Song and Tan *Cybersecurity* (2020) 3:21
https://doi.org/10.1186/s42400-020-00061-7

Cybersecurity

RESEARCH Open Access

Practical pairing-Free sensor cooperation scheme for cloud-Assisted wireless body area networks

Yuanzhao Song[1] and Haowen Tan[2*]

Abstract

Nowadays, the design and construction of efficient internet of things (IoTs) has become a new strategies for improving living quality of all aspects. Emerging as one of the most significant extension of medical IoTs, wireless body area networks (WBANs) is capable of monitoring crucial physiological and behavioral information through wearable sensors, offering a new paradigm for the next-generation healthcare systems. As a matter of fact, due to the inherent open wireless communicating characteristics, data security and user privacy issues of WBANs have attracted attentions from both industry and academia. So far, lots of relevant researches emphasize on secure transmission and privacy protection. However, the computation and communication limitations for individual WBAN sensor have not been taken proper consideration. Moreover, the implementation of cloud computing infrastructure has provided WBANs with superior transmission and processing qualities. Emphasizing on the above issues, this paper construct a pairing-free authentication and sensor cooperation scheme in cloud-assisted WBANs, where most of the practical requirements for WBAN sensors could be satisfied. Our design guarantee the sensor anonymity in the whole transmission session. Note that our design offers pairing-free validation procedure followed with active sensor cooperation, which is suitable for massive sensor scenarios. The security analysis proves that our designed scheme is capable of achieving desired security properties and offer adequate resistances to the charted malicious attacks. Meanwhile, security comparison demonstrates that the proposed protocol is secure compared with the state-of-the-arts.

Keywords: WBANs, Security, Authentication, Anonymous identity, Conditional privacy

Introduction

Wireless Body Network (WBAN) is considered to be the basic infrastructure of IoT-based healthcare system in the future. Recent rapid advances in wireless communications and sensor manufacturing have accelerated the explosive popularity of WBAN applications and services. WBAN provides real-time, reliable medical monitoring for specific users (Liu et al. 2014). In the medical fields, WBAN can be used to continuously monitor the patient's health and to send menstrual information to medical institutions such as hospitals, community clinics, and first aid centers. In this case, doctors can provide timely medical help after performing the remote diagnosis of the patient (Zhang et al. 2020). In addition, pre-warning and preventive measures against certain diseases can be implemented. Today, WBAN is committed to state-of-the-art communication and data processing strategies such as 5G network and cloud computing technologies to be used in heterogeneous IoT environments, which could exchange high-speed, stable data with centralized servers (Hu et al. 2016; Zhou et al. 2020).

In order to meet different needs in different practical situations, WBAN's architecture varies widely. The typically designed WBAN consists of the heathcare center (HC),

*Correspondence: tan_halloween@foxmail.com
[2]Department of Computer Engineering, Chosun University, 309 Pilmun-daero, 61452 Dong-gu, Gwangju, Korea
Full list of author information is available at the end of the article

the personal controller (PC), and many wireless medical sensors. These sensors can perform important biomedical information collection in various ways (Ji et al. 2018; Sambandam et al. 2020). Therefore, appropriate physiological data related to heart rate, body temperature and blood pressure can be measured separately through sensors. The collected personal physical information is then sent to the HC and processed. Based on this, regular medical services can be provided to large numbers of patients simultaneously (Zhang et al. 2013). It is important to note that HC is considered as a secure data center and an effective entity responsible for distributing core information. Hence, we assume that all participating sensors and PC secret key information is always safely stored at the HC side. Personal controller (PC) is a portable device used to aggregate personal sensor data (Yuan et al. 2020). Sensitive biomedical data is then transmitted to the remote server via PC. WBAN sensors (includes wearable and implantable sensors) are the low-power wireless medical devices subject to computing, communication, power supply, and storage (Liu et al. 2020; Anjum et al. 2020). On the other hand, increasing the calculation and transmission load on the sensor side will release more energy into heat and eventually damage the human organs. As a result, low-cost operations should be performed in WBAN sensors side.

In actual WBAN scenarios, the frequent data exchange between the sensor and the PC is carried out in the open wireless environment, and the important biometric data transmitted is easily affected by various security attacks and privacy risks (Yang and Chang 2009; Li et al. 2018; Huang et al. 2020; Xiong and Qin 2015). In this case, advanced security strategies and privacy protection technologies are essential to WBANs. The effective authentication mechanism between wireless entities is mandatory, providing preliminary protection for WBAN interactions (Shen et al. 2016; He et al. 2017). Therefore, various charts and unknown security threats such as eavesdropping, impersonation, message replaying can be prevented (Liu et al. 2020). After mutual authentication, efficient group key distribution and management of all verified wearable sensors is of great significance (Anjum et al. 2020). Therefore, subsequent private biometric data can be safely transmitted. Message broadcasting between all legal sensors can also be realized (Liu et al. 2014).

In this paper, we develop a pairing-free authentication and sensor cooperation scheme in cloud-assisted WBANs, where major security requirements for WBAN sensors could be satisfied. Our design guarantee the sensor anonymity in the whole transmission session. Note that our design offers pairing-free validation procedure followed with active sensor cooperation, which is suitable for massive sensor scenarios. The security analysis proves that our designed scheme is capable of achieving desired security properties and offer adequate resistances to the charted malicious attacks. Meanwhile, security comparison demonstrates that the proposed protocol is superior to other existing schemes.

