Copyright © 2019 Tech Science Press CMC, vol.59, no.3, pp.903-924, 2019

EIAS: An Efficient Identity-Based Aggregate Signature Scheme for WSNs Against Coalition Attack

Yong Xie[1], Fang Xu[2], Xiang Li[1], Songsong Zhang[1], Xiaodan Zhang[1,*] and Muhammad Israr[3]

Abstract: Wireless sensor networks (WSNs) are the major contributors to big data acquisition. The authenticity and integrity of the data are two most important basic requirements for various services based on big data. Data aggregation is a promising method to decrease operation cost for resource-constrained WSNs. However, the process of data acquisitions in WSNs are in open environments, data aggregation is vulnerable to more special security attacks with hiding feature and subjective fraudulence, such as coalition attack. Aimed to provide data authenticity and integrity protection for WSNs, an efficient and secure identity-based aggregate signature scheme (EIAS) is proposed in this paper. Rigorous security proof shows that our proposed scheme can be secure against all kinds of attacks. The performance comparisons shows EIAS has clear advantages in term of computation cost and communication cost when compared with similar data aggregation scheme for WSNs.

Keywords: Wireless sensor networks (WSNs), big data, signature aggregation, efficiency, coalition attack.

1 Introduction

With the rapid development of information technology, various new significant services continuously spring up, such as cloud computing [Sookhak, Gani, Khan et al. (2017)], social networks [Su, Xu and Qi (2016)], and Internet of things [Sun, Song, Jara et al. (2016)]. To provide better services, a great deal of data are gathered by cameras, sensory nodes, sound recorders, information-sensing mobile devices, software logs and so on [Botta, De Donato, Persico et al. (2016)]. Wireless sensor networks (WSNs) are the major contributors to data acquisition for more and more exciting network services based on big data.

WSNs are consisted of a large number of sensor nodes that integrated senor model,

[1] Department of Computer Technology and Application, Qinghai University, Xining, China.
[2] School of Computer and Information Science, Hubei Engineering University, Xiaogan, China.
[3] Department of Computer Sciences, COMSATS University, Abbottabad, Pakistan.
[*] Corresponding Author: Xiaodan Zhang. Email: zhangxd@ipp.ac.cn.

CMC. doi:10.32604/cmc.2019.05309 www.techscience.com/cmc

data processing model and wireless communication module. The sensor nodes can achieve various of data monitors, such as temperature, humidity, noise and light intensity, atmospheric pressure, trajectory of moving object and soil composition and so on, by embedding a variety of sensing devices. The primary goal of WSNs system is to acquire a large number of real-time data from sensors and store all data in a data center, then provide all manner of services based on the big data. Therefore, the nodes in WSNs are self-organized into a large-scale unattended intelligent or semi-intelligent distributed network system through multi-hop communication [Mahmood, Seah and Welch (2015)]. Nowadays, WSNs have very broad application prospects in environmental monitoring (such as transportation, living area, safety monitoring), industrial inspection (such as work flow control, equipment diagnosis), key infrastructure assurance (such as power grids, water conservancy, fire monitoring), process control in hazardous areas. The powerful data acquisition and processing potential of WSNs have been highly valued by the military, academia and industry in many countries, therefore, WSNs possess important scientific research and practical value. However, as a new type of large-scale self-organization system, there are many challenges in WSNs, from the physical layer signal modulation and wireless receiving and sending technique, to the media access technology of data link layer and error control mechanism, to the data routing protocol of transport layer and so on [Li, Tryfonas and Li (2016)].

Because the true sensing data is the basic guarantee for realizing various complex data application services, the factual collection, secure transmission and secure storage of sensing data are the core goal of implementing the WSNs tasks [Rashid and Rehmani (2016)]. To realize true sensing data transmission, more and more scholars have devoted themselves to design secure authentication protocols for WSNs. However, unlike traditional networks, WSNs possess an inherent characteristics of resource constraint and design limitation, such as low band width, short communication distance, limited energy, processing and storage. Therefore, it is a great challenge to design secure and efficient authentication protocol for WSNs for their limited resources [Di Pietro, Guarino, Verde et al. (2014)].

To address the problems caused by the limited resources, Boneh et al. [Boneh, Gentry, Lynn et al. (2003)] proposed a general aggregate signature scheme in 2003. This scheme allows anyone to generate a short aggregate signature by combining multiple signatures from different users, which can reduce nodes? energy consumption during data transmission. Since then, aggregate signature has been widely researched for its unparalleled advantage in decreasing communication cost and energy consumption. As with other communications technologies, security issue is an unavoidable issue for data aggregation, some special security attacks with hiding feature and subjective fraudulence become more threatening, such as coalition attack. Coalition attack means that attackers use one or more invalid single signatures together with other valid signatures to construct a valid aggregate signature [Bellare, Micciancio and Warinschi (2003)]. Obviously, coalition attack can subtly destroy the validity and integrity of aggregated messages, and breach the security requirements of aggregate signature schemes. Therefore, to design a secure and efficient data aggregation scheme that is secure against coalition attack is of great significance to WSNs.

