The user's private key is produced by a trusted third party named private key generator (PKG). Authenticity of a public key is explicitly achieved without an attached certificate. Therefore, the IBC eliminates certificate management trouble of the traditional PKI, including generation, distribution, storage, verification and revocation. Although the lightweight IBC is very suitable for resource-constrained WBANs, it has key escrow problem since the PKG learns all users' private keys. That is, the PKG is capable of decrypting a ciphertext in an IBE scheme and forging a signature for a message in an identity-based signature (IBS) scheme. Therefore, the IBC only fits small networks, such as the WBANs, and does not fit large-scale networks, such as the Internet. However, the goal of the access control

Manuscript received February 18, 2016; revised April 8, 2016; accepted April 11, 2016. Date of publication April 15, 2016; date of current version June 2, 2016. This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2013J069 and in part by the National Natural Science Foundation of China under Grant 61073176, Grant 61272525, Grant 61302161, and Grant 61462048. The associate editor coordinating the review of this paper and approving it for publication was Prof. M. R. Yuce.

The authors are with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: fagenli@uestc.edu.cn; 735838075@qq.com).

Digital Object Identifier 10.1109/JSEN.2016.2554625

1558-1748 © 2016 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

for the WBANs is to restrict the Internet users to access the WBANs. Therefore, total IBC can not satisfy the goal. Recently, Liu *et al.* [15] used certificateless signature to design two anonymous authentication schemes for the WBANs. A user should be authenticated before accessing the health information stored in a network server. The advantage of Liu et al.'s schemes is to use the certificateless cryptography (CLC) that has neither public key certificates nor key escrow problem [16]. The CLC still requires a trusted third party named key generating center (KGC) who is responsible for producing a partial private key using a master key and a user's identity. Then the user generates a secret value and combines the secret value with the partial private key to form a full private key. Since the KGC does not possess the secret value, it does not know the full private key. The key escrow problem is avoided. However, Liu et al.'s scheme is design to restrict the users to access a network server, not the WBANs.

There are some good works about the access control for the WBANs. In 2011, Cagalaban and Kim [17] designed an efficient access control scheme for the WBANs by using identity-based signcryption (IBSC) [18] (hereafter called CK). The novelty of CK is the use of signcryption that is capable of simultaneously authenticating the users and protecting the query messages. Signcryption [19] is a cryptographic technique that is capable of gaining both the functions of public key encryption and digital signature in a logical single step, with a cost significantly lower than that needed by the traditional signature-then-encryption method. That is, a signcryption scheme is capable of simultaneously achieving confidentiality, integrity, authentication and non-repudiation with a lower cost. However, CK has the key escrow weakness since it is based on the IBC. In 2013, Hu *et al.* [20] designed a fuzzy attribute-based signcryption (FABSC) that can be used in the data encryption, access control, and digital signature in the WBANs (hereafter called HZLCL). The weakness of HZLCL is that it requires some costly cryptographic operations in the FABSC. In 2014, Ma *et al.* [21] also designed an access control scheme using PKI-based signcryption (hereafter called MXH). However, MXH has a heavy certificate management issue since it is based on the PKI.

B. Motivation and Contribution

The previous access control schemes using signcryption have the following weaknesses: (1) They either require the public key certificates or have key escrow problem. (2) They do not have ciphertext authenticity. The controller must first decrypt a ciphertext and then verify its validity. If the ciphertext is not valid, the decryption work will be wasted. The motivation of this paper is to find a new methodology for design of an access control scheme for the WBANs without the above weaknesses. Only authorized users can access the WBANs and the query messages are protected. It is important to protect the query messages for preserving the privacy of the users [21]. Our methodology uses certificateless signcryption (CLSC) [22] with public verifiability and ciphertext authenticity. The contributions of this paper are summarized as follows.

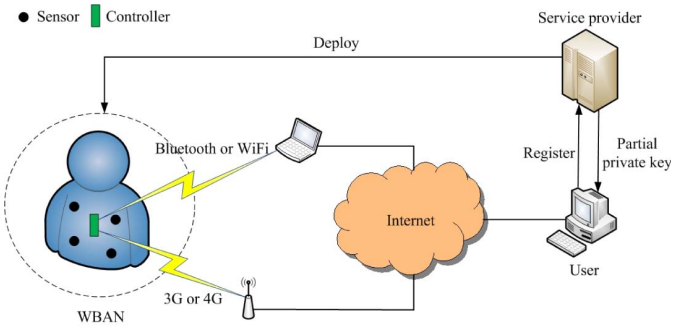


Fig. 1. Network model.

