A Novel Identity-based Broadcast Authentication Scheme with Batch Verification for Wireless Sensor Networks

Meng Feng[1], Chin-Feng Lai[3], Hong Liu[4], Rongxin Qi[1], Jian Shen[1,2]

[1] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, China
[2] Cyberspace Security Research Center, Peng Cheng Laboratory, China
[3] Department of Computer Science and Information Engineering, National Chung Cheng University, Taiwan
[4] Shanghai Trusted Industrial Control Platform Co., Ltd.
fengmeng1031@163.com, cinfon@ieee.org, liuhong@ticpsh.com, q_qirongxin@126.com, s_shenjian@126.com

Abstract

Message broadcasting is a fundamental data transmission service in wireless sensor networks (WSNs), which enables a great many users to join the network dynamically and spread messages. However, due to the open network environment, attackers can easily eavesdrop on traffic, inject false data messages, or modify legitimate content. So, many broadcast authentication schemes have been proposed to ensure the integrity and authenticity of messages transmitted in WSN, but these schemes suffer from higher computational overhead due to hash-to-point operation or certification management. To reduce the computational and communication costs, we first propose a novel Identity (ID)-based signature scheme with message recovery, and then construct an identity-based signature broadcast authentication scheme (ISBAS). In our scheme, the original messages do not require to be transmitted with its generated signature. Authentication process can recover the original message. Moreover, a larger number of messages can be verified simultaneously with batch verification. The security analysis indicates our scheme achieve known security requirements and the performance analysis proves it to be efficient.

Keywords: Wireless sensor networks, Broadcast authentication, Identity-based signature, certification

1 Introduction

Wireless Sensor Networks (WSNs) is a multi-hop, self-organizing network system composed of a large number of miniature sensor nodes deployed in the monitoring area and formed by wireless communication [1]. The WSNs can enhance electrical systems, positioning systems, surveillance system and intelligent transportation systems, which is widely regarded as a promising technology [2].

Data need to be transmitted between corresponding sensor nodes in WSNs. To increase the efficiency and expand the scope of information dissemination, broadcast is widely applied in WSNs. on the one hand, the base station transmits messages to the router and controller, and finally the sensor nodes broadcast the messages to other nodes. On the other hand, users, such as vehicles, can join in the network and broadcast messages to other nodes for requesting the latest road information. Due to the openness of the wireless channel, simple radio transceivers can easily be eavesdropped or modified packets [3]. In order to broadcast messages to a large number of sensor nodes in a more secure way, a Broadcast Authentication (BA) [4] protocol is necessary needed in WSNs. In a multi-users broadcast authentication protocol, users broadcast messages to a group of sensor nodes, and then sensor nodes verify the authentic of the messages.

Many broadcast authentication schemes based on (SKC) have been proposed [5-10]. Perrig et al. [5] proposed a Timed Efficient Streaming Loss-tolerant Authentication (TESLA) broadcast protocol. The protocol that meets the requirements of continuous media certification has improved certification speed and computational efficiency. The authors also claimed that message integrity is provided with a one-way hash function. However, data need to be authenticated by groups and transmitted repeatedly in this scheme, which increases the communication cost. Besides, the scheme is vulnerable to denial of service (DoS) attack due to the delay in authenticating the received data for nodes. Their scheme is not suitable for the environment with a large number of users. To improve the performance of scheme in [5], a scalable broadcast authentication scheme called multi-level μ TESLA was proposed in [6]. However, the scalability of their scheme is limited by the initial parameter distribution based on unicast. This method is suitable for the environment with a large number of users, but it is also vulnerable to Dos attack. Meanwhile, many schemes based on μ TESLA [8-9] were proposed recently, but

*Corresponding Author: Jian Shen; E-mail: s_shenjian@126.com
DOI: 10.3966/160792642020092105007

these schemes are vulnerable to active attacks because of the authentication delay. Later, the X-TESLA was proposed by Kwon and Hong in [7]. It lowers computational cost and butter occupation. However, it still does not solve the main problem of the data transmission delay in TESLA.

PKC-based BA schemes [11] solve the above problems. PKC is more suitable for data communication in WSNs than SKC. On one hand, RSA is widely regarded as more effective encryption algorithm, which has less computation time and more accurate computation results. On the one hand, ECC has smaller security key size with the same security, which reduces the storage space and computational cost. Therefore, PKC-based BA schemes are suitable for bandwidth-limited communication channels in WSNs. Benenson et al. [12] applied PKC to WSNs in order to provide multi-user authentication for BA schemes. However, the public key certificate needs to be transmitted to sensor nodes and verified by them, which will lead to much communication cost and computation overhead. Jiang et al. improved Benenson's scheme in [13]. Their scheme is based on the self-certified keys cryptosystem (SCK) and ECC to compute keys, which is very lightweight for WSNs applications. However, each sensor nodes need to keep its private key pair in the local in this protocol, thus an attacker may attack the sensor node and obtain its private key.

