Group authentication and key distribution for sensors in wireless body area network

Yong Ding¹,², Hui Xu³, Meng Zhao¹, Hai Liang¹ and Yujue Wang⁴

Abstract
Wireless body area network can be employed to collect patient’s electronic health data. To guarantee the reliability and confidentiality of the collected data, secure data transmission in wireless body area network is required. In wireless body area network, a mutual authentication process has to be carried out between the controller and sensors to ensure their legitimacy, and a key distribution mechanism is required to secure communication after successful mutual authentication. Li et al. proposed a cryptographic solution, which allows group device pairing authentication and key agreement but has low authentication efficiency and key leakage problems. To address these issues, a group authentication and key distribution scheme is proposed in this article. It enables effectively mutual authentication between controller and sensors, supports all signatures of sensors in the group to be checked by the controller through aggregation verification to achieve efficient authentication, and allows key distribution during authentication to improve the computation efficiency. Security analysis indicates that the proposed scheme enjoys existentially unforgeability, and theoretical and experimental comparison demonstrates its practicality in terms of computation and communication cost.

Keywords
Wireless body area network, identity authentication, aggregate validation, key exchange, unforgeability

Date received: 4 February 2021; accepted: 15 August 2021

Handling Editor: Benny Lo

Introduction
Wireless body area network (WBAN) is an important branch of the Internet of things (IoT).¹ With the development of the sensor technology, WBAN has great practical significance in remote medicine detection, health care and service,² and so on. WBAN is mainly composed of sensors equipped or implanted into a human body. Sensor nodes can sense and collect physiological data of a human body as well as surrounding environmental information.³ The collected data can be sent to the controller with powerful storage and computing capacities. The data are forwarded to the remote medicine data center for processing and analysis. According to these data, the doctor would be able to make treatment plan. For example, wearable pulse oximetry sensors can be used by patients with vascular disease to measure blood oxygen saturation.⁴ For

¹Guangxi Key Laboratory of Cryptography and Information Security, School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China
²Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen, China
³School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, China
⁴Hangzhou Innovation Institute, Beihang University, Hangzhou, China

Corresponding author:
Meng Zhao, Guangxi Key Laboratory of Cryptography and Information Security, School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China.
Email: mzhao@guet.edu.cn
emergency case detected by sensors, relevant measures can be taken to relieve the suffering of patients, for example, implanted blood glucose sensors can be employed to analyze the blood glucose index of the patient in real-time to trigger the insulin pump for insulin injection when necessary.

While WBAN brings convenience to patients, some security and privacy issues are also arising. The collected data may contain the private information of users, which are at risk of being leaked and tampered during transmission. Therefore, it is extremely important to protect the security and privacy of users' sensitive data. Due to the openness of the transmission channel, attackers can affect the accuracy of data by replaying, forgery, and interference, which may lead to misdiagnosis of patients, slow down the recovery speed, and even worsen the condition.

For preventing malicious nodes from joining WBAN, the entities authentication is an effective way to ensure the authenticity of entities. Since there are a lot of sensors in WBAN, it is necessary to use group authentication to improve the efficiency of one-by-one authentication. Li et al. proposed a group device pairing authentication method based on secure sensor association and key management. All sensor nodes should be authenticated not only by the controller, but also by each sensor in the same group. The system assigns a serial number to each node in advance, so that the authentication message and group key can be computed using the parameters of adjacent nodes in the authentication and key negotiation phase. Note that it is difficult to ensure the true identity of each node due to the authentication process mainly depends on the verification of the group size. Thus, malicious nodes can impersonate honest nodes to participate in the authentication process and key negotiation without being detected.

Our contributions
This article proposes a group authentication and key distribution scheme, which supports mutual authentication between controller and sensors. The main contributions of this article are summarized as follows:

- The controller in our scheme is able to aggregate the signatures of sensor nodes, which improves the authentication efficiency. It is especially suitable for WBAN with a large number of sensor nodes.
- Secure distribution of session key can be accomplished during authentication. No additional communication for key agreement is required after authentication.
- The proposed protocol can prevent malicious entities from joining the system, ensure the authenticity of sensor nodes, and guarantee the confidentiality of the session key. It can also resist traditional attacks.
- Theoretical comparison and experimental results show that our scheme has higher transmission and communication efficiency than existing schemes.

Compared with the preliminary version, this article provides a secure session key distribution method during authentication, security model, security proof, and experimental results of the proposed scheme.

Article organization
The rest of the article is arranged as follows. Section “Related works” reviews related works. Section “System model and security requirements” presents system model and security requirements. Section “Identity based aggregate authentication” provides the proposed scheme. Sections “Security analysis” and “Performance analysis” show the security analysis and the performance analysis, respectively. Finally, section “Conclusion” concludes the article.

Related works
To address the key management issue against malicious key generation center in public key cryptosystems, many certificateless signature schemes have been proposed and proved unforgeable under adaptively chosen message attacks. Due to the key escrow problem, Mwitende et al. proposed a pairing-based certificateless authentication scheme. Restricted by the computing and storage resources of entities in WBAN, Huang et al. presented an identity-based signature scheme suitable for sensor networks, which reduces the online computation cost and resists replay attacks effectively. Xu et al. proposed a lightweight anonymous authentication scheme with only hash operations and XOR operations. Thumbur et al. presented an efficient certificateless signature scheme for resource-constrained devices using lightweight computing operations. However, Xu et al. found that Thumbur et al.'s scheme cannot resist signature forgery attack and proposed an improved scheme with high efficiency.