1) We give a CLSC scheme with public verifiability and ciphertext authenticity.
2) We design an access control scheme for the WBANs using the CLSC with public verifiability and ciphertext authenticity. Our scheme achieves confidentiality, integrity, authentication, non-repudiation, public verifiability and ciphertext authenticity. In addition, the proposed scheme has neither key escrow problem nor public key certificates. The controller can verify the validity of a ciphertext without decryption. Compared with existing three access control schemes using signcryption, our scheme has the least computational cost and energy consumption for the controller.

C. Organization

The rest of this paper is organized as follows. The network model, security requirements and bilinear pairings are described in Section II. An efficient CLSC scheme is given in Section III. We give an efficient certificateless access control scheme for the WBANs in Section IV. The performance and security of our access control scheme are discussed in Section V. Finally, the conclusions are given in Section VI.

II. Preliminaries

In this section, we give the network model, security requirements and bilinear pairings.

A. Network Model

Fig. 1 shows the overview of the network model that mainly consists of three entities, the WBAN of a patient, a service provider (SP) and a user (e.g., a nurse, a doctor, a government agency or an insurance company). The WBAN consists of some sensor nodes and a controller. The sensor nodes can communicate with the controller and the controller can communicates with not only the sensor nodes but also the Internet. The SP deploys the WBAN that monitors a patient's vital signs and environmental parameter. If a user hopes to access the WBAN, it must be authorized by the SP. The SP is responsible for the registration for both the user and the WBAN and producing a partial private key for the user and the private keys for the WBAN. That is, the SP plays the KGC in the CLC. We suppose that the SP is honest and curious (the SP follows the protocol but hopes to know the transmitted messages). That is, we do not need to fully trust the SP since it only knows the partial private key of the user. This is an

important advantage of the CLC than the IBC. When a user hopes to access the monitoring data of the WBAN, it first sends a query message to the WBAN. Then controller checks if the user has been authorized to access the WBAN. If yes, the controller sends collected data to the user in a secure way. Otherwise, the controller refuses the query request.

B. Security Requirements

The communication between the user and the controller should satisfy at least four security properties, i.e. confidentiality, authentication, integrity and non-repudiation. Confidentiality keeps query messages secret from the others except the user and the controller. Authentication ensures that only the authorized user can access the WBAN. Integrity ensures that a query message from the user has not been altered by some unauthorized entities. Non-repudiation prevents the denial of previous queries submitted by the user. That is, if the user has submitted a query message to the WBAN, it can not deny its action. In addition, we also hope that this communication satisfies public verifiability and ciphertext authenticity. The public verifiability means that a third party can verify the validity of a ciphertext without knowing the controller's private key. The ciphertext authenticity means that a third party can verify the validity of a ciphertext without decrypting it.

C. Bilinear Pairings

Let G_1 and G_2 be two cyclic groups that have the same prime order p. G_1 is an additive group and G_2 is a multiplicative group. Let P be a generator of G_1. A bilinear pairing is a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$, $a, b \in \mathbb{Z}_p^*$.
2) Non-degeneracy: There are $P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$. Here 1 is the identity element of G_2.
3) Computability: $\hat{e}(P, Q)$ can be efficiently computed for all $P, Q \in G_1$.

The modified Weil pairing and Tate pairing supply admissible maps of this type. Please refer to [14] for details.

III. A Certificateless Signcryption Scheme

In 2008, Barreto *et al.* [22] proposed an efficient certificateless signcryption scheme (hereafter called BDCPS). However, this scheme can not be directly used to design an access control scheme for the WBANs because it can not provide public verifiability and ciphertext authenticity. In this section, we first review BDCPS and then point out its weakness. Finally, we give a modified scheme that is suitable for the design of an access control scheme for the WBANs.

A. The BDCPS Scheme

The BDCPS consists of the following nine algorithms.

Setup: Given a security parameter k, the KGC chooses an additive group G_1 and a multiplicative G_2 of the same prime order p, a generator P of G_1, a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$, and four hash functions $H_1 : G_2^2 \times \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_2 : G_2 \times \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_3 : G_2 \rightarrow \{0,1\}^n$ and $H_4 : (G_2 \times \{0,1\}^*)^3 \rightarrow \mathbb{Z}_p^*$. Here n is the number of bits of a message to be sent. The KGC randomly selects a master secret key $s \in \mathbb{Z}_p^*$ and computes the corresponding public key $P_{pub} = sP$. The KGC publishes the system parameters $\{G_1, G_2, p, \hat{e}, n, P, P_{pub}, g, H_1, H_2, H_3, H_4\}$ and keeps s secret. Here $g = \hat{e}(P, P)$ is a generator of G_2.

Set-Secret-Value: A user with identity ID_U chooses a random $x_U \in \mathbb{Z}_p^*$ as the secret value.

Set-Public-Value: Given a secret value x_U, this algorithm returns the public value $y_U = g^{x_U}$.

