Accepted Manuscript

Efficient certificateless access control for industrial Internet of Things

Fagen Li, Jiaojiao Hong, Anyembe Andrew Omala

PII: S0167-739X(16)30866-4
DOI: http://dx.doi.org/10.1016/j.future.2016.12.036
Reference: FUTURE 3277

To appear in: *Future Generation Computer Systems*

Received date: 6 November 2015
Revised date: 23 December 2016
Accepted date: 29 December 2016

Please cite this article as: F. Li, J. Hong, A.A. Omala, Efficient certificateless access control for industrial Internet of Things, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.12.036

Highlights

- We revised the BDCPS certificateless signcryption scheme to realize the public verifiability, ciphertext authenticity and insider security.
- We designed an access control scheme for the industrial wireless sensor networks in the context of the industrial Internet of Things using the certificateless signcryption.

Efficient certificateless access control for industrial Internet of Things☆

Fagen Li*, Jiaojiao Hong, Anyembe Andrew Omala

Center for Cyber Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract

Industrial wireless sensor networks (IWSNs) play an important role in monitoring the industrial equipment and creating a highly reliable industrial system. To query of the network to gain useful information from anywhere and anytime, we need to integrate the IWSNs into the Internet as part of the industrial Internet of Things (IoT). In this case, it is crucial to design an access control scheme that can authorize, authenticate and revoke a user to access the IWSNs. In this paper, we first give a certificateless signcryption scheme and then design an access control scheme for the IWSNs in the context of the industrial IoT using the certificateless signcryption. Compared with existing two access control schemes using traditional signcryption, our scheme achieves public verifiability, ciphertext authenticity and insider security. In addition, the computational cost of the sensor node in our scheme is reduced by about 62% and 77%, respectively and the energy consumption of the sensor node in our scheme is reduced by about 64% and 75%, respectively.

Keywords: Industrial wireless sensor network, Internet of Things, Security, Signcryption, Certificateless cryptography.

1. Introduction

Wireless sensor networks (WSNs) are ad hoc networks that usually are composed of a large number of tiny sensor nodes with the capabilities of sensing, computation and communication [1, 2]. WSNs have important application in military sensing and tracking, target tracking, environment monitoring, and so on. Industrial wireless sensor network (IWSNs) are an important application of the WSNs in the industrial manufacturing field. In the IWSNs, many tiny sensor nodes are deployed on the industrial equipment. These tiny sensor nodes monitors the

☆This work is supported by the National Natural Science Foundation of China (Grant Nos. 61073176, 61272525, 61302161 and 61462048) and the Fundamental Research Funds for the Central Universities (Grant No. ZYGX2013J069).

*Corresponding author
Email address: fagenli@uestc.edu.cn (Fagen Li)

efficiency of each industrial equipment by measuring vibration, pressure, temperature, power quality, and so on. If a factory personnel find a potential problem by collecting the data from the IWSNs, he or she can replace or repair the equipment before the efficiency of the equipment drops or the equipment fails entirely. Therefore, by using the IWSNs, we can avoid some catastrophic equipment failures and associated loss. Compared with the traditional wired industrial monitoring system, the IWSNs have lower cost for development and maintenance and higher flexibility and intelligent process capability [3, 4]. IWSNs has the potential to make our cities smarter. The industry is an important part of a city. A smart industry can be obtained by using the IWSNs. We can stay in the office and monitor equipment operation. If the data collected by the IWSNs deviate the normal value, we can switch to the redundant equipment and repair the the failed equipment. While the IWSNs supply a great flexibility for establishing communications, it also bring some technical challenges. In [3], Gungor and Hancke gave eight technical challenges for the IWSNs. The fifth challenge is the security due to all the characteristics of these networks, such as open nature of wireless communication, dynamically changing topology, and the limited capabilities of sensor nodes in terms of processing power, storage, energy and bandwidth. The eighth challenge is the integration with the Internet. To query of the IWSNs to gain the useful information from anywhere and anytime, we need to integrate the IWSNs into the Internet as part of the industrial Internet of Things (IoT). Roman and Lopez [5] gave three methods to gain this integration, front-end proxy solution, gateway solution and TCP/IP overlay solution. In the front-end proxy solution, the sensor nodes can not communicate with the Internet hosts directly. The base station acts as an interface between the IWSNs and the Internet and parses all incoming and outgoing information. That is, the users issue data queries to the sensor nodes through the base station and the base station forwards the results to the users. In this solution, the base station may become the bottleneck and the single point of failure. In both gateway solution and TCP/IP overlay solutions, the sensor nodes can communicate with the Internet hosts directly. In the gateway solution, the base station acts as an application layer gateway which translates the lower layer protocols from both networks. In the TCP/IP overlay solution, the sensor nodes communicate with other nodes using TCP/IP. The base station acts as a router that forwards the packets from and to the sensor nodes.

To prevent abuse of the data collected by the IWSNs, only authorized users are allowed to access the IWSNs. However, it is not an easy thing to design an access control scheme for the IWSNs in the context of the industrial IoT since the resource of the sensor nodes is very limited.

