Body Area Network Security: A Fuzzy Attribute-Based Signcryption Scheme

Chunqiang Hu, Nan Zhang, *Member, IEEE*, Hongjuan Li, Xiuzhen Cheng, *Senior Member, IEEE,* and Xiaofeng Liao, *Senior Member, IEEE*

***Abstract*—Body Area Networks (BANs) are expected to play a major role in the field of patient-health monitoring in the near future. While it is vital to support secure BAN access to address the obvious safety and privacy concerns, it is equally important to maintain the elasticity of such security measures. For example, elasticity is required to ensure that first-aid personnel have access to critical information stored in a BAN in emergent situations. The inherent tradeoff between security and elasticity calls for the design of novel security mechanisms for BANs.**

In this paper, we develop the Fuzzy Attribute-Based Signcryption (*FABSC*), a novel security mechanism that makes a proper tradeoff between security and elasticity. *FABSC* leverages fuzzy Attribute-based encryption to enable data encryption, access control, and digital signature for a patient's medical information in a BAN. It combines digital signatures and encryption, and provides confidentiality, authenticity, unforgeability, and collusion resistance. We theoretically prove that FABSC is efficient and feasible. We also analyze its security level in practical BANs.

***Index Terms*—Body area networks (BANs); BAN controller; signcryption; attribute-based cryptosystem; access control structure; elasticity.**

I. Introduction

BODY Area Networking is enabled by the rapid development of wireless sensor networks and biomedical engineering techniques [1]–[3]. A typical body area network (BAN) consists of a number of BAN devices (implanted sensors and wearable sensors) and a BAN controller. BANs are designed to monitor the parameters of human bodies and the surrounding environments and to assist the human body by providing life support, visual/audio feedback, etc. As a BAN stores and processes personal health information (e.g., health history, vital signs, etc.), it raises a number of privacy and safety concerns [4]–[8]. In general, there exist two types of threats:

- *Unauthorized data-access.* An adversary gains access to a patient's medical information stored in the BAN, or eavesdrops such information when it is transmitted via wireless communications, without permission of the patient. This attack raises significant privacy concerns - e.g., a patient may not wish his/her vital information to be disclosed to an insurance company.
- *Message modification.* An adversary modifies the messages (e.g., content, timing, sequence order, etc.) generated within a BAN before they are transmitted, or manipulates the message contents being transmitted between a BAN and an external entity (e.g., a medical doctor). This attack raises significant safety concerns - e.g., wrong diagnosis/treatment of the patient, or even the malfunction of life-critical devices such as an implantable cardioverter-defibrillator (ICD) [9] [10] [11].

On one hand, a security mechanism for a BAN must provide access control, data encryption, and message authentication, in order to effectively defend against the attacks mentioned above. On the other hand, such a mechanism must not prevent access to the patient's medical information in emergency situations. For example, when an unconscious patient carrying an ICD is sent to an emergency room in an area far away from his/her primary doctor, the emergency-room physician must be able to access the medical information stored in the BAN and deactivate the ICD before a surgery, even if the physician cannot reach the patient's primary doctor in time to obtain the proper access credentials. This requires the security mechanism to be elastic enough such that emergency situations can be properly handled.

In this paper, we develop the Fuzzy Attribute-based Signcryption (FABSC), a novel security mechanism for access control, data encryption, and message authentication in BANs. FABSC employs an attribute-based encryption (ABE) scheme [12] [13] to make a proper tradeoff between security and elasticity. It allows a patient to specify a set of attributes (i.e., credentials) a physician is expected to possess in order to access a certain piece of sensitive information. It also allows a physician to access the data if the intersection between the physician's credentials and the required ones exceeds a pre-determined threshold. With such a fuzzy control, an emergency-room physician does not have to possess exactly the same credentials as the patient's primary doctor in order to access the patient's medical information. Instead, as long as the emergency-room physician provides enough credentials, he/she should be granted the access to the patient data in

Manuscript received February 15, 2012; revised July 14, 2012.

C. Hu is with the College of Computer Science, Chongqing University, Chongqing, China, 400031, and with the Department of Computer Science, The George Washington University, Washington DC, USA, 20052 (e-mail: chu@gwu.edu).

N. Zhang is with the Department of Computer Science, The George Washington University, Washington DC 20052 (e-mail: nzhang10@gwu.edu).

H. Li is with School of Computer Science and Technology, Dalian University of Technology, Dalian 116024, China, and with the Department of Computer Science, The George Washington University, Washington DC 20052 (e-mail: hongjuanli86@gmail.com).

X. Cheng is with the Department of Computer Science, The George Washington University, Washington DC 20052 (e-mail: cheng@gwu.edu).

X. Liao is with the College of Computer Science, Chongqing University, Chongqing, China 400031 (e-mail: xfliao@cqu.edu.cn).

Digital Object Identifier 10.1109/JSAC.2013.SUP.0513004

order to properly treat the patient. Obviously, this satisfies the elasticity requirement discussed above.

Attribute-based encryption has been considered particularly suitable for our purpose because it significantly reduces the cost of certificate verification. However, although ABE could achieve data security, it does not check data authenticity and integrity. The FABSC proposed in this paper, on the other hand, provides both security and authentication for BANs. FABSC has two desired properties: Sincryption (signature and encryption) and error-tolerance, which enables data confidentiality, authenticity, unforgeability, and collusion resistance.

We outline the main contributions of this paper as follows:

- We develop FABSC, a novel scheme that integrates encryption and signature without requiring any certificate for verification. This provides a certain level of error-tolerance for the identities (sets of attributes).
- We theoretically prove the correctness of the proposed scheme and analyze its efficiency and feasibility. In particular, we prove the security of FABSC from four different angles: resistant against collusion attacks, confidentiality, authenticity, and unforgeability.
- We evaluate the performance of FABSC in terms of energy consumption and communication/computation overhead.

The rest of the paper is organized as follows. Section II introduces the motivation of the study. We present the problem formulation in Section III and develop the main idea of FABSC in Section IV. Section V presents the performance analysis, and SectionVI overviews the related work, followed by the conclusions in Section VII.

II. Motivation

In a healthcare or assisted-living BAN, the controller should be accessed by a number of parties involved - e.g., the primary doctor of the patient, and the doctors and nurses on duty of the day when the patient is hospitalized. To make the matter even more complex, a patient might be sent to a different hospital each time. One can see that different parties have different access rights - e.g., the primary doctor and the doctors on duty should have the full access rights, a nurse should have restricted access rights compared with a doctor, and the patient him/herself should have even less access rights to avoid misconfiguration of the system by mistake. In the design of BAN security mechanisms, we therefore face a critical technical challenge: how to properly regulate the access rights of these involved personnel while providing strong access control to the BAN controller? How to verify the identity of a person?

To tackle this challenge, we propose to design an attribute-based security scheme that can support not only differentiated encryption mechanisms but also role-based strong access control. To protect against information exposure due to theft or loss of the BAN controller, the personnel identification should be verified when they connect with the controller. To control the access to the controller, the attribute-based encryption over IBE [13] [14] will be investigated. In attribute-based encryption, a ciphertext is labeled with a set of attributes and a private keys is associated with an access structure that controls which ciphertext the person is able to decrypt.