In Identity-based encryption or signature schemes, the public key of a user is computed by its identity, thus the public-key certificates are eliminated. Ren et al. [14] presented a BA scheme based on an Identity-based signature scheme. They claimed that their scheme could withstand Dos attacks that were presented in the previous schemes. However, the computational cost of their scheme is high due to the expensive bilinear pairing operations. A BA scheme based on lightweight operations was proposed in [15]. They designed a mechanism to protect the private key of users, which can resist compromise attacks. To solve the above problems, a practical multi-user broadcast scheme with message recovery was proposed by Kyung-Ah in [16]. Their scheme also does not need expensive pairing computations and is simulated on MICAz and Tmote Sky. However, a group of messages cannot be authenticated with batch verification in their scheme.

To provide a better service for WSN, this paper first proposes a new ID-based signature scheme with message recovery, then construct our ISBAS and apply it to wireless sensor network. Our contributions can be concluded as follows:

(1) A novel ID-based signature scheme with message recovery is proposed and our ISBAS is constructed. In the proposed scheme, the original message does not require to be transmitted with its generated signature, which reduces the communication cost and is suitable for bandwidth-limited channels in WSNs.

(2) The proposed scheme supports batch verification where a larger number of messages can be verified simultaneously, which avoids authentication delays and DoS attacks. Meanwhile, the computational cost can be reduced.

(3) The security analysis indicates our scheme can resist DoS attacks, relay attacks, compromise attacks and Sybil attacks. In addition, the performance analysis proves it to be efficient.

The remaining of this paper is organized as follows. In Section 2, we present the preliminaries introduced in this paper. In Section 3, we describe the proposed ISBAS scheme in detail. The security analysis and performance analysis are demonstrated in Section 4 and Section 5 respectively. Finally, Section 6 concludes this paper.

2 Preliminaries

This section introduces the system model and the adversary model used in this paper.

2.1 System Model

This paper mainly considers the WSNs application environment that includes a great many sensor nodes, a sink and many data users. Network users can access the WSN to get data services at a specific time. As shown in Figure 1, these data users can be numerous soldiers, vehicles and aircrafts. These three entities in the system are described as follows.

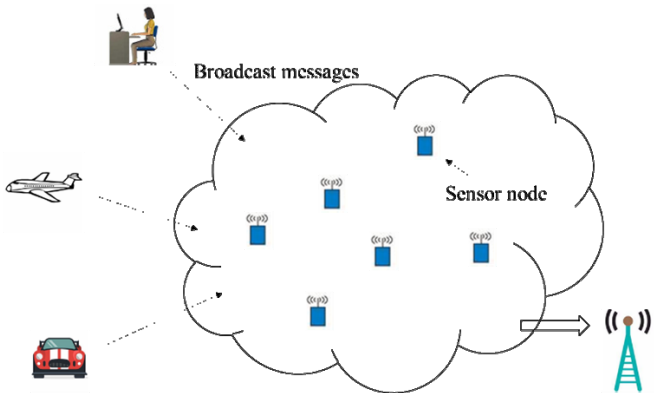

Figure 1. The system model

2.1.1 Sink

The sink is trustworthy, which acts as a Private Key Generator (PKG). It is aimed to initialize the system and produce a private key for the user. The sink has more powerful computation capability and storage space than sensor nodes. Besides, the sink may broadcast some commands to sensor nodes in specific situations.

2.1.2 Data Users

Data users can be vehicles and aircrafts which need to broadcast messages to WSN to obtain some services and expect the latest network information. The users are equipped with devices that have more powerful computation capability and storage space than sensor nodes. Moreover, the users can join in or leave WSN dynamically.

2.1.3 Sensor Nodes

Sensor nodes usually have limited computation capability, storage space and power supply. They will receive the signatures transmitted by the users, recover the original messages and verify the signatures.

2.2 Adversary Model

We mainly consider adversaries inside the network or outside the network. Several important attack types are lised in this section.

2.2.1 Impersonation Attack

Impersonation attack refers to an attacker where the attacker can pretend a legal entity to communicate with other entities in the system, so that the attacker obtains secret communication messages. Meanwhile, private keys and data will be stolen by the attacker using the corresponding operations.

2.2.2 Relay Attack

Relay Attack is a form of an attacker where the attacker transmits data packets maliciously or fraudulently which the recipient has received. The attacker may eavesdrop or intercept messages on the communication channels and sent that to the destination repeatedly for further communication.

2.2.3 Compromise Attack

Compromise attack refers to an attack where some entities are attacked by attackers and leak the private information. An attacker may steal the users' devices and capture the stored private information. Besides, sensor nodes may be attacked by attackers. If sensor nodes store the private information, attackers will obtain the secret information.