Partial-Private-Key-Extract: A user submits its identity ID_U and public value y_U to the KGC. The KGC computes the partial private key

$$D_U = \frac{1}{H_2(y_U, ID_U) + s} P$$

and sends D_U to the user.

Set-Private-Key: Given a partial private key D_U and a secret value x_U, this algorithm returns a full private key $S_U = (x_U, D_U)$.

Set-Public-Key: Given a full private key $S_U = (x_U, D_U)$ and a public value y_U, the user does the following steps:

1) Choose $\alpha \in \mathbb{Z}_p^*$ randomly.
2) Compute $r_U = g^{\alpha}$
3) Compute $h_U = H_1(r_U, y_U, ID_U)$.
4) Compute $T_U = (\alpha - x_U h_U) D_U$.
5) Output a full public key (y_U, h_U, T_U).

Public-Key-Validate: Given a full public key (y_U, h_U, T_U), a verifier checks that y_U has order p (i.e. $y_U \neq 1$ but $y_U^p = 1$) and follows the steps below:

1) Compute $r_U = \hat{e}(H_2(y_U, ID_U)P + P_{pub}, T_U) y_U^{h_U}$
2) Compute $h'_U = H_1(r_U, y_U, ID_U)$.
3) Accept the public key if and only if $h'_U = h_U$.

Signcrypt: Given a message m, a sender's secret value x_A, identity ID_A and public value y_A, and a receiver's identity ID_B and public value y_B, this algorithm works as follows.

1) Choose $\beta \in \mathbb{Z}_p^*$ randomly.
2) Compute $r = y_B^{\beta}$.
3) Compute $c = m \oplus H_3(r)$.
4) Compute $h = H_4(r, m, y_A, ID_A, y_B, ID_B)$.
5) Compute $z = \beta / (h + x_A) \bmod p$
6) Output a ciphertext $\sigma = (c, h, z)$.

Unsigncrypt: Given a ciphertext $\sigma = (c, h, z)$, a sender's identity ID_A and public value y_A, and a receiver's secret value x_B, identity ID_B and public value y_B, this algorithm works as follows.

1) Compute $r = y_A^{x_B z} y_B^{hz}$.
2) Compute $m = c \oplus H_3(r)$.
3) Compute $h' = H_4(r, m, y_A, ID_A, y_B, ID_B)$.
4) Accept the message if and only if $h' = h$, return the false symbol $\perp$ otherwise.

The main characteristic of BDCPS is that BLMQ identity-based signature [23], Schnorr signature [24], and Zheng signcryption [19] are integrated into a certificateless signcryption. In fact, in *Signcrypt* and *Unsigncrypt* algorithms, BDCPS is similar to Zheng signcryption scheme except the h value. In BDCPS, the identities and public values of both

the sender and the receiver are included in H_4. This change can thwart the key replacement denial-of-decryption attack. In addition, *Set-Public-Key* and *Public-Key-Validate* bind the identity ID_U and public value y_U. A user can generate a full public key (y_U, h_U, T_U) only if it know the corresponding full private key $S_U = (x_U, D_U)$. The BDCPS has been proved to satisfy confidentiality (i.e. indistinguishability against adaptive chosen ciphertext attack (IND-CCA2)) and unforgeability (i.e. existential unforgeability against adaptive chosen messages attack (EUF-CMA)) in [22].

B. A Modified BDCPS Scheme

Although BDCPS is very efficient, it can not be directly used to design an access control scheme for the WBANs because of the following two weaknesses: (1) It can not provide the public verifiability since the receiver's secret value x_B is required in the verification process. We need to use the other complex protocols [22] if we hope to achieve the full non-repudiation. (2) It can not provide the ciphertext authenticity [25]. That is, the message m is required in the verification process. Therefore, we can not throw away an invalid ciphertext before the decryption. The controller may consume many meaningless computation time and energies.

Zheng signcryption [19] also has the above two weaknesses. Gamage *et al.* [26] modified Zheng signcryption to achieve public verifiability and ciphertext authenticity. Here we use the same method in [26] to give a modified BDCPS scheme. The first seven algorithms keep unchanged, the last two algorithms are modified as follows.

Signcrypt: Given a message m, a sender's secret value x_A, identity ID_A and public value y_A, and a receiver's identity ID_B and public value y_B, this algorithm works as follows.

1) Choose $\beta \in \mathbb{Z}_p^*$ randomly.
2) Compute $t = g^{\beta}$ and $r = y_B^{\beta}$.
3) Compute $c = m \oplus H_3(r)$.
4) Compute $h = H_4(t, c, y_A, ID_A, y_B, ID_B)$.
5) Compute $z = \beta/(h + x_A) \bmod p$
6) Output a ciphertext $\sigma = (c, h, z)$.