Related work

Recently, many research papers have been published, which focus on secure data transmission for WBANs. Firstly, the traditional public key cryptography (TPKC) techniques has been utilized to the wireless mobile environment (Horn and Preneel 1998; Shen et al. 2017; Zhang et al. 2020). However, relatively large computation cost is made, which is not practical for resource-constrained sensors. Thereafter, many schemes with elliptic curve cryptography (ECC) have been presented (Zhang et al. 2013).

Meanwhile, several identification and key agreement mechanisms have been proposed in (Yang and Chang 2009; Wang 2015), which all adopt the identity-based key cryptography (ID-PKC). In ID-PKC, the key generation center (KGC) is responsible for generating public keys, which could drastically decrease the computation cost for encrypting and decrypting procedure.

However, ID-PKC schemes is vulnerable to key escrow problem. Hence, certificateless public key cryptography (CL-PKC) is proposed (Al-Riyami and Paterson 2003). So far many certificateless authentication schemes have been proposed. Xiong (2014) proved that protocols of (Liu et al. 2014) cannot provide scalability and forward security. Liu et al. (2014) designed the enhanced CL-PKC protocol for WBAN scenarios. Meanwhile, the certificateless encrypting and signing mechanism is developed in (Xiong and Qin 2015). The efficient and scalable identity revocation mechanism is adopted. Li et al. (Li and Hong 2016) designed an efficient certificateless signcryption scheme with the corresponding access control method. Thereafter, ciphertext-policy attribute-based encryption is deployed (Hu et al. 2016). Focusing on preserving the user real identity, another anonymous-identity authenticating scheme is presented (He et al. 2017), which overcomes the security vulnerability in (Liu et al. 2014). In 2018, Ji et al. presented an certificateless conditional privacy-preserving authentication (CPPA) scheme for WBAN (Ji et al. 2018). The proposed method offers batch authentication towards massive number of participant users, which could significantly reduce the computational cost of the WBAN service provider (SP). Currently, several novel WBAN authentication mechanisms are proposed (Li et al. 2018). Thereafter, X. Li and L. Wang (Li and Wang 2012) proposed a fast certificateless authentication scheme employing bilinear pairing in wireless communication scenarios.

Model definition and preliminaries

In this section, the related preliminaries are introduced. Thereafter, the corresponding notations, and system model are illustrated as follows.

Elliptic curve cryptosystem (ECC)

We define $p > 3$ as a large prime, $\mathbb{F}_p$ be the finite field of order p, where $a, b \in \mathbb{F}_p$ could satisfy $4a^3 + 27b^2 \pmod{p} \neq 0$. The elliptic curve $E_p(a, b)$ on a finite field $\mathbb{F}_p$ is defined as follows

$$y^2 = x^3 + ax + b \bmod p,$$

where $(x, y) \in \mathbb{F}_p$. As for $E_p(a, b)$, the addition operation on this curve is defined as point doubling when the two points are identical. Otherwise, it is defined as point addition. All the points on the curve $E_p(a, b)$, and the point at the infinity ∞ could form an additive Abelian group $E(\mathbb{F}_p)$. In this way $\infty = (-\infty)$ acts as the identity element.

Bilinear pairing

We define $\mathbb{G}_1$ as a cyclic additive group generated by the large prime number q, and $\mathbb{G}_2$ as the cyclic multiplicative group with the same prime order. A mapping function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is constructed as the bilinear pairing if and only if the following three properties could be satisfied all:

1 *Bilinearity:* $\forall P, Q, R \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_q^*$, there is

$$\begin{cases} \hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab} \\ \hat{e}(P, Q + R) = \hat{e}(Q + R, P) = \hat{e}(P, Q)\,\hat{e}(P, R) \end{cases}.$$

2 *Non-degeneracy:* $\exists P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ is defined as the identity element of $\mathbb{G}_2$.
3 *Computability:* $\forall P, Q \in \mathbb{G}_1$, there exists an efficient algorithm to compute $\hat{e}(P, Q)$.

In this way, the bilinear map $\hat{e}$ that satisfies the above three properties can be constructed with the modified Weil pairing or Tate pairing under the supersingular elliptic curve $\mathbb{G}_1$. The following related characteristics are presented.

Computational diffie-Hellman problem (CDHP)

We define $P, aP, bP \in \mathbb{G}_1$ for $a, b \in \mathbb{Z}_q^*$, where P is the generator of $\mathbb{G}_1$, the advantage for any probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$ in computing abP so as to solve the CDHP problem is negligible, which can be defined as:

$$Adv_{\mathcal{A},\mathbb{G}_1}^{CDHP} = \Pr\left[\mathcal{A}(P, aP, bP) \rightarrow abP : a, b \in \mathbb{Z}_q^*\right].$$

Elliptic curve discrete logarithm problem (ECDLP)

Given $P, Q \in \mathbb{G}_1$, where $Q = aP$. In order to solve the ECDLP problem, the advantage for any probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$ in finding the integer $a \in \mathbb{Z}_q^*$ can be defined as:

$$Adv_{\mathcal{A},\mathbb{G}_1}^{ECDLP} = \Pr\left[\mathcal{A}(P, aP) \rightarrow a : a \in \mathbb{Z}_q^*\right].$$

Hash function

The one-way hash function is defined to be secure if the following three properties can be satisfied:

1 If input a message x which is of arbitrary length, it is computationally easy to compute a message digest of the fixed length output $h(x)$.
2 With y, it is difficult to compute $x = h^{-1}(y)$.
3 With x, it is computationally infeasible to get $x' \neq x$ such that $h(x') = h(x)$ holds.