1.1. Related work

In 2009, Le et al. [6] designed an energy-efficient access control scheme for the WSNs using elliptic curve cryptography (ECC). The advantage of ECC is that it can use smaller key size to achieve comparable security level to the other public key cryptosystem such as RSA [7]. For instance, to obtain the 80-bit security level, the modulus size of RSA should be 1024 bits but the key size of ECC only needs 160 bits. In 2011, He et al. [8] proposed a privacy-preserving access control scheme for the WSNs using ring signature [9, 10]. In a ring signature scheme, a signer can anonymously sign a message on behalf of a set of users including itself. A verifier knows that the message comes from a member of a ring, but does not exactly know who the signer is. Therefore, the ring signature can protect the privacy of the signer. Yu, Ren and Lou [11] gave a fine-grained data access control scheme for the WSNs using attribute-based encryption (ABE) [12]. Hur [13] also used ABE to propose a fine-grained data access control scheme with efficient user revocation. In 2012, Zhang, Zhang and Ren [14] designed a new privacy-preserving access control scheme for the WSNs using blind signature. In 2013, Yu et al. [15] designed a novel access control scheme for the WSNs in the context of IoT using signcryption [16, 17] (hereafter called YHZXZ). In 2014, Ma, Xue and Hong [18] also used signcryption to design an access control scheme for the WSNs (hereafter called MXH). The advantage of using signcryption in access control for the WSNs is that it can simultaneously authenticates the users and protects the query messages with a lower cost. Signcryption is a new cryptographic technique that can gain both the functions of public key encryption and digital signature in a logical single step, with a cost significantly lower than that required by the traditional encryption-then-signature or signature-then-encryption methods. That is, a signcryption scheme can simultaneously achieve confidentiality, integrity, authentication and non-repudiation with a lower cost. However, both YHZXZ [15] and MXH [18] are based on the traditional public key infrastructure (PKI). In the PKI system, each user has a private key and a corresponding public key. To ensure the authenticity of the public key, a certificate authority (CA) needs to issue a digital certificate that affords an unforgeable and trusted link between a user's identity and the public key by the digital signature of the CA. The main difficulty in the WSNs using PKI system is the certificates management, including distribution, storage and revocation. In addition, each user should verify the validity of a certificate before using the corresponding public key. If a certificate is not valid, the corresponding public key can not be used in any cryptographic protocols. Otherwise, the public key is believable and can be used. For the access control for the IWSNs in the context of the IoT, it is a heavy burden for the sensor nodes to verify the validity of the public key certificates. To reduce the burden of the sensor nodes, identity-based cryptosystem (IBC) [19]

was used to design the security schemes for the WSNs [20, 21, 22, 23]. Compared with the PKI system, the IBC does not need public key certificates. A user's public key is computed from its identity information, such as telephone numbers, email addresses and IP addresses. The user's private key is produced by a trusted third party called private key generator (PKG). Authenticity of a public key is explicitly verified without a certificate. Therefore, the lightweight IBC is very suitable for design the security schemes for the WSNs. However, the lightweight IBC has a weakness called key escrow problem since the PKG possesses all users' private keys. That is, the PKG can decrypt any ciphertext and forge a signature for any message. Therefore, the IBC is only suitable for small networks, such as the WSNs, and is not suitable for large-scale networks, such as the Internet. For design an access control scheme for the IWSNs in the context of the IoT, we need to find a new solution that has neither key escrow problem nor public key certificates. In 2013, Li and Xiong [24] discussed the secure communication in the IoT using heterogeneous online/offline signcryption. Cirani et al. [25] discussed the security challenges of the IoT. In 2015, Cirani et al. [26] proposed an OAuth-based authorization mechanism for the IoT.

1.2. Motivation and contribution

The motivation of this paper is to find a new solution for design of an access control scheme for the IWSNs in the context of the IoT. The scheme has neither key escrow problem nor public key certificates. Only authorized users can access the IWSNs and the query messages are protected. It is important to protect the query messages for preserving the privacy of the users [18]. Our solution is to use certificateless signcryption (CLSC) [27]. The concept of certificateless cryptography (CLC) was proposed by Al-Riyami and Paterson [28]. The main advantage of the CLC is neither public key certificates nor key escrow problem. The CLC still needs a trusted third party called the key generating center (KGC) who is responsible for producing a partial private key using a master key and a user's identity. Then the user generates some secret value and combines the secret value with the partial private key to get a full private key. Note that the KGC does not know the full private key since it does not know the secret value. We give an access control scheme for the IWSNs in the context of the IoT using the CLSC technique. Our scheme has the ciphertext authenticity that allows us shift the computational cost of the sensor nodes to the gateway. In addition, our scheme also satisfies the public verifiability and insider security. Compared with existing two access control schemes using PKI-based signcryption [15, 18], the computational cost of the sensor node in our scheme is reduced by about 62% and 77%, respectively and the energy consumption of the sensor node in our scheme is reduced by about 64% and 75%, respectively.

1.3. Organization

The rest of this paper is arranged as follows. The network model, security requirements and bilinear pairings are introduced in Section 2. An efficient CLSC scheme is given in Section 3. We give a certificateless access control scheme for the IWSNs in the context of the IoT in Section 4. The performance and security of the proposed access control scheme are discussed in Section 5. Finally, the conclusions are given in Section 6.

2. Preliminaries

In this section, we give the network model, security requirements and bilinear pairings.

2.1. Network model

Fig. 1 shows the overview of the network model that consists of four kinds of entities, a service provider (SP), the sensor nodes, a gateway and the Internet hosts (users). The SP deploys an IWSN that monitors the efficiency of each industrial equipment. The users who hope to access the IWSN should be authorized by the SP. The SP is responsible for the registration for users and sensor nodes and produces the partial private keys for users and the private keys for sensor nodes. That is, the SP acts as the KGC in the CLC environment. The sensor nodes have limited storage resource and computational power while the gateway has higher storage and processing capability. We assume that the SP is always trusted and can never be compromised and the gateway is honest and curious. When a user wants to access the monitoring data of the IWSN, it first sends a query message to a sensor node. Then the gateway checks if the user has been authorized to access the IWSN. If yes, the gateway forwards the query to the sensor node and the node sends collected data to the user in a secure way. Otherwise, the gateway rejects the query request. The model supplies an end-to-end secure communication between the Internet hosts and the IWSN.