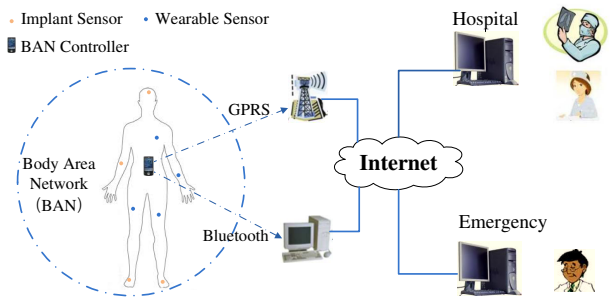


Fig. 1. A BAN Architecture of a health care application.

Similarly, access structures are used to control the access rights of different users of the BAN controller. In this paper, we will design algorithms to regulate the access rights to the controller based on the attribute-based encryption over IBE. The performance of this design in terms of energy consumption and communication/conputation overhead will be extensively studied.

III. System Model and Preliminaries

A. Network Model

We consider a health-care system depicted in Fig. 1. There are two main entities in this system: the BAN of a patient and the external user(s). In particular, the BAN consists of one BAN controller and a number of (implantable or wearable) devices. These devices are usually sensors that monitor vital body parameters or movements, and control the human body by providing life support, visual/audio feedback, etc. The BAN devices communicate with the BAN controller directly or via multi-hop communications. The BAN controller communicates with not only the BAN devices but also the Internet. Moreover, BAN controllers in close proximity may form an ad hoc network with wireless personal area network (WPAN) techniques.

In this paper, we assume the existence of a trusted third party *KS* - i.e., a key distribution server - which is able to verify the identity of a legitimate external user (e.g., a doctor) and distribute credentials to the external user accordingly. The identify of the external user is a set of attributes describing the basic information of the user. Note that *KS* is not required to be online when an emergency-room doctor needs to communicate with the BAN of a patient - i.e., it does not become a single point-of-failure for the system.

B. Adversary Model

In this paper, we consider both types of adversaries outlined in Section I: 1) passive adversaries that eavesdrop messages transmitted (wirelessly) within the BAN or between the BAN and the external user; 2) active adversaries that manipulate the transmitted messages. We also consider the collusion of multiple adversaries. Note that an adversary may be either an external user without any authorized access to the BAN, or an "insider" [15] which aims to retrieve/manipulate the medical information it is not authorized to access.

C. Security Requirements

We now outline the requirements of secure communications in a BAN:

- *Access Control:* The security mechanism must be able to properly enforce different access rights for different users. Note that such access rights are applicable not only to sensitive data stored in the BAN, but also to a command/instruction/query from an external user, because the BAN needs to decide whether to accept an external query or not. Besides, the access control mechanism must be resilient to attacks from colluding adversaries and from cloned devices [16], [17].
- *Authentication*: In the BAN, an active adversary may alter the content, sequence, and/or timing of a transmitted message. Thus, a security mechanism must properly authenticate the messages received by the BAN as well as by the external users.
- *Unforgeability*: An active adversary may also masquerade the BAN controller by creating a signed and encrypted text to deceive legal external users. An effective security mechanism must be able to properly defend against such masquerading attacks.

D. Preliminaries

We now introduce preliminaries for the cryptographic primitives used in FABSC.

1) Bilinear Maps and Bilinear Diffie-Hellman problems: Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two bilinear groups of prime order p, and g be a generator of $\mathbb{G}_1$. Our proposed FABSC makes use of a bilinear map: $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, with the following properties:

1) *Bilinear:* $\forall P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p$, there is $e(P^a, Q^b) = e(P, Q)^{ab}$. Here $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ is a Galois field of order p.
2) *Non-degeneracy:* The generator g satisfies $e(g, g) \neq 1$.
3) *Computability:* There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

With a bilinear map, one has the following variation of the Diffie-Hellman problem. Note that the hardness [12] of the decision version of it - i.e., the decisional bilinear Diffie-Hellman problem (DBDH) - forms the basis for the security of our FABSC scheme.

Bilinear Diffie-Hellman problem (BDH): Given two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with the same prime order p, let $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map and g be a generator of $\mathbb{G}_1$. The objective of BDH is to compute $e(g, g)^{abc}$ in $(\mathbb{G}_1, \mathbb{G}_2, e)$ from the given (g, g^a, g^b, g^c), where $a, b, c \in \mathbb{Z}_p$.

Decisional Bilinear Diffie-Hellman problem (DBDH): Given (g, g^a, g^b, g^c, h) where $h \in \mathbb{G}_2$ and $a, b, c \in \mathbb{Z}_p$ are previously unknown random numbers, the objective of DBDH is to decide whether $h = e(g, g)^{abc}$.

2) Secret sharing schemes: Another important cryptographic primitive used by FABSC is secret sharing. Secret sharing schemes were first developed by Shamir [18] and then extensively studied [19]–[21]. We provide a brief overview as follows: In the context of a *dealer* sharing a secret with a number of *participants* $u_1, \ldots, u_n$, with the objective that a participant learns the secret iff it can cooperate with at least $t-1$ other participants (on sharing what they learn from the dealer), where $t \leq n$ is a pre-determined parameter. The secret to be shared by the dealer is $s \in \mathbb{Z}_p$, where $p > n$. Before secret sharing, each respondent u_i holds a secret key $x_i \in \mathbb{Z}_p$, which is only known by u_i and the dealer.

The dealer follows a two-step process. First, it constructs a polynomial function $f(x)$ of degree $t-1$, i.e.,

$$f(x) = s + \sum_{j=1}^{t-1} a_j x^j, \tag{1}$$

by randomly choosing each a_j i.i.d. with a uniform distribution from $\mathbb{Z}_p$. Note that all (additive and multiplication) operations used in (1) and throughout the rest of the paper are modular arithmetic (defined over $\mathbb{Z}_p$) as opposed to real arithmetic. Also note that s forms the constant component of $f(x)$ - i.e., $s = f(0)$. Then, in the second step, the dealer transmits to each u_i a shared secret $s_i = f(x_i)$.

We now show how t or more users can cooperate to recover s by sharing the secrets received from the dealer. Without loss of generality, let $u_1, \ldots, u_t$ be the cooperating users. These t users can reconstruct the secret $s = f(0)$ from $s_1 = f(x_1), \ldots, s_t = f(x_t)$ by computing

$$s = f(0) = \sum_{j=1}^{t} \left(s_j \prod_{i \in [1,n], i \neq j} \frac{0 - x_i}{x_i - x_j} \right). \tag{2}$$

Note that the cumulative product in (2) is essentially the Lagrange coefficient. The correctness of (2) can be easily verified based on the definition of $f(x)$.

E. Security Measure

We now define the security measure for FABSC along the same spirit as the notion of selective-ID game [12] [22]. In particular, we consider an (n, ϵ)-security game consisting of the following four steps:

Init: The adversary *Adv* declares its identity α in the game.

Setup: A simulator $\mathcal{B}$ selects the parameters for the signcryption algorithm proposed in this paper. Note that the parameter settings for $\mathcal{B}$ reflect the fact that *Adv* is not authorized to access the message being encrypted.

Query: *Adv* is allowed to execute the simulator over at most $\min(poly(n), poly(1/\epsilon))$ arbitrary inputs, where $poly(\cdot)$ is a polynomial function, n is the length of the message being encrypted (i.e., the length of the patient's medical data), and ϵ is a parameter used below.