Notations

The notations used in our design are briefly introduced in Table 1.

System model

The structure of our cloud-assisted WBANs is shown in Fig. 1, where the whole WBAN system consists of three essential entities: the cloud-based healthcare center (HC), the personal controller (PCs) and the medical sensors. Note that the HC consists of medical database, central authority (CA), and law enforcement agency (LEA). Description of these entities are respectively illustrated below.

Table 1 Notations

Notation	Description
PCs	Personal Controllers
HC	Healthcare Center
Λ_i	Original Identity Number i
κ_i	Password of Sensor i
s	Master Key of PC
$\mathbb{G}_{\mathcal{H}}$	Cyclic Additive Group
P	Generator of $\mathbb{G}_{\mathcal{H}}$
ξ_i	Pseudo-Random Value Generated by i
K_i	Pseudo-Random Value Generated by CA
H_1, H_2, H_3, H_4	Secure Hash Function
$\mathcal{M}_i$	Transmitting Medical Data for Sensor i
$Enc_x(y)$	Symmetric Encryption of y using x
$Dec_x(y)$	Symmetric Decryption of y using x
ω	Pseudo-Random Value Generated by PC
P_{pub}	CA Public Key
$\mathcal{K}$	Final Group Key
$\mathbb{I}$	Numbers of Sensors

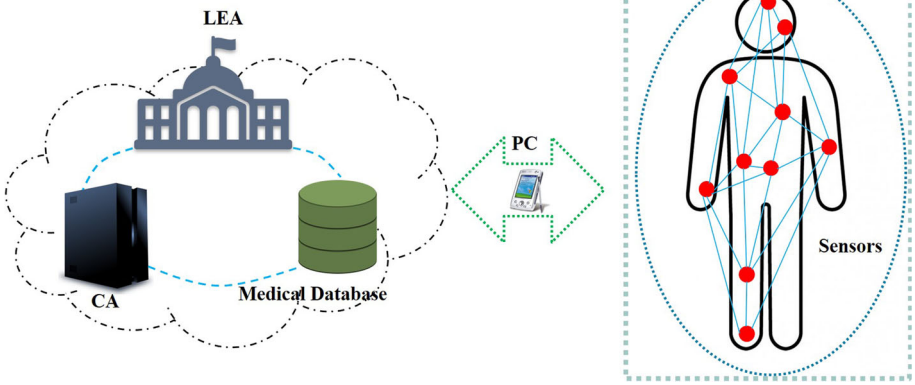

Fig. 1 Cloud-Assisted WBANs System Model

Healthcare center (HC)

HC is mainly composed of the central authority (CA), the medical database, and the law enforcement agency (LEA). Each of the entities play different roles. CA is responsible for processing the vital system operations, including patient registration and secret key generation. The significant user personal information, such as identity number and the private password, are stored in the medical database. It is worth noting that the remote cloud server could provide adequate storage for database. CA is infeasible to be compromised by the adversaries. The remaining LEA is for the illegal behavior management, which is usually performed as the government department. All the sensor revocation and registration process by CA should be fully acknowledged to the LEA department. The three entities: LEA, CA, and database together, are considered as the cloud-assited HC. Typically, HC is defined as a medical service provider and a trusted key management center. The important personal data will be transmitted to HC, which could reflect the patient's real-time physical condition. Therefore, the corresponding medication for the specific patient is available.

Personal controllers (PCs)

In general, personal controllers (PCs) are defined as specialized medical equipment with specific medical purposes. It is assumed that the PC is a portable device with a function of collecting and communicating biometric information with HC. In other words, the importan physiological data collected from several WBANs sensors will be delivered to the personal controller. Note that each user of WBAN is connected with a specific personal controller.

Sensors

The sensor is assumed to be implanted or attached to the user's body as a wireless biomedical device. Sensors have limited computational power and battery capacity. The sensor is responsible for real-time measurement of various physiological indicators of specific user. Typically, multiple sensors, each responsible for monitoring different biometrics, are effective within the human body range. All important personal data collected is transferred to the PC via an open wireless connection. Note that all physiological sensor data collected are time-related parameters.

Proposed authentication and key distribution scheme

In this section, we describe the proposed practical authentication and key distribution scheme in cloud-assisted WBANs. The proposed scheme consists of two subsections: PC-to-sensor mutual authentication, and group key generation between sensors, which will be described respectively.

PC-to-Sensor mutual authentication

Our design on PC-to-sensor authentication does not need the secure transmission channels for crucial key extraction. As a matter of fact, the constant device identity and private password are the only two required parameters. The security assurance of our mechanism is based on the hardness of the previously introduced CDH problem, which has been briefly introduced in the previous section. The authenticating process of our design is shown in Fig. 2.

