Flexible and Efficient Authenticated Key Agreement Scheme for BANs Based on Physiological Features

Wenjuan Tang, *Student Member, IEEE,* Kuan Zhang, *Member, IEEE,* Ju Ren, *Member, IEEE,* Yaoxue Zhang, *Senior Member, IEEE,* and Xuemin (Sherman) Shen *Fellow, IEEE*

Abstract—In Body Area Networks (BANs), bio-sensors can collect personal health information and cooperate with each other to provide intelligent health care services for medical users. Since personal health information is highly privacy-sensitive, the flourish of BANs still faces critical security challenges, especially secure communication between bio-sensors. In this paper, we propose a flexible and efficient authenticated key agreement scheme (PBAKA) to provide secure communication for BANs. Specifically, we employ a control unit (e.g., smart phone) to launch authentication based on physiological features collected from BANs, and integrate bilinear pairings to negotiate session keys for bio-sensors. Since physiological features can be collected from various kinds of bio-sensors in real time, PBAKA is flexible for adding new bio-sensors without pre-distributed keys. Meanwhile, PBAKA is computationally efficient by offloading authentication burden from resource-limited bio-sensors to the control unit. Security analysis demonstrates that PBAKA is provably secure under the decisional bilinear Diffie-Hellman assumption. Extensive experimental results validate efficient communication, computation and energy consumption of our scheme when compared with several existing solutions.

Index Terms—Key Agreement, Privacy, Authentication, Physiological Features, BANs, E-Healthcare

1 Introduction

Body Area Networks (BANs) are emerging with the development of e-healthcare systems, which can monitor medical users' health information and transmit it to remote health centers for intelligent healthcare services [1] [2]. A BAN is composed of one control unit (smart phone) and some bio-sensors that are integrated with wireless transceivers and constrained by limited computing resources. Bio-sensors can be worn on or implanted in human body to measure diverse physiological values (blood pressure, electrocardiogram, blood oxygen level, glucose level, activity recognitions etc.) [3], and provide intelligent treatments through the cooperation of various bio-sensors. For instance, automatic insulin pump administers insulin when receiving the health information of high-glucose level [4]. With the development of BANs, medical users can receive efficient and intelligent health care services at any time and any where.

Although BANs can benefit medical users by providing convenient healthcare monitoring services, the flourish of BANs still hinges upon how we fully understand and address the challenges faced in BANs. Especially, owning to the openness of wireless network environment and the privacy sensitiveness of personal health data, security and privacy challenges in BANs are urgent to be addressed [5]-[7]. First, malicious attackers may access the bio-sensors and transmit incorrect health information to bio-sensors, such that they can affect the treatment procedures even blackmail medical users that are equipped with bio-sensors. For instance, severe brainjacking risks in deep brain stimulation implants may happen if malicious devices access them [8]. Second, the information transmitted between bio-sensors may be tampered or disclosed, such that medical users' treatment may be affected and their lives may be in danger. For instance, the dosage of Hospiras Symbiq drug pumps can be changed when they are delivered to patients [9]. To protect the health information from being accessed, tampered, and disclosed by malicious attackers, it is imperative for BANs to be equipped with authentication and confidentiality mechanisms that can guarantee secure communication [10] - [12]. To this aim, authenticated key agreement schemes are established as the basis for secure BANs communication [13] - [15].

Key agreement schemes between bio-sensors in BANs can be implemented by pre-deployed keys [16] [17], which are required to be distributed and stored in bio-sensors by manufacturers. However, in the pre-deployed key agreement schemes, bio-sensors cannot recognize identities of other bio-sensors, and these schemes are not flexible especially when new bio-sensors are added into BANs. Meanwhile, if bio-sensors are abandoned or

- *Wenjuan Tang, Ju Ren and Yaoxue Zhang are with the College of Information Science and Engineering, Central South University, Changsha, China, 410083. E-mail: {wenjuantang, renju, zyx}@csu.edu.cn.*
- *Kuan Zhag is with the Department of Electrical and Computer Engineering, University of Neberaska-Lincoln, NE, USA T6G 1H9. E-mail: k52zhang@ualberta.ca.*
- *Xuemin (Sherman) Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, N2L 3G1. E-mail: {xshen}@bbcr.uwaterloo.ca.*
- *Dr. Ju Ren is the corresponding author of this paper.*

captured, their keys may be disclosed to adversaries, who may disrupt the key generation function even compute other bio-sensors' keys to obtain personal sensitive information [18]. Furthermore, unscrupulous businessmen can utilize the disclosed key hardware modules to fabricate bio-sensors and put them into the marketplace, which may cause critical security and privacy problems. Channel-based key agreement schemes are proposed by integrating received signal strength [19] - [22], because RSS is more stable between bio-sensors in BANs than that among sensors out of BANs. However, the channel-based schemes have limitations caused by channel interference in wireless environment. For instance, in hospitals or communities where many medical users that are equipped with BANs crowd, the channel interference in BANs can seriously impedes channel-based key agreement schemes to be applied for bio-sensors. Thus, it is necessary to design flexible authenticated key agreement schemes with the consideration of key pre-distribution and environmental interference.

Physiological-feature-based key agreement schemes [23] - [29] are promising candidate solutions since some physiological features are unique in the human body. For the cardiovascular physiological features (ECG, PPG, heart sounds, blood pressure and blood flow), they are evaluated to have intrinsic characteristics of uniqueness between different individuals to make identity recognition for bio-sensors [30] [31]. Meanwhile, the stability of cardiovascular physiological features have been assessed in [32] - [34]. As a result, physiological-feature-based authenticated key agreement schemes [35] - [37] are proposed, in which bio-sensors can extract the session keys that are hidden in physiological features. However, existing physiological-feature-based key agreement schemes introduce high authentication burden from the aspects of computation and storage, which is not applicable for resource-limited bio-sensors. Meanwhile, they can only work for dedicated bio-sensors collecting the same kind of physiological features, which is not feasible and scalable. Furthermore, they cannot guarantee both authentication rate and key strength simultaneously. The difficulty for adversaries to obtain session keys increases with physiological feature size, while the authentication rate of bio-sensors decreases at the same time [29].

In this paper, we propose a flexible and efficient authenticated key agreement scheme (PBAKA), which integrates physiological features and bilinear pairings to achieve secure communication between cardiovascular bio-sensors in BANs. First, PBAKA employs the control unit as the authentication server to make identity recognition based on cardiovascular physiological features. Then we utilize bilinear parings to negotiate determined session keys for the authenticated bio-sensors. Specifically, our contributions can be summarized as follows:

- We employ the intrinsic physiological features collected from bio-sensors as the basis for authenticated key agreement between bio-sensors. Such that PBAKA can be flexibly applied for newly-added bio-sensors, and release the pre-deployed key management burden.
- We utilize the control unit to launch authentication for various bio-sensors collecting different kinds of physiological features. Such that our scheme is computationally efficient by offloading the authentication burden from resource-limited bio-sensors to the control unit.
- We apply bilinear pairings to negotiate session keys for bio-sensors through certificates generated from physiological features. Such that PBAKA can provide deterministic security level for different physiological feature sizes. Meanwhile, we analyze PBAKA is secure under the decisional bilinear Diffie-Hellman assumption with key forward secrecy.
- We conduct extensive experiments based on ECG signals to demonstrate the performance efficiency with low computation overhead, communication overhead and energy consumption on bio-sensors when compared with some existing key agreement schemes.

The remainder of this paper is organized as follows. Section II reviews the related works on key agreement schemes in BANs and authentication based on physiological features, and Section III introduces models and goals. Then, we define the preliminaries and notations in Section IV, and provide the details of PBAKA in Section V. The security analysis and performance evaluation are presented in Section VI and VII respectively, followed by a conclusion in Section VIII.

2 Related Works

2.1 Key Agreement Schemes in BANs

The key agreement schemes based on specific characteristics of BANs can be divided into channel-based schemes and physiological-feature-based schemes.

Since wireless channel has a special characteristic: the underlying channel response between any two parties is unique and decorrelates rapidly in space, the channel provides a basis for secret information sharing [19]. In [20], Wang et al. analyzed that the communication channel between two devices worn on the same body is much more stable than that between a body-worn device and a faraway device off the body. Shi et al. [21] proposed a lightweight and fast authenticated secret key extraction scheme for intra-BANs communication based on channel signals. Revadigar et al. [22] introduced dual antennas and frequency diversity for obtaining uncorrelated channel samples to improve the entropy of key bit rate in static channel conditions.