In order to achieve efficient and secure data transmission, many schemes have been proposed to support mutual authentication and session key establishment between sensor nodes and controller in the form of groups. Keoh et al. presented a sensor association scheme based on synchronous LED flashing mode, where the controller and each sensor need to be authenticated by digital signatures and then the user verifies the flashing result of LEDs. Therefore, multiple associations between sensors and the controller would bring
more time costs. Li et al. proposed a scheme of sensor association and key management, which supports mutual authentication of group membership through group device pairing. Shen et al. proposed a lightweight multi-layer authentication and secure session key generation scheme. This scheme allows one-to-many authentication and group key to be established between the controller and each sensor node, which has the advantage of efficient authentication. Liu et al. noticed that Shen et al.’s scheme is vulnerable to impersonation attacks and proposed an improved two-layer authentication scheme. Tan and Chung proposed a group key management scheme with cooperative sensors association, which utilizes the Chinese remainder theorem to realize group key management and supports batch key update. Shu et al. proposed aggregated signatures for WBAN applications, whose computational efficiency is independent of the number of signers. The secret sharing is used to realize multi-group key establishment protocol, where users only need to keep one share to recover multiple group keys. When a group member leaves or joins, there is no need to rebuild the key.

Secure key distribution is the basic requirement for achieving secure data transmission. The scheme proposed by Kuo et al. can send the key material to designated sensors without being eavesdropped, where the closed Faraday-cage is used as a secure channel for key distribution. The cage not only prevents the joining of external malicious sensor nodes but also increases the difficulty of new nodes joining. Bennmansour et al. designed a secure key management scheme to improve the system security, which enables all information can be communicated in ciphertext format. Owing to the limited sensor resources, most WBAN systems have the structure of distributed perception acquisition and centralized processing mechanism. Besides, WBAN has small network scale, and there is no necessity to communicate with sensor nodes. Thus, the star topology structure is often adopted in the distributed acquisition phase. In Li et al.’s scheme, WBAN is divided into two layers, where sensors act as the second layer to send the collected data to the central node through the first layer with powerful storage, calculation, and communication capabilities. Li et al.’s scheme also divides WBAN into two layers, and the data collected by sensor nodes in the second layer is transmitted to users through controllers in the first layer.

When the decryption key is exposed, the decryption functionality of the key needs to be revoked. Almuhaideb and Alqudaihi introduced the user revocation function to the factor authentication scheme. Xiong and Qin proposed a certificate-free remote anonymous authentication scheme supporting scalable revocation, which is suitable to the large-scale WBAN. However, Shim pointed out Xiong and Qin’s scheme cannot resist forgery attacks. Also, it requires resource-intensive bilinear pairings, which is not suitable for WBAN applications. Shen et al. improved the efficiency of the schemes by Li et al. and Xiong and Qin. Besides, Cai and Niu proposed a lightweight data fusion method to solve the problems of long data transmission time and low efficiency. To make the authentication process more efficient and secure, the verification process needs to be simplified to reduce the number of interactions between the sensor and the controller. Therefore, Abro et al. proposed an authentication scheme based on ElGamal, which can reduce communication overhead and resist man-in-the-middle attacks. Jegadeesan et al. and Wang et al. also proposed an efficient and secure mutual authentication scheme for privacy protection, which can reduce the cost of computation and communication, and introduces time stamp to prevent replay attacks.

**System model and security requirements**

**System model**

As shown in Figure 1, a WBAN system consists of two types of entities, namely, sensors deployed on and around users and the controller for data collection. There is a private key generator (PKG) to initialize the system and issue private keys for all entities.

The sensors can collect physiological data of users and information of surrounding environment. Limited by the storage space of sensors, the collected data need to be transmitted to the controller for storing and computing. Before collection data, sensors and the controller need to perform mutual authentication to confirm their authenticity. When the controller is legal, the sensor sends the collected data to the controller. During the mutual authentication procedure, the controller is able to securely distribute a session key to the sensors in a group, so that all sensors in the same group can share the same session key.

**Security requirements**

In WBAN, it is important to prevent malicious sensors and controller from impersonating honest entities and eavesdropping sensitive data during data collection and transmission. Therefore, a secure WBAN authentication and key distribution scheme supporting aggregate verification needs to meet the following security requirements.

**Authenticity of controller:** The signature issued by the legal controller can be successfully verified by sensor nodes in a group. A malicious attacker cannot forge a signature to pass the verification conditions.
Authenticity of sensors: The signatures issued by legitimate sensors in a group can be successfully verified by the controller by means of aggregation. Malicious nodes cannot impersonate legitimate sensor nodes to pass the authentication conditions, so as to join the group communication.

Confidentiality of session key: When the controller and sensors in a group perform mutual authentication, the session key can be securely shared.

Efficiency: As the number of sensor nodes increases, the computations during authentication will be increased at both sides of the controller and sensors. Therefore, the WBAN system should support aggregate verification to improve the authentication efficiency.

Security model

The security model for the unforgeability of sensor’s identity in WABN is defined by the following game between a probabilistic polynomial time adversary \(A_1\) and challenger.

- The challenger runs the initialization algorithm and gives the system public parameter \(\text{param}\) to \(A_1\).
- When \(A_1\) issues private key generation query for an entity \(u\), the challenger runs the key generation algorithm to obtain the corresponding private key \(sk_u\) and sends it to \(A_1\).
- When \(A_1\) issues group registration query for an entity \(u\), the challenger runs the group registration algorithm and returns group key \(t\) to \(A_1\).
- When \(A_1\) issues signature generation query on some message \(m\) with regard to identity \(u\), the challenger returns signature \(\sigma_1\).
- Finally, \(A_1\) outputs \((u', m', \sigma_1')\), where \(\sigma_1'\) is a signature of message \(m'\) for entity \(u'\).

Adversary \(A_1\) wins the game if \(u'\) has not been queried for the private key and \(m'\) has not been queried for the signature with regard to identity \(u'\). The adversary’s advantage \(Adv\) is defined as the probability of winning the game. If the probability of \(A_1\) outputs a valid signature \(\sigma_1'\) of identity \(u'\) in polynomial time \(t\) is at most \(\varepsilon_1\) after the adversary \(A_1\) makes no more than \(q_{s}\) key generation queries, \(q_{g}\) group registration queries and \(q_{s}\) signing queries, then the scheme is said to be \((\varepsilon_1, t)\)-secure under \(A_1\) attack in the sense of existentially unforgeable against adaptively chosen message attacks.