1.1 Motivations and contributions

Aimed to decrease the energy consumption and ensure data integrity during data transmission, we proposed a secure identity-based aggregate signature scheme (EIAS) for WSNs in this paper. The proposed scheme can achieve data integrity protection, user authentication and data aggregation by combining multiple signatures that signed on sensing data from different sense nodes into one single short aggregate signature. Hence, the proposed scheme not only could protect data integrity, but also can decrease communication cost and storage cost for WSNs. In summary, the proposed scheme has four major contributions as follows.

First, we present a system model for WSNs with data aggregation function. The data cluster nodes can authenticate sensing data from sensor nodes and aggregate them into one message before sending them to the data center, as shown in Fig. 1.

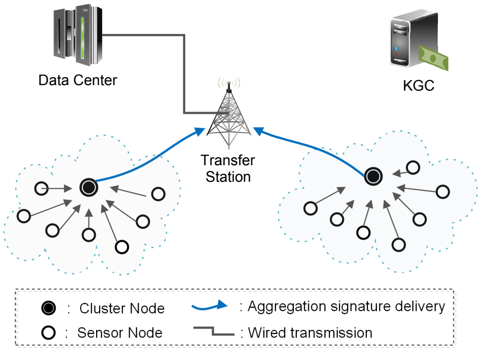

Figure 1: A typical structure of aggregation signature system in WSNs

Second, we present an efficient and secure identity-based aggregate signature scheme (EIAS) by using elliptic curve cryptosystem, which has efficient message signing algorithm, message verification algorithm and data aggregation algorithm.

Third, based on elliptic curve discrete logarithm problem under random oracle model, a rigorous security proof is presented to show that EIAS can resist all kinds of security attacks (included coalition attack) and ensure data integrity, which achieves the key safeguard for superior service based on WSNs.

Four, the detailed performance comparisons between EIAS and Shenet al.'s recently proposed scheme [Shen, Ma, Liu et al. (2016)] is presented in this paper. The results show that EIAS have clear advantages in computation and communication cost during the data collection and delivery.

1.2 Organization of the paper

The rest of this paper is arranged as follows. Section 2 introduces the related works that proposed recently. Section 3 introduces the preliminaries demanded in this paper and Section 4 shows the system model and security requirement. Next, we propose identity-based aggregate signature scheme for WSNs in Section 5. The security proof and analysis are presented in Section 6. The performance comparisons are discussed in Section 7. At last, conclusion and future work are drawn in Section 8.

2 Related works

In recent years, data security and data integrity are two key issues in data gathering of WSNs, and have received a considerable research attention [Kumari, Khan and Atiquzzaman (2015)], and many related security schemes have been presented for WSNs. There security schemes have their own advantages in different core applications. However, most of them have different security vulnerabilities and are not able to achieve certain security requirements under some known or unkown attacks [He, Zeadally, Kumar et al. (2017)]. Das [Das (2009)] presented a password-based authentication scheme by using smart card for WSNs. However, this scheme was proven to be vulnerable to Dos attack and capture attack. Based on this work, some improved security schemes [Turkanovic and Holbl (2013); Yuan (2014); Chen and Shih (2010)] have been presented. To overcome the deficiency of Das [Das (2009)], Das et al. [Das, Sharma, Chatterjee et al. (2012)] proposed an improved two factors password-based authentication scheme for hierarchical WSNs. Unfortunately, It has been pointed out that its implementation is infeasible in practical applications [Turkanovic and Holbl (2013)]. Xue et al. [Xue, Ma, Hong et al. (2013)] proposed a temporal-credential-based mutual authentication scheme for gateway nodes in WSNs. But Li et al. [Li, Weng and Lee (2013)] pointed that Xue et al.'s scheme is subject to identity guessing attack, tracking attack, privileged insider attack and weak stolen smart card attack, and then presented an improved scheme. Jiang et al. [Jiang, Ma, Lu et al. (2015)] also proposed an improved message authentication scheme with unlinkability over Xue et al.'s [Xue, Ma, Hong et al. (2013)] scheme. However, Jiang et al.'s scheme [Jiang, Ma, Lu et al. (2015)] was demonstrated that has several drawbacks, such as suffering from privileged insider attack and failing to provide proper authentication. In order to eliminate those drawbacks, Das [Das (2016)] proposed an improved three-factor user authentication scheme over Jiang et al.'s scheme. Turkanovic et al. [Turkanović, Brumen and Hölbl (2014)] presented a lightweight key agreement protocol for heterogeneous WSNs. But soon later, Changet al. [Chang and Le (2016)] demonstrated that Turkanovic et al.'s [Turkanović, Brumen and Hölbl (2014)] scheme cannot be secure against stolen verifier attack, impersonation attack, spoofing attack and so on. To eliminate security pitfalls, Chang et al. [Chang and Le (2016)] proposed two schemes, one is efficient scheme overcoming the weaknesses of Turkanovic et al.'s [Turkanović, Brumen and Hölbl (2014)] scheme, the other is an improved scheme over the former which can provide perfect forward secrecy with less modification. However, Chang et al.'s scheme is vulnerable to session key breach attack and session specific temporary information attack. Amin et al. [Amin and Biswas (2016)] proposed an authentication and key agreement scheme for WSNs with a novel architecture. But it can not be secure against tracking attack and achieve user untraceability [Jiang, Zeadally, Ma et al. (2017)]. To solve this deficiency, Jiang et al. [Jiang, Zeadally, Ma et al. (2017)] proposed a secure user authentication protocol by using Rabin cryptosystem. However, all of the above mentioned schemes focus little on data aggregation and reducing communication overhead for WSNs.