Since bio-sensors that belong to the same BANs have a distinct advantage of measuring human body's physiological features, key agreement schemes are emerging based on the same or similar physiological features. [28] [29] proposed schemes to agree on a symmetric cryptographic key generated from overlapping of physiological features for bio-sensors that belong to the same BANs. ELPA [23] performed a secure and transparent node pairing by generating a symmetric key based on ECG signals by introducing Linear Prediction Coding (LPC)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2848644, IEEE Transactions on Mobile Computing

to hide cryptographic key. Zhao et al. [24] proposed a key negotiation scheme based on the fuzzy extractor technology and an improved linear interpolation encryption method. Rostami et al. [25] introduced a cryptographic device paring scheme to ensure access by a medical instrument in physical contact with an IMD-bearing patient based on ECG signals. Seepers et al. [26] explored von Neumann entropy extractor to increase the randomness of inter-pulse-interval (IPI) to improve key agreement accuracy. Zhou et al. [27] proposed a privacy-preserving key management scheme by exploiting blinding technique and embedding human body's symmetric structure into bloom's symmetric key mechanism with modified proactive secret sharing. The work in [13] illustrated that physiological-feature-based key agreement schemes can work in both sparse and crowded environments compared with channel-based key agreement schemes.

2.2 Authentication Based on Physiological Features

Poon et al. [38] conducted several experiments to show that Inter-Pulse-Intervals (IPI) of physiological features can be used for authentication in e-health networks. IPI is available for different kinds of bio-sensors that collect different kinds of physiological signals (e.g., ECG, PPG, heart sounds, blood pressure wave and blood flow). Meng et al. [39] studied the development of authentication techniques by using biometrics on mobile phones, and identified that physiological biometrics can provide high authentication accuracy. Nanni et al. [40] proposed a framework for biometric fusion based on a single acquisition device and multiple matching units. It demonstrated that even if a single matcher is weak, or degrades its performance in presence of hostile environmental conditions, different matchers can provide complementary information to improve the authentication accuracy. Miao et al. [41] proposed a single-window Fourier transform scheme to improve the identification performance of generated entity identifiers based on physiological features. Kang et al. [42] introduced cross correlation to make fast authentication based on ECG signals in mobile and wearable devices with low false acceptance rate and false rejection rate. [43] analyzed that the extracted ECG features from time domain and frequency domain can be used for authentication. Time domain features include IPIs, statistics, Hjorth features, Non-Stationary index, fractal dimension and high order crossings of the physiological signal.

Since severe channel interference may affect the signal strength and the accuracy of the negotiated keys [45], most of the channel-based key agreement schemes cannot be applied to mobile crowded environment, which is a significant application scenario in BANs. Existing authentication technologies based on physiological features establish strong basis for secure communication between bio-sensors, which enable the physiological-feature-based key agreement scheme a promising solution. However, existing physiological-feature-based key agreement schemes can only negotiate session keys for bio-sensors that collect the same kind of physiological features, which is not feasible for bio-sensors that collect different kinds of physiological features. In addition, existing physiological-feature-based key agreement schemes cannot provide session keys with a deterministic security level. Therefore, an authenticated key agreement scheme with high flexibility and security should be developed for BANs.

3 Models and Design Goals

3.1 Network Model

A typical BAN that equipped by medical users consists of some bio-sensors and a control unit.

Bio-sensors are resource-limited sensors that are usually worn on or implanted in the human body to measure physiological signals. They communicate with each other to provide cooperative treatment services and transmit the collected health information to the control unit for health monitoring.

The control unit is a relay server that has more powerful resources than bio-sensors in terms of storage, communication and computation. The control unit can be played by a smart phone to provide health information storage and management services. The control unit performs functions of collecting physiological signals, extracting physiological features, and authenticating the identities of bio-sensors.

3.2 Security Threats and Design Goals

- **Security Threats**

In our scheme, control unit is trusted. Bio-sensors are honest to keep their keys secret. Devices beyond one specific BAN generally cannot sense personal physiological information. Even if some devices are able to sense physiological features, they can hardly to be adversaries because if they intend to play as adversaries and obtain the negotiated keys, they should be supposed to be physically close to users, which is easy to discover for general medical users. The security threats faced by a BAN are the adversaries that can transmit incorrect health data to access the medical users or eavesdrop physiological information for health data privacy leakage. We categorize the security threats into active adversaries and passive eavesdroppers as follows. **(1)** ***Active Adversaries.*** Active adversaries may intend to control medical users through bio-senors. They may transmit incorrect health information to bio-sensors for affecting medical users' treatments. **(2)** ***Passive Eavesdroppers.*** Passive eavesdroppers may be unscrupulous vendors. They can capture the health information and use it to blackmail medical users or sell it for money from black market trade.

- **Security Goals**

(1) ***Resist Threats from Active Adversaries and Passive Eavesdroppers.*** The authenticated key agreement

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2848644, IEEE Transactions on Mobile Computing

scheme should protect the communication between bio-sensors from active adversaries and passive eavesdroppers.

(2) ***Key Correctness.*** Under the condition of there exist attackers between communicating bio-sensors, the communicating bio-sensors can negotiate the same session keys, and the keys obey uniform distribution.

(3) ***Key Unforgeability.*** Any adversaries cannot forge the negotiated keys between bio-sensors or obtain the session keys in the polynomial time.

(4) ***Key Reliability.*** The strength of the negotiated keys should be reliable and the length of the negotiated keys should be independent of the physiological feature size.

(5) ***Forward Secrecy.*** When private keys of the communicating bio-sensors and the system master key are disclosed, previous session keys between the communicating bio-sensors should still be secret.

- **Performance Goals**

PBAKA should guarantee secure communication based on various kinds of physiological signals to meet the communication requirements from different bio-sensors. Meanwhile, since bio-sensors are resource-limited, PBAKA is designed to offload the authentication burden from bio-sensors to the control unit. The storage, computation, communication, and energy consumption burden on bio-sensors should be acceptably efficient.

4 Preliminaries and Notations

In this section, we briefly introduce some preliminaries on physiological feature extraction, physiological feature matching, bilinear maps and decisional bilinear Diffie-Hellman assumption, as well as the important notations frequently used throughout the paper in Table 1.

4.1 Physiological Feature Extraction

The physiological feature extraction methods can be divided into time-domain and frequency-domain methods, and they are not totally the same for different cardiovascular physiological signals. We demonstrate ECG, PPG and PCG feature extraction in this subsection. For the ECG signal, the physiological features can be extracted from the time domain after filtering the lower frequency by fast Fourier transform. Fiducial points include R peaks, S peaks, Q peaks, P peaks, T peaks, LP valleys, TP valleys, and QRS complex can be detected from ECG signals [49]. We can compute IPIs between these fiducial points and take them as physiological features. In addition, the amplitudes of R peaks, T peaks, P peaks can also be computed as physiological features. Photoplethysmography (PPG) is to measure the volume of tissue blood. The widely used physiological features are based on local marks of heart beats from the time domain, which include systolic peak, dicrotic notch, diastolic peak, pulse interval, peak to peak, augmentation index, alternative augmentation index and a series of peak time. For the PCG signal, the physiological features can be extracted through frequency domain from the S1 tone (it has an average duration of 100ms-200ms and its spectrum is concentrated within 25Hz-45Hz) and S2 tone (it lasts for about 0.12s with a frequency less than 150Hz). First, the power spectral density of the signals is estimated with the Short Time Fourier Transform (STFT). Then, the magnitude of the spectral coefficients is passed through the Mel-frequency filter and subjected to Linear Discriminant Analysis (LDA) in order to reduce dimensionality.

4.2 Physiological Feature Matching

After feature extraction, a physiological signal can be denoted as feature vectors for matching. In physiological feature matching, two key components are threshold searching and distance computation. First, the batch process can be used to conduct the search for the threshold value T through the threshold searching. Then, we can compute the distance by using the distance functions (Euclidean distance function, Manhattan distance and Mahalabonis distance) and dynamic time warping [46]. The smaller the distance is, the more similarities the two physiological signals F and $\hat{F}$ have. Finally, we can compare the threshold and the distance. Only if the distance is smaller than the threshold, the two physiological signals are matching with each other, and we take them as the physiological signals collected from the same body.

4.3 Bilinear Maps

The bilinear pairings namely Weil pairing and Tate paring of algebraic curves are defined as a map $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$, where $\mathbb{G}_0$ is a cyclic additive group generated by g, whose order is a prime p, and $\mathbb{G}_1$ is a cyclic multiplicative group of the same order q. Bilinear pairings have the following properties:

- Bilinearity: for any $u, v \in \mathbb{G}_0$, and $a, b \in \mathbb{Z}_p$, it has $e(u^a, v^b) = e(u, v)^{ab}$;
- Non-degeneracy: $e(g, g) \neq 1$, 1 is the unit parameter in $\mathbb{G}_1$.
- Computability: for all $u, v \in \mathbb{G}_0$, there is an efficient algorithm to compute $e(u, v)$.

4.4 Decisional Bilinear Diffie-Hellman (DBDH) Assumption

A challenger chooses a group $\mathbb{G}$ of prime order p based on the security parameter of system. Let $a,\ b,\ c,\ z \in \mathbb{Z}_p$ be selected randomly and g be a generator of $\mathbb{G}$. With $(g,\ A = g^a,\ B = g^b,\ C = g^c)$, the adversary distinguish a valid tuple $e(g, g)^{abc}$ from $e(g, g)^z$.