The security model for the unforgeability of controller’s identity in WABN is defined by the following game between a probabilistic polynomial time adversary \(A_2\) and challenger.

- The challenger runs the initialization algorithm and gives the system public parameter \(\text{param}\) to \(A_2\).
- When \(A_2\) issues private key generation query for an entity \(u_0\), the challenger runs the key generation algorithm to obtain the corresponding private key \(sk_{u_0}\) and sends it to \(A_2\).
- When \(A_2\) issues signature generation query on some message \(m\) with regard to identity \(u_0\), the challenger returns signature \(\sigma_2\).
- Finally, \(A_2\) outputs \((u_0', m', \sigma_2')\), where \(\sigma_2'\) is a signature of message \(m'\) for entity \(u_0'\).

Adversary \(A_2\) wins the game if \(u_0'\) has not been queried for the private key and \(m'\) has not been queried for the signature with regard to identity \(u_0'\). If the
probability of \( A_2 \) outputs a valid signature \( s_{20} \) of identity \( u_0 \) in polynomial time \( t \) is at most \( e_2 \) after the adversary \( A_2 \) makes no more than \( q_k \) key generation queries and \( q_s \) signing queries, then the scheme is said to be \((e_2, t)\)-secure under \( A_2 \) attack in the sense of existentially unforgeable against adaptively chosen message attacks.

**Identity-based aggregate authentication scheme**

The security of the proposed scheme depends on the following discrete logarithm (DLog) problem.

Discrete logarithm problem: Let \( \mathbb{G} \) be a cyclic group of prime-order \( q \) with generator \( g \). Given an element \( g^x \in \mathbb{G} \) where \( x \in \mathbb{Z}_q \), compute \( x \). If no algorithm with running time at most \( t \) can solve the DLog problem with probability at least \( \epsilon \), it is said that the \((\epsilon, t)\)-DLog assumption holds in cyclic group \( \mathbb{G} \).

**Scheme design**

The controller performs mutual authentication with sensor nodes in a group, where the validity of each entity’s identity can be checked through aggregate authentication. Figure 2 shows the authentication process of the proposed scheme.

**Initialization.** PKG chooses a cyclic group \( \mathbb{G} \) of order \( q \), where \( q \) is a large prime and \( g \) is a generator of \( \mathbb{G} \). PKG randomly chooses \( w \in \mathbb{Z}_q^* \), computes \( W = g^w \), and picks a cryptographic hash function \( H: \{0, 1\}^* \rightarrow \mathbb{Z}_q^* \). The system public parameter is \( \text{param} = (\mathbb{G}, q, g, W, H) \), and the master key is \( \text{msk} = w \).

**KeyGen.** PKG chooses a random integer \( r_j \in \mathbb{Z}_q^* \) for each entity \( u_j \) where \( u_0 \) is the controller and other \( u_j \) represents sensor nodes. PKG computes

\[
R_j = g^{r_j}, \quad s_j = r_j + H(R_j \| u_j)w \mod q
\]

and gives the private key \((R_j, s_j)\) to entity \( u_j \) through a secure channel.

**Group registration.** The controller chooses \( l \) group keys \( t_1, t_2, \ldots, t_l \in \mathbb{Z}_q^* \) corresponding to groups \( S_i(i = 1, 2, \ldots, l) \). When each sensor node \( u_j(j = 1, 2, \ldots, n) \) performs group registration, the controller specifies a group \( S_i \) for it and returns the corresponding group key \( t_i \).

**Group authentication request.** When the controller communicates with group \( S_i \), it needs to mutually authenticate with all nodes in such group. The controller sets

\[
S_i = \{u_\ell : 1 \leq \ell \leq \lambda_i\}
\]
where $\lambda_i$ denotes the number of sensor nodes in the group $S_i$. The controller randomly chooses $y_i, v_i, k_i \in \mathbb{Z}_q^*$ for group $S_i$, and computes

$$Y_i = g^{y_i}$$

and

$$f_i(x) = \prod_{\ell = 1}^{\lambda_i} \left( x - H(u_\ell, v_\ell, t_\ell) \right) + k_i = \sum_{\ell = 0}^{\lambda_i} a_\ell x^\ell \mod q$$

where $a_0 = 1$. The controller constructs a string

$$m_i = a_0 \parallel a_1 \parallel \cdots \parallel a_{\lambda_i - 1}$$

computes

$$h_i = H(Y_i \parallel R_0 \parallel m_i \parallel S_i)$$

and broadcasts signature $(R_0, Y_i, z_i)$, identity $u_0$, and tuple $(v_i, m_i)$ to all sensor nodes in group $S_i$.

Sensor verification and response. After receiving the signature and tuple, each sensor node in group $S_i$ computes $h_i = H(Y_i \parallel R_0 \parallel m_i \parallel S_i)$ and checks the following equality

$$g^{z_i} = Y_i R_0^h W^{hH(R_0||u_0)}$$

If equation (1) does not hold, the authentication request from the controller will be rejected. Otherwise, each sensor node $u_\ell$ reconstructs $f_i(x)$ according to $m_i$ and computes

$$k_i = f_i(H(u_\ell, v_\ell, t_\ell)) \mod q$$

as session key for secure communication. Then each sensor node $u_\ell$ chooses a random integer $y_\ell \in \mathbb{Z}_q^*$, computes

$$Y_\ell = g^{y_\ell}$$

$$h_\ell = H(Y_\ell \parallel R_\ell \parallel H(k_i) \parallel S_i)$$

and

$$z_\ell = y_\ell + h_\ell s_\ell \mod q$$

and sends the signature $(R_\ell, Y_\ell, z_\ell)$ and identity $u_\ell$ to the controller.