2.2.4 Sybil Attack

Sybil attacks are attacks that use several nodes to get multiple false identities, thereby using these false identities to attack other normal nodes in the network [17-19]. Sybil attacks can be prevented by using identity registration and random key distribution schemes to establish secure connections between nodes.

3 The Proposed Scheme

In this section, we first propose a novel ID-based signature scheme with message recovery, then construct our ISBAS and apply it to wireless sensor network.

3.1 A Novel ID-based Signature Scheme with Message Recovery

We propose a novel ID-based signature scheme and use it as the basis of our broadcast authentication scheme to reduce the computational and communication costs. The proposed signature scheme comprises five algorithms: Setup, Extract, Sign, Verify and Bverify. The details are described as follows.

3.1.1 Setup

This algorithm is executed by a trust third party KGC to generate system public parameters, master private key and master public key.

(1) Given a security parameter λ, KGC randomly chooses a large prime q and two groups G_1, G_2 with the order q.

(2) KGC randomly chooses a generator P in G_1, a generator Q in G_2 and a **bilinear pairing** $e: G_1 \times G_1 \to G_2$.

(3) KGC randomly chooses a value $x \in Z_q^*$ as the master private key and calculates the master public key P_{pub} as $P_{pub} = x \cdot P$.

(4) Then, KGC picks four secure cryptographic one-way hash functions $h_1, h_2 : \{0,1\}^* \to Z_p^*$, $F_1 : \{0,1\}^{k_2} \to \{0,1\}^{k_1}$ and $F_2 : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$, where $|q| = k_1 + k_2$.

(5) KGC sets the public parameters as $\{q, G_1, G_2, e, P, Q, P_{pub}, h_1, h_2, F_1, F_2\}$, but keeps x secret.

3.1.2 Extract

This algorithm is executed by KGC to generate the private key for each user, and the specific steps are as follows.

(1) Give a user's identity ID, KGC randomly chooses a secret $r \in Z_p^*$, then computes

$$\alpha = h_1(ID, R) \quad \textbf{(1)}$$

$$S = (r + \alpha \cdot x) \cdot Q \quad \textbf{(2)}$$

(2) Then, KGC sends the private key (R, S) to the user via secure channel.

3.1.3 Sign

In this algorithm, the user excute the following steps to produce a digital signature of the message, and the specific steps are as follows.

(1) Given a private key (R,S) of the user with ID and its message m to be broadcasted, randomly choose a value $r_s \in Z_q^*$ and compute

$$R_s = r_s \cdot P \tag{3}$$

(2) Hide the message m as f, and m can be recovered from its signature in verification process. Set

$$f = F_1(m) \| F_2(F_1(m)) \oplus m) \tag{4}$$

(3) To generate a signature σ of m, compute

$$y = R_s \oplus f \tag{5}$$

$$v = S \cdot Q^{-1} + r_s \tag{6}$$

$$\alpha_s = h_2(m, ID, R) \tag{7}$$

$$S_m = S + \alpha_s \cdot r_s \cdot Q \tag{8}$$

Then, $\sigma=\{S_m, R, y, v\}$ is a signature of m corresponding to the user with ID.

3.1.4 Verify

Upon receiving a signature $\sigma=\{S_m, R, y, v\}$, the verifier executes this algorithm to judge the authenticity of the signature. It needs to recover the message m from the signature and verify the signature. The specific steps are as follows.

(1) Compute the following equations to recover the message m.

$$\alpha^{'} = h_1(ID, R) \tag{9}$$

$$f = y \oplus (vP - R - \alpha^{'} P_{pub}) \tag{10}$$

$$m^{'} = [f]_{k_2} \oplus F_2({}_{k_1}[f]) \tag{11}$$

(2) To verify the signature σ, compute

$$\alpha_s^{'} = h_2(m^{'}, ID, R) \tag{12}$$

$$R_s^{'} = y \oplus f \tag{13}$$

(3) The verifier checks if $e(S_m, P)$ and $e(R + \alpha^{'} P_{pub} + \alpha_s^{'} R_s^{'}, Q)$ are equal. If they are equal, the message is authentic. Otherwise, the verifier rejects the message.

Since $P_{pub} = x \cdot P$, $S_m = S + \alpha_s \cdot r_s \cdot Q$, $S = (r + \alpha \cdot x) \cdot Q$, $R = r \cdot P$ and $R_s = r_s \cdot P$, the following equations can be obtained.

$$\begin{aligned} e(S_m, P) &= e(S + \alpha_s \cdot r_s \cdot Q, P) \\ &= e(r \cdot Q + \alpha \cdot x \cdot Q + \alpha_s \cdot r_s \cdot Q, P) \\ &= e((r + \alpha \cdot x + \alpha_s \cdot r_s) \cdot Q, P) \\ &= e((r + \alpha \cdot x + \alpha_s \cdot r_s) \cdot P, Q) \\ &= e(r \cdot P + \alpha \cdot x \cdot P + \alpha_s \cdot r_s \cdot P, Q) \\ &= e(R + \alpha P_{pub} + \alpha_s R_s, Q) \\ &= e(R + \alpha^{'} P_{pub} + \alpha_s^{'} R_s^{'}, Q) \end{aligned} \tag{14}$$

Therefore, the correctness analysis of the algorithm is shown as above.