An algorithm B that outputs a guess $\mu \in \{0, 1\}$ has the advantage ε in solving DBDH if the following formula was satisfied.

$$\left| \begin{array}{l} Pr[B(g, A, B, C, e(g, g)^{abc}) = 0] \\ -Pr[B(g, A, B, C, e(g, g)^{z}) = 0] \end{array} \right| \geq \varepsilon \qquad (1)$$

We say that DBDH assumption holds if no polynomial algorithm has a non-negligible advantage in solving the DBDH problem.

TABLE 1: Notations

Notation	Definition
ID_s	ID number of sender
ID_r	ID number of receiver
F_s	Physiological features collected by the sender
F_r	Physiological features collected by the receiver
$Cert_r$	Certificate of the receiver
$Cert_s$	Certificate of the sender
SK_s	Secret key of the sender
SK_r	Secret key of the receiver
T_s	Intermediate crypto generated by the sender
T_r	Intermediate crypto generated by the receiver
CK_{sr}	Common key computed by the sender
CK_{rs}	Common key computed by the receiver
K_{sr}	Final session key computed by the sender
K_{rs}	Final session key computed by the receiver

5 Authenticated Key Agreement Scheme

In this section, we present the detailed framework and construction of PBAKA.

5.1 PBAKA Framework

The framework of PBAKA is defined as follows.

Definition 2 (PBAKA). PBAKA consists of a collection of algorithms that combine $Setup$, $FeaGen$, $Auth$, $SKeyGen$, $TKeyTran$ and $KeyAgree$.

- $Setup$ $(1^\lambda) \rightarrow (e, \mathbb{G}_0, PK, MSK)$. The $Setup$ algorithm is run by the control unit. It takes no input other than the implicit security parameter λ. It outputs bilinear pairings e, cyclic additive group G_0, public key PK, and system master key MSK.
- $FeaGen$ $(Physiological\ Sample) \rightarrow (F)$. The $FeaGen$ algorithm is run by the control unit. It takes specific physiological signals as inputs, and outputs physiological features F.
- $Auth$ $(F, F') \rightarrow (Authsig, Cert)$. The $Auth$ algorithm is run by the control unit. It takes physiological features as inputs. It outputs $Authsig$ signal. The $Authsig$ is true if authentication successes, otherwise the $Authsig$ is false. It outputs certificates $Cert$ of authenticated bio-sensors if $Authsig$ is true.
- $SKeyGen$ $(Cert, PK, MSK) \rightarrow (SK)$. The $SKGen$ algorithm is run by the control unit. It takes certificate $Cert$ of the bio-sensor, public key PK and system master key MSK as inputs. For each authenticated bio-sensor, it generates a random number, then computes and outputs a pair of secret keys SK.
- $TKeyTran$ $(Cert, PK) \rightarrow (T)$. The $TKeyTran$ algorithm is run by bio-sensors. Each bio-sensor takes certificate $Cert$ of another bio-sensor and public key PK as inputs. It outputs a pair of intermediate keys T and transmits it to another communicating bio-sensor node.
- $KeyAgree$ $(Cert, SK, PK, T) \rightarrow (K)$. The $KeyAgree$ algorithm is run by bio-sensors. They take certificates, secret keys, public key, both intermediate crypto information of themselves and another bio-sensor as inputs. And outputs the final session key K.

5.2 Construction of PBAKA

PBAKA consists of five phases: System Initialization, Feature Extraction, Authentication, Secret Key Generation and Key Negotiation as illustrated in Fig. 1. Let e: $\mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ be a bilinear map, and $\mathbb{G}_0$ be a bilinear group of prime order p with generator g. Two hash functions H_1: $\{0,1\}^* \times Z_p \rightarrow Z_p$ and H_2: $Z_p \times Z_p \times \mathbb{G}_1 \rightarrow (0,1)^\lambda$ are used in the proposed scheme.

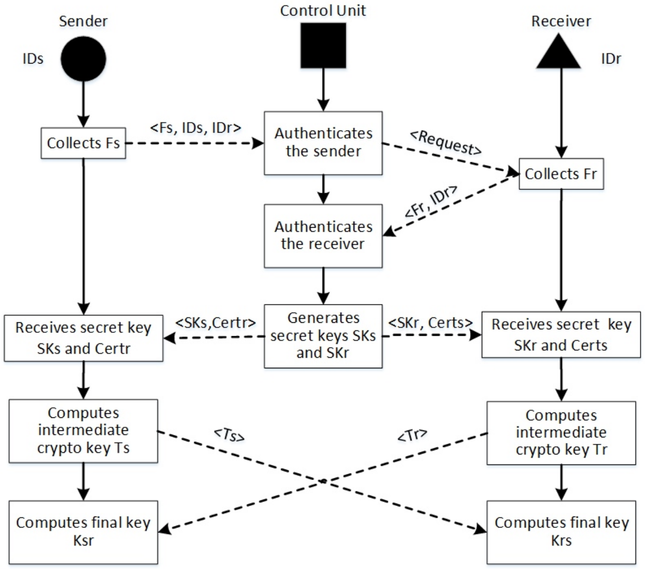
Sender
Control Unit
Receiver
IDs
IDr
Collects Fs
<Fs, IDs, IDr>
Authenticates the sender
<Request>
Collects Fr
<Fr, IDr>
Authenticates the receiver
Receives secret key SKs and Certr
<SKs,Certr>
Generates secret keys SKs and SKr
<SKr, Certs>
Receives secret key SKr and Certs
Computes intermediate crypto key Ts
<Ts>
<Tr>
Computes intermediate crypto key Tr
Computes final key Ksr
Computes final key Krs

Fig. 1: Authenticated Key Agreement Process

Phase 1: System Initialization

The control unit runs algorithm $Setup$, which takes security parameter λ as input and chooses three random numbers $a, \alpha, \beta \in Z_p$, outputs public key PK and system master key MSK.

$$PK = \{\mathbb{G}_0, g_1 = g^a, h = g_1^\beta, e\} \tag{2}$$

$$MSK = \{g_2 = g_1^\alpha, \beta\} \tag{3}$$

Phase 2: Physiological Feature Generation

The control unit runs the physiological feature generation algorithm $FeaGen$. Bio-sensors collect a few kinds of physiological signals and transmit them to the control unit. To improve the recognition rate, we can add historical physiological features collected on different places of human body and store them on the control unit, such that we have more template physiological features for matching. Before the biometric authentication, the control unit pre-processes the biometric signals to remove the noises and extract physiological features.

First, we pre-process the biometric signal from overall perspective. We analyze the noises of biometric signals, which include power-line interference, baseline wander and unpredictable band components. We address the noise reduction by Gaussian derivative filter [58], which can remove baseline wanders and eliminate high-frequency noises, meanwhile preserve the shapes of pulsatile waveforms.

We can compute the Gaussian derivative kernel as Equation (4) and (5).

$$g[m] = e^{-\frac{1}{2}\frac{(m-\frac{M}{2})^2}{\sigma^2}} \quad m = 1, 2, 3, ..., M \tag{4}$$

$$h[m] = g[m+1] - g[m] \quad m = 1, 2, 3, ..., M-1 \tag{5}$$

where M denotes the length of Gaussian kernel and σ denotes the width spread, which can be determined empirically. We can obtain the filtered signal $f[n]$ by taking the convolution of a signal $x[n]$ and Gaussian derivative kernel $h[n]$.

Second, we pre-process the biometric signal to reduce noises for different physiological features respectively. For the ECG authentication, we usually extract P wave, T wave and QRS complex as the physiological features. According to the experiments of [59], QRS complex and T wave inherit most uniqueness and are not easily affected by noises, while P wave gets easily corrupted with noises since it possesses the lowest amplitude. Specifically, we use proper precautionary measurements to remove the effects of noises and artifacts, to provide better uniqueness for P wave alone.

After the above noise reduction of biometric signal, we can extract physiological features to enroll in the biometric-based authentication. Two physiological feature templates are required: 1) enrollment feature template and 2) authentication feature template. The enrollment feature template is generated in the initiation process and the authentication feature template is generated when bio-sensors intend to communicate with other bio-sensors. Both of these two features are extracted in the same way. We take the ECG signal as the example. First, the fiducial points of ECG signal can be detected as: R peaks, S peaks, Q peaks, P peaks, T peaks, LP valleys and TP valleys. Second, the physiological feature template can be expressed by ten vectors F_i (i is from 0 to 9), and the value of each vector corresponds to the median value of the IPIs between R peaks and the other fiducial points, as well as the amplitudes of the fiducial points. For simplicity, we term the enrollment feature template $F = \{F_i\}$, where $F_i = \{f_{i1}, f_{i2}, \ldots, f_{iN}\}$, and authentication feature template $\hat{F} = \{\hat{F_i}\}$, where $\hat{F_i} = \{\hat{f_{i1}}, \hat{f_{i2}}, \ldots, \hat{f_{iN}}\}$. N is the number of the feature size, which varies upon specific physiological features.