2.2. Security requirements

The communication between the users and sensor nodes should satisfy at least four security properties, i.e. confidentiality, authentication, integrity and non-repudiation. Confidentiality is keeping query messages secret from the others except the users and sensor nodes. Even the gateway can not know the contents of the message. Authentication is the assurance that only the authorized users can access the IWSN. Integrity is ensuring that the query messages from the users have not been modified by unauthorized entities. Non-repudiation is preventing the denial of previous queries issued by the users. That is, if a user has submitted a query message to a sensor node, it can not deny its action.

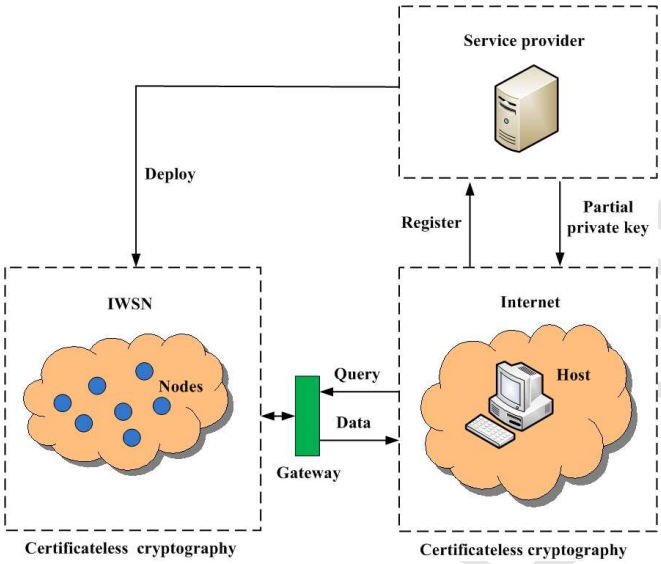

Figure 1: Network model

2.3. Bilinear pairings

Let G_1 and G_2 be two cyclic groups with same prime order p. G_1 is an additive group and G_2 is a multiplicative group. Let P be a generator of G_1. A bilinear pairing is a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ that satisfies the following properties:

1. Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$, $a, b \in \mathbb{Z}_p^*$.
2. Non-degeneracy: There are $P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$, where 1 is the identity element of G_2.
3. Computability: $\hat{e}(P, Q)$ can be efficiently computed for all P,$Q \in G_1$.

The modified Weil pairing and Tate pairing provide admissible maps of this kind. For more details, please refer to [19].

3. A certificateless signcryption scheme

In 2008, Barreto et al. [27] proposed an efficient certificateless signcryption scheme (hereafter called BDCPS). However, this scheme can not be directly used to design an access control scheme for the IWSNs in the context of the IoT. In this section, we first review the BDCPS scheme and then point out its weakness. Finally, we give a modified scheme that is suitable for the design of an access control scheme for the IWSNs in the context of the IoT.

3.1. The BDCPS scheme

The BDCPS scheme consists of the following nine algorithms.

Setup: Given a security parameter k, the KGC selects an additive group G_1 and a multiplicative G_2 of the same prime order p, a generator P of G_1, a bilinear map $\hat{e} : G_1 \times G_1 \to G_2$, and four secure hash functions $H_1 : G_2^2 \times \{0,1\}^* \to \mathbb{Z}_p^*$, $H_2 : G_2 \times \{0,1\}^* \to \mathbb{Z}_p^*$, $H_3 : G_2 \to \{0,1\}^n$ and $H_4 : (G_2 \times \{0,1\}^*)^3 \to \mathbb{Z}_p^*$. Here n is the number of bits of a message to be sent. The KGC randomly chooses a master secret key $s \in \mathbb{Z}_p^*$ and computes the public key $P_{pub} = sP$. The KGC publishes the system parameters $\{G_1, G_2, p, \hat{e}, n, P, P_{pub}, g, H_1, H_2, H_3, H_4\}$ and keeps s secret. Here $g = \hat{e}(P, P)$ is a generator of G_2.

Set-Secret-Value: A user with identity ID_U chooses a random $x_U \in \mathbb{Z}_p^*$ as the secret value.

Set-Public-Value: Given a secret value x_U, this algorithm returns the public value $y_U = g^{x_U}$.

Partial-Private-Key-Extract: A user submits its identity ID_U and public value y_U to the KGC. The KGC computes the partial private key $D_U = \frac{1}{H_2(y_U, ID_U)+s} P$ and sends D_U to the user.

Set-Private-Key: Given a partial private key D_U and a secret value x_U, this algorithm returns a full private key $S_U = (x_U, D_U)$.

Set-Public-Key: Given a full private key $S_U = (x_U, D_U)$ and a public value y_U, the user performs the following steps:

1. Choose $\alpha \in \mathbb{Z}_p^*$ randomly.
2. Compute $r_U = g^{\alpha}$
3. Compute $h_U = H_1(r_U, y_U, ID_U)$.
4. Compute $T_U = (\alpha - x_U h_U) D_U$.
5. Output a full public key (y_U, h_U, T_U).

Public-Key-Validate: Given a full public key (y_U, h_U, T_U), a verifier checks that y_U has order p (i.e. $y_U \neq 1$ but $y_U^p = 1$) and performs the following steps:

1. Compute $r_U = \hat{e}(H_2(y_U, ID_U)P + P_{pub}, T_U) y_U^{h_U}$
2. Compute $h'_U = H_1(r_U, y_U, ID_U)$.
3. Accept the public key if and only if $h'_U = h_U$.

Signcrypt: Given a message m, a sender's secret value x_A, identity ID_A and public value y_A, and a receiver's identity ID_B and public value y_B, this algorithm works as follows.