Firstly, in our design, each medical sensor should register to the LEA initially before use. Each sensor is assigned the unique identity number, which is defined as the static parameter representing the original identity of certain sensor. It is worth noting that the allocated identity will be kept unchanged since the beginning. Meanwhile, the confidential password for each sensor will be randomly generated by the WBAN managing system. In this way, the identity number, and the confidential password for each sesnor i, which are respectively denoted as Λ_i and κ_i, are

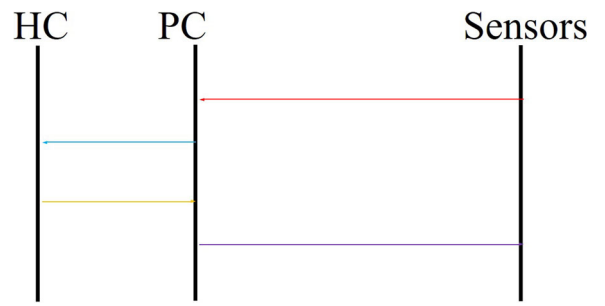

Fig. 2 PC-to-Sensor Mutual Authentication

stored in the cloud medical database, where only CA and LEA have access to.

We define $\mathbb{G}_{\mathcal{H}}$ as the cyclic additive group which is generated by the generator P with an order q. CA then chooses the system master key s randomly and then computes the system public key P_{pub} in the way of

$$P_{pub} = sP. \tag{1}$$

The secure hash functions used in our method H_1, H_2 and H_3 are respectively defined as follows:

$$\begin{cases} H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_{\mathcal{P}}^* \\ H_2 : \{0,1\}^* \times \mathbb{G}_{\mathcal{H}} \rightarrow \mathbb{Z}_{\mathcal{P}}^* \\ H_3 : \{0,1\}^* \times \mathbb{G}_{\mathcal{H}} \rightarrow \mathbb{Z}_{\mathcal{P}}^* \end{cases}. \tag{2}$$

where $\mathbb{Z}_{\mathcal{P}}^*$ is defined as the nonnegative integer set less than the predefined large prime number $\mathcal{P}$.

It is worth noting that the generator P, the public key P_{pub}, the three one-way hash function H_1, H_2, and H_3, as well as $\mathbb{G}_{\mathcal{H}}$ will all be published to the nearby WBAN devices, while the system master key s is kept secret during the whole session. The detailed steps for WBAN authentication are as follows:

First, each sensor i random generates ξ_i as the original key seed. Hence, sensor will compute $\mathcal{R}_i$ according to

$$\mathcal{R}_i = \xi_i P. \tag{3}$$

Thereafter, the parameter υ_i is calculated, which combines the original identity number Λ_i and the generated random number ξ_i. Note that the value of Λ_i remain constant. Hence, the random value ξ_i could help improve the resistance to several malicious attacks. The υ_i is calculated as

$$\upsilon_i = H_1(\Lambda_i) + \xi_i. \tag{4}$$

For different authentication session, the υ_i is dynamic in this case. Also, it is worth emphasizing that CA will not reveal the identity number Λ_i of individual i to any user (PC). In this way, the real identity of sensor is beyond PC's reach. Thus, under extreme occasions with collision by malicious PC, the adversaries cannot retrieve the confidential message by tracing the unique identity of particular sensor. Moreover, instead of using the private secret key totally from the PC, the generated ξ_i is considered as the partial private key and safely stored in sensor side.

Subsequently, the corresponding ϕ_i is generated by sensor i as follows:

$$\phi_i = H_2(\Lambda_i, \mathcal{R}_i, \kappa_i), \tag{5}$$

where the sensor i adopts its previous generated password κ_i. Vehicle i then gathers $\langle \mathcal{R}_i, \upsilon_i, \phi_i \rangle$ and forwards it to PC.

As mentioned above, our method assign the heavy computation and storage task to the remote cloud server (medical database and CA). In this way, the portable PCs does not need to process the heavy tasks. Instead, PCs perform as the forwarding channel between massive sensors and cloud CA. It means a lot for practical consideration since the computation and storage of each PC are related restricted compared to the cloud server.

Moreover, in our system model we consider the PCs as the benign entities in most of the time. As mentioned above, in certain cases the PCs may be compromised or disabled physically. Hence in our assumption the PCs do not need to act as the vital key generation and verification center. In fact, in our design, upon receiving the message $\langle \mathcal{R}_i, \upsilon_i, \phi_i \rangle$ from sensor i, PC is designed to directly forward the acquired medical data to the cloud-based CA, which is responsible for partial secret key distribution and identification.

As illustrated previously, the sensor i's identity number Λ_i and the corresponding password κ_i are stored in cloud medical database. Initially, the value of $H_1(\Lambda_i)$ for all the sensors are also calculated and stored in database. In this case, upon receiving the request, CA computes

$$\Gamma_i = \upsilon_i P \tag{6}$$

using the received υ_i. Then CA first add $\mathcal{R}_i$ to all the stored $H_1(\Lambda_i)$ as follows

$$\Delta_i = H_1(\Lambda_i) + \xi_i. \tag{7}$$

In this way, CA compares the computed Δ_i with the received υ_i and finally searches the $I\Lambda_i$ of the requesting sensor from remote database. Then CA checks the correctness of

$$\Gamma_i \stackrel{?}{=} H_1(\Lambda_i)P + \mathcal{R}_i. \tag{8}$$

The correctness is elaborated as follows:

$$\begin{aligned} \Gamma_i &= \upsilon_i P \\ &= (H_1(\Lambda_i) + \xi_i)\, P \\ &= H_1(\Lambda_i)P + \xi_i P \\ &= H_1(\Lambda_i)P + \mathcal{R}_i \end{aligned}. \tag{9}$$

If the above Γ_i is validated, CA will also check the correctness of the received ϕ_i by combing the stored sensor information (Λ_i, κ_i) with the received $\mathcal{R}_i$.