Phase 3: Authentication

The control unit runs authentication algorithm $Auth$, which takes the enrollment feature template and authentication feature template as inputs, and outputs the certificates of the authenticated bio-sensors. We define two communicating sensors as the sender and the receiver. The control unit authenticates both of them respectively.

The sender transmits ID_s, ID_r of receiver, physiological sample F and timestamp t of the receiver to the control unit. First, the sender computes:

$$\hat{F} = MAC(ID_s||ID_r||F||t) \tag{6}$$

Where MAC is the message authentication code. Then the sender transmits $(ID_s, ID_r, F, \hat{F}, t)$ to the control unit (t is the timestamp).

After checking whether $\hat{F} = MAC(ID_s||ID_r||F||t)$, the control unit extracts the enroll feature template F_s as described above, and compares it with the authentication feature template $\hat{F_s}$ stored in the control unit. The threshold T_i of each feature vector is designed in advance, and we compare each vector respectively and compute the similarity. If the similarity between the enrollment feature template and the authentication feature template reaches to a pre-defined threshold T, the control unit takes the bio-sensor as an authenticated bio-sensor in the BAN.

The authentication process of physiological features can be detailed as Algorithm 1.

Algorithm 1 Authentication algorithm based on physiological features

```
Data: There exist two physiological feature sets $F_i$ and $\hat{F_i}$, from which the control unit intends to derive the similarity $Count$ of the two physiological features. We set $Count = 0$ in the initial state, and $T$ is the pre-defined threshold. If $Count \geq T$, control unit sets $Authsig = true$, else sets $Authsig = false$.
for $i = 0$ to $i = 9$ do
    if $Distance(F_i, \hat{F_i}) \geq T_i$ then
        $Count++$, $i++$
    else
        $i++$
    end if
end for
if $Count \geq T$ then
    Sets $Authsig = true$
else
    Sets $Authsig = false$
end if Outputs $Authsig$
```

If $Authsig = true$, the bio-sensor is an authenticated node. The control unit selects a random number $No_s \in Z_p$, and computes a certificate $Cert_s$, then sends it to the bio-sensor via secure channel based on the physiological features.

$$Cert_s = H_1(F_s, No_s) \tag{7}$$

Similarly, the control unit performs the same authentication process for the receiver as described above. The control unit selects a random number No_r and computes $Cert_r$ for the receiver.

$$Cert_r = H_1(F_r, No_r) \tag{8}$$

The control unit sends $Cert_s$ to the receiver and $Cert_r$ to the sender.

Phase 4: Secret Key Generation

The control unit runs $SKeyGen$ algorithm to generate secret keys for communicating bio-sensors. It takes certificate $Cert_r$, certificate $Cert_s$, public key g_1 and master

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2848644, IEEE Transactions on Mobile Computing

key g_2 as inputs, and outputs secret key pairs SK_s and SK_r. For the sender, the control unit selects a random number $s \in Z_p$, computes SK_s and sends it to the sender.

$$SK_s = \{SK_{s1}, SK_{s2}\} = \{g_2 \cdot h^{s \cdot Cert_s}, g_1^s\} \tag{9}$$

For the receiver, it selects a random number $r \in Z_p$, computes SK_r and sends it to the receiver.

$$SK_r = \{SK_{r1}, SK_{r2}\} = \{g_2 \cdot h^{r \cdot Cert_r}, g_1^r\} \tag{10}$$

It is important to note that secret key pairs SK_s can only be known by the sender and the control unit, and SK_r can only be known by the receiver and the control unit.

Phase 5: Key Negotiation

This phase is for key negotiation between the sender and the receiver. The sender and the receiver run $TKeyTran$ algorithm respectively. They take certificate $Cert$ of another bio-sensor, and public key g_1 as inputs, output the intermediate crypto information T_s and T_r. The sender selects a random number $x \in Z_p$, computes T_s and sends it to the receiver.

$$T_s = \{T_{s1}, T_{s2}\} = \{g_1^{x \cdot Cert_r}, g_1^x\} \tag{11}$$

Respectively, the receiver selects a random number $y \in Z_p$, computes T_r and sends it to the sender.

$$T_r = \{T_{r1}, T_{r2}\} = \{g_1^{y \cdot Cert_s}, g_1^y\} \tag{12}$$

Then the communicating bio-sensors run $KeyAgree$ algorithm to compute $K_{s,r}$. The sender and receiver take their certificates $Cert_s$ and $Cert_r$, secret key pairs SK_s and SK_r, public key g_1, intermediate crypto information T_s and T_r, as well as their selected random numbers x, y as inputs, and output the final session key.

The sender computes:

$$CK_{sr} = e(SK_{s1}, T_{r2} \cdot T_{s2}) e(SK_{s2}^{-1} \cdot h, T_{r1} \cdot g_1^{x \cdot Cert_s}) \tag{13}$$

$$K_{sr} = H_2(Cert_r, Cert_s, CK_{sr}) \tag{14}$$

The receiver computes:

$$CK_{rs} = e(SK_{r1}, T_{s2} \cdot T_{r2}) e(SK_{r2}^{-1} \cdot h, T_{s1} \cdot g_1^{y \cdot Cert_r}) \tag{15}$$

$$K_{rs} = H_2(Cert_s, Cert_r, CK_{rs}) \tag{16}$$

After above phases, authentication bio-sensors successfully negotiate session keys.

6 Security Analysis and Discussions

In this section, we first analyze that PBAKA can resist threats from active adversaries and passive eavesdroppers. Then, we prove that the negotiated session keys satisfy key correctness and key unforgeability under DBDH assumption. Followed by deterministic security level analysis compared with other two physiological-feature-based schemes and forward secrecy discussions.

6.1 Resist Threats from Active Adversaries and Passive Eavesdroppers

We use physiological features in BANs to authenticate the bio-sensors, and our scheme only allow the authenticated bio-sensors to make secure communication with each other. As a result, the active adversaries that collect irrelevant physiological information can be resisted to access the bio-sensors. Meanwhile, our scheme enables bio-sensors to negotiate symmetric session keys and encrypt information under the negotiated session keys before information is transmitted. Eavesdroppers cannot gain the session keys to decrypt the encrypted information. As a result, our scheme can resist the passive eavesdroppers.

6.2 Key Correctness

The communicating bio-sensors can negotiate the same session keys. According to the equation $(9) - (12)$, we can compute that $K_{sr} = K_{rs}$.

$$\begin{aligned} &CK_{sr} \\ &\quad = e(SK_{s1},\ T_{r2} \cdot T_{s2})\ e(SK_{s2}^{-1} \cdot h,\ T_{r1} \cdot g_1^{x \cdot Cert_s}) \\ &\quad = e(g_2 \cdot g_1^{\beta \cdot s \cdot Cert_s},\ g_1^y \cdot g_1^x)\ e(g_1^{-\beta \cdot s},\ g_1^{y \cdot Cert_s} \cdot g_1^{x \cdot Cert_s}) \\ &\quad = \Big(e(g_2 \cdot g_1^{\beta \cdot s \cdot Cert_s},\ g_1)\ e(g_1^{-\beta \cdot s},\ g_1^{Cert_s})\Big)^{x+y} \\ &\quad = \Big(e(g_2,\ g_1)\ e(g_1^{\beta \cdot s \cdot Cert_s},\ g_1)\ e(g_1^{-\beta \cdot s},\ g_1^{Cert_s})\Big)^{x+y} \\ &\quad = e(g_1,\ g_2)^{x+y} \end{aligned} \tag{17}$$

$$\begin{aligned} &CK_{rs} \\ &\quad = e(SK_{r1},\ T_{s2} \cdot T_{r2})\ e(SK_{r2}^{-1},\ T_{s1} \cdot g_1^{y \cdot Cert_r}) \\ &\quad = e(g_2 \cdot g_1^{\beta \cdot r \cdot Cert_r},\ g_1^x \cdot g_1^y)\ e(g_1^{-\beta \cdot r},\ g_1^{x \cdot Cert_r} \cdot g_1^{y \cdot Cert_r}) \\ &\quad = \Big(e(g_2 \cdot g_1^{\beta \cdot r \cdot Cert_r},\ g_1)\ e(g_1^{-\beta \cdot r},\ g_1^{Cert_r})\Big)^{x+y} \\ &\quad = \Big(e(g_2,\ g_1)\ e(g_1^{\beta \cdot r \cdot Cert_r},\ g_1)\ e(g_1^{-\beta \cdot r},\ g_1^{Cert_r})\Big)^{x+y} \\ &\quad = e(g_1,\ g_2)^{x+y} \end{aligned} \tag{18}$$

As detailed above, $CK_{sr} = CK_{rs} = e(g_1,\ g_2)^{x+y}$, and $K_{sr} = K_{rs} = H_2(Cert_s, Cert_r, e(g_1,\ g_2)^{x+y})$.

6.3 Key Unforgeability

In this subsection, we prove that no polynomial time adversary can break the proposed key agreement scheme under the DBDH assumption.