Challenge: *Adv* chooses two equal-length plaintext messages M_0 and M_1 such that $M_0 \neq M_1$. The simulator picks b uniformly at random from $\{0, 1\}$, encrypts M_b with $\mathcal{B}$, and transmits the ciphertext to *Adv*.

Guess: *Adv* outputs its estimation of b. It wins the game if the output is correct. Otherwise the defender wins.

Based on the definition of such an (n, ϵ)-security game, we say that a polynomial-time adversary has *negligible advantage* - i.e., the signcryption algorithm is secure - iff for $\forall \epsilon > 0$,

$$\Pr\{\textit{Adv} \text{ wins an } (n, \epsilon)\text{-game}\} \leq \frac{1}{2} + \epsilon. \tag{3}$$

TABLE I
NOTATIONS

Notations	means
$\mathbb{G}_1, \mathbb{G}_2$	The two bilinear groups of prime order p
H	A Hash function
$\mathbb{Z}_p$	The Integers Modulo p
α	The adversary's identity, consisting of his/her attributes
M	Plaintext message
E_i, S_1, S_2	Ciphertext
Id	The user's identity, consists of his/her attributes
g	A generator of $\mathbb{G}_1$
$T(i)$	A function
$\triangle_{i,N}(x)$	The Lagrange coefficients. In $\triangle_{i,S}(x)$, S is a subset of N

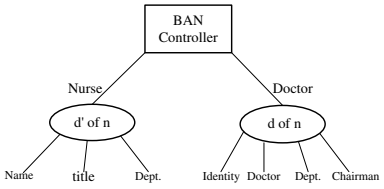


Fig. 2. An example access control structure in a BAN.

F. Notations

The notations and their semantic meanings utilized in this paper to describe our scheme are presented in Table I:

IV. Our Solution: FABSC

In this section, we first describe the main idea of our access control structure which enforces different access rights for different users. Then, we detail the four algorithms of FABSC.

A. Access Control Structure

Our main idea is to design an attribute-based security scheme which views identities (of external users) as sets of attributes, and enforces a lower bound on the number of common attributes between a user's identity and the access rights specified for the sensitive data. In particular, we assume an identity consists of n attributes, and each attribute can be considered as a string of arbitrary length. Examples of identities include Id_1={*doctor*, *Identity*, *department*, *title*}, Id_2={*Name*, *title*, *Dept.*}, etc. This further enables us to specify access privileges of users based on attributes. We may designate the access structure of a user as: 'd out of n attributes', which allows the user to obtain the data from the BAN controller when the user has at least d attributes possessed by the data. We specify an error-tolerance d to each identity. Fig. 2 illustrates the aforementioned access structure in our health-monitoring BAN.

Notably, we can define a set of attributes for each user from the access control structure because a personal BAN usually does not have a large number of users. We distribute the access rights to users and set up a different threshold d for each.

B. The proposed scheme

Assume that a patient is hospitalized. Now the doctor *Victor* communicates with the BAN Controller *Ctr* to get the physical data of the patient's body. The data is stored in the BAN controller and is assigned to different categories such as $\mu_1 = \{Temperature, Pulse, Blood\text{-}Pressure\}$, $\mu_2 = \{Medical\text{-}History\}$, and $\mu_3 = \{Age, Name\}$. Then the message can be represented by $M = \{\mu_1, \mu_2, \mu_3\}$. We define a time stamp tt. Assume that δ is a predefined time limit for message decryption. *KS* is used to represent a trusted third party *Key Server*.

Algorithm 1 Setup (n, d) – run by the key server *KS*

1) Randomly picks a secret value $y \in \mathbb{Z}_p$ and an element $g_2 \in \mathbb{G}_1$, computes $g_1 = g^y$ and $U = e(g_1, g_2)$.
2) Selects $t_1, t_2, ..., t_{n+1}$ uniformly and randomly from $\mathbb{G}_1$. Let N be the set $\{1, 2, ..., n+1\}$ and define a function T as follows:
$$T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\triangle_{i,N}(x)}. \quad (4)$$
3) Selects an $I' \in \mathbb{G}_1$ and a vector $\mathbf{I} = \{I_1, I_2, ...I_m\}$ randomly, where $I_i \in \mathbb{Z}_p, 1 < i < m$, with m being the plaintext length.
4) The public parameters of the system and the master key are given by,
$$\begin{aligned} PubParams &= (g_1, g_2, t_1, t_2, ..., t_{n+1}, \nu' = g^{I'}, \\ &\quad \nu_1 = g^{I_1}, ..., \nu_m = g^{I_m}, U) \end{aligned}$$
The master key $MSK = y$.

Algorithm 2 Key Generation (*PubParams*, *MSK*, Id) – run by the key server *KS*

1) Randomly selects a $d-1$ degree polynomial q such that $q(0) = y$.
2) Picks up $r_1, r_2, ..., r_n \in \mathbb{Z}_p$ and obtains the key sets $K_{Id} = (\{D_i\}, \{d_i\})$ constructed by
$$D_i = g_2^{q(i)} T(i)^{r_i} \quad (5)$$
$$d_i = g^{-r_i} \quad (6)$$
3) The private keys of the sender (Controller) and the receiver (e.g. the doctor *Victor*) can be computed by
$$K_{Id_{Ctr}} = (\{D_{Ctr}\}, \{d_{Ctr}\}) = (g_2^{qCtr(i)} T(i)^{r_{Ctr}}, g^{-r_{Ctr}}) \quad (7)$$
$$K_{Id_V} = (\{D_V\}, \{d_V\}) = (g_2^{qV(i)} T(i)^{r_V}, g^{-r_V}) \quad (8)$$

Our scheme consists of four Algorithms; (1) **Algorithm** 1 provides system initialization; (2) **Algorithm** 2 is used to generate the private keys for the users; (3) The signcryption procedure is detailed in **Algorithm** 3, which combines encryption and signature; and (4) **Algorithm** 4 implements decryption and authentication.

The communication procedure for doctor *Victor* to get the patient's data from the BAN controller is sketched as follows:

1) The Key Server *KS* publishes the PubParams computed from **Algorithm** 1, and then executes **Algorithm** 2 to obtain doctor *Victor*'s private key $K_{Id_V} = (g_2^{qV(i)} T(i)^{r_V}, g^{-r_V})$ and the Controller's private key $K_{Id_{Ctr}} = (g_2^{qCtr(i)} T(i)^{r_{Ctr}}, g^{-r_{Ctr}})$.
2) The controller signcrypts the message M according to **Algorithm** 3, and then sends the ciphertext E to doctor

Algorithm 3 Signcryption – run by the controller *Ctr*

1) Signs the message M represented as a bit string $M = (\mu_1, ..., \mu_m)$ for the doctor possessing the set of attributes defined by Id';
2) Selects $r_1, r_2, ..., r_m \in \mathbb{Z}_p$;
3) Computes $t = \sum_{i=1}^{m} r_i$ and $E_1 = M \cdot U^t$;
4) Computes $E_2 = g^{-t}$;
5) Computes $E_3 = \{T(i)^t\}$;
6) Computes $\widetilde{M} = H(M||tt)$, where tt is the current time;
7) Computes $S_1 = g_2^{q_{Ctr}(i)} T(i)^{r_{Ctr}} \cdot (\nu' \prod_{j=1}^{m} \nu_j^{\mu_j} \widetilde{M})^t$;
8) Computes $S_2 = g^{-r_{Ctr}}$.
9) The ciphertext is the concatenation of E_1, E_2, E_3, S_1, S_2, tt, and Id':

$$E = (E_1, E_2, E_3, S_1, S_2, tt, Id') \tag{9}$$

Victor.