In practical application scenario with n assumed sensors, the verifying process in CA side is similar to the above single sensor situation. CA will then check the correctness as

$$\sum_1^n \Gamma_i \stackrel{?}{=} \sum_1^n H_1(\Lambda_i)P + \sum_1^n \mathcal{R}_i. \tag{10}$$

That is,

$$\begin{aligned}\sum_1^n \Gamma_i &= \sum_1^n \upsilon_i P \\ &= \sum_1^n (H_1(\Lambda_i) + \xi_i) P \\ &= \sum_1^n H_1(\Lambda_i)P + \sum_1^n \xi_i P \\ &= \sum_1^n H_1(\Lambda_i)P + \sum_1^n \mathcal{R}_i\end{aligned}. \tag{11}$$

In the occasions where both υ_i and ϕ_i are proved to be correct, CA is then capable of deriving ξ_i by

$$\xi_i = \upsilon_i - H_1(\Lambda_i), \tag{12}$$

where ξ_i is stored in the medical database. The database processing is briefly shown in Fig. 3. Note that ξ_i is shared between CA and sensor i, while PC has zero knowledge about it.

In the next, CA generates random value k_i for each sensor i. The value of W_i and y_i are calculated in the way of

$$\begin{cases} W_i = k_i\mathcal{R}_i = k_i\xi_i P \\ y_i = H_3(\Lambda_i, \kappa_i, W_i, \xi_i)s + k_i \end{cases}. \tag{13}$$

Note that $\langle \mathcal{R}_i, W_i, y_i \rangle$ will be broadcast to sensor i through PC. Sensor derives the assigned key PSK_i by

$$PSK_i = \xi_i^{-1} W_i = k_i P. \tag{14}$$

The validity of the received information will also be checked by sensor i:

$$y_i P \stackrel{?}{=} H_3(\Lambda_i, \kappa_i, W_i, \xi_i)P_{pub} + PSK_i. \tag{15}$$

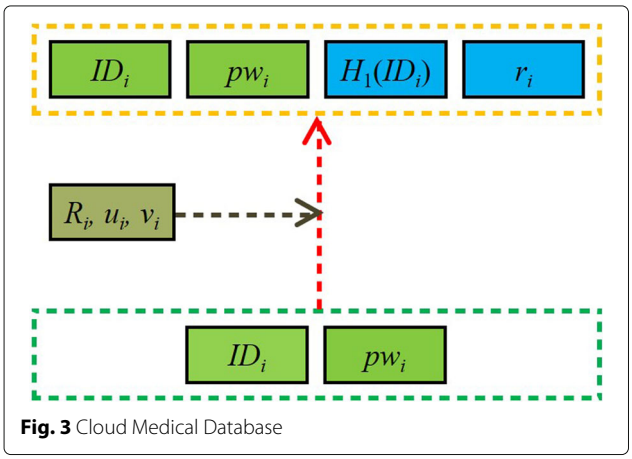

Fig. 3 Cloud Medical Database

That is,

$$\begin{aligned} y_i P &= H_3(\Lambda_i, \kappa_i, W_i, \xi_i)sP + k_i P \\ &= H_3(\Lambda_i, \kappa_i, W_i, \xi_i)P_{pub} + PSK_i \end{aligned}. \tag{16}$$

As for multiple sensors, the following batch checking process can be done:

$$\begin{aligned} \sum_1^n y_i P &= \sum_1^n H_3(\Lambda_i, \kappa_i, W_i, \xi_i)sP + \sum_1^n k_i P \\ &= \sum_1^n H_3(\Lambda_i, \kappa_i, W_i, \xi_i)P_{pub} + \sum_1^n PSK_i \end{aligned}. \tag{17}$$

In this way, the sensor and CA are mutually authenticated. As for PC, necessary information are allocated by remote CA to help build the secure data transmission channel. Thus CA computes

$$\begin{cases} \Psi_i = s\kappa_i\mathcal{R}_i = \xi_i\kappa_i P_{pub} \\ \Upsilon_i = k_i P_{pub} = k_i sP \end{cases} \tag{18}$$

and send to PC.