The security game is played by an adversary and a challenger in the polynomial time. The challenger makes responses upon requests from the adversary. After the game ends, the challenger chooses a random number $b = \{0, 1\}$. If $b = 0$, it outputs the correct session key; otherwise, it chooses a session key randomly within its own key space as output. The adversary obtains the output from the challenger and guesses b' from $\{0, 1\}$. If $b' = b$, the adversary wins the game. Otherwise,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2848644, IEEE Transactions on Mobile Computing

the adversary loses the game. The guess advantage of winning the game is $Adv_{\mathcal{A}_{Game}} = |pr[b' = b] - 1/2|$ ($\mathcal{A}$ represents the adversary).

If there is a polynomial time adversary $\mathcal{A}$ has a non-negligible advantage $\varepsilon = Adv_{\mathcal{A}}$ to break our scheme, then we can construct a polynomial time adversary $\mathcal{B}$ that can distinguish a DBDH tuple from a random tuple at the advantage of $\varepsilon \cdot Con$ (Con is a constant).

We construct two security games to prove key unforgeability. In the first security game, players are the DBDH challenger and the DBDH adversary $\mathcal{B}$. In the second security game, $\mathcal{B}$ is played as the challenger, and $\mathcal{A}$ is the adversary who aims to obtain the session keys in PBAKA by performing $Send$, $Corrupt$ and $Reveal$ requirements from the challenger.

Let $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ be an efficiently computable map, where $\mathbb{G}_0$ has the prime order p with the generator g. In the first security game, DBDH challenger randomly selects $\{a, b, c\} \in \mathbb{Z}_p$, $\mu \in \{0, 1\}$, generator $g \in \mathbb{G}_0$ and a random element $R \in \mathbb{G}_1$. The challenger defines T to be $e(g, g)^{abc}$ if $\mu = 0$. Otherwise, it sets $T = R$. Then, the DBDH challenger gives $< g, A, B, C, T > = < g, g^a, g^b, g^c, T >$ to $\mathcal{B}$. In the second security game, $\mathcal{B}$ is a simulator that can execute all the algorithms in PBAKA, and $\mathcal{B}$ plays as the challenger with adversary $\mathcal{A}$. We define $\prod S_{ij}$ as a session oracle, i and j represent the i_{th} and j_{th} bio-sensors respectably. The adversary $\mathcal{A}$ can make the following requirements in two phases.

Phase 1 $\mathcal{A}$ can make $Send$, $Corrupt$ and $Reveal$ requirements from $\mathcal{B}$ regardless of order.

- $Send(S_{ij}, M)$ $\mathcal{A}$ initiates a session or sends information to $\mathcal{B}$. $\mathcal{B}$ outputs information m, or outputs a signal to accept or refuse this session.
- $Corrupt(i)$ $\mathcal{A}$ desires to obtain the secret key of i_{th} node.
- $Reveal(S_{ij})$ $\mathcal{A}$ desires to acquire the session key through this requirement. If $\mathcal{B}$ accepts the session, it outputs the session key, otherwise, it outputs the end signal.

Phase 2 $\mathcal{A}$ makes the $Test(S_{ij})$ requirement. $\mathcal{B}$ chooses $\mu = \{0, 1\}$ through toss fair agreement, and sends session keys to $\mathcal{A}$. Finally, $\mathcal{A}$ outputs a guess μ' of μ.

In the polynomial time, $\mathcal{A}$ can make $Corrupt$ requirement from q_0 bio-sensors; $\mathcal{A}$ can make $Send$ requirement for q_1 times; $\mathcal{A}$ can make $Reveal$ requirement for q_2 times. $\mathcal{B}$ chooses the random number O in $(0, q_2)$ and stores it in its own system secretly. We set the $\prod O_{IJ}$ be the challenge oracle in the $Test$ requirement, O means the O_{th} oracle, I and J are the i_{th} and j_{th} bio-sensors, who intend to negotiate session keys.

$\mathcal{B}$ provides these parameters $\{e, g_1, g_2, R\}$ to the adversary $\mathcal{A}$, where $g_1 = g^a$ and $g_2 = g^b$. $\mathcal{A}$ and $\mathcal{B}$ play the security game as follows.

- Corrupt (ID_i): $\mathcal{B}$ maintains a list $L_1 = \{ID_i, r_i, Cert_i, SK_i\}$, and the initialized state is $\{null, null, null, null\}$. ID_i represents the number of the bio-sensor, r_i represents the random number chosen by the challenge oracle to compute the secret key of the bio-sensor. If the element $(ID_i, r_i, Cert_i, SK_i)$ in the list L_1 exists, $\mathcal{B}$ outputs r_i and SK_i; else, $\mathcal{B}$ generates a random number r_i and computes the secret key SK_i by running the algorithm $SKeyGen$, then resets r_i and SK_i, updates the list L_1, outputs r_i and SK_i.
- Send (S_{ij}, M): $\mathcal{B}$ maintains a list $L_2 = \{S_{ij}, r, M, M', K\}$, its initial state is $\{null, null, null, null, null\}$. S_{ij} is the requesting oracle; r is the random number to generate the intermediate crypto information; M is the reception information; M' is the generation information computed by the challenger; K is the negotiated session key.

(1) If M is the security parameter, then S_{ij} is the sender. We discuss it according to the following 2 cases:

Case 1: $S = O$. $\mathcal{B}$ runs the $TKeyTran$ algorithm and computes the intermediate crypto information T_i, $T_i = (T_{i1}, T_{i2})$, $T_{i1} = C^{Cert_j}$, $T_{i2} = C$, $M' = (T_{i1}, T_{i2}) = (C^{Cert_j}, C)$, and then updates the list $L_2 = \{S_{ij}, null, null, M', null\}$.

Case 2: $S \neq O$. $\mathcal{B}$ chooses a random number $r \in \mathbb{Z}_q$, and runs the $TKeyTran$ algorithm and computes the intermediate crypto information, then updates list L_2.

(2) If M is not the security parameter, $\mathcal{B}$ deals with this requirement according to the following 3 cases:

Case 1: There is no element record (S_{ij}, r, M, M', K) in list L_2. $\mathcal{B}$ sets S_{ij} as the session receiver, and chooses the random number r, then computes the value of M', K, and updates list L_2.

Case 2: There exists an element record $(S_{ij}, r, null, M', null)$. S_{ij} is the session sender. $\mathcal{B}$ computes M' and K by running the algorithms $TKeyTran$ and $KeyAgree$, and updates the list L_2 (S_{ij}, r, M, M', K).

Case 3: There exists an element record $\{S_{ij}, null, null, M', null\}$. S_{ij} is the member of Test assumption, that means $S = O$. If $M = (g_1^{y \cdot Cert_j}, g_1^y)$, then the challenger chooses a number z randomly from $\{0, 1\}$.

If $z = 0$, $\mathcal{B}$ computes $e(g_1, g_2)^y$, sets $SK = R \cdot e(g_1, g_2)^y$, and updates the list L_2 with an element record $\{S_{ij}, null, M, M', SK\}$.

If $z = 1$, $\mathcal{B}$ chooses a random session key in space $\{0, 1\}^\lambda$ as the negotiated session key K, and updates the list L_2 with an element record $\{S_{ij}, null, M, M', K\}$.

- Reveal (S_{ij}): If S_{ij} is the assuming Test session, i.e., $S = O$, $\mathcal{B}$ ends this game (**E1**); else, $\mathcal{B}$ searches from the list L_2 and returns the value of K.
- Test (S_{ij}): After the first phase ends, $\mathcal{A}$ makes a Test requirement. If $S \neq O$, $\mathcal{B}$ ends the game (**E2**); otherwise, $\mathcal{B}$ searches from the list L_2, and returns the relative K to $\mathcal{A}$.

Once $\mathcal{A}$ finishes the requirements, $\mathcal{A}$ outputs a guess z' of z as the guess to the session key; $\mathcal{B}$ receives z', and takes it as the guess of μ in the first DBDH security game.

Analysis:

$$\begin{aligned} if\ R &= e(g, g)^{abc} \\ &= e(g_1, g_2)^c \end{aligned} \tag{19}$$

$$then\ K = R \cdot e(g_1, g_2)^y = e(g_1, g_2)^{y+c} \tag{20}$$

K is the session key computed by the oracle.

If $\mathcal{A}$ has a non-negligible guess advantage $Adv\mathcal{A}_{Game(k)}$ to win the game, $\mathcal{A}$ can guess right about z and learn whether the session key is correct or not from the output of $\mathcal{B}$ in $Test$ phase. Then the $\mathcal{B}$ can guess right about μ and know if $R = e(g, g)^{abc}$ or not.

If none of **E1** and **E2** happens, $\mathcal{B}$ continues the game, and the game is indistinguishable to the real world. If adversary $\mathcal{A}$ can obtain the session key successfully, $\mathcal{B}$ can also solve the DBDH problem. We compute the probability:

$$\begin{aligned} Pr[B_w] &= Pr[\overline{E1} \cap \overline{E2} \cap A_w] \\ &= Pr[\overline{E1}] \cdot Pr[\overline{E2}] \cdot Pr[A_w] \\ &= (q_2 - 1)/q_2 \cdot (1/q_2) \cdot Pr[A_w] \\ &= \varepsilon \cdot (q_2 - 1)/q_2^2 \end{aligned} \tag{21}$$

Since DBDH assumption holds in polynomial time, the key agreement scheme is provably secure.