Since Boneh et al. [Boneh, Gentry, Lynn et al. (2003)] proposed a general aggregate signature scheme in 2003, data aggregation technology has been widely used for WSNs. Without doubt, the security issue of data aggregation technology is an unavoidable issue in WSNs. Recently, researchers have proposed plenty of aggregate signature scheme for WSNs [Wen, Ma and Huang (2011); Zhang and Zhang (2009); Liu, Zhu, Ma et al. (2014); Zhang, Hu, Wu et al. (2016)]. Wen et al. [Wen, Ma and Huang (2011)] used bilinear pairings to constructed an aggregate signature scheme based on specified verifier. Hartung et al. [Hartung, Kaidel, Koch et al. (2016)] proposed a new fault-tolerant aggregate signature scheme by fixed number of messages in one aggregate signature. Zhang et al. [Zhang, Wu, Domingo-Ferrer et al. (2017)] proposed an identity-based aggregate signature scheme with privacy-preserving for VANETs, and this scheme provides hierarchical aggregation and batch verification to decrease communication cost. Tang et al. [Tang, Liu, Zhao et al. (2018)] proposed an aggregate signature scheme by using trust routing, in which the trust routing takes is difficult in deployment. However, it is a pity that the above mentioned schemes have one or more security flaws, especially can not secure against coalition attack [Shen, Ma, Liu et al. (2016)]. As mentioned earlier, coalition attack can destroy the validity and integrity of aggregated messages.

3 Preliminaries

3.1 Elliptic curve cryptosystem (ECC)

Elliptic curve in cryptography is firstly proposed by Miller [Miller (1984)] in 1984. Soon later, based on the difficulty of elliptic curve discrete logarithm problem (ECDLP), Koblitz [Koblitz (1987)] presented an ECC instance. From then on, many cryptographic protocols and secure schemes is designed by using ECC because of its effectiveness in both computation cost and communication cost. The ECC is defined as following.

Let p is a large prime number, F_p is defined as a finite field determined by p. Based on equation $y^2 = x^3 + ax + b \bmod p$, E/E_p is a set of elliptic curve point over F_p, where $x, y, a, b \in F_p, (4a^3 + 27b^2) \bmod p \neq 0$. Point Θ at infinite and all point on E/E_p consist of a additive group G_p. G_p satisfy the following essential properties [Liu, Guo, Fan et al. (2018)].

Point addition: Assume P and Q be two points of E/E_p and $P \neq Q$, a line joining P and Q will intersect E/E_p at a point $-R$. If $P = Q$, a line joining P and Q will be a tangent line of E/E_p.

Point subtraction: Assume P and Q be two points of E/E_p and $Q = -p$, the two point subtraction is express as $P + Q = P - P = \Theta$, i.e. the line joining P and Q will intersect E/E_p at a infinite point Θ

Scalar point multiplication: Assume P be a point of E/E_p, m point P's addition is defined as scalar multiplication, i.e., $m \cdot P = P + P + \cdots + P(m\text{times})$, where, $m \in Z_p, m > 0$.
Order of group: Assume $n > 0, m \in Z_p$, we call n is the order of group G_p if n is smallest number that makes $n \cdot P = \Theta$,

3.2 Complexity assumptions

In this subsection, the computational hard problem related to ECC is described as follows.

Elliptic curve discrete logarithm problem (ECDLP): Given two random point $P, Q \in E/E_p$, $Q = \alpha \cdot P$, to calculate α from Q for unknown $\alpha \in {}_R Z_p^*$. The probability for a probabilistic-polynomial-time (PPT) adversary A to solve the ECDLP problem is $Adv_A^{\mathbf{ECDLP}} = \Pr[A(P, Q = \alpha \cdot P) = \alpha]$. The hardness is that the $Adv_A^{\mathbf{ECDLP}}$ to solve the ECDLP problem is negligible in polynomial time.

3.3 Identity-based cryptography

The identity-based cryptography was introduced by Shamir in 1984 [Shamir (1984)]. The identity-based cryptography can ease key management problem because the public key certificate is no longer needed. In the identity-based cryptography, each unique identity information of the users, such as identity number, email address and telephone number, can be used to generate their identical public key. The private key generator (PKG) is charge of generating and issuing the private key of each user according to its identical public key. The signature system using identity-based cryptography is called identity-based signature (IBS) system, in which signature verification only needs public parameters, signer's identity and signature pair. Thus, there is no longer requires certificates in IBS system.