3) Upon receiving the ciphertext E, doctor *Victor* executes **Algorithm** 4. It first checks the current time $\overline{tt}$. If $|\overline{tt} - tt| \leq \delta$, *Victor* decrypts the message and verifies the signature; otherwise, he asks the controller to resend the message as the previous one is not fresh enough.

Algorithm 4 Designcryption – run by doctor *Victor*

1) Upon receiving Message E, the receiver doctor *Victor* possessing Id_V checks the current time $\overline{tt}$;
2) If $|\overline{tt} - tt| \leq \delta$, *Victor*
computes $S = Id' \cap Id_V$;
decrypts the ciphertext using his secret key $(g_2^{q_V(i)} T(i)^{r_V}, g^{-r_V})$:

$$M' = E_1 \prod_{i \in S} \left(\frac{e(d_V, E_3)}{e(D_V, E_2)}\right)^{\triangle_{i,S}(0)} \tag{10}$$

computes $\widetilde{M'} = H(M'||tt)$;
checks whether the following equation holds:

$$\prod_{i \in S} (e(S_1, g) \cdot e(S_2, T(i)) \cdot e(E_2, \nu' \prod_{j=1}^{m} \nu_j^{\mu_j} \widetilde{M'}))^{\triangle_{i,S}(0)} = U \tag{11}$$

If yes, M' is *valid*: $M = M'$; otherwise, M' is *invalid*.

3) else asks the controller to resend the message.

V. Analysis of the Proposed Scheme

In this section, we prove the correctness of the scheme, analyze its security from the aspects of collusion resistance, confidentiality, authenticity, and unforgeability, and then evaluate its performance in terms of energy consumption and communication/computation overhead.

A. The Correctness of the Proposed Scheme

In this subsection, we show that our proposed scheme is indeed feasible and correct.

Theorem 1: **Algorithm** 4 can correctly decrypt the ciphertext E if $|\overline{tt} - tt| \leq \delta$ and $|Id \bigcap Id'| \geq d$ hold.

Proof: The secret key of *Victor* is $(g_2^{q_V(i)} T(i)^{r_V}, g^{-r_V})$ according to **Algorithm** 2. Then the decryption procedure can be shown as follows when $|\overline{tt} - tt| \leq \delta$ and $|Id \bigcap Id'| \geq d$ hold:

$$\begin{aligned}
M' &= E_1 \prod_{i \in S} \left(\frac{e(d_V, E_3)}{e(D_V, E_2)}\right)^{\triangle_{i,S}(0)} \\
&= Me(g_1, g_2)^t \prod_{i \in S} \left(\frac{e(g^{-r_V}, T(i)^t)}{e(g_2^{q(i)} T(i)^{r_V}, g^{-t})}\right)^{\triangle_{i,S}(0)} \\
&= Me(g_1, g_2)^t \prod_{i \in S} \left(\frac{e(g^{-r_V}, T(i))^t}{e(g_2^{q(i)}, g^{-t}) e(T(i)^{r_V}, g^{-t})}\right)^{\triangle_{i,S}(0)} \\
&= Me(g, g_2)^{yt} \prod_{i \in S} \frac{1}{e(g^t, g_2)^{q(i)\triangle_{i,S}(0)}} \\
&= \frac{Me(g, g_2)^{yt}}{e(g, g_2)^{t\sum_{i \in S} q(i)\triangle_{i,S}(0)}} = M
\end{aligned}$$

This completes the proof. ∎

Theorem 2: **Algorithm** 4 can verify whether the received message has been forged or falsified according to **Equation** (11).

Proof: If the message is not forged or falsified, **Equation** (11) should be established as follows:

$$\begin{aligned}
&\prod_{i \in S} (e(S_1, g) \cdot e(S_2, T(i)) \cdot e(E_2, \nu' \prod_{j=1}^{m} \nu_j^{\mu_j} \widetilde{M'}))^{\triangle_{i,S}(0)} \\
&= \prod_{i \in S} (e(g_2^{q_{Ctr}(i)} T(i)^{r_{Ctr}} \cdot (\nu' \prod_{j=1}^{m} \nu_j^{\mu_j} \widetilde{M'}_j)^t, g) \cdot e(g^{-r_{Ctr}}, \\
&T(i)) \cdot e(g^{-t}, \nu' \prod_{j=1}^{m} \nu_j^{\mu_j} \widetilde{M'}_j))^{\triangle_{i,S}(0)} \\
&= \prod_{i \in S} (e(g_2^{q_{Ctr}(i)}, g))^{\triangle_{i,S}(0)} \\
&= e(g_2, g)^{\sum_{i \in S} (q_{Ctr}(i)\triangle_{i,S}(0))} = e(g_2, g)^y = e(g_1, g_2) = U
\end{aligned}$$

where $y = \sum_{i \in S} (q_{Ctr}(i) \triangle_{i,S}(0))$ holds since the polynomial $sq(x)$ is of degree $d-1$, which can be interpolated using $d-1$ points. This completes the proof. ∎

B. Security analysis

In this subsection, we analyze the security strength of the proposed scheme by examining how it can counteract possible major attacks.

1) Collusion Attack Resistance: In FABSC, the set of attributes composes the identity. In order to provide different users with different access rights, FABSC provides an error-tolerance by only requiring a subset of the attributes (d of the attributes) for designcryption. Thus FABSC can defend against collusion attacks although the original ABE can not.

For example, assuming that neither a nurse nor a doctor possesses a sufficient number of attributes to successfully decrypt the ciphertext E alone. There are two reasons to make a successful collusion attack impossible. First, the nurse and the doctor have different error-tolerance d, because they have different rights to access the patient's data. Second, the nurse and the doctor have their private key components generated with different random polynomials $q(x)$; thus when the nurse and the doctor collude, they are still unable to combine their

private key components in any useful way. Therefore we conclude that FABSC is secure against collusion attacks.

2) Confidentiality: The confidentiality of our scheme is based on the hardness of the DBDH assumption.

Theorem 3: Suppose that an adversary *Adv* is an attacker that makes at most q_1 key queries, q_2 signcrypt queries, and q_3 designcrypt queries with advantage ϵ. Then there is an algorithm *Alg* that can solve the DBDH problem in $\mathbb{Z}_p$ with a non-negligible advantage ϵ'.

$$\epsilon' = \frac{\epsilon}{2q_1q_2q_3} \tag{12}$$

Proof: The proof is based on the approach proposed in [12] [23]. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two bilinear groups of prime order p, and g is a generator of $\mathbb{G}_1$. Let $a, b, c, z \in \mathbb{Z}_p$ be random integers. A simulator chooses a coin η from {0,1}. If $\eta = 0$, it sets $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^{abc})$; otherwise it sets $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^z)$. Then the simulator selects a random identity α, which is a *n*-element set of members in $\mathbb{Z}_p$, where $|\alpha| < d$, with d being the required minimum number of overlapping attributes in order for a legitimate user to successfully designcrypt the message.