At this point, the sensitive medical data $\mathcal{M}_i$ from sensor i is delivered as

$$\left\langle \mathcal{R}_i, TS, Enc_{H_3(\Psi_i)}[\mathcal{M}_i, TS], H_3(\mathcal{M}_i, TS, \mathcal{R}_i, \upsilon_i)k_i P \right\rangle. \tag{19}$$

The related verification can be done by PC as

$$\sum_1^n [H_3(\mathcal{M}_i, TS, \mathcal{R}_i, \upsilon_i)k_i P]\, s \stackrel{?}{=} \sum_1^n H_3(\mathcal{M}_i, TS, \mathcal{R}_i, \upsilon_i)\Upsilon_i \tag{20}$$

The batch verification process is as follow:

$$\begin{aligned} \sum_1^n [H_3(\mathcal{M}_i, TS, \mathcal{R}_i, \upsilon_i)k_i P]\, s &= \sum_1^n H_3(\mathcal{M}_i, TS, \mathcal{R}_i, \upsilon_i)k_i sP \\ &= \sum_1^n H_3(\mathcal{M}_i, TS, \mathcal{R}_i, \upsilon_i)[k_i sP]. \\ &= \sum_1^n H_3(\mathcal{M}_i, TS, \mathcal{R}_i, \upsilon_i)\Upsilon_i \end{aligned} \tag{21}$$

Sensor revocation

If expired or illegal sensors detected, the relevant acknowledgment message should be sent to the law enforcement agency. After approval, the PC will revoke the sensors by deleting the stored Ψ_i and Υ_i from its storage. The revocation can be done in this way.

Sensor group key distribution

In this subsection the sensor group key distribution scheme is presented, where all the participating sensors will cooperate with each other as shown in Fig. 4. The detailed steps are presented as follows:

We assume there are n legitimate sensor in PC's effective range. At first, all the sensors ($i \in [1, n]$) randomly generates its own γ_i and computes

$$\begin{cases} \mathcal{W}_i = \gamma_i P_{pub}. \\ z_i = H_1(\gamma_i, \kappa_i) \end{cases} \tag{22}$$

Then $\langle z_i, \mathcal{W}_i, H(\mathcal{W}_i)\rangle ((i \in [1, n])$ is broadcast to all. All the n sensors can be informed of the rest $n-1$ messages.

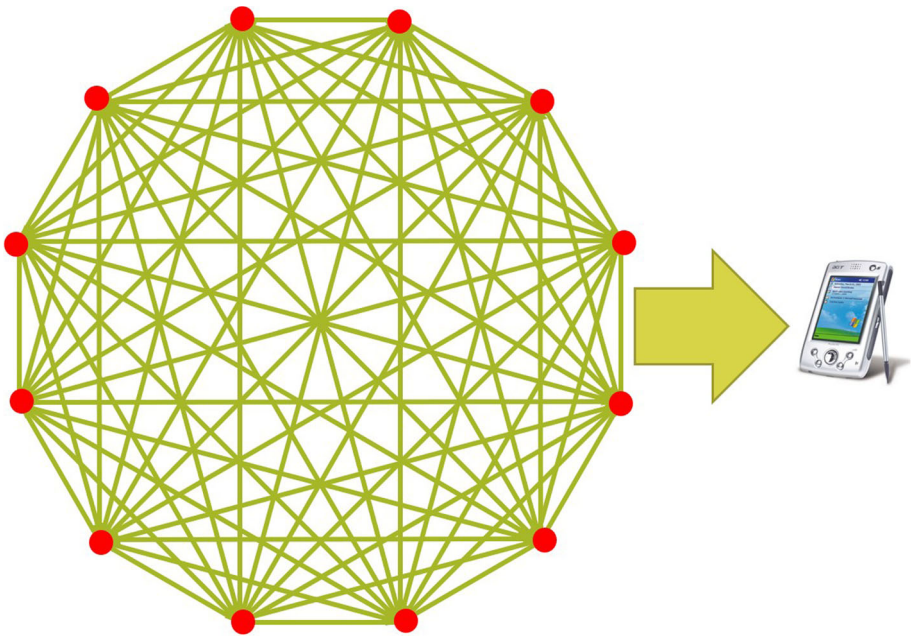

Fig. 4 Sensor Communicating Structure

According to the value of z_i, the sensor i could sort the received message. Then the sequence of

$$\langle z_1, ..., z_{i-1}, z_i, z_{i+1}, ..., z_n \rangle . \tag{23}$$

is generated. Each sensor listed in this sequence computes

$$\mathbb{F}_i = \gamma_i(\mathcal{W}_{i-1} - \mathcal{W}_{i+1}), \tag{24}$$

where $\mathcal{W}_{i-1}$ and $\mathcal{W}_{i+1}$ refers to the values from sensor i's neighbors, that is, sensor $i-1$ and sensor $i+1$. In this way, all the n sensors acquire $\mathbb{F}_i$ and then broadcast $\langle \mathbb{I}, \mathbb{F}_i, H_2(\mathbb{I}, \mathbb{F}_i) \rangle$ to all, where $\mathbb{I}$ is the sequence number of sensors in $\langle z_1, ..., z_{i-1}, z_i, z_{i+1}, ..., z_n \rangle$ ($\mathbb{I} \in [1, n]$) The sensor cooperation procedure is shown in Fig. 5.