4 System model and security model

4.1 System model

Wireless sensor networks (WSNs) are widely used in various fields, so system models are changed due to application requirements. According to Shen et al. [Shen, Ma, Liu et al. (2016); He, Zhang, Gu et al. (2017)], we can analysis the system model of WSNs in this paper from two aspects: roles and data.

Roles: According to Shen et al. [Shen, Ma, Liu et al. (2016); He, Zhang, Gu et al. (2017)], the system model of WSNs in this paper is considered to be consisted of four network roles, i.e., Key Generation Center (KGC), Sensor nodes, Cluster nodes and Data Center. There are other relay roles, such as transfer stations, that only need to relay messages without authentication or aggregation.

• KGC: The KGC is in charge of generating system parameters and generating the identity key for each sensor node. The KGC is assumed to be infeasible to compromise by any adversaries. And the KGC is also assumed as a trusted role and can be trusted by all roles.

• Sensor Nodesbf: Sensor nodes are in charge of obtaining sensing and sending data to data center via cluster nodes and other relay role, such as transfer stations. Before sending data, sensor nodes should make signatures on the data.

• Cluster Nodes: Cluster nodes are in charge of signature verification and aggregation. Cluster nodes authenticate data from sensor nodes, then aggregate signatures into one aggregate signature, finally send the aggregated message to the data center via other relay roles.

• Data Center: The data center is in charge of verifying aggregated messages and storing the data.

Data: The sensory data are the core of various of services based on WSNs. Generally speaking, the data in WSNs includes the sensing data, acquisition time and other related information. To protect data integrity and authentication, sensing data must be signed. The data that have been signed by sensor nodes can be divided into two type in term of signature: One is valid data that their signature can pass verification, the other is invalid that their signature cannot pass verification.

In WSNs, the data flow from data generation to storage can be illustrated as follows: Sensor nodes periodically collect sensory data, then add acquisition time and other information to the data, then make a signature on the data. Next, sensor nodes send the signed message to the cluster nodes. Upon receiving messages from sensor nodes, cluster nodes verify the signatures then aggregate these signatures, then send the aggregated message to data center via other relay roles. Other relays roles in the systme only relays messages without verification or aggregation. The data flow is illustrated in Fig. 1.

4.2 Security model

Security requirements in WSNs mainly are integrity, authenticity, availability and flexibility, etc. In our system model, our main concern is the data integrity protection during the data collection and delivery process under the premise of improving the verification efficiency and reducing the communication cost [He, Kumar and Chilamkurti (2015)]. Therefore, providing message authentication, being secure against modification attack, data tampering attack, impersonation attack, relay attack are the main security requirements for the security system in WSNs [Liu, Zhong, Chang et al. (2016)].

According to the network model of WSNs system and the definitions of adversary? ability, we define the security model by a game played between a challenger $\mathcal{C}$ and adversary $\mathcal{A}$ under the random oracle model for the proposed scheme. In the game, the adversary $\mathcal{A}$ can ask for any queries as follows.

$Initialization$-Oracle: In this query, the challenger $\mathcal{C}$ will generate the public parameters and the private key of the system. Then $\mathcal{C}$ sends the pubic parameters to the adversary $\mathcal{A}$.

h-Oracle: When $\mathcal{A}$ makes this kind query, $\mathcal{C}$ selects a number $\Upsilon_{\hbar} \in {}_R Z_q^*$, and sets a tuple $(\Delta, \Upsilon_{\hbar})$ into Oralc-List hL and answers $\mathcal{A}$ with $\Upsilon_{\hbar}$.

$Sign$-Oracle: When $\mathcal{A}$ makes this query with message $\{data_i\}$, $\mathcal{C}$ creates a reply message $\{\sigma_i, R_i, U_i, ID_i, data_i\}$ to $\mathcal{A}$.

In this game, $\mathcal{A}$ could break the signature scheme ∇ only if it can forge a valid request message. Assume $Adv_{\nabla}^{Sign}(\mathcal{A})$ is the probability that $\mathcal{A}$ can break the signature scheme ∇ in this game.

Definition 1 A signature scheme for WSNs can be determined to be secure if the probability $Adv_{\nabla}^{Sign}(\mathcal{A})$ is negligible for any PPT adversary $\mathcal{A}$.

5 The proposed scheme (EIAS)

In this section, we present an Identity-based signature scheme with message aggregation by using ECC. The proposed scheme no longer needs any bilinear paring operations. The proposed scheme consists of five phases: system initialization phase, identity key generation phase, message signing phase, message aggregation phase and aggregation verification phase. For simplicity, the notations and corresponding descriptions are listed in Tab. 1.

Table 1: Notations used and Description

Symbol	Description
KGC	The Key Generation Center
ID_i	The i^{th} sensor node
$E_p(a, b)$	An elliptic curve:$y^2 = x^3 + ax + b \bmod p$
P	The base point of the elliptic curve
s	The secret key of the KGC
P_{pub}	$P_{pub} = sP$, it denotes the public key of KGC
$data_i$	The sensing data including current time
$h(.)$	one-way hash function

Next, the five phases are described as following subsections.