Setup: The simulator sets the public parameters $g_1 = g^a = A$ and $g_2 = g^b = B$, picks a random n-degree polynomial $f(x)$, and then computes an n-degree polynomial $v(x)$:

$$\begin{aligned} v(x) &= -x^n, \text{ if } x \in \alpha; \\ v(x) &\neq -x^n, \text{ if } x \notin \alpha. \end{aligned}$$

Our scheme ensures that for $\forall x$, $v(x) = -x^n$ iff $x \in \alpha$.

Then, for i from 1 to $n+1$, the simulator assigns $t_i = g_2^{v(i)} g^{f(i)}$. Note that each t_i is chosen independently at random in the construction. We have $T(i) = g^{i^n + v(i)} g^{f(i)}$.

Query: *Private key queries:* The adversary *Adv* requests for a private key from the simulator. Assume that *Adv* requests a private key for the identity Id, where $|Id \cap \alpha| < d$. We first define three sets Γ, Γ', S as follows: $\Gamma = Id \cap \alpha$, Γ' is any set with $\Gamma \subseteq \Gamma' \subseteq Id$ and $|\Gamma'| = d-1$, and $S = \Gamma' \cup \{0\}$.

Then we define the decryption key components D_i and d_i for $i \in \Gamma'$ as follows: $D_i = g_2^{\lambda_i} T(i)^{r_i}$ and $d_i = g^{r_i}$, where r_i and λ_i are selected randomly from $\mathbb{Z}_p$.

We implicitly choose a $d-1$ degree polynomial $q(x)$ by randomly picking the values for the $d-1$ points from Γ, and setting $q(i) = \lambda_i$ in addition to having $q(0) = a$.

The simulator needs to obtain the decryption key for $i \in Id - \Gamma'$. The key components are computed as follows:

$$D_i = (\prod_{j \in \Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_1^{\frac{-f(i)}{i^n + v(i)}} (g_2^{i^n + v(i)} g^{f(i)})^{r'_i})^{\Delta_{0,S}(i)} \tag{13}$$

and

$$d_i = (g_1^{\frac{-1}{i^n + v(i)}} g^{r'_i})^{\Delta_{0,S}(i)} \tag{14}$$

Let $r_i = (r'_i - \frac{a}{i^n + v(i)})^{\Delta_{0,S}(i)}$. We have:

$$\begin{aligned} D_i &= (\prod_{j \in \Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_1^{\frac{-f(i)}{i^n + v(i)}} (g_2^{i^n + v(i)} g^{f(i)})^{r'_i})^{\Delta_{0,S}(i)} \\ &= (\prod_{j \in \Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)}) g_2^{a \Delta_{0,S}(i)} (T(i))^{r_i} = g_2^{q(i)} T(i)^{r_i} \end{aligned}$$

In addition, we have:

$$d_i = (g_1^{\frac{-1}{i^n + v(i)}} g^{r'_i})^{\Delta_{0,S}(i)} = (g^{r'_i - \frac{a}{i^n + v(i)}})^{\Delta_{0,S}(i)} = g^{r_i}.$$

Thus the simulator can construct a private key for the identity Id. Furthermore, this private key is identical to that in the original scheme, as the choices of λ_i induce a random $d-1$ degree polynomial and the private key components d_i and D_i.

Signcryption queries: At any time, the adversary can perform a signcryption query for a plaintext. The simulator runs **Algorithm** 3 to answer the adversary's query.

Designcryption queries: At any time, the adversary can perform a designcryption query for a ciphertext. The simulator runs **Algorithm** 4 to answer the adversary's query.

Challenge: The adversary *Adv* provides two challenge messages m_1 and m_0 with the same length to the simulator: $m_1 = (\mu_1, ..., \mu_l)$ and $m_0 = (\mu'_1, ..., \mu'_l)$. The simulator selects a coin ϑ and returns the encryption of m_ϑ. The ciphertext output is denoted by:

$$E = (\alpha, E_1 = m_\vartheta Z, E_2 = C, E_3 = C^{f(i)}).$$

If $\eta = 0$, then $Z = e(g,g)^{abc}$. Thus the ciphertext is $E = (\alpha, E_1 = m_\vartheta e(g,g)^{abc}, E_2 = g^c, E_3 = (g^c)^{f(i)} = T(i)^c)$. This indicates that the ciphertext is valid for the message m_ϑ under the identity α. If $\eta = 1$, then $Z = e(g,g)^z$ and $E_1 = m_\vartheta e(g,g)^z$. Because z is picked randomly, E_1 is a random element of $\mathbb{G}_2$ from the view of the Adv and thus the message does not release any information about m_ϑ to Adv.

Guess: The adversary Adv submits ϑ'. If $\vartheta' = \vartheta$, the simulator outputs $\eta' = 0$, which indicates that it receives a BDH-tuple from Adv; otherwise it outputs $\eta' = 1$, which indicates that it receives a random 4-tuple from Adv.

There are q_1 key queries, q_2 signcrypt queries, and q_3 designcrypt queries with advantage ϵ. According to the analysis in [12], when $\eta = 1$, the adversary obtains no information about ϑ. So we have $Pr[\vartheta \neq \vartheta' | \eta = 1] = \frac{1}{2q_1q_2q_3}$. Since the simulator guesses $\eta' = 1$ when $\vartheta \neq \vartheta'$, we have $Pr[\eta = \eta' | \eta = 1] = \frac{1}{2q_1q_2q_3}$.

If $\eta = 0$, then the adversary gets a signcryption of m_ϑ. The advantage in this situation is ϵ by definition. Thus we have $Pr[\vartheta = \vartheta' | \eta = 0] = \frac{1}{2q_1q_2q_3} + \frac{\epsilon}{q_1q_2q_3}$. Since the simulator guesses $\eta' = 0$ when $\vartheta = \vartheta'$, we have $Pr[\eta = \eta' | \eta = 0] = \frac{1}{2q_1q_2q_3} + \frac{\epsilon}{q_1q_2q_3}$.

Therefore we could estimate the advantage of the adversary solving the DBDH problem by $Pr_{Alg}[Adv] = \frac{1}{2} Pr[\eta = \eta' | \eta = 0] + \frac{1}{2} Pr[\eta = \eta' | \eta = 1] - \frac{1}{2q_1q_2q_3} = \frac{1}{2}(\frac{1}{2q_1q_2q_3} + \frac{\epsilon}{q_1q_2q_3}) + \frac{1}{2} \times \frac{1}{2q_1q_2q_3} - \frac{1}{2q_1q_2q_3} = \frac{\epsilon}{2q_1q_2q_3}$. Because of the hardness of solving the DBDH problem, our scheme possesses confidentiality. ■

3) Authentication: Assume that doctor *Victor* wants to get a message M from the BAN controller. First, *Victor* should get his private key $K_{Id_V} = (g_2^{q_V(i)} T(i)^{r_V}, g^{-r_V})$ according to **Algorithm** 2. Second, the BAN controller generates the ciphertext $E = (E_1, E_2, E_3, S_1, S_2, tt, Id')$ on the message by **Algorithm** 3, where tt is the current time of the BAN controller. Third, when the doctor gets the ciphertext, he checks whether or not the message is fresh by verifying $|\overline{tt} - tt| \leq \delta$. If the verification succeeds, he can decrypt and verify the ciphertext according to **Algorithm** 4. If **Equation**

TABLE II
THE COMPUTATION COST OF DIFFERENT FUNCTIONS AND OPERATIONS IN FABSC

Operations	**Algorithm** 2	**Algorithm** 3	**Algorithm** 4
Exponent computation	6n	2m+5	1
e evaluation	0	0	5
Hash	0	1	1
Multiplication	2n	3	2d+3
Addition	0	m	0

(11) is established, the message *M* is valid; otherwise, the message is discarded and not be replayed.