Aggregate verification. After the controller receives the signatures and identities from a group $S_i$ of sensor nodes, it performs aggregate verification as follows. The controller computes

$$z = \sum_{\ell = 1}^{\lambda_i} z_\ell \mod q$$

$$Y = \prod_{\ell = 1}^{\lambda_i} Y_\ell$$

and $h_\ell$ of each sensor node $u_\ell \in S_i$, and verifies the following equation

$$g^{z_i} = Y \left( \prod_{\ell = 1}^{\lambda_i} R_\ell^h \right) W^{\sum_{\ell = 1}^{\lambda_i} h_\ell H(R_\ell||u_\ell)}$$

(2)

If equation (2) does not hold, the authentication responses from sensors will be rejected. Otherwise, the controller is able to communicate with sensor nodes in group $S_i$ via session key $k_i$.

Correctness verification

Theorem 1. The proposed authentication scheme for WBAN is correct.

Proof. To prove the correctness of the proposed scheme, we only need to show both equations (1) and (2) hold.

First, each sensor node $u_\ell$ in the group $S_i$ can verify the authenticity of the controller by checking equation (1), which is shown as follows

$$Y_i R_0^h W^{hH(R_0||u_0)} = g^{y_i} g^{\ell_i h_i} g^{w_i H(R_0||u_0)} = g^{y_i + \ell_i h_i} = g^{z_i}$$

Second, the controller can verify the authenticity of all sensor nodes in group $S_i$ by checking equation (2), which is shown as follows

$$Y \left( \prod_{\ell = 1}^{\lambda_i} R_\ell^h \right) W^{\sum_{\ell = 1}^{\lambda_i} h_\ell H(R_\ell||u_\ell)} = g^{\sum_{\ell = 1}^{\lambda_i} y_\ell} g^{\sum_{\ell = 1}^{\lambda_i} \ell_i h_i} g^{\sum_{\ell = 1}^{\lambda_i} h_\ell H(R_\ell||u_\ell)} = g^{\sum_{\ell = 1}^{\lambda_i} y_\ell + \ell_i h_i + w_i H(R_\ell||u_\ell)} = g^{z_i}$$

Therefore, the signatures generated by the controller and all sensor nodes in a group can be successfully verified. Thus, the proposed authentication scheme for WBAN is correct. \qed
Security analysis

This section analyzes the security of the proposed scheme.

Theorem 2. The proposed scheme can ensure the authenticity of sensors during the authentication process. That is, the proposed scheme is \((\varepsilon_1, t')\)-secure in the sense of existentially unforgeability against adaptively chosen message attacks under the \((e_1', t')\)-DLog assumption, where

\[
\varepsilon_1' = \left(1 - \frac{q_h(q_k + q_r + q_t)}{q}\right)\left(1 - \frac{1}{q}\right)^3 \varepsilon_1
\]

\[t' = t + O(q_k + q_r)e\]

and \(q_k, q_r, q_t, q_h\) are the number of key generation, group registration, signing, and hash queries that the adversary \(A_1\) is allowed to make, respectively, and \(e\) is the time for an exponentiation operation.

Proof. Suppose an adversary \(A_1\) can forge a valid signature of an entity \(u\). We construct an algorithm \(B_1\) to solve the DLog problem using \(A_1\). \(B_1\) is given a cyclic group \(G\) with generator \(g\) and prime-order \(q\), and an element \(a \in G\). The goal of \(B_1\) is to find \(\alpha \in \mathbb{Z}_q\) so that \(g^\alpha = A\). The following proof for Theorem 2 follows the standard framework established in Liu et al.'s scheme.

Initialization: \(B_1\) selects a hash function \(H: \{0, 1\} \rightarrow \mathbb{Z}_q\). \(B_1\) sets \(W = A\), and sends the public parameter \(\text{param} = (G, g, q, W, H)\) to \(A_1\).

Key generation queries: When \(A_1\) queries the KeyGen for identity \(u\), \(B_1\) performs the following simulation operation. It first randomly selects \(a, b \in \mathbb{Z}_q\), and then calculates \(R = W^ag^b\). \(B_1\) sends \((R, s)\) to \(A_1\) and stores \((R, s, H(R \parallel u), u)\) in list \(L_1\).

Group registration queries: When \(A_1\) queries the Group registration for a group \(S\), \(B_1\) randomly selects \(t \in \mathbb{Z}_q\) as the group key and sets it to the corresponding \(S\).

Hash queries: We consider the following cases.

- **Queries 1:** When \(A_1\) issues a query on \(H(u_i \parallel v_i \parallel t_i)\), \(B_1\) checks whether \(H(u_i \parallel v_i \parallel t_i)\) is in list \(L_2\). If not, \(B_1\) selects \(h_i \in \mathbb{Z}_q\), sets \(h_i = H(u_i \parallel v_i \parallel t_i)\) and stores \((u_i, v_i, t_i, h_i)\) in the list \(L_2\). \(B_1\) gives \(h_i\) to \(A_1\).

- **Queries 2:** When \(A_1\) issues a query on \(H(h_k)\), \(B_1\) checks whether \(H(h_k)\) is in list \(L_3\). If not, \(B_1\) selects \(h \in \mathbb{Z}_q\), sets \(h = H(h_k)\) and stores \((k, h)\) in the list \(L_3\). \(B_1\) gives \(h\) to \(A_1\).

- **Queries 3:** When \(A_1\) issues a query on \(H(Y_i \parallel R_i \parallel H(h_k) \parallel S_i)\), if the query tuple does not exist in list \(L_4\), then \(B_1\) selects \(h_i \in \mathbb{Z}_q\), sets \(H(Y_i \parallel R_i \parallel H(h_k) \parallel S_i) = h_i\) and stores \((Y_i, R_i, H(h_k), S_i, h_i)\) in the list \(L_4\). \(B_1\) gives \(h_i\) to \(A_1\).