6.4 Key Reliability

Our scheme is reliable due to the fixed size of the negotiated session keys. PSKA [28] and OPFKA [29] use fuzzy vault [47] to hide physiological features among a much larger vault size of physiological features. As a result, the adversary can hardly identify the authentic physiological features from a combination of authentic and inauthentic features, and the key length is higher when the feature size increases, but the authentication rate decreases. The negotiated key size of our scheme depends on the computational hardness of the hash function. We illustrate the security comparison between PBAKA, PSKA and OPFKA as seen in Fig. 2, it is obviously observed that the key bits of PSKA and OPFKA increase along with feature size, while the key bits of PBAKA is unrelated with the feature size.

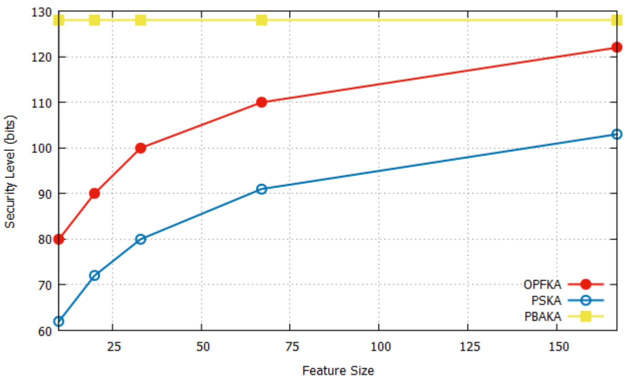

Fig. 2: Security Level of PBAKA, PSKA and OPFKA

6.5 Forward Secrecy

Our scheme can achieve forward secrecy. We introduce the control unit to distribute secret keys generated from system master key to bio-sensors. Session keys negotiated in our scheme rely on the physiological features and the random numbers selected by bio-sensors. If the system master key and secret keys of the bio-sensors are disclosed, session keys in the previous communication between bio-sensors cannot be deduced. The session keys negotiated in our scheme are unique since they depend on random numbers selected by communicating bio-sensors. In other physiological-feature-based key agreement schemes, since session keys only rely on physiological features, non-communicating bio-sensors that collect the same kind of physiological information as communicating bio-sensors can also compute the session key.

From the above security analysis, our scheme can provide authenticated access and keep communicating information confidential based on physiological features. The session keys negotiated based on bilinear parings are proved to be secure under the DBDH assumption, and they can provide deterministic security level and forward secrecy for BANs communication.

7 Performance Evaluation

In this section, we evaluate the performance of PBAKA in terms of recognition rate, storage cost, computation cost, communication cost and energy cost.

7.1 Recognition rate

We take the ECG signals as the example to show the performance of authentication. ECG signals can be downloaded from PhysioBANK database (https://physionet.org/physioBANk/database/). Firstly, fiducial points can be detected as: R peaks, T peaks, P peaks, LP valleys, TP valleys, and QRS complex of ECG records by using the technology [48], then ECG features are extracted as ten vectors by using the technology presented in [49] for mobile sensors. These features are for further authentication process. The physiological feature generation process is shown as Fig. 3.

Recognition rate can be denoted by TAR and FAR, TAR represents the probability that the valid bio-sensors are authenticated successfully, and FAR represents the probability that the bio-sensors not belong to the BANs are authenticated as the valid bio-sensors. The authentication accuracy is higher when TAR is higher and the FAR is lower reversely. The recognition rate can be 84.93% TAR and 1.29% FAR by using the hierarchical authentication algorithm [49] and Polynomial Distance Measurement (PDM) [59].

7.2 Storage cost

The communicating bio-sensors are only required to store their own unique IDs, physiological features (F_s and F_r), secret keys (SK_s and SK_r), their selected random numbers (r and s), and their intermediate crypto

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2848644, IEEE Transactions on Mobile Computing

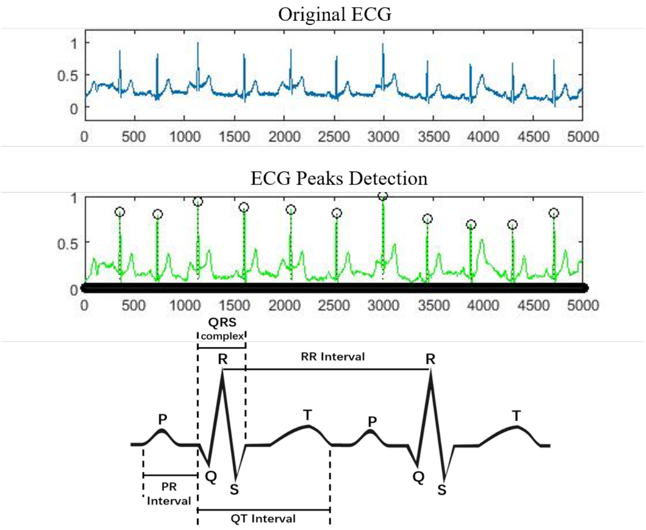

Fig. 3: ECG Peaks Detection Process

transaction information (T_s and T_r) for key agreement scheme. In PBAKA, ID_s and ID_r take 16 bytes each, the feature points are 2.5 bytes each, the feature length varies from 20 to 100, the random numbers r and s are 2 bytes each, Sk_s, Sk_s, T_s and T_r are 20 bytes. Thus, the total storage cost is as follows. Fig. 4 illustrates the comparison of storage cost between OPFKA and our scheme. We can demonstrate that the storage cost increases linearly with the feature size in both of these two schemes, and PBAKA consumes less storage cost than OPFKA [29] on bio-sensors.

$$ID_s + ID_r + F_s + F_r + SK_s + SK_r + r + s + T_s + T_r \tag{22}$$

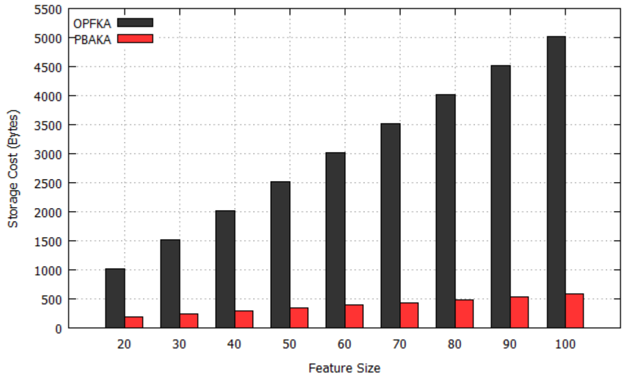

Fig. 4: Storage Cost of OPFKA and PBAKA

7.3 Computation cost

We evaluate our scheme based on TinyPBC [51] on the platform of 4KB RAM, 128KB ROM, and 7.3828-MHz 8-bit ATmega128L micro-controller, which is one kind of most resource-limited sensors. The main operation is on the η_T paring using binary fields ($\mathbb{F}_{2^m}$) on elliptic curve $y^2 + y = x^3 + x$. Our scheme takes 12.67s, and costs 0.8KB RAM usage to negotiate session keys. On the same evaluation platform, we can validate that our scheme can achieve secure key agreement with acceptable cost when compared with several existing solutions. The implementation in [52] costs 22s for key agreement, which is nearly twice as much as our time usage and demonstrates the efficiency of our scheme. Compare with the key establishment algorithm in [53], which consumes 4s and 1.7KB RAM usage, our scheme requires more computation time. However, we integrate field element and point compression [55] to significantly save 0.9KB RAM storage, which can be used to perform physiological feature sensing and analysis. Meanwhile, our scheme can provide stronger security than [53] by providing key unforgeability and forward secrecy according to the security analysis in Section 6 of the revised manuscript. Generally, biometric sensors equip with stronger ability than the ATmega128L micro-controller, and are expected to demonstrate better performance. For example, Samsung Bio-Processor [54] that can measure PPG and ECG biometrics, is designed with the 256KB RAM, 512KB flash and 168-MHz 32-bit Cortex-M4 controller. On this modern biometric sensor, our scheme is evaluated to consume less than 0.05s, which offers a great performance improvement to realize efficient key agreement on biometric sensors.

7.4 Communication cost

The communication cost can be divided into two parts: communication cost between bio-sensors and the control unit, and communication cost between two communicating bio-sensors. In the authentication process, the bio-sensor sends its ID_s and F_s to the control unit, the control unit compares F_s with its stored physiological information to confirm sender's identity, and sends a secret key SK_s to the sender. The receiver performs the same authentication process. In the key negotiation process between two communicating bio-sensors, the communication cost is T_s and T_r. Fig. 5 shows the relation between the communication cost and the feature size. We observe that the communication cost increases along with the feature size, and our scheme is more efficient than OPFKA [29].

$$ID_s + ID_r + F_s + F_r + SK_s + SK_r + T_s + T_r \tag{23}$$

7.5 Energy consumption

The energy consumption of bio-sensors in our scheme consists of energy consumption in computation part and communication part.