4) Unforgeability: The adversary who wishes to forge the ciphertext of the BAN controller must have the BAN controller's private key. However, the adversary cannot infer the private key $K_{Id_{Ctr}} = (g_2^{q_{Ctr}(i)} T(i)^{r_{Ctr}}, g^{-r_{Ctr}})$ because $q_{Ctr}(i)$ and r_{Ctr} are chosen randomly. On the other hand, the adversary cannot create a new, valid ciphertext from other user's ciphertexts. Even if the adversary changes the ciphertext of the message, the receiver can still verify that the ciphertext is illegal by **Algorithm** 4. For the case of the adversary colluding with other users to forge the ciphertext, it cannot succeed according to the above security analysis on defending collusion attacks. Thus we claim that our proposed scheme is unforgeable under chosen message attacks.

C. Performance analysis

In this subsection, we present a quantitative performance study. Our main concern is the energy consumption spent on message computation and transmission. Since the message size is directly related to the energy consumption on message transmissions, we start from analyzing the message size.

1) Efficiency: The major contributors to the computation cost of FABSC come from **Algorithm** 2, **Algorithm** 3, and **Algorithm** 4. Let n be the number of elements in $\mathbb{G}_1$, m be the bit string in the message M, and d be the error tolerance. The computation costs of the involved functions and operations are shown in Table II.

2) Message Size: In our proposed scheme, the total message size of a ciphertext can be computed as follows according to **Equation** (9):

$$|E_1| + |E_2| + |E_3| + |S_1| + |S_2| + |tt| + |Id_i'| \qquad (15)$$

For a typical BAN, it is sufficient for Id_i' to be 2-byte for each user. so is each time stamp tt. The size of the parameters in **Equation** (15) is variable. In our evaluation, the bilinear e employs the Tate pairing. The elliptic curve is defined over $\mathbb{F}_p$. The order q of $\mathbb{G}_1$ and $\mathbb{G}_2$ is a 20-byte prime. In order to deliver a level of security equivalent to that of 1024-bit RSA, p should be a 64-byte prime if $\mathbb{G}_2$ is a q-order subgroup of the multiplicative group of the finite field $\mathbb{F}^*_{p^2}$. In the following analysis, we set p to be 42.5 bytes in length for the finite field $\mathbb{F}^*_{p^3}$, and 20 bytes in length for the finite field $\mathbb{F}^*_{p^6}$. Therefore, the total message size according to **Equation** (15) is $4 + 5|p|$ bytes, ranging from 104 to 324 bytes.

Fig. 3 demonstrates the relationship between the total message size and the number of users at different security levels. The curves in Fig. 3 indicate that the message size is independent of the number of users. Fig. 4 shows the functional relationship between the message size and the security level. From Fig. 4, we observe that the message size has a linear relationship with the security level.

TABLE III
ENERGY CONSUMPTION ON COMMUNICATIONS

The schemes	Energy consumption (mJ)
FABSC scheme, $\|p\| = 20$ bytes	$9.13W$
FABSC scheme, $\|p\| = 42.5$ bytes	$19.01W$
FABSC scheme, $\|p\| = 64$ bytes	$28.45W$
* Certificate-based scheme $N = 512$	$146.99W$
* Merkle hash tree scheme $N = 512$	$144.56W$
* ID-based scheme $N = 512$	$111.02W$

Note: The certificate-based scheme, Merkle hash tree based scheme, and ID-based scheme are all proposed in [24].
* The computation is based on the assumption that each sensor has about 20 neighbors.
* The number of users is W.

3) Communication Overhead: From communication aspect, signcryption is the main contributor to the communication overhead, i.e., the communication overhead is mainly associated with the message size of signcryption. The overhead in terms of p is $5|p| + 4$ for signcryption and 1 for designcryption. Fig. 5 illustrates the relationship between the communication overhead and the security level. We notice that the communication overhead is increasing along with the security level.

4) Energy Consumption on Communications: In this subsection, we evaluate the energy consumption of Sincryption in FABSC by employing the method proposed in [24]. As shown in [25], a Chipcon CC1000 radio used in Crossbow MICA2DOT motes consumes 28.6 μJ and 59.2 μJ to respectively receive and transmit one byte. For our FABSC scheme, the total message size is $5|p|+4$ bytes, leading to a total energy consumption (on both transmitting and receiving messages) of $(5|p|+4)*(28.6+59.2)\mu J = (0.439|p|+0.3512)\ mJ$ for one user. When there are W users, the total energy consumption on communications is $(W * (0.439|p| + 0.3512))mJ$. We report the comparison results between FABSC and the baseline approaches proposed in [24] on energy consumption in Table III. Note that to evaluate the energy consumptions of the baseline approaches that make use of broadcast, we adopt the model in [24].

Fig. 6 illustrates the energy consumption on communications as a function of the number of users. One can see from the figure that FABSC consumes significantly lower energy than the Merkle hash tree based scheme, the Certificate-based scheme, and the ID-based scheme [24].

5) Computation Cost: We now consider the computation overhead of FABSC, specifically on a 32-bit Intel PXA255 processor running at 400 MHz. According to [26], it takes approximately 752 ms to compute the Tate pairing (as used in our approach) on a 32-bit ST22 smartcard microprocessor running at 33 MHz. Correspondingly, the computation of Tate pairing on PXA255 takes about $33/400 \times 752 \approx 62.04$ ms. Using the same estimation method, we can estimate that it takes 18.48 ms to verify the ECDSA-160 signature according to the analysis in [24]. Note that we omit the negligible computation overhead of hash operations.

We assume that there are W number of users. In the certificate-based scheme [24], the computation cost is mainly

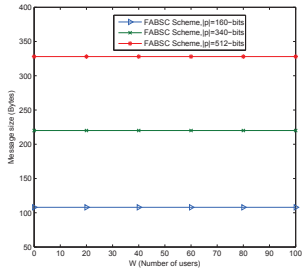


Fig. 3. Message size *vs.* the number of users.

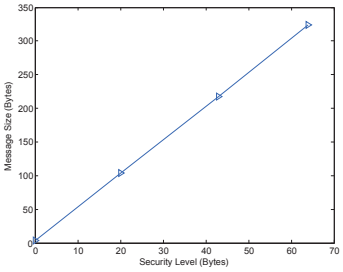


Fig. 4. Message size *vs.* the security level.

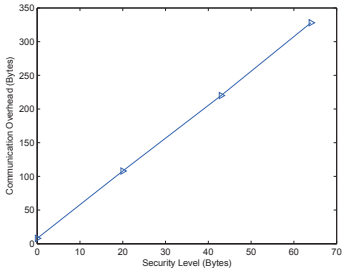


Fig. 5. The communication overhead *vs.* the security level.