In this way, each sensor could finally received $n-1$ requests. After checking the validity of the hashed value $H_2(\mathbb{I}, \mathbb{F}_i)$, sensor i will combine all the values together in the way as follows

$$\begin{aligned} \mathcal{Y} &= \mathbb{F}_1 + 2\mathbb{F}_2 + , ..., + i\mathbb{F}_i + , ..., + n\mathbb{F}_n + H_3(\mathcal{W}_1, ..., \mathcal{W}_n)P \\ &= \sum_1^n i\mathbb{F}_i + H_3(\mathcal{W}_1, ..., \mathcal{W}_n)P \\ &= \sum_1^n i[\gamma_{i-1}\gamma_i - \gamma_i\gamma_{i+1}] P_{pub} + H_3(\mathcal{W}_1, ..., \mathcal{W}_n)P \\ &= \sum_1^n \gamma_i\gamma_{i+1} P_{pub} + H_3(\mathcal{W}_1, ..., \mathcal{W}_n)P \end{aligned} , \tag{25}$$

where $\mathcal{Y}$ is defined as the intermediate key. In this way, all the sensors acquire the same $\mathcal{Y}$. As we previous introduced, PC randomly choose ω and delivered ωP_{pub} to all the sensors i first. Hence the final group key $\mathcal{K}$ is achieved by combing $\mathcal{Y}$ with ωP generated by PC. That is,

$$\begin{aligned} \mathcal{K} &= \mathcal{Y} + \omega P_{pub} \\ &= \left(\sum_1^n \gamma_i\gamma_{i+1} + \omega\right) P_{pub} + H_3(\mathcal{W}_1, ..., \mathcal{W}_n)P. \end{aligned} \tag{26}$$

Security analysis

In this section, we briefly describe the security properties of the proposed authentication scheme.

Certificateless authentication

As illustrated above, certificateless key distribution design is adopted in our scheme. That is, the CA only generates part of the secret for each sensors. Hence the key escrow problem can be addressed. That is, during the

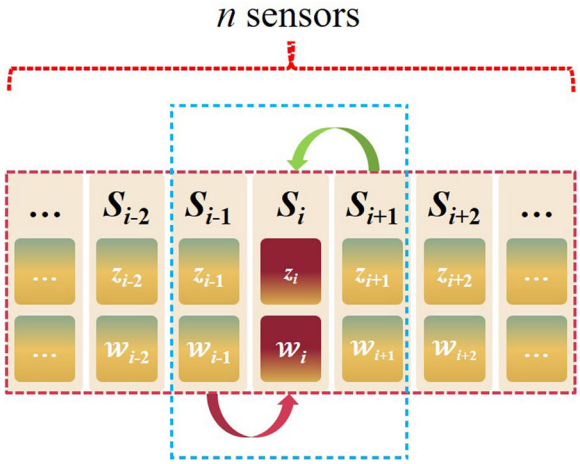

Fig. 5 Sensor Association

Table 2 Notations

Scheme	MLAP (Shen et al. 2018)	ATCC (Jiang et al. 2017)	HAKE (Drira et al. 2012)	Our Scheme
Unforgeability	√	√	√	√
Replay Attack Resistance	√	√	√	√
Identity Privacy Preservation	×	√	√	√
Session Key Establishment	√	√	√	√
Certificateless Authentication	√	×	×	√

authentication phase, both HC and PC have zero knowledge on the self-generated random partial secret key in the sensor side. In this way, impersonation attack on specific sensor cannot pass the validation. The generated key is not revealed to PC during the whole process. Hence, the compromising of PC will not brings negative effect to the whole WBAN system. In this way, the certificateless authentication property is provided.

Mutual authentication

Our scheme deploys the proper authenticating strategies, which is able to provide mutual authentication property between the remote CA and sensors. Note that only two communication rounds are required during our mutual authentication process. Moreover, the batch authentication on multiple sensors is also available, which provides new prospect for practical implementation of WBANs.

Sensor anonymity & conditional privacy

In our design, instead of using the device's real identity, we apply the self-generated anonymous identity, which also combines the stored static identity information Λ_i. Hence illegal tracing towards certain sensor can be prevented. Moreover, the real identity of the sensor can be revealed if abnormal behavior is detected under extreme situations. Hence the accountability is presented.

Resistance to mITM attack

In the proposed scheme, the hash function is utilized in the whole authentication session with the purpose of resisting the Man-In-The-Middle attack. The MITM attack is conducted by modifying the legitimate messages without being detected. In our design, the receiver side will check the validity upon receiving every message. With the adopted hash function for message confidentiality preservation, the MITM attack can be prevented.

Resistance to replay attack

As mentioned above, the pseudo-random value generator is adopted in both HC and sensor side, which could guarantee the resistance to replay attack. In this way, the reusing on the previously acquired information can not pass the current authentication session. On the other hand, each transmitted packet set contain obvious time-related information (time-stamp) revealing precise time sequence.

Cooperative sensor key establishment

In our scheme, the sensors group key is cooperatively generated by all the participating sensors. Note that neither CA nor PC has full control of the group key generation.

Comparison on security properties

In this section, we present the comparison in terms of the crucial security properties for WBANs authentication scenarios. Our WBAN authentication design is compared with the state-of-the-art WBAN authentication and key agreement schemes including MLAP (Shen et al. 2018), ATCC (Jiang et al. 2017), and HAKE (Drira et al. 2012) with the aim of demonstrating its superiority on security. The security comparison results are presented in Table 2, showing that the proposed scheme could satisfy all the desired security requirements.

Conclusion

In this paper, an efficient cloud-assisted pairing-free grouping authentication scheme in cloud-assisted WBANs is presented. In our design, the sensor anonymity is provided during the whole communication. Moreover, the cooperative sensor association mechanism is given, where the sensor group key is generated by the inter-communication between the legitimate participating WBAN sensors. The proposed scheme could satisfy desired security properties and provide resistance to major security attacks.