Unsigncrypt: Given a ciphertext $\sigma = (c, h, z)$, a sender's identity ID_A and public value y_A, and a receiver's secret value x_B, identity ID_B and public value y_B, this algorithm works as follows.

1) Compute $t = y_A^z g^{hz}$.
2) Compute $h' = H_4(t, c, y_A, ID_A, y_B, ID_B)$.
3) Check if $h' = h$ holds. If yes, perform the following step 4. Otherwise, output the false symbol $\perp$.
4) Compute $r = t^{x_B}$ and recover $m = c \oplus H_3(r)$.

Gamage *et al.* [26] have proved that such modifications do not weaken the security of signcryption. Therefore, the modified BDCPS scheme has the same security as the original BDCPS. In addition, the modified BDCPS scheme has the public verifiability and ciphertext authenticity. Any third party can verify the validity of ciphertext σ without knowing the message m and the receiver's secret value x_B by the first three steps of *Unsigncrypt*. If the ciphertext σ is not valid, the receiver can immediately throw away it without decryption.

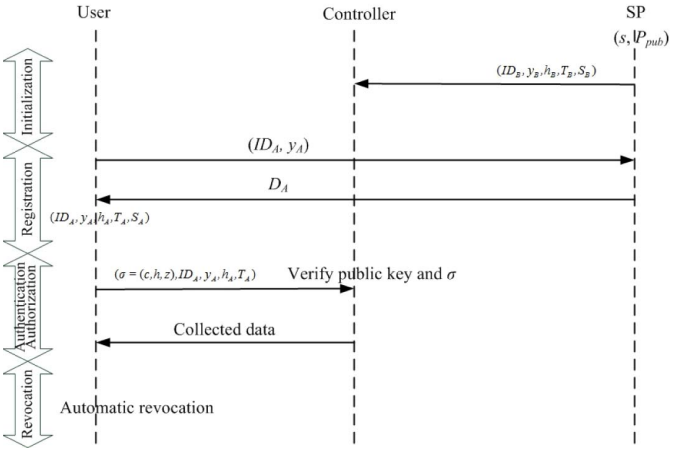


Fig. 2. A certificateless access control scheme.

If the ciphertext σ is valid, the receiver performs the fourth step of *Unsigncrypt* to recovering the message.

IV. A Certificateless Access Control Scheme

In this section, we design an efficient certificateless access control scheme for the WBANs based on identity-based access control (IBAC) model that associates access privilege with specific users. Our methodology uses CLSC with public verifiability and ciphertext authenticity. Such design has the following advantages: (1) It has neither key escrow problem nor public key certificates. (2) It allows the controller to check the valid of query messages without decryption. Such design saves the computational cost and energy consumption. Now we describe a concrete access control scheme using the modified BDCPS scheme. This access control scheme is composed of four phases: the initialization phase, the registration phase, the authentication and authorization phase, and the revocation phase. We summarize the proposed access control scheme in Fig. 2.

A. Initialization Phase

In this phase, the SP runs *Setup* algorithm and deploys a WBAN. The controller is assigned an identity ID_B, a public key (y_B, h_B, T_B) and a private key $S_B = (x_B, D_B)$ (the SP may run *Set-Secret-Value*, *Set-Public-Value*, *Partial-Private-Key-Extract*, *Set-Private-Key* and *Set-Public-Key* algorithms).

B. Registration Phase

A user should register with the SP to gain an access privilege of the WBAN. The user first submits its identity ID_A and public value y_A to the SP and then the SP checks if the identity is valid. If not, the SP rejects the registration request. Otherwise, the SP sets an expiration date ED and runs *Partial-Private-Key-Extract* algorithm to producing a partial private key

$$D_A = \frac{1}{H_2(y_A, ID_A||ED) + s} P.$$

Here $||$ is a concatenation symbol. After receiving D_A, the user runs *Set-Secret-Value*, *Set-Public-Value*, *Set-Private-Key* and *Set-Public-Key* to get a full private key $S_A = (x_A, D_A)$ and a full public key (y_A, h_A, T_A).

TABLE I
COMPARISON OF PERFORMANCE

Schemes	Computational cost		Controller communication cost*		Methodology
	User	Controller	Receive	Transmit	
CK [17]	1P+3M	3P+M	$2\|G_1\|+\|ID\|+\|m\|$	—	IBSC
HZLCL [20]	5P+M	$(2\|m\|+5)$M	—	$4\|G_1\|+\|G_2\|+\|ID\|$	FABSC
MXH [21]	2M	5M	$\|G_1\|+\|\mathbb{Z}_p^*\|+\|Cert\|+\|m\|$	—	PKI-based signcryption
Ours	2E	1P+1M+1E	$\|G_1\|+\|G_2\|+3\|\mathbb{Z}_p^*\|+\|ID\|+\|m\|$	—	CLSC

*The timestamp is omitted in the communication cost for all schemes.