3.1.5 Bverify

When a large number of users generate a group of signatures $\sigma_i = \{S_{m_i}, R_i, y_i, v_i\}_{i=1}^n$ about messages $\{m_i\}_{i=1}^n$, where $\{ID_i\}_{i=1}^n$ are identities of a group of users, the proposed scheme performs batch verification on group signatures using Camenisch et al. Method [20]. The batch verification process of signatures is computed as followed.

(1) The verifier computes the following equations for $i = 1, \cdots, n$.

$$\alpha_i^{'} = h_1(ID_i, R_i) \tag{15}$$

$$\alpha_{s_i}^{'} = h_2(m_i^{'}, ID_i, R_i) \tag{16}$$

$$R_{s_i}^{'} = y_i \oplus f_i \tag{17}$$

(2) The verifier checks if $e(\sum_{i=1}^n S_{m_i}, P)$ and $e(\sum_{i=1}^n (R_i + \alpha_{s_i}^{'} R_{s_i}^{'}) + (\sum_{i=1}^n \alpha_i^{'}) P_{pub}, Q)$ are equal. If they are equal, a group of messages are authentic. Otherwise, the verifier rejects these messages.

Since $P_{pub} = x \cdot P$, $S_{m_i} = S_i + \alpha_{s_i} \cdot r_{s_i} \cdot Q$, $S_i = (r_i + \alpha_i \cdot x) \cdot Q$, $R_i = r_i \cdot P$ and $R_{s_i} = r_{s_i} \cdot P$, the following equations can be obtained.

$$\begin{aligned} e(\sum_{i=1}^n S_{m_i}, P) &= e(\sum_{i=1}^n (S_i + \alpha_{s_i} \cdot r_{s_i}) \cdot Q, P) \\ &= e(\sum_{i=1}^n (r_i + \alpha_i \cdot x) \cdot Q + \alpha_{s_i} \cdot r_{s_i} \cdot Q, P) \\ &= e(\sum_{i=1}^n (r_i + \alpha_i \cdot x + \alpha_{s_i} \cdot r_{s_i}) \cdot Q, P) \\ &= e(\sum_{i=1}^n (r_i + \alpha_i \cdot x + \alpha_{s_i} \cdot r_{s_i}) \cdot P, Q) \\ &= e(\sum_{i=1}^n r_i \cdot P + \alpha_i \cdot x \cdot P + \alpha_{s_i} \cdot r_{s_i} \cdot P, Q) \\ &= e(\sum_{i=1}^n (R_i + \alpha_i P_{pub} + \alpha_{s_i} R_{s_i}), Q) \\ &= e(\sum_{i=1}^n (R_i + \alpha_{s_i}^{'} R_{s_i}^{'}) + (\sum_{i=1}^n \alpha_i^{'}) P_{pub}, Q) \end{aligned} \tag{18}$$

Therefore, the correctness analysis of the algorithm is shown as above.

3.2 An ID-based Signature Broadcast Authentication Scheme (ISBAS)

Now, we propose an identity-based signature broadcast authentication scheme, ISBAS, based on the new identity-based signature scheme above. Our ISBAS comprises four phases: system initialization, user registration, broadcast authentication and user revocation.

3.2.1 System Initialization

A sink acts as a KGC to generate the necessary system parameters in wireless sensor network. The sink performs Setup algorithm to select the system parameters $\{q, G_1, G_2, e, P, Q, P_{pub}, h_1, h_2, F_1, F_2\}$, where $P_{pub} = x \cdot P$, $h_1, h_2 : \{0,1\}^* \to Z_p^*$, $F_1 : \{0,1\}^{k_2} \to \{0,1\}^{k_1}$ and $F_2 : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$. x is the master private key and P_{pub} is the master public key. Then the system parameters are preloaded into each sensor nodes.

3.2.2 User Registration

In this phase, a sink generates a private key for each user. Input a user's identity ID_i, the sink perform the Extract algorithm to generate a private key $SK_i = (R_i, S_i)$ for the user ID_i.

3.2.3 User Broadcast Authentication

When a user U_i with a private key $SK_i = (R_i, S_i)$ and an identity ID_i needs to broadcast a message m_i to sensor nodes, it needs to execute the following steps.

(1) The user U_i chooses a current timestamp t_i, and performs Sign algorithm to generate a signature $\sigma_i = \{S_{m_i}, R_i, y_i, v_i\}$ on m_i.