1. Choose $\beta \in \mathbb{Z}_p^*$ randomly.
2. Compute $r = y_B^{\beta}$.
3. Compute $c = m \oplus H_3(r)$.
4. Compute $h = H_4(r, m, y_A, ID_A, y_B, ID_B)$.

5. Compute $z = \beta/(h + x_A) \bmod p$
6. Output a ciphertext $\sigma = (c, h, z)$.

Unsigncrypt: Given a ciphertext $\sigma = (c, h, z)$, a sender's identity ID_A and public value y_A, and a receiver's secret value x_B, identity ID_B and public value y_B, this algorithm works as follows.

1. Compute $r = y_A^{x_B z} y_B^{hz}$.
2. Compute $m = c \oplus H_3(r)$.
3. Compute $h' = H_4(r, m, y_A, ID_A, y_B, ID_B)$.
4. Accept the message if and only if $h' = h$, return the false symbol $\perp$ otherwise.

The main characteristic of the BDCPS scheme is that BLMQ identity-based signature [29], Schnorr signature [30], and Zheng signcryption [16] are integrated into a certificateless signcryption. In fact, in *Signcrypt* and *Unsigncrypt* algorithms, the BDCPS scheme is similar to Zheng signcryption scheme except the h value. In the BDCPS scheme, the identities and public values of both the sender and the receiver are included in H_4. This change can thwart the key replacement denial-of-decryption attack. In addition, *Set-Public-Key* and *Public-Key-Validate* bind the identity ID_U and public value y_U. A user can generate a full public key (y_U, h_U, T_U) only if it know the corresponding full private key $S_U = (x_U, D_U)$. The BDCPS scheme has been proved to satisfy confidentiality (i.e. indistinguishability against adaptive chosen ciphertext attack (IND-CCA2)) and unforgeability (i.e. existential unforgeability against adaptive chosen messages attack (EUF-CMA)).

3.2. A modified BDCPS scheme

Although the BDCPS scheme is very efficient, the scheme can not be directly used to design an access control scheme for the IWSNs in the context of the industrial IoT because of the following weaknesses:

1. It can not provide the public verifiability since the verification needs the receiver's secret value x_B. If we hope to achieve the full non-repudiation, we needs to use the other complex protocols [27].
2. It can not provide the ciphertext authenticity [31]. That is, the message m is needed in the verification process. Therefore, we can not shift the computational cost of the sensor nodes to the gateway.
3. It does not satisfy the insider security for confidentiality of signcryption [32]. That is, if an adversary knows the sender's secret value x_A, it can unsigncrypt a ciphertext $\sigma = (c, h, z)$

because the following equation holds.

$$r = y_A^{x_B z} y_B^{hz} = y_B^{x_A z} y_B^{hz}$$

The adversary can compute r using the sender's secret value x_A and recover the message m by computing $m = c \oplus H_3(r)$.

Zheng signcryption [16] also has the above three weaknesses. Gamage, Leiwo, and Zheng [33] modified Zheng scheme to achieve public verifiability and ciphertext authenticity. Jung et al. [34] modified Zheng scheme to achieve insider security. The insider security guarantees the forward security of signcryption. Here we combine Gamage, Leiwo, and Zheng's method [33] and Jung et al.'s method [34] to give a modified BDCPS scheme. The first seven algorithms remain unchanged, the last two algorithms are described as follows.

Signcrypt: Given a message m, a sender's secret value x_A, identity ID_A and public value y_A, and a receiver's identity ID_B and public value y_B, this algorithm works as follows.

1. Choose $\beta \in \mathbb{Z}_p^*$ randomly.
2. Compute $t = g^\beta$ and $r = y_B^\beta$.
3. Compute $c = m \oplus H_3(r)$.
4. Compute $h = H_4(t, c, y_A, ID_A, y_B, ID_B)$.
5. Compute $z = \beta/(h + x_A) \bmod p$
6. Compute $R = g^h$
7. Output a ciphertext $\sigma = (c, R, z)$.

Unsigncrypt: Given a ciphertext $\sigma = (c, R, z)$, a sender's identity ID_A and public value y_A, and a receiver's secret value x_B, identity ID_B and public value y_B, this algorithm works as follows.

1. Compute $t = (y_A R)^z$.
2. Compute $h' = H_4(t, c, y_A, ID_A, y_B, ID_B)$.
3. Check if $g^{h'} = R$ holds. If yes, perform the following step 4. Otherwise, output the false symbol $\perp$.
4. Compute $r = t^{x_B}$ and recover $m = c \oplus H_3(r)$.

Gamage, Leiwo, and Zheng [33] and Jung et al. [34] have proved that such modifications do not weaken the security of signcryption. Therefore, the modified BDCPS scheme has the same security as the original BDCPS scheme. In addition, the modified BDCPS scheme has the public verifiability, ciphertext authenticity and insider security. Any third party can verify the

validity of ciphertext σ without knowing the message m and the receiver's secret value x_B. If the ciphertext σ is not valid, we can immediately throw away it without recovering the message m. Even if an adversary knows the sender's secret value x_A, it can not unsigncrypt a ciphertext $\sigma = (c, R, z)$ because the following equation holds.

$$r = t^{x_B} = (y_A R)^{z x_B} = (y_B^{x_A} R^{x_B})^z = (y_B^{x_A} y_B^h)^z$$

It is impossible for the adversary to compute r because the adversary does not know the receiver's secret value x_B and h.