C. Authentication and Authorization Phase

When the user with identity ID_A wants to access the monitoring data of the WBAN, it first produces a query message m and runs *Signcrypt* algorithm to generate a ciphertext $\sigma = (c, h, z)$. To resist the replay attack, we may concatenate the query message and a timestamp to form a new signcrypted message. Then the user sends the controller the ciphertext σ, its identity ID_A and full public key (y_A, h_A, T_A). When getting the query request from the user, the controller first runs *Public-Key-Validate* algorithm to check the validity of the received public key (y_A, h_A, T_A). If the public key is not valid, the controller immediately rejects the query request. Otherwise, the controller further computes $t = y_A^z g^{hz}$ and $h' = H_4(t, c, y_A, ID_A, y_B, ID_B)$ and checks if $h' = h$ holds. If not, it rejects the query request. Otherwise, the user is authorized to access the data of the WBAN. In this case, the controller computes $r = t^{x_B}$ and recovers the message $m = c \oplus H_3(r)$. Then the controller can encrypt the collected health data employing a symmetric cipher (such as AES [27]) with the session key $H_3(r)$ according to the query requirement m. This session key has been established between the controller and the user. Because the session key is only known by the controller and the user, we can achieve the confidentiality for future communication between them. In this access process, confidentiality, integrity, authentication and non-repudiation are simultaneously achieved. In addition, an important advantage of our scheme is to achieves the public verifiability and ciphertext authenticity. By using this modified BDCPS scheme, full non-repudiation can be easily obtained. In addition, any third party can verify the validity of the ciphertext σ without knowing the controller's private key and the message m. Finally, the controller can throw away some invalid ciphertexts without decryption. That is, the controller does not perform the fourth step of *Unsigncrypt*, which saves computational cost and energy consumption. If required, the anonymity also can be gained by scrambling the user's identity ID_A and full public key (y_A, h_A, T_A) together with the message at the third step of *Signcrypt* algorithm. That is, we compute $c = (ID_A||y_A||h_A||T_A||m) \oplus H_3(r)$ instead of $c = m \oplus H_3(r)$. Of course, we should alter the output length of H_3 to adapt the length of the encrypted message. Such modification do not affect the security and efficiency of our scheme.

D. Revocation

The access privilege is revoked automatically by the expiration date ED. For example, if the expiration date ED is "2016-12-31", the user only can access the WBAN before December 31, 2016. That is, the full private key and full public key of the user automatically become illegal after December 31, 2016. If we need to revoke the user's access privilege before the expiration date due to some reasons, the SP can submit the revoked identity to the controller. The controller keeps a list of revoked identities to identify the validity of users.

V. ANALYSIS OF THE ACCESS CONTROL SCHEME

In this section, we analyze the performance and security properties of our access control scheme. First, we compare the main computational cost and communication cost of our scheme with those of CK [17], HZLCL [20] and MXH [21] in Table I. The four schemes use different methods to design the access control schemes. CK uses the IBSC, HZLCL uses FABSC, MXH uses PKI-based signcryption and our scheme uses CLSC. We use the symbol P to denote a pairing operation, the symbol M to denote a point multiplication operation in G_1 and the symbol E to denote an exponentiation operation in G_2. The other operations are ignored since the three operations consume the most running time of the whole algorithm. Let $|x|$ be the number of bits of x. Since MXH is based on the traditional PKI system, we must verify the public key certificate before using a public key. Here we assume that the public key certificates are signed using ECDSA (elliptic curve digital signature algorithm) [28]. The ECDSA requires one point multiplication operation in signing a message and two point multiplication operations in verifying a signature. Therefore, in MXH, the controller needs two point multiplication operations to verify a user's public key certificate. From Table I, we know that our scheme has less computational cost than the other three schemes for both the user and the controller. For the communication cost of the controller, MXH needs to receive the user's certificate $Cert$ to verify its validity.