For energy consumption in computation part, as presented in [56], one time of bilinear paring operation consumes approximately 25.5mJ. Compared with bilinear paring operation, the total energy consumption of exponentiation operation and multiplication operation on

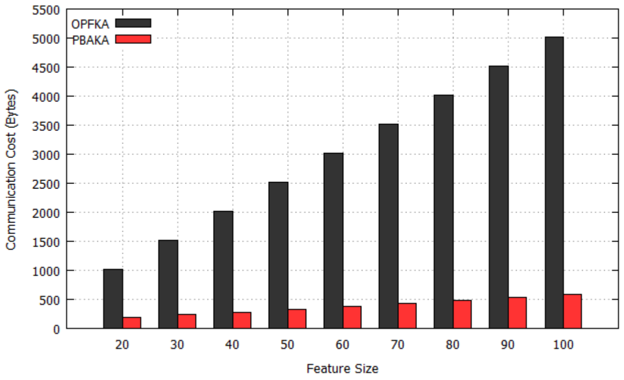

Fig. 5: Communication Cost of OPFKA and PBAKA

groups approximate to $1/5$ times of energy consumption of bilinear paring operation. In our scheme, bio-sensors process operation on groups for 4 times. For the sake of simplicity, we use $25.5 \times (1 + 1/5 \times 4) = 45.9mJ$ as the energy consumption in computation part.

For energy consumption in communication part, as presented in [57], a Chipcon CC1000 radio used in Crossbow MICA2DOT motes consumes $28.6\mu J$ and $59.2\mu J$ to receive and transmit one byte, respectively. Bio-sensors send their ID, physiological feature to control unit, and send their intermediate crypto transaction information to communicating bio-sensors. Respectively, bio-sensors receive their secret keys from the control unit, and receive the intermediate crypto transaction information from communicating bio-sensors. The energy consumption on transmitting and receiving the message equals to $(16 + 2.5|F| + 21) \times 59.2\mu J + (160 + 160)/8 \times 28.6\mu J = (3.2 + 0.148|F|)mJ$.

Thus, the total energy consumption in PBAKA equals to $(49.1 + 0.148|F|)mJ$. For OPFKA [29], the energy consumption equals to $(9.9 + 4.2|F|)mJ$ ($|F|$ means the feature size). Fig. 6 shows the relation between the energy consumption and the feature size. We can observe that our scheme consumes less energy in bio-sensors than OPFKA [29].

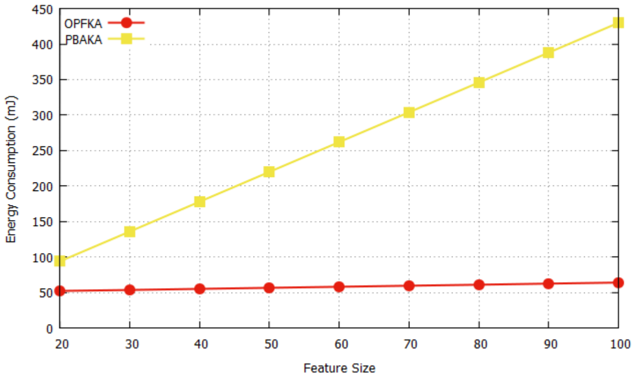

Fig. 6: Energy consumption of OPFKA and PBAKA

8 Conclusion

In this paper, we have proposed a secure authenticated key agreement scheme PBAKA for bio-sensors in BANs. Our scheme can obtain an authenticated key agreement without key pre-deployment, and is flexible for bio-sensors that collect different kinds of physiological features with deterministic security level. Moreover, PBAKA is computationally efficient for bio-sensors by offloading the authentication burden to the control unit, and is provably secure under the DBDH assumption. In our future work, we will extend our research to negotiate session keys among a group of bio-sensors that collect non-unique physiological signals based on accelerator.

9 Acknowledgements

This work is supported by China Scholarship Council, the Innovation Foundation for Postgraduate of Central South University under Grant Number 2016zzts057, Innovation-Driven Project of Central South University (No. 2016CXS013), 111 project (No. B18059), International Science & Technology Cooperation Program of China (No. 2013DFB10070), China Hunan Provincial Science & Technology Program (No. 2012GK4106), and NSERC of Canada.

References

[1] K. Zhang, X. Liang, J. Ni, K. Yang and X. Shen, ”Exploiting social network to enhance human-to-human infection analysis without privacy leakage,” *IEEE Transactions on Dependable and Secure Computing*, to appear.

[2] O. Chris, A. Milenkovic, C. Sanders and E. Jovanov, “System architecture of a wireless body area sensor network for ubiquitous health monitoring,” *Journal of mobile multimedia*, vol. 1, no. 4, pp. 307-326, 2006.

[3] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen and H. Luo, “Security and privacy for mobile healthcare networks: From a quality of protection perspective,” *IEEE Wireless Communications*, vol. 22, no. 4, pp. 104-112, 2015.

[4] M. Seyedi, B. Kibret, D. Lai, and M. Faulkner. “A survey on intrabody communications for body area networks applications,” *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 8, pp. 2067-2079, 2013.

[5] M. Ameen, J. Liu, and K. Kwak, “Security and privacy issues in wireless sensor networks for healthcare applications,” *Journal of medical systems*, vol. 36, no. 1, pp. 93-101, 2012.

[6] R. Lu, X. Lin, and X. Shen, “SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614-624, 2013.

[7] M. Rushanan, A. Rubin, D. Kune and C. Swanson, “SoK: Security and privacy in implantable medical devices and body area networkss,” in *Proc. of S&P*, 2014, pp. 524-539.

[8] L. Pycroft, S. Boccard, S. Owen, J. Stein, J. Fitzgerald, A. Green and T. Aziz, “Brainjacking: Implant security issues in invasive neuromodulation,”, *World neurosurgery*, vol. 92, pp. 454-462, 2016.

[9] “FDA Issues Alert Over Vulnerable Hospira Drug Pumps,” 2015. [online]. Available: http://www.securityweek.com/fda-issues-alert-over-vulnerable-hospira-drug-pumps

[10] C. Camara, P. Peris and J. Tapiador, “Security and privacy issues in implantable medical devices: A comprehensive survey,” *Journal of biomedical informatics*, vol. 55, No.1, pp. 272-289, 2015.

[11] J. Ren, Y. Zhang, Q. Ye, K. Yang, K. Zhang and X. Shen, “Exploiting secure and energy efficient collaborative spectrum sensing for cognitive radio sensor networks,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6813-6827, 2016.

[12] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen and S. Chaudhry, “Efficient end-to-end authentication protocol for wearable health

monitoring systems," *Computers & Electrical Engineering*, to appear.

[13] A. Ali and A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *Journal of medical systems*, vol. 39, no. 10, pp. 1-14, 2015.

[14] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu and X. Sun, "Enhanced secure sensor association and key management in wireless body area networks," *Journal of Communications and Networks*, vol. 17, no. 5, pp. 453-462, 2015.

[15] W. Drira, E. Renault and D. Zeghlache, "A hybrid authentication and key establishment scheme for wBANs," in *Proc. of TrustCom*, 2012, pp. 78-83.

[16] P. Maura and D. Stinson, "A unified approach to combinatorial key predistribution schemes for sensor networks." *Designs, Codes and Cryptography*, vol. 71, no. 3, pp. 433-457, 2014.

[17] C. Chen and H. Chao, "A survey of key distribution in wireless sensor networks," *Security and Communication Networks*, vol. 7, no. 12, pp. 2495-2508, 2014.

[18] Q. Jiang, S. Zeadally, J. Ma and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, no. 1, pp. 3376-3392, 2017.

[19] M. Suhas, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. of MobiCom*, 2008, pp. 128-139.

[20] W. Wang, W. Zhan, T. Wen, and W. Lei, "WAVE: Secure wireless pairing exploiting human body movements," in *Proc. of TrustCom*, 2015, pp. 1243-1248.

[21] L. Shi, J. Yuan, S. Yu, and M. Li, "MASK-BANs: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet of Things Journal*, vo. 2, no. 1, pp. 52-62, 2015.

[22] G. Revadigar, C. Javali, H. Asghar, K. Rasmussen and S. Jha, "Mobility independent secret key generation for wearable healthcare devices," in *Proc. of BodyNet*, 2015, pp. 294-300.

[23] E. Zaghouani, A. Jemai, A. Benzina and R. Attia, "ELPA: A new key agreement scheme based on linear prediction of ECG features for WBANs," in *Proc. of EUSIPCO*, 2015, pp. 81-85.

[24] H. Zhao, C. Chen, J. Hu and J. Qin, "Securing body sensor networks with biometric methods: A new key negotiation method and a key sampling method for linear interpolation encryption," In *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, pp. 1-11, 2015.