4. A certificateless access control scheme

In this section, we propose an efficient certificateless access control scheme for the IWSNs in the context of the IoT using the modified BDCPS scheme. The access control scheme consists of four phases: the initialization phase, the registration phase, the authentication phase, and the revocation phase. In this scheme, the SP acts as the KGC in the CLC environment. The proposed access control scheme is summarized in Fig. 2

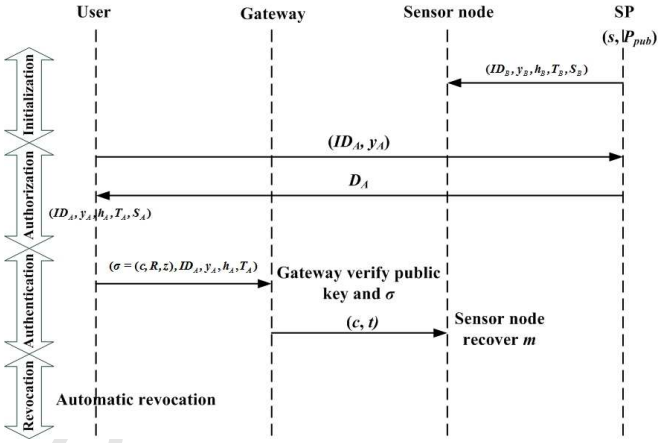

Figure 2: A certificateless access control scheme

4.1. Initialization phase

In this phase, the SP runs *Setup* algorithm and deploys an IWSN. Each sensor node is assigned an identity ID_U, a public key (y_U, h_U, T_U) and a private key $S_U = (x_U, D_U)$ (the SP may run *Set-Secret-Value*, *Set-Public-Value*, *Partial-Private-Key-Extract*, *Set-Private-Key* and *Set-Public-Key* algorithms).

4.2. Registration phase

A user should register with the SP to obtain the access privilege of the IWSN. The user first sends its identity ID_U and public value y_U to the SP and then the SP checks if the identity is valid. If the identity is valid, the SP sets an expiration date ED and runs *Partial-Private-Key-Extract* algorithm to generate a partial private key $D_U = \frac{1}{H_2(y_U, ID_U||ED)+s}P$. Here $||$ is a concatenation symbol. If the identity is not valid, the SP rejects this registration. After receiving D_U, the user runs *Set-Secret-Value*, *Set-Public-Value*, *Set-Private-Key* and *Set-Public-Key* to get a full private key $S_U = (x_U, D_U)$ and a full public key (y_U, h_U, T_U).

4.3. Authentication phase

We assume that a user with identity ID_A want to access the data of a sensor node with identity ID_B. The user first produces a query message m and runs *Signcrypt* algorithm to generate a ciphertext $\sigma = (c, R, z)$. To resist the replay attack, we can concatenate the query message and a timestamp to form a new signcrypted message. Then the user sends the gateway the ciphertext σ, its identity ID_A and full public key (y_A, h_A, T_A). When receiving the query message from the user, the gateway first runs *Public-Key-Validate* algorithm to check the validity of the received public key (y_A, h_A, T_A). If the public key is not valid, the gateway rejects the query request. Otherwise, the gateway further computes $t = (y_A R)^z$ and $h' = H_4(t, c, y_A, ID_A, y_B, ID_B)$ and checks if

$$g^{h'} = R$$

holds. If the above equation does not hold, it rejects the query request. Otherwise, the gateway sends the (c, t) to the sensor node. The sensor node computes $r = t^{x_B}$ and recovers the query message $m = c \oplus H_3(r)$. Then the sensor node can encrypt the collected data using a symmetric cipher (such as AES [35]) with the key $H_3(r)$. The symmetric key $H_3(r)$ is only known by the sensor node and the user, which assures the confidentiality for future communication between the sensor node and the user. In this communication, confidentiality, integrity, authentication and non-repudiation are simultaneously achieved. In addition, an important advantage of our scheme is to achieves the public verifiability and ciphertext authenticity. By using this modified BDCPS scheme, the gateway can verify the validity and the origin of the ciphertext without knowing the receiver' secret value x_B and the message m. Thus, we can shift the most of computational cost of *Unsigncrypt* from the sensor node to the gateway. If required, the anonymity also can be achieved by scrambling the user's identity ID_A and full public key (y_A, h_A, T_A) together with the message at the third step of *Signcrypt* algorithm. That is, we compute $c = (ID_A||y_A||h_A||T_A||m) \oplus H_3(r)$ instead of $c = m \oplus H_3(r)$. Of course, we should

modify the output value of H_3 to adapt the length of the encrypted message. Such changes do not affect the efficiency of our scheme.

4.4. Revocation

The registration is revoked automatically by the expiration date ED. For example, if the expiration date ED is "2015-12-31", the user only can access the IWSN before December 31, 2015. That is, the full private key and full public key of the user automatically become illegal after December 31, 2015. If we must revoke a user's access privilege before the expiration date due to some reasons, the SP can send the revoked identity to the gateway. The gateway keeps a list of revoked identities to identify the validity of users.

5. Analysis of the access control scheme

In this section, we evaluate the performance and security of our access control scheme. First, we compare the computational cost and communication cost of our scheme with those of YHZXZ [15] and MXH [18] in Table 1.