Then, the user broadcasts $M_i = \{ID_i, t_i, \sigma_i\}$ to senor nodes.

(2) Upon receiving M_i, each sensor node firstly needs to verify the timestamp t_i. If the timestamp t_i is fresh, the sensor node then performs the Verify algorithm to recover the original message m_i and verifies the signature σ_i. If the result is positive, the scheme will excute the next step. Otherwise, the message will be discarded.

(3) When the sensor node receives n signatures, the sensor node can perform the BVerity algorithm to verify the authenticity of signatures. If the result is positive, the sensor node sends the messages to the next. Otherwise, it discards the messages.

3.2.4 User Revocation

If a user needs to be revoked, the sink broadcasts a revoke message to all sensor nodes. Sensor nodes receives the message and maintains a revocation list in the local. When receiving messages from the user, sensor nodes need to first check if the identity of the user is in the revocation list. If positive, sensor nodes will reject these messages. Otherwise, these message will be accepted.

4 Security Analysis

We now analyze the security of the proposed scheme and demonstrate security properties that it meets.

Theorem 1: The proposed scheme can be proved secure in the random oracle model, assuming the CDH problem is hard.

Proof of Theorem 1: As demonstrated in [21], the probability that the challenger solves the CDH problem is

$$Pr_C \geq \frac{\varepsilon}{9 \cdot qh_1 \cdot qh_2} \tag{19}$$

Where qh_1 and qh_2 denote the number of h_1 and h_2 queries respectively, ε is a non-negligible probability that an adversary can win the game in [22]. Therefore, the challenger can solve the CDH problem with a non-negligible probability Pr_C. However, since the CDH problem is hard, the proposed scheme is secure under the random oracle model.

Theorem 2: The proposed scheme can provide message integrity and source authentication.

Proof of Theorem 2: The signature scheme used in this paper has existential unforgeability against adaptive selective identity and adaptive chosen message attack [21]. Therefore, attackers cannot masquerade as a legitimate user to access network services and only legitimate users can be authenticated by sensor nodes. Also, attackers cannot modify broadcast messages or inject fake broadcast messages into the network. Therefore, the proposed scheme can achieve message integrity and source authentication.

4.1 Security Discussion

Our protocol also satisfies other security properties such as replay attack resistance, DoS attack resistance and compromise attack resistance.

4.1.1 Resistance to Relay Attack

Replay attacks use legitimate messages before retransmission as the current message to attack schemes. In the proposed scheme, the transmitted messages contain a timestamp, which can resist relay attack. When receiving the broadcasting packets, the sensor nodes need to verify the freshness of the timestamp. If it is fresh, the messages are considered to be legitimate. Otherwise, the messages will be dropped.

It is worth noting that using timestamps to defend against replay attacks must have a synchronization mechanism.

4.1.2 Resistance to Compromise Attack

Some sensor nodes and users' devices may be attacked by attackers. Attackers may steal some private data stored in sensor nodes or devices, then use these data to obtain more secret information except some system public parameters. However, in our scheme, all sensor nodes only store the system public parameters, but do not store any secret data. Moreover, sensor nodes do not generate their signatures and they only verify signatures generated by users. Therefore, attackers cannot obtain any secret information from the compromised nodes.

4.1.3 Resistance to Sybil Attack

Sybil attacks disrupts network protocols by illegally claiming multiple identities. In the proposed scheme, a KGC generates a private key for a user with a unique identity ID. Users can always use his private key to compute signatures on the messages, and signatures are different based on users' ID. To be able to forge the identity of a user, attackers have to forge a new private key using the system private key x. However, the system private key x is invaluable to attackers because the KGC is a trusted entity as we assumed. Therefore, Sybil attacks can be resisted in our scheme.

5 Performance Analysis

In this section, we will analyze the performance of the proposed scheme in terms of computational cost and communication cost. Moreover, the comparisons with two related schemes are also presented in this section.

5.1 Computational Cost

In this section, we analyze the computational cost of our scheme. To ensure a common security level, we use the bilinear pairing $e: G_1 \times G_1 \to G_2$ in the experiments. G_1 with order q is generated by a point on a elliptic curve defined on the fine field F_p. p is a prime number with 163 bits. Form the description of the proposed scheme in section 3, we can find that our scheme mainly contains point multiplication operations, point addition operations, one-way hash operations, and bilinear paring operations. Let T_h, T_{bp}, T_{pm}, T_{pa}, T_{exp}, T_{mul}, T_{mth} donate the time to compute a hash function, a bilinear paring, point multiplication 1, a point addition, an exponentiation, point multiplication 2 and hash-to-point function. To enable a fair comparison, we implement the corresponding calculation operations on a personal computer using the PBC libraries. We have $T_h \approx 0.050$, $T_{bp} \approx 9.760$, $T_{pm} \approx 3.620$, $T_{pa} \approx 0.020$, $T_{exp} \approx 0.580$, $T_{mul} \approx 0.004$ and $T_{mth} \approx 9.750$. Notations used to describe the runtime of the respective cryptographic operations and the experiment execution time are concluded in Table 1.