5.1 System initialization phase

In this phase, the KGC is in charge of generating system parameters. First, the KGC defines the security parameter λ (such as security level on 80 bits), then selects an elliptic curve $E_p(a, b)$ defined by equation $y^2 = x^3 + ax + b \bmod p$, where p is a large prime, $a, b \in F_p$, and then selects a point P on $E_p(a, b)$ as a generator of group G with order q ,where G is a point set including all point on and the point at infinity Θ. Next, the KGC selects a key $s \in Z_q^*$ as its private secret key, and calculates $P_{pub} = sP$ as its public key. Next, it selects three secure hash functions, $h_1 : G \times \{0, 1\}^* \rightarrow Z_q$, $h_2 : G \times G \times \{0, 1\}^* \times \{0, 1\}^* \rightarrow Z_q$, $h_3 : \underbrace{G \times G \times \cdots \times G}_{n} \times \{0, 1\}^* \times \{0, 1\}^* \rightarrow Z_q$, as cryptographic hash function used in scheme. At last, the KGC publics system public parameters *paras*=$\{E_p(a, b), p, q, P, h_1, h_2, h_3, P_{pub}\}$.

5.2 Identity key generation phase

In this phase, the KGC generates the identity key for each sensor node. Assume current sensor node's identity with $ID_i \in \{0,1\}^*$ is in the registration process, the KGC selects a random number $u_i \in Z_q^*$, and computes $U_i = u_i P$, $\xi_i = h_1(U_i, ID_i)$, $s_i = u_i + \xi_\mathrm{i} s$. At last the KGC sends $\{U_i, s_i\}$ as identity key $IDkey$ to the sensor node ID_i in a secure way.

5.3 Message signing phase

When the sensor nodes have obtained sensing data. Assume a node with identity ID_i has $data_i$. The node selects a random number $r_i \in Z_q^*$, computes $R_i = r_i P$, $\rho_i = h_2(R_i, U_i, ID_i, data_i)$, $\sigma_i = s_i + \rho_\mathrm{i} r_i$. Then the node ID_i sends message $\{\sigma_i, R_i, U_i, ID_i, data_i\}$ to the cluster node ID_j.

5.4 Message aggregation phase

In this phase, the cluster node authenticates messages from sensor nodes, then aggregates these authenticated messages into one aggregated message, finally sends the aggregated message to the data center.

• Message verifying

On receiving a message $\{\sigma_i, R_i, U_i, ID_i, data_i\}$, the cluster node ID_j computes $\xi_i = h_1(U_i, ID_i)$, $\rho_i = h_2(R_i, U_i, ID_i, data_i)$, then verifies it satisfies the verification equation Eq. (1).

$$\sigma_i P = U_i + \xi_i P_{pub} + \rho_i R_i \tag{1}$$

If not, ID_j declines the message $\{\sigma_i, R_i, U_i, ID_i, data_i\}$. Else, ID_j accepts. Because $\sigma_i = s_i + \rho_\mathrm{i} r_i$ and $s_i = u_i + \xi_\mathrm{i} s$, the correctness of verification equation (1) can be proved as the following:

$$\begin{aligned} \sigma_i P &= (s_i + \rho_\mathrm{i} r_i)P \\ &= (u_i + \xi_\mathrm{i} s + \rho_\mathrm{i} r_i)P \\ &= u_i P + \xi_\mathrm{i} sP + \rho_\mathrm{i} r_i P \\ &= U_i + \xi_i P_{pub} + \rho_i R_i \end{aligned}$$

Therefore, the verification equation (Eq. (1)) is correct.

• Message aggregation

After receiving n messages $\{\sigma_1, R_1, U_1, ID_1, data_1\}$, $\{\sigma_2, R_2, U_2, ID_2, data_2\}$, $\cdots$,$\{\sigma_n, R_n, U_n, ID_n, data_n\}$, the cluster node ID_j can aggregate these messages for saving communication cost and computation cost for later delivering and verification. It computes $\lambda^j = h_3(U_1 + \xi_1 P_{pub} + \rho_1 R_1, U_2 + \xi_2 P_{pub} + \rho_2 R_2, \cdots, U_n + \xi_n P_{pub} + \rho_n R_n, \sum_{i=1}^{n} \xi_i, \sum_{i=1}^{n} \rho_i)$, $\delta^j = \lambda^j \sum_{i=1}^{n} \sigma_i$, and sends $\{\sigma_j^*, \{R_j^k, U_j^k, ID_j^k, data_j^k\}^{k=\{1,2,\cdots,n\}}\}$ as the aggregated message to the data center.