We give a quantitative evaluation for CK [17], HZLCL [20], MXH [21] and our scheme. Here we only consider the cost of controller part since its resource is limited. For MXH, we adopt the experiment result in [29] on MICA2 which is equipped with an ATmega128 8-bit processor clocked at 7.3728 MHz, 128 KB ROM and 4 KB RAM. From [29], we learn that a point multiplication operation costs 0.81 s using an elliptic curve with 160 bits p which represents 80-bit security level. For the other three scheme, we adopt the result in [30] on the same processor ATmega128. A pairing operation costs 1.9 s and an exponentiation operation in G_2 costs 0.9 s using a supersingular curve $y^2 + y = x^3 + x$

with an embedding degree 4 and implementing an η_T pairing: $E(\mathbb{F}_{2^{271}}) \times E(\mathbb{F}_{2^{271}}) \rightarrow \mathbb{F}_{2^{4\cdot 271}}$, which is also equivalent to the 80-bit security level. According to the results in [29] and [30], we know that the computational time on the controller of CK, HZLCL, MXH and our scheme are $3*1.9+1*0.81 = 6.51$ s, $(2|m|+5)*0.81$ s, $5*0.81 = 4.05$ s and $1*1.9+1*0.81+1*0.9 = 3.61$ s, respectively. As in [30]–[32], we suppose that the power level of MICA2 is 3.0 V, the current draw in active mode is 8.0 mA, the current draw in transmitting mode is 27 mA, the current draw in receiving mode is 10 mA, and the data rate is 12.4 kbps. For energy consumption, according to the evaluation method in [21] and [33], a pairing operation consumes $3.0*8.0*1.9 = 45.6$ mJ, a point multiplication operation consumes $3.0*8.0*0.81 = 19.44$ mJ and an exponentiation operation in G_2 consumes $3.0*8.0*0.9 = 21.6$ mJ. Therefore, the computational energy consumption on the controller of CK, HZLCL, MXH and our scheme are $3*45.6+1*19.44 = 156.24$ mJ, $(2|m|+5)*19.44 = 38.88|m|+97.2$ mJ, $5*19.44 = 97.2$ mJ and $1*45.6+1*19.44+1*21.6 = 86.64$ mJ, respectively.

For the communication cost, we suppose that $|m| = 160$ bits, $|ID| = 80$ bits and $|hash| = 160$ bits. In addition, the size of a digital certificate is at least 688 bits [34]. For MXH, the size of an element in group G_1 is 1024 bits employing an elliptic curve with 160 bits p. Using standard compression method [30], the size of an element in group G_1 can be compressed to 65 bytes. So, in MXH, the controller should receive

$$|G_1|+|\mathbb{Z}_p^*|+|Cert|+|m| \text{ bits} = 65+20+86+20 = 191 \text{ bytes}$$

messages. CK, HZLCL and our scheme use a curve over the binary field $\mathbb{F}_{2^{271}}$ with the G_1 of the 252 bits prime order. The size of an element in group G_1 is 542 bits and can be compressed to 34 bytes. The size of an element in group G_2 is 1084 bits. So in CK, the controller needs to receive

$$2|G_1|+|ID|+|m| \text{ bits} = 2*34+10+20 = 98 \text{ bytes}$$

messages. In HZLCL, the controller needs to transmit

$$4|G_1|+|G_2|+|ID| \text{ bits} = 4*34+136+10 = 282 \text{ bytes}$$

messages. In our scheme, the controller needs to receive

$$|G_1|+|G_2|+3|\mathbb{Z}_p^*|+|ID|+|m| \text{ bits} = 34+136+3*32+10+20 = 296 \text{ bytes}$$

messages. From [30], we know the controller takes $3*27*8/12400 = 0.052$ mJ and $3*10*8/12400 = 0.019$ mJ to transmit and receive one byte messages, respectively. Therefore, in CK, HZLCL, MXH and our scheme, then communication energy consumption of the controller are $0.019*98 = 1.86$ mJ, $0.052*282 = 14.66$ mJ, $0.019*191 = 3.63$ mJ and $0.019*296 = 5.62$ mJ. The total energy consumption of CK, HZLCL, MXH and our schemes are $156.24+1.86 = 158.1$ mJ, $38.88*160+97.2+14.66 = 6,332.66$ mJ, $97.2+3.63 = 100.83$ mJ and $86.64+5.62 = 92.26$ mJ respectively.

The computational time and total energy consumption of the controller are summarized in Fig. 3 and Fig. 4, respectively

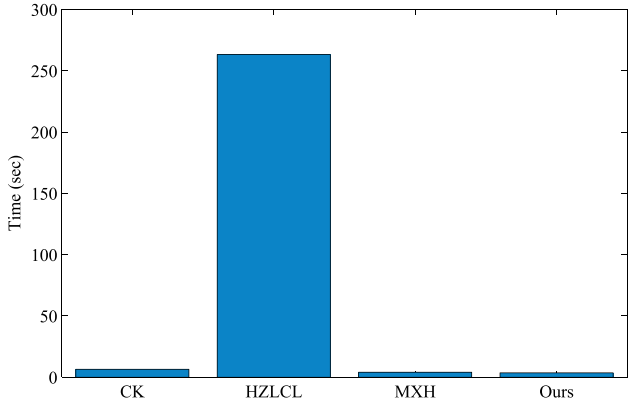


Fig. 3. The computational time of the controller.