Table 1. Execution times of various cryptographic operations (in millisecond)

Symbols	Descriptions	Runtime
T_h	One-way hash function	0.050
T_{mth}	Hash-to-point function	9.750
T_{bp}	Bilinear paring operation	9.760
T_{pm}	Point multiplication operation 1	3.620
T_{pa}	Point addition operation	0.020
T_{exp}	Exponentiation operation	0.580
T_{mul}	Point multiplication operation 2	0.004

In the proposed scheme, we consider the runtime of the whole scheme except the system initialization phase. Firstly, to generate a private key for a user, the computational cost of the sink is $2 \times T_{pm} + T_h = 2 \times 3.620 + 0.050 = 7.290$ ms. To generate a signature on a message m, the computational cost of the user is $3 \times T_{pm} + 2 \times T_{pa} + 3 \times T_h = 11.050$ ms. To recover the a message m, the execute time of the node is $2 \times T_{pm} + 2 \times T_h = 7.340$ ms. To verify the authenticity of the signature on a message m, the execute time is $2 \times T_{pm} + 2 \times T_{pa} + 1 \times T_h + 2 \times T_{bp} = 2 \times 3.620 + 2 \times 0.020 + 1 \times 0.05 + 2 \times 9.760 = 26.850$ ms. Therefore, the total execute time of the node is $7.340 + 26.850 = 34.190$ ms. To verify the authenticity of a group of signatures $\sigma_i = \{S_{m_i}, R_i, y_i, v_i\}_{i=1}^n$ simultaneously, the total execute time of the node is $2 \times T_{bp} + 2n \times T_h + 2n \times T_{pa} + 2n \times T_{pm} = 7.380n + 19.52$ ms.

In Shim's scheme [19], to generate a private key for a user, the runtime of the PKC is $T_{pm} + T_{mth} = 13.840$ ms. To generate a signature on a message m, the runtime of the user is $3 \times T_{pm} + T_{pa} = 10.880$ ms. To verify the authenticity of the signature on a message m, the runtime of the verifier is $T_{pa} + T_{mth} + 2 \times T_{bp} + T_{pm} = 33.380$ ms. To verify the authenticity of a group of signatures, the total execute time is $(T_{pa} + T_{mth} + T_{pm}) \times n + 2 \times T_{bp} = 13.86n + 19.52$ ms.

In Ren's scheme [14], the runtime of the PKC is $T_{pm} + T_{mth} = 3.620 + 10.220 = 13.840$ ms. To generate a signature on a message m, the runtime of the user is

$2\times T_{pm}+T_h+T_{bp}+T_{pa}+T_{exp}=17.65$ ms. To verify the authenticity of the signature on a message m, the total execute time of the node is $T_{mth}+2\times T_{bp}+T_{exp}=30.32$ ms. To verify the authenticity of a group of signatures, the total execute time of the node is $(T_{mth}+2\times T_{bp}+T_{exp})\times n=30.32n$ ms.

We compare our scheme with Shim's scheme and Ren's scheme in terms of computational cost in Table 2, and the cost of the BVerify algorithm in these three schemes (see Figure 2). Note that we only compare the cost of verifying the signature in three schemes. Hence, the cost of recovering the message in our scheme is not considered. From Table 2, we can find that our scheme has a lower computational cost than Ren's scheme in Extract, Sign, Verify and BVerify algorithms. In addition, our scheme has a lower computational cost than Shim's scheme in Extract, Verify and BVerify algorithms. From Figure 2, we can find that the runtime of the BVerify algorithms of the three protocols increases as n increases. However, the increase in the runtimes of Shim's scheme and Ren's scheme is much larger than that of our scheme. In addition, the gap between the runtimes of these two protocols and our scheme increases as the number of signatures increases. It is clear that our scheme is more efficient than Ren's scheme and Shim's scheme in terms of computational cost.

Table 2. Comparisons: computational cost (in millisecond)

Schemes	Extract	Sign	Verify	BVerify
[19]	13.840	10.880	33.380	$13.86n+19.52$
[14]	13.840	17.650	30.320	$30.32n$
ISBAS	7.290	11.050	26.850	$7.380n+19.52$