5.5 Aggregation verification phase

When the data center receives the aggregated message $\{\sigma^j, \{R_k^j, U_k^j, ID_k^j, data_k^j\}^{k=\{1,2,\cdots,n\}}\}$ from the cluster node ID_j, it computes each message in the aggregated messages as $\xi_i = h_1(U_i, ID_i)$, $\rho_i = h_2(R_i, U_i, ID_i, data_i)$, $\lambda^j = h_3(U_1+\xi_1 P_{pub}+\rho_1 R_1, U_2+\xi_2 P_{pub}+\rho_2 R_2, \cdots, U_n+\xi_n P_{pub}+\rho_n R_n, \sum_{i=1}^{n}\xi_i, \sum_{i=1}^{n}\rho_i)$. Then it checks whether the following aggregation verification equation (Eq. (2)) holds or not.

$$\sigma^j P = \lambda^j(\sum_{i=1}^{n} U_i + (\sum_{i=1}^{n}\xi_i)P_{pub} + \sum_{i=1}^{n}\rho_i R_i) \tag{2}$$

If holds, it accepts these messages. Or, it drops these messages.
Because $\sigma_i = s_i + \rho_{\mathrm{i}} r_i$, $s_i = u_i + \xi_{\mathrm{i}} s$, $\lambda^j = h_3(U_1 + \xi_1 P_{pub} + \rho_1 R_1, U_2 + \xi_2 P_{pub} + \rho_2 R_2, \cdots, U_n + \xi_n P_{pub} + \rho_n R_n, \sum_{i=1}^{n}\xi_i, \sum_{i=1}^{n}\rho_i)$ and $\delta^j = \lambda^j \sum_{i=1}^{n}\sigma_i$, the correctness of verification equation (Eq. (2)) can be proved as the following:

$$\begin{aligned}
\sigma^j P &= \lambda^j \sum_{i=1}^{n}\sigma_i P \\
&= \lambda^j \sum_{i=1}^{n}(s_i + \rho_i r_i)P \\
&= \lambda^j \sum_{i=1}^{n}(u_i + \xi_i s + \rho_i r_i)P \\
&= \lambda^j \sum_{i=1}^{n}(u_i P + \xi_i sP + \rho_i r_i P) \\
&= \lambda^j(\sum_{i=1}^{n} U_i + (\sum_{i=1}^{n}\xi_i)P_{pub} + \sum_{i=1}^{n}\rho_i R_i)
\end{aligned}$$

Therefore, the verification equation Eq. (2) is correct.

6 Security proof and analysis

In this section, we firstly present the security proof that the proposed scheme (EIAS) is secure against adaptive chosen ciphertext attacks, then we demonstrate that EIAS can satisfy the security requirements of WSNs system.

6.1 Security proof

In this subsection, the proposed identity-based signature scheme for WSNs is assessed on the security under the random oracle model.

Theorem 1 The proposed scheme is existentially unforgeable against an adaptive chosen-message attack under the random oracle model.

Proof. Assume an adversary $\mathcal{A}$ can forge a signature $\{\sigma_i, R_i, U_i, ID_i, data_i\}$ on the sensor $data_i$. Let $(P, Q = xP)$ be an ECDLP instance for two random point P and Q on E/E_p. $\mathcal{C}$ can solve the ECDLP problem with non-negligible probability by run $\mathcal{A}$ as subprogram.

Initialization. The challenger $\mathcal{C}$ runs system initialization procedure, defines $P_{pub} = Q = xP$ as system public key, and obtains *paras*=$\{E_p(a,b), p, q, P, h_1, h_2, h_3, P_{pub}\}$, and sets two oracle-lists. The two lists are hL_1 with form of $< U_i, ID_i, \tau_1 >$ and hL_2 with form of $< R_i, U_i, ID_i, data_i, \tau_2 >$ respectively. hL_1 consists of the queries and answers of h_1-Oracle. hL_2 consists of the queries and answers of h_2-Oracle. The two lists are empty at their initialization. At last $\rfloor$ sends params to $\mathcal{A}$.

h_1-queries. When $\mathcal{A}$ makes this query with message $\{U_i, ID_i\}$, $\mathcal{C}$ checks if the tuple $< U_i, ID_i, \tau_1 >$ is in hL_1. If so, $\mathcal{C}$ sends $\tau_i = h_1(U_i, ID_i)$ to $\mathcal{A}$. Or $\mathcal{C}$ selects $\tau_1 \in {}_R Z_q^*$, then adds $< U_i, ID_i, \tau_1 >$ to hL_1. Finally, $\mathcal{C}$ answers $\mathcal{A}$ with τ_1.

h_2-queries. When $\mathcal{A}$ makes this query with messages $< R_i, U_i, ID_i, data_i >$, $\mathcal{C}$ checks if the tuple $< R_i, U_i, ID_i, data_i >$ is in hL_2. If so, $\mathcal{C}$ sends $\tau_2 = h_2(R_i, U_i, ID_i, data_i)$ to $\mathcal{A}$. Or $\mathcal{C}$ selects $\tau_2 \in {}_R Z_q^*$, then adds $< R_i, U_i, ID_i, data_i, \tau_2 >$ to hL_2. Finally, $\mathcal{C}$ answers $\mathcal{A}$ with τ_2.

Sign-queries. When $\mathcal{A}$ makes this query with message $data_i$, $\mathcal{C}$ chooses $\sigma_i, \xi_i \in {}_R Z_p^*$, computes $U_i = \sigma_i P - \rho_i R_i - \xi_i P_{pub}$, then $\mathcal{C}$ adds $< R_i, U_i, ID_i, data_i, \sigma_i >$ to hL_2, next $\mathcal{C}$ answers $\mathcal{A}$ with $\{R_i, U_i, ID_i, data_i, \sigma_i\}$.