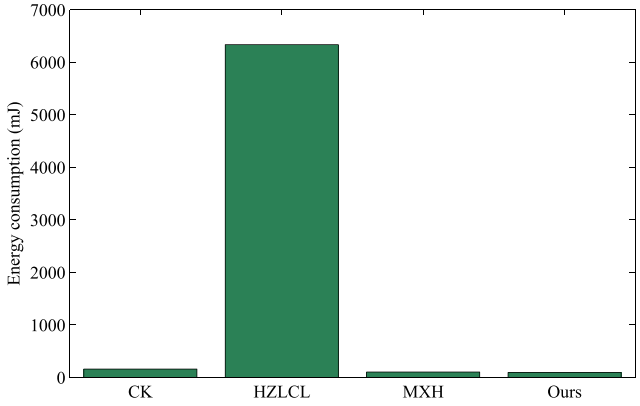


Fig. 4. The energy consumption of the controller.

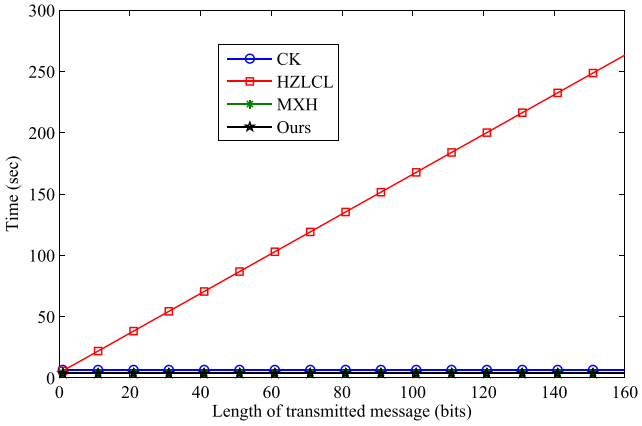


Fig. 5. The computational time versus length of transmitted message.

(here we suppose $|m| = 160$ bits). From Fig. 3 and Fig. 4, we find that our scheme has the least computational time and energy consumption among the four schemes.

We give the relationship between the computational time and length of sent message in Fig. 5 and the relationship between the energy consumption and length of sent message in Fig. 6. We find that both the computational time and the energy consumption increase linearly with the length of the sent message in HZLCL. However, the other three schemes have a little effect on the length of the sent message.

We compare the security properties of the four schemes in Table II. Here we use Con, Int, Aut, Non, PubVer and

TABLE II
COMPARISON OF SECURITY

Schemes	Con	Int	Aut	Non	PubVer	CipAut	No certificate	No key escrow
CK [17]	√	√	√	√	√	×	√	×
HZLCL [20]	√	√	√	√	√	×	√	×
MXH [21]	√	√	√	√	×	×	×	√
Ours	√	√	√	√	√	√	√	√

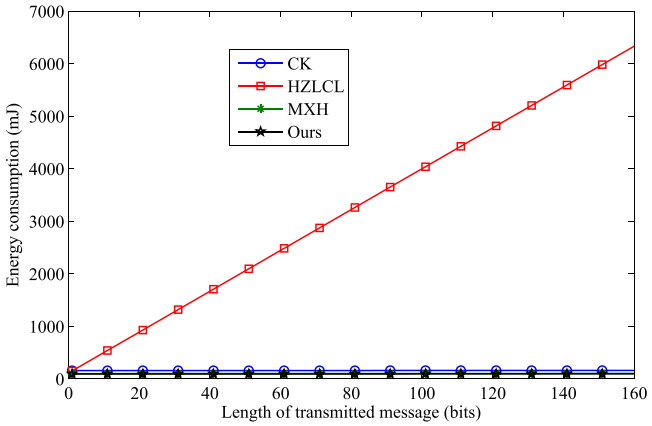


Fig. 6. The energy consumption versus length of transmitted message.

CipAut to denote confidentiality, integrity, authentication, non-repudiation, public verifiability, and ciphertext authenticity, respectively. A symbol √ denotes that the scheme satisfies this security property and a symbol × denotes that the scheme does not satisfy this security property. CK, HZLCL and MXH do not satisfy ciphertext authenticity and our scheme satisfies such security property. In addition, CK and HZLCL have the key escrow problem since they are based on the IBC. MXH has the public key certificates problem since it is based on the PKI. Our scheme has neither key escrow problem nor public key certificates since it is based on the CLC.

VI. CONCLUSION

In this paper, we proposed a modified certificateless signcryption scheme that satisfies public verifiability and ciphertext authenticity. We also gave a certificateless access control scheme for the WBANs using the modified signcryption. Compared with existing four access control schemes using signcryption, our scheme has the least computational time and energy consumption. In addition, our scheme is based on the CLC that has neither key escrow problem nor public key certificates.