† "n" denote that the number of signatures

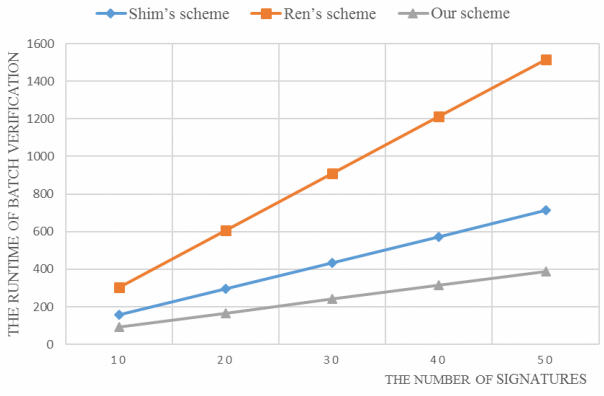

Figure 2. Computational Cost of The BVerify Algorithm

5.2 Communication Cost

In this section, we analyze the communication cost of our scheme, Shim's scheme and Ren's scheme. In our scheme, the user needs to broadcast the message $M_i=\{ID_i,t_i,\sigma_i\}$ to sensor nodes. The signature is $\sigma_i=\{S_{m_i},R_i,y_i,v_i\}$, where $S_{m_i},R_i,y_i,v_i\in G_1$. The size of prime p is 163 bits. Therefore, an element in G_1 is 163+163=326 bits and the communication cost of the signature is $326\times 4=1304$ bits. The communication cost of our scheme is 1304+32+32=1368 bits. In Shim's scheme [19], the transmitted message consists of the signature, the identity, the original message and the timestamp. Therefore, the communication cost of Shim's scheme is $326\times 3+32+326+32=1368$ bits. In Ren's scheme [14], the user needs to broadcast the message $M_i=\{U_{id},tt,M,\sigma,c\}$ to sensor nodes. The communication cost of Ren's scheme is $32\times 4+326\times 4=1432$ bits. As shown in Table 3, the communication cost of our scheme is the same as that of Shim's scheme and lower than Ren's scheme. In addition, Figure 3 shows the communication cost comparisons when the number of signatures is different.

Table 3. Comparisons: communication cost (in bit)

Schemes	Communication cost
Shim's scheme [19]	1368
Ren's scheme [14]	1432
Our scheme	1368

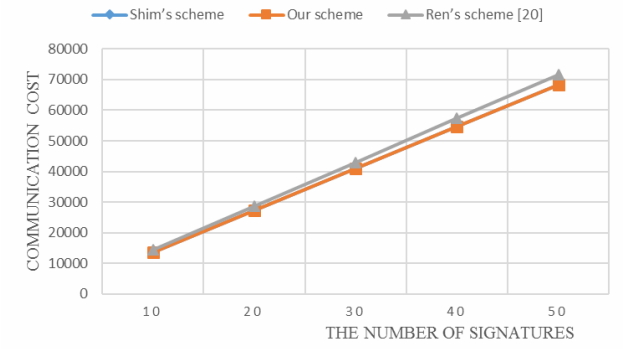

Figure 3. Communication Cost Comparisons

6 Conclusion

In this paper, we propose a novel ID-based signature scheme with message recovery, then construct an identity-based signature broadcast authentication scheme (ISBAS). In our scheme, the original message does not require to be transmitted with its generated signature, which reduces the communication cost of the scheme. And the original message can be resumed in authentication process. Moreover, a larger number of messages can be verified simultaneously with batch verification. Specifically, the performance analysis indicates that our scheme outperforms Shim's scheme and both Ren et al.'s schemes.

Further work will optimize the construction of the scheme to remove the biller pairings to reduce the

overhead of the scheme. Besides, this work will be evaluated in a real environment. Moreover, we will extend this scheme to have the property of anonymity.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grants No. U1836115, No. 61672295, No. 61922045, the Natural Science Foundation of Jiangsu Province under Grant No. BK20181408, the Foundation of State Key Laboratory of Cryptology under Grant No. MMKFKT 201830, the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004, the CICAEET fund, and the PAPD fund, the Opening Project of Shanghai Trusted Industrial Control Platform under Grant No. TICPSH202003011-ZC.

References

[1] H. Yang, K. Tang, An Adaptable CS-based Transmission Scheme in Wireless Sensor Network, *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 31, No. 2, pp. 123-132, June, 2019.

[2] Y. -H. Liao, C. -L. Lei, Y. -I. Ko, Y. -S. Chen, C. -H. Chiu, Enhanced Tame-based Key Predistribution Scheme for Sensor Networks, *Journal of Internet Technology*, Vol. 18, No. 7, pp. 1499-1514, December, 2017.

[3] A. Shafiq, I. Altaf, K. Mahmood, S. Kumari, C. -M. Chen, An ECC Based Remote User Authentication Protocol, *Journal of Internet Technology*, Vol. 21, No. 1 , pp. 285-294, January, 2020.

[4] D. Liu, P. Ning, Broadcast Authentication, *Security for Wireless Sensor Networks. Advances in Information Security*, Vol. 28, Springer, Boston, MA, 2007, pp. 9-57.

[5] A. Perrig, J. D. Tygar, *Secure Broadcast Communication*, Springer, Boston, MA, 2003.