Signing queries: When \(A_1\) requests the signature of a sensor \(u_i\) in group \(S_i\), \(B_1\) first checks whether \(u_i\) has been queried for private key and the group key of group \(S_i\). If so, \(B_1\) retrieves \((R, s, H(R \parallel u), (u_i, v_i, t_i, h_i), (k, h))\), and \((Y_i, R_i, H(h_k), S_i, h_i)\) from \(L_1, L_2, L_3, \) and \(L_4\) respectively, and produces a signature \(\sigma_1\) accordingly. If not, \(B_1\) first invokes key generation query, group registration query, and hash query and then produces the signature.

Output: \(A_1\) outputs a forged signature \(\sigma_1' = (Y^*, R^*, z_1^*)\) about message \(m^*\) and identity \(u^*\). Repeat again, \(A_1\) outputs another two valid signatures \(\sigma_2^* = (Y^*, R^*, z_2^*)\) and \(\sigma_3^* = (Y^*, R^*, z_3^*)\). Let \(h_i^j = h_i^j(j = 1, 2, 3)\) represent the different outputs of the hash queries.

Note that \(z_i^* = y + h_i^j0 + h_i^j0wH(R^* \parallel u) \mod q\) for \(j = 1, 2, 3\), where \(y, r, w\) are not known by \(B_1\). Let \(Y = g^y, R = g^r\), and \(W = A = g^a\). As long as the above three linear equations are solved, \(B_1\) can get the value of \(\alpha\), which solves the given DLog problem instance.

Reduction analysis: If \(H(R \parallel u)\) assigned by the random oracle is inconsistent with that in \(L_1\), then the key generation queries simulation fails, and the probability is at most \(q_h/q\). Therefore, the simulation of a valid signature is successful \(q_k + q_r + q_t\) times with probability at least \(1 - (1 - (q_h/q)^q + q_r + q_t)/q\).

\[
(1 - \frac{q_h}{q})^q + q_r + q_t \geq 1 - \frac{q_h(q_k + q_r + q_t)}{q}
\]

In the hash queries, due to its ideal randomness, the hash query is always queried with a probability of \(1 - (1/q)\). \(B_1\) queries \(H(u_i \parallel v_i \parallel t_i)\) matches \(h_i\) in \(L_2\) with probability of \(1/q_h\). \(H(k, h)\) matches \(h\) in \(L_3\) with probability of \(1/q_h\). \(H(Y_i \parallel R_i \parallel H(k, h) \parallel S_i)\) matches \(h_1\) in \(L_4\) with probability of \(1/q_h\). Thus, the overall probability of success is

\[
\varepsilon_1' = \left(1 - \frac{q_h(q_k + q_r + q_t)}{q}\right)\left(1 - \frac{1}{q}\right)^3 \varepsilon_1
\]

The time complexity of \(B_1\) is determined by key generation queries and signing queries, which is

\[
t' = t + O(q_k + q_r)e.
\]

Theorem 3. The proposed scheme can ensure the authenticity of controller during the authentication process. That is, the proposed scheme is \((\varepsilon_2, t)\)-secure in the sense of existentially unforgeability against adaptively chosen message attacks under the \((e_2', t')\)-DLog assumption, where
\[w_2' = \left(1 - \frac{q_h(q_k + q_s)}{q}\right)^2 \left(1 - \frac{1}{q} \left(\frac{1}{q_h}\right)^e\right)^2 w_2\]
\[t' = t + O(q_k + q_s)\]

and \(q_h, q_s,\) and \(q_k\) are the number of key generation, signing, and hash queries that the adversary \(A_2\) is allowed to make, respectively, and \(e\) is the time for an exponentiation operation.

Proof: Suppose an adversary \(A_2\) can forge a valid signature of an entity \(u_0\). We construct an algorithm \(B_2\) to solve the DLog problem using \(A_2. B_2\) is given a cyclic group \(\mathbb{G}\) with generator \(g\) and prime order \(q\), and an element \(A \in \mathbb{G}\). The goal of \(B_2\) is to find \(\alpha \in \mathbb{Z}_q\) so that \(g^\alpha = A\).

Initialization: This phase directly follows from the Initialization of Theorem 2.

Key generation queries: This phase directly follows from the Key generation queries of Theorem 2.

Hash queries: We consider the following cases.

Queries 1: When \(A_2\) issues a query on \(H(Y_i \parallel R_0 \parallel m_i \parallel S_i)\), if the query tuple does not exist in \(L_3\), then \(B_2\) selects \(h_i \in \mathbb{Z}_q\), sets \(h_i = H(Y_i \parallel R_0 \parallel m_i \parallel S_i)\) and stores \((Y_i, R_0, m_i, h_i)\) in the list \(L_3\). \(B_2\) gives \(h_i\) to \(A_2\).

Queries 2: The hash queries here are consistent with the Queries 1 in Theorem 2.

Signing queries: When \(A_2\) requests the signature of identity \(u_0\) and message \(m_i\) to communicate with group \(S_i, B_2\) first checks whether the private key of \(u_0\) has been queried. If so, \(B_2\) retrieves \((R_0, s, H(R_0 \parallel u_0), u_0)\), \((Y_i, R_0, m_i, h_i)\), and \((u_i, v_i, t_i, h_i)\) from \(L_1, L_2,\) and \(L_3\), respectively, and generates the signature \(\sigma_2^*\) accordingly. If not, \(B_2\) first invokes key generation query on \(u_0\) and hash queries, and then produces the signature.

Output: \(A_2\) outputs a forged signature \(\sigma_2^* = (Y_i, R_0, z_2^*)\) about message \(m_i\) and identity \(u_0\).