REFERENCES

[1] T. Y. Wu and C. H. Lin, "Low-SAR path discovery by particle swarm optimization algorithm in wireless body area networks," *IEEE Sensors J.*, vol. 15, no. 2, pp. 928–936, Feb. 2015.

[2] C. Yi, L. Wang, and Y. Li, "Energy efficient transmission approach for WBAN based on threshold distance," *IEEE Sensors J.*, vol. 15, no. 9, pp. 5133–5141, Sep. 2015.

[3] J. He, Y. Geng, Y. Wan, S. Li, and K. Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3826–3836, Oct. 2013.

[4] D. Liu, Y. Geng, G. Liu, M. Zhou, and K. Pahlavan, "WBANs-Spa: An energy efficient relay algorithm for wireless capsule endoscopy," in *Proc. IEEE 82nd Veh. Technol. Conf. (VTC-Fall)*, Boston, MA, USA, Sep. 2015, pp. 1–5.

[5] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 1, pp. 316–326, Jan. 2014.

[6] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, Jan. 2014.

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

[8] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in *Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Secur. Privacy (HotWiSec)*, Budapest, Hungary, 2013, pp. 31–35.

[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[10] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.

[11] H. Zhao, J. Qin, and J. Hu, "An energy efficient key management scheme for body sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2202–2210, Nov. 2013.

[12] D. He, S. Chan, Y. Zhang, and H. Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 2, pp. 440–448, Mar. 2014.

[13] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-Lite: A lightweight identity-based cryptography for body sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 926–932, Nov. 2009.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[15] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.

[16] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2894. New York, NY, USA: Springer-Verlag, 2003, pp. 452–474.

[17] G. Cagalaban and S. Kim, "Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption," in *Proc. 13th Int. Conf. Adv. Commun. Technol. (ICACT)*, Seoul, Korea, Feb. 2011, pp. 863–867.

[18] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 3386. New York, NY, USA: Springer-Verlag, 2005, pp. 362–379.

[19] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption)," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1294. New York, NY, USA: Springer-Verlag, 1997, pp. 165–179.

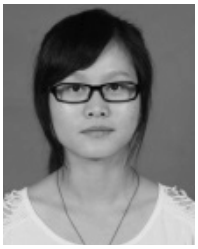
[20] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 37–46, Sep. 2013.

[21] C. Ma, K. Xue, and P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks," *Secur. Commun. Netw.*, vol. 7, no. 4, pp. 759–773, Apr. 2014.

[22] P. S. L. M. Barreto, A. M. Deusajute, E. de Souza Cruz, G. C. F. Pereira, and R. R. da Silva, "Toward efficient certificateless signcryption from (and without) bilinear pairings," in *Proc. Brazilian Symp. Inf. Comput. Syst. Secur.*, 2008, pp. 115–125.

[23] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3788. New York, NY, USA: Springer-Verlag, 2005, pp. 515–532.
[24] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.
[25] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Information Security and Cryptology* (Lecture Notes in Computer Science), vol. 2971. New York, NY, USA: Springer-Verlag, 2004, pp. 352–369.
[26] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 1560. New York, NY, USA: Springer-Verlag, 1999, pp. 69–81.
[27] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer, 2002.
[28] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.
[29] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 3156. New York, NY, USA: Springer-Verlag, 2004, pp. 119–132.
[30] K.-A. Shim, Y.-R. Lee, and C.-M. Park, "EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks," *Ad Hoc Netw.*, vol. 11, no. 1, pp. 182–189, Jan. 2013.
[31] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," *Comput. Commun.*, vol. 31, no. 4, pp. 659–667, Mar. 2008.
[32] F. Li, Z. Zheng, and C. Jin, "Secure and efficient data transmission in the Internet of Things," *Telecommun. Syst.*, vol. 62, no. 1, pp. 111–122, 2016.
[33] K. A. Shim, "S^2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks," *Ad Hoc Netw.*, vol. 19, pp. 1–8, Aug. 2014.
[34] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 11, pp. 4136–4144, Nov. 2007.

Fagen Li (M'14) received the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2007. He was a Post-Doctoral Fellow with Future University-Hakodate, Hokkaido, Japan, from 2008 to 2009, which is supported by the Japan Society for the Promotion of Science. He was a Research Fellow with the Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan, from 2010 to 2012. He is currently an Associate Professor with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. He has authored more than 70 papers in international journals and conferences. His recent research interests include cryptography and network security.



Jiaojiao Hong received the B.S. degree from Anhui University, Hefei, China, in 2014. She is currently pursuing the master's degree with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. Her research interests include cryptography and information security.