According to the designation of EIAS, all the $\mathcal{A}$'s answers to the **Sign-queries** are valid: message $\{R_i, U_i, ID_i, data_i, \sigma_i\}$ could meet the signature verification equation (Eq. (3)).

$$\begin{aligned}\sigma_i P &= U_i + \xi_i P_{pub} + \rho_i R_i \\ &= (\sigma_i P - \rho_i R_i - \xi_i P_{pub}) + \xi_i P_{pub} + \rho_i R_i \\ &= \sigma_i P\end{aligned} \tag{3}$$

Output. At last, $\mathcal{A}$ can output a message $\{R_i, U_i, ID_i, data_i, \sigma_i\}$ in non-negligible probability. the message can be verified by Eq. (4).

$$\sigma_i P = U_i + \xi_i P_{pub} + \rho_i R_i \tag{4}$$

If not hold, $\mathcal{C}$ abandons the current game.

On the basis of the forgery lemma [Pointcheval and Stern (1996)], another valid message $\{R_i, U_i, ID_i, data_i, \sigma_i^*\}$ can be generated if $\mathcal{A}$ does a repetition of the game by using another ξ_i^*. Under these circumstances, this message can meet equation (Eq. (5)).

$$\sigma_i^* P = U_i + \xi_i^* P_{pub} + \rho_i R_i \tag{5}$$

It can deduce a new equation with Eq. (4) and Eq. (5) as following.

$$\begin{aligned}&(\sigma_i - \sigma_i^*) \cdot P = \sigma_i \cdot P - \sigma_i^* \cdot P\\ &= U_i + \xi_i \cdot P_{pub} + \rho_i R_i - (U_i + \xi_i^* \cdot P_{pub} + \rho_i R_i)\\ &= (\xi_i - \xi_i^*) \cdot P_{pub}\\ &= (\xi_i - \xi_i^*) \cdot x \cdot P\end{aligned} \tag{6}$$

From Eq. (6), we could obtain equation Eq. (7).

$$(\delta_i - \delta_i^*) = (\xi_i - \xi_i^*) \cdot x \bmod q \tag{7}$$

Therefore, $\mathcal{C}$ can solve the instance of the ECDLP problem by the output of Eq. (7) (i.e., $(\delta_i - \delta_i^*) \cdot (\xi_i - \xi_i^*)^{-1}$). But, it is in contradiction with the hardness hypothesis of ECDLP problem. Therefore, it can draw a conclusion that EIAS is secure against adaptive chosen message attack under random oracle model.

Theorem 2 Assume h_3 is a collision resistant hash function, the aggregate signature of EIAS is secure and valid only on the condition that each individual signature is valid.

Proof. Assume the aggregate signature σ^j is a valid, then λ^j can be calculated by $\lambda^j = h_3(U_1 + \xi_1 P_{pub} + \rho_1 R_1, U_2 + \xi_2 P_{pub} + \rho_2 R_2, \cdots, U_n + \xi_n P_{pub} + \rho_n R_n, \sum_{i=1}^{n} \xi_i, \sum_{i=1}^{n} \rho_i)$ and the aggregation verification equation is held as following.

$$\sigma^j P = \lambda^j (\sum_{i=1}^{n} U_i + (\sum_{i=1}^{n} \xi_i) P_{pub} + \sum_{i=1}^{n} \rho_i R_i) \tag{8}$$

Because $\delta^j = \lambda^j \sum_{i=1}^{n} \sigma_i$ and h_3 is a collision resistent hash function, the following equation Eq. (9) can be deduced.

$$\begin{aligned}&\sigma^j P = \sum_{i=1}^{n} \lambda^j \sigma_i P\\ &= \sum_{i=1}^{n} \lambda^j (u_i + \xi_i s + \rho_i r_i) P\\ &= \sum_{i=1}^{n} \lambda^j (U_i P + \xi_i P_{pub} + \rho_i R_i)\end{aligned} \tag{9}$$

From Eq. (9), it can derive the following equation.

$$\sigma_i P = U_i + \xi_i P_{pub} + \rho_i R_i \tag{10}$$

where $i = 1, 2, \cdots, n$. Therefore, it illustrates that each signature σ_i in the n messages is valid.

Next, we analyze the validity of the aggregate signature from n valid single signature.

If the n signature $\{\sigma_1, R_1, U_1, ID_1, data_1\}$, $\{\sigma_2, R_2, U_2, ID_2, data_2\}, \cdots, \{\sigma_n, R_n, U_n, ID_n, data_n\}$ are valid, we can get $\sigma_i = s_i + \rho_{\mathrm{i}} r_i$, $s_i = u_i + \xi_{\mathrm{i}} s$, $\lambda^j = h_3(U_1 + \xi_1 P_{pub} + \rho_1 R_1, U_2 + \xi_2 P_{pub} + \rho_2 R_2, \cdots, U_n + \xi_n P_{pub} + \rho_n R_n, \sum\limits_{i=1}^{n} \xi_i, \sum\limits_{i=1}^{n} \rho_i)$.