Repeat again, \(A_2\) outputs another two valid signatures \(\sigma_2^* = (Y_i, R_0, z_2^*)\) and \(\sigma_2^* = (Y_i, R_0, z_2^*)\). Let \(h_i^{(j)} (j = 1, 2, 3)\) represent the different outputs of the hash queries.

Note that \(z_2^* = y + h_i^{(j)} r + h_i^{(j)} w H(R_0 \parallel u_0) \mod q\) for \(j = 1, 2, 3\), where \(y, r, w\) are not known by \(B_2\). Let \(Y = g^y, R_0 = g^m,\) and \(W = A = g^\alpha.\) As long as the above three linear equations are solved, \(B_2\) can get the value of \(\alpha\), which solves the given DLog problem instance.

Reduction analysis: If \(H(R_0 \parallel u_0)\) assigned by the random oracle is inconsistent with that in \(L_1\), then the key generation queries simulation fails, and the probability is at most \(q_h/q\). Therefore, the simulation of a valid signature is successful \(q_k + q_s\) times with probability at least \((1 - (q_h/q))^{q_k + q_s}\)
\[
\left(1 - \frac{q_h}{q}\right)^{q_k + q_s} \geq 1 - \frac{q_h(q_k + q_s)}{q}
\]

In the hash queries, due to its ideal randomness, the hash query is always queried with a probability of \(1 - (1/q)\). \(B_2\) guesses that \(H(Y_i \parallel R_0 \parallel m_i \parallel S_i)\) matches \(h_i\) in \(L_3\) with probability of \(1/q_h\), and \(H(u_i \parallel v_i \parallel t_i)\) matches \(h_i\) in \(L_2\) with probability of \(1/q_s\). Thus, the overall probability of success is
\[
w_2' = \left(1 - \frac{q_h(q_k + q_s)}{q}\right)^2 \left(1 - \frac{1}{q} \left(\frac{1}{q_h}\right)^e\right)^2 w_2
\]

The time complexity of \(B_2\) is determined by key generation queries and signing queries, which is \(t' = t + O(q_k + q_s e)\).

Theorem 4. The proposed scheme can guarantee the confidentiality of the session key, that is, only the legitimate controller and sensor nodes in the group can get the session key after authentication.

Proof: The session key \(k_i\) of the scheme is selected by the controller and used to construct polynomial \(f_i(x)\). All sensor nodes in the group can get the the group key \(k_i\) in the group registration phase, which can be used to recover \(k_i\). For recovering the session key \(k_i\), the sensor nodes have to conduct the verification procedure to confirm the authenticity of the controller. If the authentication request sent by the legitimate controller can be successfully verified by the sensor node in the group, the sensor nodes can obtain the session key \(k_i\) and then use it to communicate with the controller. The controller can performs aggregate authentication when it received all responses of sensors. Only when the verification is passed, \(k_i\) will be used as the communication key. Thus, the privacy and security of the session key can be guaranteed by the proposed scheme.

Replay attack. In the authentication phase of the proposed scheme, random numbers \((v_i, k)\) will be reselected in every authentication request. Therefore, the proposed scheme can effectively resist replay attacks.

Forward security. In the proposed scheme, the session key is randomly selected. Thus, if the adversary obtains a session key, it would be unable to deduce the session keys in previous stages. Therefore, the proposed scheme can ensure the forward security.

Table 1 shows the comparison of security property. All schemes except SCSLS [20] allow mutual authentication between sensors and the controller in the form of
group. The difference is that the controller in our scheme can perform aggregate authentication on all signatures of sensor nodes in the group, which improves the efficiency of authentication. Whereas the other authentication schemes do not support aggregation verification and require the members in the group to be authenticated one by one. Moreover, our scheme and the ones in Tan and Chung’s scheme and Huang et al.’s scheme support the distribution of the session key during authentication, while GDP and SCSLS require symmetric encryption to obtain the group key after authentication and then establish the session key. Thus, the solutions in GDP and SCSLS do not enjoy high efficiency in session key generation.

Moreover, GDP is vulnerable to replay attack and forgery attack, SCSLS cannot resist replay attacks, and Tan and Chung’s scheme and Huang et al.’s scheme cannot achieve forward security. It can be seen from the Table 1 that the proposed scheme has more security functionalities than the existing schemes.

Performance analysis

Efficiency analysis

This section compares the efficiency of the proposed scheme with existing ones in terms of computation costs at each stage. In Table 2, the exponentiation operation is represented as \( E \), the hash operation as \( H \), the bilinear pairing computation as \( B \), and the number of sensor nodes participating in authentication as \( n \).

As shown in Table 2, for the group authentication request generation phase, the computational complexity of our scheme and the ones in SCSLS and Huang et al.’s scheme are determined by the number of sensor nodes in the group, while the complexity in GDP and Tan and Chung’s scheme is independent of the number \( n \). Note that the computational complexity of our scheme is higher than that of SCSLS and Huang et al.’s scheme, since our scheme needs to construct a polynomial containing the session key. In sensor verification phase, the computation complexity of GDP is determined by the number of sensors in the group to evaluate hashes. For the controller verification phase, the computation complexity of existing schemes are determined by the number of sensor nodes. The proposed scheme requires more \((n+2)\) and \(2n\) operations than GDP and SCSLS, respectively, since our scheme allows strict authentication between the controller and sensor nodes. Also, the proposed scheme requires less \((7n-1)\) exponentiation operations and \((4n+2)\) hash operations than Tan and Chung’s scheme. Besides, Huang et al.’s scheme requires \(n\) hash operations and \(2n\) pairing operations. Note that in the group key generation phase, there is no heavy computations in our scheme, since the group key has been distributed to the sensors in the group registration phase, while SCSLS has to take \(n\) exponentiation operations.