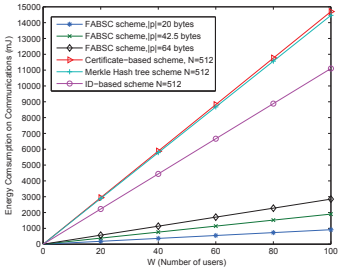


Fig. 6. Energy consumption on communications with regard to the number of users.

TABLE IV
COMPUTATION COST WITH REGARD TO THE NUMBER OF USERS

The schemes	computation cost (ms)
* Certificate-based scheme $N = 512$	$36.96W$
* Merkle hash tree scheme $N = 512$	$18.48W$
* ID-based scheme $N = 512$	$124.08W$
FABSC scheme, $\|p\| = 64$ bytes	$310.2W$

Note: The certificate-based scheme, the Merkle hash tree based scheme, and the ID-based scheme are proposed in [24].

* The number of users is W.

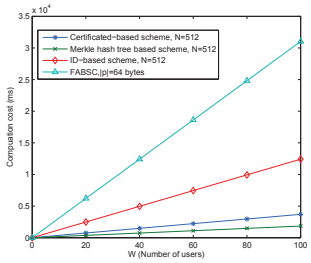


Fig. 7. Computation cost *vs.* the number of users.

incurred by the verification of two ECDSA signatures. Thus, the total computation cost is $2{*}18.48W = 36.96W$ ms. In the Merkle hash tree based scheme, the computation cost is mainly incurred by the verification of one ECDSA signature (i.e., $18.48W$ ms). In the ID-based scheme, the computation cost is mainly incurred by the two Tate pairings, with a total computation cost of $2 * 62.04W = 124.08W$ ms. In our FABSC scheme, the computation cost is mainly resulted from the five Tate Pairings, with a total cost of $5 * 62.04W = 310.2W$ ms. We summarize the results of the energy consumption for FABSC and other schemes in Table IV.

Fig. 7 depicts the computation cost of FABSC and the other schemes. One can make the following observations from the figure: First, FABSC has a higher computation cost than other schemes. Nonetheless, when we consider the (energy) consumption incurred by both computation and communication, FABSC is still relatively efficient when W is large. Moreover, syncryption is an emerging technique, which is under rapid development. Thus one can expect that the computation cost of FABSC can decrease significantly in the future. Finally, since the BAN controller is supposed to have a high computation capacity, FABSC can be best used to secure communications between the controller and external devices.

D. Limitation of the Proposed Scheme

FABSC has the following limitations:

- The computation cost of FABSC is higher than other schemes in our comparison, leading to potential efficiency concerns. Nonetheless, it is important to note that when both computation and communication costs are taken into consideration, FABSC is more desirable.
- While FABSC ensures security for communications between the controller and external devices, the security of the controller itself (from software security perspective) still needs to be properly maintained by other techniques.

In our future work, we shall design more efficient signcryption schemes to further reduce computation and storage costs and better meet the design requirements of BANs. We also plan to design efficient signcryption schemes for ensuring the security of the controller itself based on attribute-based encryption, and a lightweight signcryption scheme to secure the inter-sensor communications within a BAN.

VI. RELATED WORK

In this section, we summarize the most relevant existing research along three lines: (1) securing individual (implantable) devices within a BAN; (2) securing the communications within a BAN; and (3) identity-based cryptography for BANs. To the best of our knowledge, no prior work investigated the security of communications between a BAN and its external users.

Individual BAN devices: Halperin *et al.* [9] analyzed the security and privacy properties of commercially available ICDs. They identified a number of radio-based attacks that could compromise the safety and privacy of a patient. Other studies also discussed potential security and privacy risks of Implantable Medical Decives (IMDs) [27] [28]. The existing research in this category is orthogonal to our work presented in this paper, as we focus on securing BAN communications.

Within a BAN: Most existing work in this category focused on securing the transmissions between an implantable device and a BAN controller, which can be a mobile phone carried by the patient. There have been extensive research on leveraging a unique feature of BAN - i.e., its ability to detect/measure vital signs such as inter-pulse-intervals (IPIs) - to establish secret keys and thereby enable secure communications within a BAN [10], [11], [29]–[32]. In particular, since the IPI reading of a patient is measurable and fairly consistent over different places of the body, and generally differs substantially from other patients, most existing work assumed that IPI can be retrieved by all body sensors and used as a unique

random number generator for cryptographic schemes (after a de-noising procedure such as [33]).

Nonetheless, our studies indicate that this type of vital-sign-based techniques may not suffice for the security requirement of BANs, specifically for the following reasons:

- It has been shown recently [34] that a patient's IPI information may be remotely captured by an ultra-wide-band (UWB) radar device. This leads to a significant security threat as an adversary with a UWB radar can first capture the IPI and then use it to compromise the patient's health information.
- While IPI can be measured over various places of a human body, there are still many devices in a BAN that cannot reliably capture IPI information. Examples include motion sensors placed in shoes, cameras attached to eyeglasses, etc.

There also exists extensive research on *in-situ key establishment* [35]–[37] and *key redistribution* [38], [39]. They were proposed for general sensor networks and could be applicable to BANs to secure the inter-device communications.

Identity-based cryptography: With identity-based cryptography, the public key of each user can be easily computed from a string corresponding to the user's identity. Since this eliminates the cost of certificate distribution, identity-based cryptography is especially suitable for BANs.

Tan *et al.* [40] proposed an identity-based encryption scheme for BANs. Nonetheless, it lacks the access control feature which we develop in the paper. Yu *et al.* [41] developed a distributed fine-grained access-control mechanism for wireless sensor networks. But it does not provide message authentication - another important requirement of BAN security.

While identity-based cryptography [24], [42]–[44] has been used to provide message authentication before, the application of them to BANs may not be practical for implantable devices due to their extremely limited computation/communication capacity and battery power. In contrast, we develop a signcryption scheme in this paper which has significantly lower communication overhead and power consumption.

VII. Conclusion and Future Work

In this paper, we present an efficient fuzzy attribute based signcryption approach which is a one-to-many encryption and signature method. In other words, the signcryption message is meant to be read by a group of users that satisfy certain access control rules in the BAN. We first analyze the characteristic of BANs, and then describe our signcryption algorithm and prove its security.

Our future research lies in the following two directions. First, we intend to design secure attribute-based signcryption, which has less computation and storage requirements, and could be better suitable for practical situations; second, we will design strong access control structures, which can be associated with attributes.

Acknowledgement

The authors would like to thank all the reviewers for their helpful comments. This project was supported in part by US National Science Foundation grants: CNS-1017662, CNS-0963957, CNS-1117297, and CCF-0852674, and in part by the National Natural Science Foundation of China under Grant 60973114 and Grant 61170249.

References

[1] R. Schmidt, T. Norgall, J. Mörsdorf, J. Bernhard, and T. von der Grün, "Body area network (BAN)-a key infrastructure element for patient-centered medical applications," *Biomedizinische Technik/Biomedical Engineering*, vol. 47, no. s1a, 2002.

[2] L. Schwiebert, S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors," in *MobiCom*, 2001.

[3] J. Penders, J. vande Molengraft, L. Brown, B. Grundlehner, B. Gyselinckx, and C. V. Hoof, "Potential and challenges of body area networks for personal health," in *EMBC*, 2009.

[4] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Medical Syst.*, vol. 36, 2012.

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

[6] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A review on body area networks security for healthcare," *ISRN Commun. Netw.*, vol. 2011, no. 21, 2011.