[25] M. Rostami, A. Juels and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. of CCS*, 2013, pp. 1099-1112.

[26] R. Seepers, C. Strydis, I. Sourdis, Z. De and I. Chris, "On using a von neumann extractor in heart-beat-based security," in *Proc. of TrustCom*, 2015, pp. 491-498.

[27] J. Zhou, Z. Cao, X. Dong, N. Xiong and A. Vasilakos, "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area networks in m-healthcare social networks," *Information Sciences*, vol. 314, No. 1, pp. 255-276, 2015.

[28] K. Venkatasubramanian, A. BANserjee and S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networkss," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60-68, 2010.

[29] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao and D. Chen, "OPFKA: Secure and efficient ordered-physiological-features-based key agreement for wireless body area networkss," in *Proc. of INFOCOM*, 2013, pp. 2274-2282.

[30] N. Belgacem, R. Fournier, A. Nait, and F. Bereksi, "A novel biometric authentication approach using ECG and EMG signals," *Journal of medical engineering & technology*, vol. 39, no. 4, pp. 226-238, 2015.

[31] W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones, *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1268-1293, 2015.

[32] M. Matveev, I. Christov, V. Krasteva, G. Bortolan, D. Simov, N. Mudrov, and I. Jekova, "Assessment of the stability of morphological ECG features and their potential for person verification/identification, in *Proc. of MATEC Web of Conferences*, 2017, pp. 01-04.

[33] X. Li, L. Luo, S. Zhu, B. Yang, K. Ni, Q. Zhou, and X. Wang, "Improved identification of the electrocardio-signal for pulsatile ventricular assist devices, *Computer Assisted Surgery*, vol. 22, no. 1, pp. 278-285, 2017.

[34] R. Palaniappan, S. Andrews, I. Sillitoe, T. Shira, and R. Paramesran, "Improving the feature stability and classification performance of bimodal brain and heart biometrics, in *Proc. of SIRS*, 2016, pp. 175-186.

[35] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system, in *Proc. of ACM MobiCom*, 2017, pp. 315-328.

[36] K. Rasmussen, M. Roeschlin, I. Martinovic, and G. Tsudik, "Authentication using pulse-response biometrics, in *Proc. of NDSS*, 2014, pp. 114.

[37] S. Safie, J. Soraghan, and L. Petropoulakis, "Electrocardiogram (ECG) biometric authentication using pulse active ratio (PAR), *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1315-1322, 2011.

[38] C. Poon, Y. Zhang, and S. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73-81, 2006.

[39] W. Meng, D. Wong, S. Furnell and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1268-1293, 2015.

[40] L. Nanni, L. Alessandra, F. Matteo and C. Raffaele, "Combining biometric matchers by means of machine learning and statistical approaches," *Neurocomputing*, vol. 149, No. 1, pp. 526-535, 2015.

[41] F. Miao, S. Bao and Y. Li, "Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security," *IET Information Security*, vol. 7, no. 2, pp. 87-96, 2013.

[42] S. Kang, S. Lee, H. Cho and H. Park, "ECG authentication system design based on signal analysis in mobile and wearable devices," *IEEE Signal Processing Letters*, vol. 23, no. 6, pp. 805-808, 2016.

[43] J. Robert, A. Peer and M. Buss, "Feature extraction and selection for emotion recognition from EEG," *IEEE Transactions on Affective Computing*, vol. 5, no. 3, pp. 327-339, 2014.

[44] S. Oh, Y. Lee and H. Kim, "A novel EEG feature extraction method using Hjorth parameter," *International Journal of Electronics and Electrical Engineering*, vol. 2, no. 2, pp. 106-110, 2014.

[45] J. Ren, Y. Zhang, K. Zhang and X. Shen,"Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3718-3731, 2016.

[46] J. Blasco, T. Chen, J. Tapiador, and P. Peris, "A survey of wearable biometric recognition systems," *ACM Computing Surveys*, vol. 49, no. 3, pp. 4301-4335, 2016.

[47] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237-257, 2006.

[48] P. Laguna, R. Jan, E. Bogatell, and D. Anglada, "QRS detection and waveform boundary recognition using ecgpuwave," http://www.physionet.org/physiotools/ecgpuwave, 2002.

[49] J. Falconi, H. Osman, and A. Saddik, "ECG authentication for mobile devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591-600, 2016.

[50] S. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks, *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 371-383, 2015.

[51] L. Oliveira, D. Aranha, C. Gouv ea, M. Scott, D. C amara, J. Lpez, and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks, *Computer Communications*, vol. 34, no. 3, pp. 485-493, 2011.

[52] H. Wang and Q. Li, "Efficient implementation of public key cryptosystems on mote sensors (short paper), in *Proc. of ICICS*, 2006, pp. 519-528.

[53] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks, in *Proc. of IEEE IPSN*, 2008, pp. 245-256.

[54] "Samsung Bio-Processor, 2015. [Online]. Available: http://www.samsung.com/semiconductor/products/bioprocessor/.

[55] X. Xiong, D. Wong, and X. Deng, "TinyPairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks, in Proc. of IEEE WCNC, 2010, pp. 1-6.

[56] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 11, pp. 4136-4111, 2007.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2018.2848644, IEEE Transactions on Mobile Computing

[57] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz,"Energy analysis of public-key cryptography for wireless sensor networks, in *Proc. of PerCom*, 2005, pp. 324-328.

[58] T. Choudhary and M. Manikandan, "Robust photoplethysmographic (PPG) based biometric authentication for wireless body area networks and m-health applications," in *Proc. of NCC*, 2016, pp. 1-6.

[59] F. Sufi, I. Khalil, and I. Habib, "Polynomial distance measurement for ECG based biometric authentication," *Security and Communication Networks*, vol. 3, no. 4, pp. 303-319, 2010.

Wenjuan Tang (S'17) received the B.E. degree from the Central South University, Changsha, China, in 2012. She is working toward the Ph.D. degree with the Department of Information Science and Engineering, Central South University, Changsha, China. Currently, she is a visiting scholar in the Department of Electrical and Computer Engineering, University of Waterloo, Canada. Her research interests include applied cryptography and information security, with current focus on e-healthcare systems, fog/edge computing, transparent computing, and Internet of Things.

Kuan Zhang (S'13-M'17) has been an assistant professor at the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, USA, since September 2017. He received the B.Sc. degree in Communication Engineering and the M.Sc. degree in Computer Applied Technology from Northeastern University, China, in 2009 and 2011, respectively. He received the Ph.D. degree in Electrical and Computer Engineering from the University of Waterloo, Canada, in 2016. He was also a postdoctoral fellow with the Broadband Communications Research (BBCR) group, Department of Electrical and Computer Engineering, University of Waterloo, Canada, from 2016-2017. His research interests include security and privacy for mobile social networks, e-healthcare systems, cloud/edge computing and cyber physical systems.

Ju Ren [S'13, M'16] (renju@csu.edu.cn) received the B.Sc. (2009), M.Sc. (2012), Ph.D. (2016) degrees all in computer science, from Central South University, China. From Aug. 2013 to Sept. 2015, he was a visiting Ph.D. student in the Department of Electrical and Computer Engineering, University of Waterloo, Canada. Currently, he is a professor with the School of Information Science and Engineering, Central South University, China. His research interests include Internet-of-Things, wireless communication, transparent computing and cloud computing. In these related research areas, he has published over 40 papers on prestigious international journals and conferences, including IEEE TIFS, TWC, TVT, TII and IEEE INFOCOM, etc. Dr. Ren serves/has served as an associate editor for Peer-to-Peer Networking and Applications, a leading guest editor for IEEE Network, and a Technical Program Committee member of many international conferences including IEEE INFOCOM18, Globecom17, WCNC17, WCSP16, etc. Dr. Ren also served as a track co-chair for IEEE VTC17 Fall and IEEE I-SPAN 2018, a special session co-chair of IEEE VCIP17, and an active reviewer for over 20 international journals. He is a member of IEEE and ACM.

Yaoxue Zhang (zyx@csu.edu.cn) received his B.S. degree from Northwest Institute of Telecommunication Engineering, China, in 1982, and his Ph.D. degree in computer networking from Tohoku University, Japan, in 1989. Currently, he is a professor in the Department of Computer Science at Central South University, China, and also a professor in the Department of Computer Science and Technology at Tsinghua University, China. His research interests include computer networking, operating systems, ubiquitous/ pervasive computing, transparent computing, and big data. He has published over 200 technical papers in international journals and conferences, as well as 9 monographs and textbooks. He is a fellow of the Chinese Academy of Engineering and the president of Central South University, China.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received Ph.D. degrees (1990) from Rutgers University, New Jersey (USA). Dr. Shen is a University Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. Dr. Shen served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom16, Infocom14, IEEE VTC10 Fall, and Globecom07, the Symposia Chair for IEEE ICC10. He also serves as the Editor-in-Chief for IEEE Internet of Things Journal, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo, the Premiers Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo, the Joseph LoCicero Award and the Education Award 2017 from the IEEE Communications Society. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.