Communication cost analysis

This section compares the communication cost of the proposed scheme with related ones. Suppose the length of random number, identity, time stamp, hash
value, the element in cyclic group $G$ are 160 bits, 128 bits, 32 bits, 256 bits, 512 bits, respectively. The controller in our scheme needs to send the signature, identity, and random number to sensors, which communication cost is $512 + 512 + 160 + 128 + 160 = 1472$ bits. The sensors send the response message to the controller, which communication cost is $512 + 512 + 160 + 128 = 1312$ bits. Similarly, in GDP, SCSLS I, Tan and Chung’s scheme and Huang et al.’s scheme, the communication overheads of the controller for sending messages to sensors is 2080 bits, 1568 bits, 1056 bits, 1184 bits, respectively, and the communication overheads of the sensor’s response is 2080 bits, 1408 bits, 1568 bits, 256 bits, respectively.

The comparison of communication cost is summarized in Table 3. It can be seen that the total communication cost of the proposed scheme is better than the GDP and SCSLS I schemes. Although it is higher than the schemes in Tan and Chung’s scheme and Huang et al.’s scheme, our scheme is able to resist more types of attacks.

| Scheme                                | Controller $\to$ sensor (bits) | Sensor $\to$ controller (bits) | Total cost (bits) |
|---------------------------------------|-------------------------------|-------------------------------|------------------|
| GDP                                   | 2080                          | 2080                          | 4160             |
| SCSLS I                               | 1568                          | 1408                          | 2976             |
| Tan and Chung’s scheme                | 1056                          | 1568                          | 2624             |
| Huang et al.’s scheme                 | 1184                          | 256                           | 1440             |
| Our scheme                            | 1472                          | 1312                          | 2784             |

**Experimental analysis**

In this section, the code is implemented based on the pairing-based cryptography library (PBC-0.5.14, https://crypto.stanford.edu/pbc/). The simulation is conducted run on a virtual machine with 4-core 4GB memory, 64 bit Linux Ubuntu 18.04 operating system, and Intel (R) core (TM) i7-8550u CPU (1.80 GHz). Figure 3 compares the time required in each phase of mutual authentication between 100 sensor nodes and the controller. The element of cyclic group is 512 bits, and the length of $q$ is 160 bits.

As shown in Figure 3, Tan and Chung’s scheme takes less time than our scheme in the group authentication request generation and sensor verification phases. Our scheme needs to distribute the session key during authentication, while Tan and Chung’s scheme distributes the key after authentication. Moreover, in the controller verification phase, our scheme shows distinct advantages. Another outstanding feature is that Huang et al.’s scheme needs more time in each stage than other schemes. Besides, SCSLS I and our scheme have almost the same efficiency in the group authentication request generation and sensor verification phases, and our scheme is more efficient than SCSLS I in the controller verification phase. Compared with GDP, our scheme enjoys higher computational efficiency in all phases except sensor verification.

As shown in Figure 4, the mutual authentication performance is compared, where the group size is considered to be 25, 50, ..., 200, respectively. When the number of sensors in a group is small, except Huang et al.’s scheme, other existing schemes have almost the same computational efficiency to complete mutual authentication. The number of nodes increases, the computing efficiency of our scheme is slightly better than SCSLS I. Particularly, both schemes show a linear growth of computation cost with slow growth trend. Compared with GDP and Tan and Chung’s scheme, the proposed scheme presents obvious advantages in performing controller aggregate verification to
validate the authenticity of sensor nodes. Especially, when the number of nodes increases, the time required for GDP\textsuperscript{8} to complete authentication increases rapidly, which makes the communication efficiency of GDP\textsuperscript{8} is lower than our scheme. Therefore, the aggregate authentication mechanism within a group is more efficient than validation one by one. Due to the involved bilinear pairing operations, the mutual authentication time of Huang et al.’s\textsuperscript{37} scheme has low authentication efficiency.

In the mutual authentication phase, after the controller receives the signature of all sensor nodes, it needs to verify the authenticity of their identities, so as to share the session key with sensor nodes in the group. When there are multiple sensor nodes, the efficiency comparison between aggregate verification and single verification is shown in Figure 5. It can be seen that for the same number of nodes, the time required for aggregate verification is less than that for single verification. Moreover, when the number of nodes increases, the time required for aggregate verification shows a better linear relationship with the number of nodes, and the growth rate of running time is slower than that for single verification.

From the above analysis, it can be seen that our scheme can not only ensure the authenticity of each entity’s identity in WBAN and the confidentiality of session key during mutual authentication but also enjoys higher computing efficiency than single verification. Compared with existing schemes, the proposed scheme has lower computation cost, lower communication cost, and higher authentication efficiency.

### Conclusion

To address the problems of identity authentication and key distribution of WBAN with a large number of sensor nodes, this article proposed a group authentication and session key distribution scheme supporting aggregate authentication. The controller can verify the authenticity of all sensor nodes in the way of aggregation, which improves the efficiency of mutual authentication between the controller and each sensor node. At the same time of mutual authentication, the session key can be shared between the controller and valid sensor nodes. Security analysis showed that the proposed scheme can resist impersonate attacks, assuming the discrete logarithm problem is hard and can guarantee the confidentiality of the session key. Theoretical performance analysis and experimental results indicated that, compared with existing schemes, our scheme has less computational overhead and higher authentication efficiency. Regarding future research, we would study the efficient joining and exiting of sensor nodes without revealing any private information.

### Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This article is supported in part by the National Natural Science Foundation of China (grant nos. 61772150, 61862012, and 61962012); the Guangxi Natural Science Foundation (grant nos. 2019GXNSFFA245015, 2019GXNSFGA245004, and AD19245048); the Peng Cheng Laboratory Project of Guangdong Province (grant no. PCL2018KP004); the Guangxi Young Teachers’ Basic Ability Improvement Program (grant no. 2021KY0214); the Open Program of Guangxi Key Laboratory of Cryptography and Information Security (grant no. GCIS201930); and the Innovation Projects of GUET Graduate Education (grant nos. 2021YCXS116 and 2021YCXS115).