[6] D. Liu, P. Ning, Multilevel μTESLA: Broadcast Authentication for Distributed Sensor Networks, *ACM Transactions on Embedded Computing Systems*, Vol. 3, No. 4, pp. 800-836, November, 2004.

[7] T. Kwon, J. Hong, Secure and Efficient Broadcast Authentication in Wireless Sensor Networks, *IEEE Transactions on Computers*, Vol. 59, No. 8, pp. 1120-1133, August, 2010.

[8] C. H. Lim, New Constructions of Multi-level μTESLA with Immediate Authentication, *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 16, No. 6, pp. 163-167, December, 2006.

[9] D. Liu, P. Ning, S. Zhu, S. Jajodia, Practical Broadcast Authentication in Sensor Networks, *International Conference on Mobile & Ubiquitous Systems: Networking & Services*, San Diego, CA, USA, 2005, pp. 118-129.

[10] P. Ning, A. Liu, W. Du, Mitigating DoS Attacks Against Broadcast Authentication in Wireless Sensor Networks, *ACM Transactions on Sensor Networks*, Vol. 4, No. 1, pp. 1-35, January, 2008.

[11] Y. Liu, J. Li, M. Guizani, PKC Based Broadcast Authentication Using Signature Amortization for WSNs, *IEEE Transactions on Wireless Communications*, Vol. 11, No. 6, pp. 2106-2115, June, 2012.

[12] Z. Benenson, N. Gedicke, O. Raivio, Realizing Robust User Authentication in Sensor Networks, *Real-World Wireless Sensor Networks (REALWSN)*, Stockholm, Sweden, 2005, pp. 1-5.

[13] C. Jiang, B. Li, H. Xu, An Efficient Scheme for User Authentication in Wireless Sensor Networks, *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, Niagara Falls, Ont., Canada, 2007, pp. 438-442.

[14] 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. 4136-4144, November, 2007.

[15] X. Cao, W. Kou, L. Dang, B. Zhao, IMBAS: Identity-based Multi-user Broadcast Authentication in Wireless Sensor Networks, *Computer Communications*, Vol. 31, No. 4, pp. 659-667, March, 2008.

[16] K. A. Shim, A Practical Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 7, pp. 1545-1554, July, 2017.

[17] B. Yu, C. Z. Xu, B. Xiao, Detecting Sybil Attacks in VANETs, *Journal of Parallel and Distributed Computing*, Vol. 73, No. 6, pp. 746-756, June, 2013.

[18] H. Yu, M. Kaminsky, P. B. Gibbons, A. D. Flaxman, Sybilguard: Defending Against Sybil Attacks via Social Networks, *IEEE/ACM Transactions on Networking*, Vol. 16, No. 3, pp. 576-589, June, 2008.

[19] K. A. Shim, An ID-based Aggregate Signature Scheme with Constant Pairing Computations, *Journal of Systems and Software*, Vol. 83, No. 10, pp. 1873-1880, October, 2010.

[20] J. Camenisch, S. Hohenberger, M. Ø. Pedersen, Batch Verification of Short Signatures, *Journal of Cryptology*, Vol. 25, No. 4, pp. 723-747, October, 2012.

[21] D. He, N. Kumar, K. K. R. Choo, W. Wu, Efficient Hierarchical Identity-Based Signature with Batch Verification for Automatic Dependent Surveillance-Broadcast System, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 2, pp. 454-464, February, 2017.

[22] D. Pointcheval, J. Stern, Security Arguments for Digital Signatures and Blind Signatures, *Journal of Cryptology*, Vol. 13, No. 3, pp. 361-396, June, 2000.

Biographies

Meng Feng received the B.E. degree in 2018 and is currently working toward the M.E. degree at NUIST, Nanjing, China. She focuses on the security and privacy issues in Internet of Things. Her research interests include network and data security, systems security and cryptography.

Chin-Feng Lai has been an associate professor in the Department of Computer Science and Information Engineering, National Chung Cheng University since 2013. He received PhD degree from the Department of Engineering Science of National Cheng Kung University, Taiwan, 2008. His research interests include multimedia communications, sensor-based healthcare, and embedded systems.

Hong Liu received her Ph.D. degree from the School of Electronic and Information Engineering, Beihang University in 2014. She is an associate professor at the School of Computer Science and Software Engineering, East China Normal University, Shanghai, China. Her research interests include security in edge computing and industrial control system.

Rongxin Qi received the B.E. degree in 2018 and is currently working toward the M.E. degree at NUIST, Nanjing, China. He focuses on information security and group user authentication scheme in networks. His research interests include information security, IoT security and privacy.

Jian Shen received the M.E. and Ph.D. degrees in Computer Science from Chosun University, South Korea, in 2009 and 2012, respectively. Since late 2012, he has been a professor at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include cloud computing and security, data auditing and sharing, and public cryptography.