Acknowledgements

Not applicable

Funding

Not applicable

Availability of data and materials

All data generated or analysed during this study are included in this published article and its supplementary information files.

Author details

[1] Department of Global Business, Gachon University, 1342 Seongnam-daero, 13120 Sujeong-gu, Seongnam-si, Gyeonggi-do, Korea. [2] Department of Computer Engineering, Chosun University, 309 Pilmun-daero, 61452 Dong-gu, Gwangju, Korea.

Received: 6 August 2020 Accepted: 13 September 2020
Published online: 03 November 2020

References

Al-Riyami S, Paterson K (2003) Certificateless public key cryptography. In: Proc. of Advances in Cryptology-ASIACRYPT 2003. Springer Berlin Heidelberg, Berlin. pp 452–473

Anjum M, Wang H, Fang H (2020) Prospects of 60 ghz mmwave wban: A phy-mac joint approach. IEEE Trans Veh Technol 69(6):6153–6164

Drira W, Éric Renault, Zeghlache D (2012) A hybrid authentication and key establishment scheme for wban. In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. pp 78–83

He D, Zeadally S, Kumar N, Lee J-H (2017) Anonymous authentication for wireless body area networks with provable security. IEEE Syst J 11(4):2590–2601

Horn G, Preneel B (1998) Authentication and payment in future mobile systems. In: European Symposium on Research in Computer Security. Springer Berlin Heidelberg, Berlin, Heidelberg. pp 277–293

Hu C, Li H, Huo Y, Xiang T, Liao X (2016) Secure and efficient data communication protocol for wireless body area networks. IEEE Trans Multi-Scale Comput Syst 2(2):94–107

Huang X, Wu Y, Ke F, Liu K, Ding Y (2020) An energy-efficient and reliable scheduling strategy for dynamic wbans with channel periodicity exploitation. IEEE Sensors J 20(5):2812–2824

Ji S, Gui Z, Zhou T, Yan H, Shen J (2018) An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services. IEEE Access 6:69603–69611

Jiang Q, Kumar N, Ma J, Shen J, He D, Chilamkurti N (2017) A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks. Int J Netw Manag 27(3):1937

Li F, Han Y, Jin C (2018) Cost-effective and anonymous access control for wireless body area networks. IEEE Syst J 12(1):747–758

Li F, Hong J (2016) Efficient certificateless access control for wireless body area networks. IEEE Sensors J 16(13):5389–5396

Li X, Wang L (2012) A Rapid Certification Protocol from Bilinear Pairings for Vehicular Ad Hoc Networks. In: Proc. of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, Liverpool. pp 890–895

Liu C, Liu H, Cong Y, Li P, Mao Z, Zhang H (2020) Throughput maximization by time switching in multipoint wban with fairness consideration. IEEE Access 8:107661–107668

Liu J, Zhang Z, Chen X, Kwak K (2014) Certificateless remote anonymous authentication schemes for wirelessbody area networks. IEEE Trans Parallel Distrib Syst 25(2):332–342

Sambandam P, Kanagasabai M, Natarajan R, Alsath M, Palaniswamy S (2020) Miniaturized button-like wban antenna for off-body communication. IEEE Trans Antennas Propag 68(7):5228–5235

Shen J, Chang S, Shen J, Liu Q, Sun X (2018) A lightweight multi-layer authentication protocol for wireless body area networks. Futur Gener Comput Syst 78:956–963

Shen J, Tan H, Ren Y, Liu Q, Wang B (2016) A practical rfid grouping authentication protocol in multiple-tag arrangement with adequate security assurance. In: 2016 18th International Conference on Advanced Communication Technology (ICACT). IEEE, Pyeongchang. pp 693–699

Shen J, Tan H, Zhang Y, Sun X, Xiang Y (2017) A new lightweight rfid grouping authentication protocol for multiple tags in mobile environment. Multimed Tools Appl 76(21):22761–22783

Wang H (2015) Identity-based distributed provable data possession in multicloud storage. IEEE Trans Serv Comput 8(2):328–340

Xiong H (2014) Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Trans Inf Forensic Secur 9(12):2327–2339

Xiong H, Qin Z (2015) Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE Trans Inf Forensic Secur 10:1442–1455

Yang J-H, Chang C-C (2009) An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Comput Secur 28(3):138–143

Yuan X, Tian H, Wang H, Su H, Liu J, Taherkordi A (2020) Edge-enabled wbans for efficient qos provisioning healthcare monitoring: A two-stage potential game-based computation offloading strategy. IEEE Access 8:92718–92730

Zhang L, Liu J, Sun R (2013) An efficient and lightweight certificateless authentication protocol for wireless body area networks. In: 2013 5th International Conference on Intelligent Networking and Collaborative Systems. IEEE, Xi'an. pp 637–639

Zhang X, Huang C, Zhang Y, Zhang J, Gong J (2020) Ldvas: Lattice-based designated verifier auditing scheme for electronic medical data in cloud-assisted wbans. IEEE Access 8:54402–54414

Zhou T, Shen J, Li X, Wang C, Tan H (2020) Logarithmic encryption scheme for cyber-physical systems employing fibonacci q-matrix. Futur Gener Comput Syst 108:1307–1313

Publisher's Note