### ORCID iD

Hui Xu \(https://orcid.org/0000-0002-5110-602X\)

### References

1. Islam SMR, Lloret J and Zikria YB. Internet of things (IoT)-based wireless health: enabling technologies and applications. *Electronics* 2021; 10(2): 148.
2. Malik MSA, Ahmed M, Abdullah T, et al. Wireless body area network security and privacy issue in e-healthcare. *Int J Adv Comput Sci Appl* 2018; 9(4): 209–215.
3. Wang W. Data security mix transmission mechanism in body area network. *Comput Sci* 2018; 45(5): 102–107.
4. Gao X, Liu X, Feng T, et al. Monitoring system design for rehabilitating training based on wireless body area network. *Comput Technol Develop* 2014; 24(9): 234–237.
5. Latrè B, Braem B, Moerman I, et al. A survey on wireless body area networks. *Wirel Netw* 2011; 17(1): 1–18.
6. Gao P, Yang YJ, Du ZW, et al. Research on privacy preservation in wireless body area network. *Appl Res Comput* 2013; 30(11): 3209–3215.
10. Yang X, Wang M, Pei X, et al. Security analysis and improvement of a certificateless signature scheme in the standard model. Acta Electron Sin 2019; 47(9): 1972–1978.

11. Yang X, Pei X, Chen G, et al. A strongly unforgeable certificateless signature scheme and its application in iot environments. Sensors 2019; 19(12): 2692.

12. Mwitende G, Ye Y, Ali I, et al. Certificateless authenticated key agreement for blockchain-based WBANs. J Syst Architect 2020; 110: 101777.

13. Huang YC, Zhang XH and Yu B. Efficient anti-replay identity-based signature scheme for wireless body area network. J Cryptol Res 2017; 4(5): 447–457.

14. Xu Z, Xu C, Chen H, et al. A lightweight anonymous mutual authentication and key agreement scheme for WBAN. Concurr Comput Pract Exp 2019; 31(4): e5295.

15. Thumbur G, Rao GS, Reddy PV, et al. Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices. IEEE Commun Lett 2020; 24(8): 1641–1645.

16. Xu Z, Luo M, Khan MK, et al. Analysis and improvement of a certificateless signature scheme for resource-constrained scenarios. IEEE Commun Lett 2021; 25: 1074–1078.

17. Yuan D, Peng X, Liu T, et al. A novel approach to authenticated group key transfer protocol based on AG codes. High Technol Lett 2019; 25(2): 129–136.

18. Keoh SL, Lupu EC and Sloman M. Securing body sensor networks: sensor association and key management. In: Proceedings of the 2009 IEEE international conference on pervasive computing and communications, Galveston, TX, 9–13 March 2009, pp.1–6. New York: IEEE.

19. Shen J, Chang S, Shen J, et al. A lightweight multi-layer authentication protocol for wireless body area networks. Fut Gener Comput Syst 2018; 78(3): 956–963.

20. Liu X, Jin C and Li F. An improved two-layer authentication scheme for wireless body area networks. J Med Syst 2018; 42(8): 143–157.

21. Tan H and Chung I. A secure and efficient group key management protocol with cooperative sensor association in WBANs. Sensors 2018; 18(11): 3930.

22. Shu H, Chen F, Xie D, et al. An aggregate signature scheme based on a trapdoor hash function for the internet of things. Sensors 2019; 19(19): 4239.

23. Hsu CF, Harn L and Zeng B. UMKESS: user-oriented multi-group key establishments using secret sharing. Wirel Netw 2020; 26(1): 421–430.

24. Kuo C, Luk M, Negi R, et al. Message-in-a-bottle: user-friendly and secure key deployment for sensor nodes. In: Proceedings of the 5th international conference on embedded networked sensor systems (SenSys’07), Sydney, NSW, Australia, 6–9 November 2007, pp.233–246. New York: ACM.

25. Benmansour T, Moussaoui T, Ahmed T, et al. Server-based secure key management for the IEEE 802.15.6 standard. In: Proceedings of the 2020 IEEE symposium on computers and communications (ISCC), Rennes, 7–10 July 2020, pp.1–6. New York: IEEE.

26. Zhang G and Liu W. A compressed sensing based detection for star topology WSNs. J Taiyuan Univ Technol 2018; 49(3): 473–477.

27. Li X, Ibrahim MH, Kumari S, et al. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput Netw 2017; 129(24): 429–443.

28. Almuhaideb AM and Alqudaihi KS. A lightweight three-factor authentication scheme for WHSN architecture. Sensors 2020; 20(6860): 6860.

29. Xiong H and Qin Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE Trans Inf Foren Sec 2015; 10(7): 1442–1455.

30. Shim KA. Comments on “revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks.” IEEE Trans Inf Foren Sec 2020; 15(1): 81–82.

31. Cai M and Niu D. An improved extended Kalman algorithm for pseudo code tracking optimization simulation. Comput Simul 2019; 36(8): 258–261.

32. Abro A, Deng Z and Memon KA. A lightweight elliptic-ElGamal-based authentication scheme for secure device-to-device communication. Fut Intern 2019; 11(5): 108.

33. Jegadeesan S, Azees M, Ramesh Babu N, et al. EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access 2020; 8(99): 48576–48586.

34. Wang W, Huang H, Zhang L, et al. Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer Peer Netw Appl 2021; 14: 2681–2693.

35. Liu JK, Baek J, Zhou J, et al. Efficient online/offline identity-based signature for wireless sensor network. Int J Inform Secur 2010; 9(4): 287–296.

36. Tan H and Chung I. Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. IEEE Access 2019; 7: 151459–151474.

37. Huang B, Liu G and Xu M. Security authentication protocol for nodes in wireless sensor networks based on clusters. Comput Eng 2016; 42(7): 117–122, 128.