Table 1: Comparison of performance

Schemes	Computational cost			Sensor communication cost	
	User	Sensor	Gateway	Receive	Transmit
YHZXZ [15]	8M	3M	3M	$\|\mathbb{Z}_p^*\| + 2\|G_1\| + \|hash\| + 2\|ID\|$	$2\|\mathbb{Z}_p^*\| + \|G_1\| + \|hash\| + 3\|ID\|$
MXH [18]	2M	5M	—	$\|\mathbb{Z}_p^*\| + \|m\| + \|G_1\| + \|Cert\|$	—
Ours	3E	1E	1P+1M+3E	$\|m\| + \|G_2\|$	—

We denote by P the pairing operation, M the point multiplication operation in G_1 and E the exponentiation operation in G_2. The other operations are ignored in Table 1 since the three operations consume the most running time of the whole algorithm. Let $|x|$ be the number of bits of x. Since both YHZXZ and MXH are based on the traditional PKI environment, we should verify the public key certificate before using a public key. Here we assume that the public key certificates are signed using ECDSA (elliptic curve digital signature algorithm) [36]. The ECDSA needs one point multiplication operation to sign a message and two point multiplication operations to verify a signature. Therefore, in YHZXZ, the gateway needs two point multiplication operations to verify a user's certificate and the user needs four point multiplication operations to verify the certificates of both the gateway and the sensor node. In MXH, the sensor node needs two point multiplication operations to verify a user's certificate. From Table 1, we know that our scheme has less computational cost than YHZXZ and MXH for both the user and the sensor node. Of course, for the gateway, our scheme has more computational

cost than YHZXZ and MXH. The reason is that the gateway finishes a part of *Unsigncrypt* algorithm. In *Unsigncrypt* algorithm, there are three exponentiation operations in G_2. Our scheme shifts two exponentiation operations to the gateway and the sensor node only needs one exponentiation operation. For design an access control scheme for the IWSNs in the context of IoT, the most important issue is to reduce the computational cost of the sensor node since the resource of the sensor node is very limited. Therefor, our scheme is more practical than YHZXZ and MXH.

For the communication cost of the sensor node, YHZXZ needs more cost since it is an interactive protocol. Fortunately, the sensor node is not required to receive the certificate of the user because the gateway helps to do it. In MXH, the sensor node needs to receive the user's certificate $Cert$ to verify its validity. In our scheme, the sensor node does not need to receive the user's identity or certificate. The validity of the user is verified by the gateway. For both YHZXZ and MXH, we adopt the experiment result in [37] on MICA2 that is equipped with an ATmega128 8-bit processor clocked at 7.3728 MHz, 4 KB RAM and 128 KB ROM. From [37], we know that a point multiplication operation takes 0.81 s using an elliptic curve with 160 bits p that represents 80-bit security level. For our scheme, we adopt the result in [38] on the same processor ATmega128. A pairing operation takes 1.9 s and a exponentiation operation in G_2 takes 0.9 s using the supersingular curve $y^2 + y = x^3 + x$ with an embedding degree 4 and implementing η_T pairing: $E(\mathbb{F}_{2^{271}}) \times E(\mathbb{F}_{2^{271}}) \rightarrow \mathbb{F}_{2^{4\cdot 271}}$, which is also equivalent to the 80-bit security level. According the results in [37, 38], the computational time on the sensor node of YHZXZ, MXH and our scheme are $3 * 0.81 = 2.43$ s, $5 * 0.81 = 4.05$ s and $1 * 0.9 = 0.9$ s, respectively. As in [38, 39], we assume that the power level of MICA2 is 3.0 V, the current draw in active mode is 8.0 mA, the current draw in receiving mode is 10 mA, the current draw in transmitting mode is 27 mA and the data rate is 12.4 kbps. For energy consumption, according to the method in [18, 40], a point multiplication operation consume $3.0 * 8.0 * 0.81 = 19.44$ mJ and a exponentiation operation in G_2 consume $3.0 * 8.0 * 0.9 = 21.6$ mJ. Therefore, the computational energy cost on the sensor node of YHZXZ, MXH and our scheme are $3 * 19.44 = 58.32$ mJ, $5 * 19.44 = 97.2$ mJ and $1 * 21.6 = 21.6$ mJ, respectively.

For the communication cost, we assume that $|m| = 160$ bits, $|hash| = 160$ bits and $|ID| = 80$ bits. In addition, the size of a certificate is at least 688 bits [20]. For both YHZXZ and MXH, the size of an element in group G_1 is 1024 bits using an elliptic curve with 160 bits p. By standard compression technique [38], the size of an element in group G_1 can be reduced to 65 bytes. So, in YHZXZ, the sensor node should receive

$$|\mathbb{Z}_p^*| + 2|G_1| + |hash| + 2|ID|\text{bits} = 20 + 2 * 65 + 20 + 2 * 10\text{bytes} = 190\text{bytes}$$

message and transmit

$$2|\mathbb{Z}_p^*| + |G_1| + |hash| + 3|ID|\text{bits} = 2 * 20 + 65 + 20 + 3 * 10\text{bytes} = 155\text{bytes}$$

messages. In MXH, the sensor node should receive

$$|\mathbb{Z}_p^*| + |m| + |G_1| + |Cert|\text{bits} = 20 + 20 + 65 + 86\text{bytes} = 191\text{bytes}$$

messages. Our scheme uses a curve over the binary field $\mathbb{F}_{2^{271}}$. The size of an element in group G_2 is 1084 bits. So in our scheme, the sensor node needs to receive

$$|m| + |G_2|\text{bits} = 20 + 136\text{bytes} = 156\text{bytes}$$

messages. From [38], we know the sensor node consumes $3 * 27 * 8/12400 = 0.052$ mJ and $3 * 10 * 8/12400 = 0.019$ mJ to transmit and receive one byte messages, respectively. Therefore, in YHZXZ, the sensor communication energy consumption is $0.052 * 155 + 0.019 * 190 = 11.67$ mJ. In MXH, the communication energy consumption is $0.019 * 191 = 3.63$ mJ. In our scheme, the communication energy consumption is $0.019 * 156 = 2.96$ mJ. The total energy consumption of the three schemes are $58.32 + 11.67 = 69.99$ mJ, $97.2 + 3.63 = 100.83$ mJ and $21.6 + 2.96 = 24.56$ mJ, respectively.