[7] Y. Ren, R. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," *TWC*, vol. 17, no. 1, 2010.

[8] W. Cheng, D. Wu, X. Cheng, and D. Chen, "Routing for information leakage reduction in multi-channel multi-hop ad-hoc social networks," in *WASA*, 2012.

[9] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *S&P*, 2008.

[10] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "EKG-based key agreement in body sensor networks," in *INFOCOM Workshops*, 2008.

[11] ——, "PSKA: Usable and secure key agreement scheme for body area networks," *TITB*, vol. 14, no. 1, 2010.

[12] A. Sahai. and B. Waters, "Fuzzy identity-based encryption," in *EUROCRYPT*, 2005.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *CCS*, 2006.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *S&P*, 2007, pp. 321–334.

[15] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *INFOCOM*, 2007.

[16] K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in *INFOCOM*, 2010.

[17] K. Xing, F. Liu, X. Cheng, and D. H.-C. Du, "Realtime detection of clone attacks in wireless sensor networks," in *ICDCS*, 2008.

[18] A. Shamir, "How to share a secret," *Comm. ACM 22(11)*, 1979.

[19] C. Hu, X. Liao, and X. Cheng, "Verifiable multi-secret sharing based on lrsr sequences," *Theoretical Comput. Science*, vol. 445, 2012.

[20] M. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," *Comput. Standards Interfaces*, vol. 30, no. 3, 2008.

[21] C. Hu, X. Liao, and D. Xiao, "Secret image sharing based on chaotic map and chinese remainder theorem," *International J. Wavelets, Multiresolution Inf. Process.*, vol. 10, no. 03, 2012.

[22] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, 2003.

[23] B. Waters, "Efficient identity-based encryption without random oracles," in *EUROCRYPT*, 2005.

[24] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," *TWC*, vol. 6, no. 11, 2007.

[25] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *PerCom*, 2005.

[26] G. Bertoni, L. Chen, P. Fragneto, K. Harrison, and G. Pelosi, "Computing tate pairing on smartcards," [Online]. Available: http://www.st.com/stonline/products/families/smartcard/ches2005v4.pdf, 2005.

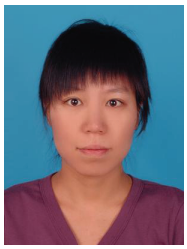
[27] W. Maisel, M. Moynahan, B. Zuckerman, T. Gross, O. Tovar, D. Tillman, and D. Schultz, "Pacemaker and icd generator malfunctions," *JAMA*, vol. 295, no. 16, 2006.

[28] D. Halperin, T. Kohno, T. Heydt-Benjamin, K. Fu, and W. Maisel, "Security and privacy for implantable medical devices," *Pervasive Comput., IEEE*, vol. 7, no. 1, 2008.

[29] C. Poon, Y. Zhang, and S. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, 2006.
[30] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *ICPP*, 2003.
[31] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Military Commun. Conf.*, 2008.
[32] 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 *INFOCOM*, 2013.
[33] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *CCS*, 1999.
[34] H. B. Lim, D. Baumann, and E.-P. Li, "A human body model for efficient numerical characterization of uwb signal propagation in wireless body area networks." *IEEE Trans. Biomedical Eng.*, vol. 58, no. 3, 2011.
[35] L. Ma, X. Cheng, F. Liu, F. An, and M. Rivera, "iPAK: An in-situ pairwise key bootstrapping scheme for wireless sensor networks," *IEEE Trans. Parallel Distributed Syst.*, vol. 18, no. 8, 2007.
[36] F. Liu and X. Cheng, "LKE: A self-configuring scheme for location-aware key establishment in wireless sensor networks," *TWC*, vol. 7, no. 1, 2008.
[37] F. Liu, X. Cheng, L. Ma, and K. Xing, "SBK: A self-configuring framework for bootstrapping keys in sensor networks," *TMC*, vol. 7, no. 7, 2008.
[38] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *CCS*, 2002.
[39] W. Du, J. Deng, Y. Han, and P. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *CCS*, 2003.
[40] C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: An identity-based cryptography approach," in *WiSec*, 2008.
[41] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," in *INFOCOM*, 2009.
[42] J. Li, D. Wei, and H. Kou, "Secure monitoring scheme based on identity-based threshold signcryption for wireless sensor networks," in *WiCOM*, 2008.
[43] J. Liu, J. Baek, J. Zhou, Y. Yang, and J. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International J. Inf. Security*, vol. 9, 2010.
[44] I. Kim and S. Hwang, "An efficient identity-based broadcast signcryption scheme for wireless sensor networks," in *ISWPC*, 2011.

Chunqiang Hu received his B.S. degree in Computer Science from Southwest University, Chongqing, China, in 2006; and M.S. degree in Computer Science from Chongqing University, Chongqing, China, in 2009. He is a PhD candidate in Computer Science at Chongqing University, Chongqing, China; and is a visiting scholar at The George Washington University. His research interests include Wireless and Mobile Security, Secret Sharing, and Cryptography.

Nan Zhang received the B.S. degree in computer science from Peking University in 2001 and the PhD degree in computer science from Texas A&M University in 2006. He is an Associate Professor of computer science at The George Washington University. His current research interests include databases and information security/privacy. Nan Zhang received the NSF CAREER Award in 2008. He is a member of the IEEE.



Hongjuan Li received her B.S. degree in Computer Science from Dalian Jiaotong University, Dalian, China, in 2008; and M.S. degree in Computer Science and Technology from Dalian University of Technology, Dalian, China, in 2011. She is currently pursuing her PhD. degree in Computer Science at Dalian University of Technology, Dalian, China, and is a visiting scholar at The George Washington University. Her research interests include Cognitive Radio Networks, Ad Hoc and Sensor Networks, Wireless and Mobile Security, Algorithm Design and Analysis.

Xiuzhen Cheng received the M.S. and Ph.D. degrees in computer science from the University of Minnesota, Twin Cities, Minneapolis, in 2000 and 2002, respectively. She is an Associate Professor with the Department of Computer Science, The George Washington University, Washington, DC. She worked as a Program Director for the US National Science Foundation (NSF) for six months in 2006 and joined the NSF again as a part-time Program Director in April 2008. Her current research interests include Wireless and Mobile Computing, Mobile Health and Safety; Wireless and Mobile Security, Cognitive Radio Networking, and Algorithm Design and Analysis. Dr. Cheng received the NSF CAREER Award in 2004. She is a Senior Member of the IEEE.

Xiaofeng Liao received the B.S. and M.S. degrees in mathematics from Sichuan University, Chengdu, China, in 1986 and 1992, respectively, and the PhD degree in circuits and systems from the University of Electronic Science and Technology of China in 1997. From 1999 to 2001, he was involved in post-doctoral research at Chongqing University, where he is currently a professor. From November 1997 to April 1998, he was a research associate at the Chinese University of Hong Kong. From October 1999 to October 2000, he was a research associate at the City University of Hong Kong. From March 2001 to June 2001 and March 2002 to June 2002, he was a senior research associate at the City University of Hong Kong. From March 2006 to April 2007, he was a research fellow at the City University of Hong Kong. He has published more than 150 international journal and conference papers. His current research interests include Neural Networks, Nonlinear Dynamical Systems, Bifurcation and Chaos, and Cryptography. He is a Senior Member of IEEE.