The computational time and total energy consumption on the sensor node are summarized in Fig. 3 and Fig. 4, respectively. From Fig. 3, we know that the computational cost of our scheme is reduced by about 62% and 77% compared to YHZXZ and MXH, respectively. From Fig. 4, we know that the energy consumption of our scheme is reduced by about 64% and 75% compared to YHZXZ and MXH, respectively. Of course, the computational cost of gateway in our scheme is higher than YHZXZ and MXH. We shift the computational cost of the sensor node to the gateway since our scheme has the ciphertext authenticity. The ciphertext authenticity allows the gateway to verify the ciphertext without the decryption.

We compare the security properties of the three schemes in Table 2. In the "Security" column, Con, Int, Aut, Non, PubVer, CipAut and InsSec denotes confidentiality, integrity, authentication, non-repudiation, public verifiability, ciphertext authenticity and insider security, respectively. A symbol $\surd$ means that the scheme satisfies the security property and a symbol $\times$ means that the scheme does not satisfy the security property. Both YHZXZ and MXH do not satisfy public verifiability, ciphertext authenticity and insider security and our scheme has such security properties. When our scheme is used to create a smart city, the public verifiability allows any third party to check the validity of a query message. In addition, the ciphertext authenticity allows the gateway to check the validity of a query message without knowing the message. If the message is valid, the gateway will forward the message to the sensor node. The

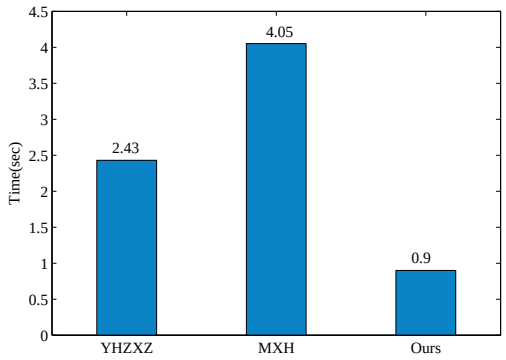

Figure 3: The computational time of the sensor node

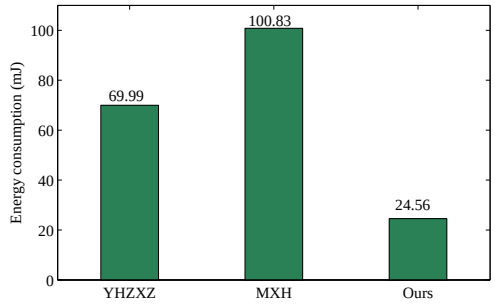

Figure 4: The energy consumption of the sensor node

sensor will decrypt the message without verification. Otherwise, the message will be thrown away by the gateway. The ciphertext authenticity reduces the burden of the sensor node. The insider security prevents an adversary from decrypting a ciphertext even if the adversary knows the secret value of the user. These properties assure the secure operation of a smart city.

Table 2: Comparison of security

Schemes	Security							Environment
	Con	Int	Aut	Non	PubVer	CipAut	InsSec	
YHZXZ [15]	√	√	√	√	×	×	×	PKI
MXH [18]	√	√	√	√	×	×	×	PKI
Ours	√	√	√	√	√	√	√	CLC

6. Conclusion

In this paper, we proposed a modified certificateless signcryption scheme that satisfies public verifiability, ciphertext authenticity and insider security. We also gave a certificateless access

control scheme for the IWSNs in the context of IoT using the modified signcryption. Compared with existing YHZXZ and MXH using PKI-based signcryption, the computational cost of the sensor node in our scheme is reduced by about 62% and 77%, respectively and the energy consumption of the sensor node in our scheme is reduced by about 64% and 75%, respectively.

References

[1] D. He, N. Kumar, N. Chilamkurti, A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks, Information Sciences 321 (2015) 263–277.

[2] R. Rios, J. Cuellar, J. Lopez, Probabilistic receiver-location privacy protection in wireless sensor networks, Information Sciences 321 (2015) 205–223.

[3] V.C. Gungor, G.P. Hancke, Industrial wireless sensor networks: challenges, design principles, and technical approaches, IEEE Transactions on Industrial Electronics 56 (10) (2009) 4258–4265.

[4] J. Niu, L. Cheng, Y. Gu, L. Shu, S.K. Das, R3E: reliable reactive routing enhancement for wireless sensor networks, IEEE Transactions on Industrial Informatics 10 (1) (2014) 784–794.

[5] R. Roman, J. Lopez, Integrating wireless sensor networks and the Internet: a security analysis, Internet Research 19 (2) (2009) 246–259.

[6] X.H. Le, S. Lee, I. Butun, M. Khalid, R. Sankar, M. Kim, M. Han, Y.K. Lee, H. Lee, An energy-efficient access control scheme forwireless sensor networks based on elliptic curve cryptography, Journal of Communications and Networks 11 (6) (2009) 599–606.

[7] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.

[8] D. He, J. Bu, S. Zhu, S. Chan, C. Chen, Distributed access control with privacy support in wireless sensor networks, IEEE Transactions on Wireless Communications 10 (10) (2011) 3472–3481.

[9] R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: Proc. Advances in Cryptology-ASIACRYPT 2001, LNCS 2248, Springer-Verlag, 2001, pp. 552–565.

[10] J.K. Liu, M.H. Au, W. Susilo, J. Zhou, Linkable ring signature with unconditional anonymity, IEEE Transactions on Knowledge and Data Engineering 26 (1) (2014) 157–165.

[11] S. Yu, K. Ren, W. Lou, FDAC: toward fine-grained distributed data access control in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 22 (4) (2011) 673–686.

[12] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proc. ACM conference on Computer and communications security–CCS'06, 2006, pp. 89–98.

[13] J. Hur, Fine-grained data access control for distributed sensor networks, Wireless Networks 17 (5) (2011) 1235–1249.

[14] R. Zhang, Y. Zhang, K. Ren, Distributed privacy-preserving access control in sensor networks, IEEE Transactions on Parallel and Distributed Systems 23 (8) (2012) 1427–1438.

[15] H. Yu, J. He, T. Zhang, P. Xiao, Y. Zhang, Enabling end-to-end secure communication between wireless sensor networks and the Internet, World Wide Web 16 (4) (2013) 515–540.

[16] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost(encryption), in: Proc. Advances in Cryptology-CRYPTO'97, LNCS 1294, Springer-Verlag, 1997, pp. 165–179 .

[17] F. Li, H. Zhang, T. Takagi, Efficient signcryption for heterogeneous systems, IEEE Systems Journal 7 (3) (2013) 420–429.

[18] C. Ma, K. Xue, P. Hong, Distributed access control with adaptive privacy preserving property for wireless sensor networks, Security and Communication Networks 7 (4) (2014) 759–773.

[19] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, SIAM Journal on Computing 32 (3) (2003) 586–615.

[20] K. Ren, W. Lou, K. Zeng, P.J. Moran, On broadcast authentication in wireless sensor networks, IEEE Transactions on Wireless Communications 6 (11) (2007) 4136–4144.

[21] D. He, C. Chen, S. Chan, J. Bu, SDRP: a secure and distributed reprogramming protocol for wireless sensor networks, IEEE Transactions on Industrial Electronics 59 (11) (2012) 4155–4163.

[22] F. Li, D. Zhong, T. Takagi, Practical identity-based signature for wireless sensor networks, IEEE Wireless Communications Letters 1 (6) (2012) 637–640.

[23] H. Lu, J. Li, M. Guizani, Secure and efficient data transmission for cluster-based wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 25 (3) (2014) 750–761.

[24] F. Li, P. Xiong, Practical secure communication for integrating wireless sensor networks into the Internet of things, IEEE Sensors Journal 13 (10) (2013) 3677–3684.

[25] S. Cirani, G. Ferrari, L. Veltri, Enforcing security mechanisms in the IP-based Internet of Things: An algorithmic overview, Algorithms 6 (2) (2013) 197–226.

[26] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, G. Ferrari, IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios, IEEE Sensors Journal 15 (2) (2014) 1224–1234.

[27] P.S.L.M. Barreto, A.M. Deusajute, E.S. Cruz, G.C.F. Pereira, R.R. Silva, Toward efficient certificateless signcryption from (and without) bilinear pairings, in: Proc. Brazilian Symposium on Information and Computer System Security, 2008, pp. 115–125.

[28] S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, in: Proc. Advances in Cryptology-ASIACRYPT 2003, LNCS 2894, Springer-Verlag, 2003, pp. 452–474.

[29] P.S.L.M. Barreto, B. Libert, N. McCullagh, J.J. Quisquater, Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, in: Proc. Advances in Cryptology-ASIACRYPT 2005, LNCS 3788, Springer-Verlag, 2005, pp. 515–532.

[30] C.P. Schnorr, Efficient signature generation by smart cards, Journal of Cryptology 4 (3) (1991) 161–174.

[31] S.S.M. Chow, S.M. Yiu, L.C.K. Hui, K.P. Chow, Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity, in: Proc. Information Security and Cryptology-ICISC 2003, LNCS 2971, Springer-Verlag, 2004, pp. 352–369.

[32] J.H. An, Y. Dodis, T. Rabin, On the security of joint signature and encryption, in: Proc. Advances in Cryptology-EUROCRYPT 2002, Springer-Verlag, 2002, LNCS 2332, pp. 83–107.

[33] C. Gamage, J. Leiwo, Y. Zheng, Encrypted message authentication by firewalls, in: Proc. Public Key Cryptography-PKC'99, LNCS 1560, Springer-Verlag, 1999, pp. 69–81.

[34] H.Y. Jung, D.H. Lee, J.I. Lim, K.S. Chang, Signcryption schemes with forward secrecy, in: Proc. Information Security Applications-WISA 2001, 2001, pp. 403–475.

[35] J. Daemen, V. Rijmen, The design of Rijndael: AES-the Advanced Encryption Standard, Springer, 2002.

[36] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), International Journal of Information Security 1 (1) (2001) 36–63.

[37] N. Gura, A. Patel, A. Wander, H. Eberle, S.C. Shantz, Comparing elliptic curve cryptography and RSA on 8-bit CPUs, in: Proc. Cryptographic Hardware and Embedded Systems-CHES 2004, LNCS 3156, Springer-Verlag, 2004, pp. 119–132 .

[38] K.A. Shim, Y.R. Lee, C.M. Park, EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks, Ad Hoc Networks 11 (1) (2013) 182–189.

[39] X. Cao, W. Kou, L. Dang, B. Zhao, IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks, Computer Communications 31 (4) (2008) 659–667.

[40] K.A. Shim, S^2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks, Ad Hoc Networks 19 (2014) 1–8.

Biographies

Fagen Li is an associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, P.R. China. He received his Ph.D. degree in Cryptography from Xidian University, Xi'an, P.R. China in 2007. From 2008 to 2009, he was a postdoctoral fellow in Future University-Hakodate, Hokkaido, Japan, which is supported by the Japan Society for the Promotion of Science (JSPS). He worked as a research fellow in the Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan from 2010 to 2012. His recent research interests include cryptography and network security. He has published more than 70 papers in the international journals and conferences. He is a member of the IEEE.

Jiaojiao Hong is now a master student in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, P.R. China. Her research interests include cryptography and information security.

Anyembe Andrew Omala is now a Ph.D. student in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, P.R. China. His research interests include cryptography and network security.