Then the aggregation verification equation (Eq. (2)) can be deduced as following.

$$\begin{aligned}
\sigma^j P &= \lambda^j \sum_{i=1}^{n} \sigma_i P \\
&= \lambda^j \sum_{i=1}^{n} (u_i + \xi_i s + \rho_i r_i) P \\
&= \lambda^j \sum_{i=1}^{n} (u_i P + \xi_i s P + \rho_i r_i P) \\
&= \lambda^j (\sum_{i=1}^{n} U_i + (\sum_{i=1}^{n} \xi_i) P_{pub} + \sum_{i=1}^{n} \rho_i R_i)
\end{aligned}$$

Therefore, the aggregate signature σ^j is proved to be valid.

If an adversary modifies the aggregate signature with one invalid message $\{R_i^*, U_i^*, ID_i^*, data_i^*\}$ instead of one valid message, it is impossible to make the same λ^j according to h_3's collision resistance. That is, the modified aggregate signature cannot satisfy the aggregation verification equation (Eq. (2)).

Through the above security analysis, we can draw a conclusion that the aggregate signature is valid only on the condition that each individual signature is valid.

6.2 Security analysis

In this subsection, the security requirements are analyzed on the basis of Theorem 1.

• **Message authentication:** When receives a message $\{R_i, U_i, ID_i, data_i, \sigma_i\}$, the cluster node can check its validity and integrity according to Eq. (1). If Eq. (1) is hold, it proves the message is valid according to Theorem 1. Therefore, EIAS for WSNs can satisfies the security requirement of message authentication.

• **Modification attack:** If a adversary has modified the message $\{R_i, U_i, ID_i, data_i, \sigma_i\}$ as $\{R_i^*, U_i^*$,$ID_i^*, data_i, \sigma_i^*\}$, the cluster node can easily distinguish the invalid message $\{R_i^*, U_i^*, ID_i^*, data_i, \sigma_i^*\}$ because it cannot make the verification equation $\sigma_i P = U_i + \xi_i P_{pub} + \rho_i R_i$ true. Therefore, EIAS is secure against modification attack.

• **Impersonation attack:** In EIAS, when an adversary impersonates a sensor node to send a message $\{R_i^*, U_i^*, ID_i^*, data_i^*, \sigma_i^*\}$ to the cluster node. According to Theorem 1, the probability of that the forged message $\{R_i^*, U_i^*, ID_i^*, data_i^*, \sigma_i^*\}$can pass the verification equation Eq. (1) can be negligible. Therefore, EIAS is secure against impersonation attack.

• **Relay attack:** As definition of the system model, the sensor nodes add the current time into $data_i$ when they generate the sensing data. If an adversary relay an outdated message $\{R_i, U_i, ID_i, data_i^*, \sigma_i\}$ with modified time in $data_i^*$, the modified time can pass the check on time freshness, however the message can not meet verification equation $\sigma_i P = U_i + \xi_i P_{pub} + \rho_i R_i$ according to Theorem 2. Therefore, EIAS is secure against relay attack.

7 Performance comparison

In this section, we present the performance comparison among EIAS and Shen et al. most recently proposed scheme (SE-IAS for short) in term of computation cost and communication cost.

To evaluate performance fairly and objectively, we construct the two authentication schemes on the security level of 80 bits. As SE-IAS uses bilinear pairing, we construct its cryptographic operations as following: A bilinear pairing $\hat{e} : G_0 \times G_0 \to G_1$. G_0 is an additive group, $\hat{P}$ is its generated point on a super-singular elliptic curve $\hat{E} : y^2 = x^3 + x \bmod \hat{p}$, $\hat{q}$ is it order. $\hat{p}$ is a 512-bit prime-number, $\hat{q} = 2^{159} + 2^{17} + 1$ is a 160-bit Solinas-prime-number. As EIAS are ECC-based authentication scheme, we construct its cryptographic operations as following: G is an additive group on a non-singular elliptic curve $E : y^2 = x^3 + ax + b \bmod p$, its generated point is P, its order is q, where $a, b \in Z_q^*$ and p, q are two 160-bit prime number. We implement the corresponding cryptographic operations on the following environments: hardware is formed by an Intel-i3 3110M processor, clock frequency is 2.40 GHz, and memory is 4 GB, operation system is windows 7. The execution times of these cryptographic operations are shown in Tab. 2. The names of cryptographic operations is abbreviated as column Abbr. in Tab. 2.

Table 2: The execution time of cryptographic operations

Cryptographic operation		Abbr.	Time (ms)
Related to bilinear pairing	$\hat{e}(\hat{P}, \hat{Q})$, where$\hat{P}, \hat{Q} \in G_0$	T_{BP}	6.4164
	$x\hat{P}$, where$\hat{P} \in G_0, x \in Z_{\hat{q}}^*$	T_{PM}	2.6439
	$\hat{P} + \hat{Q}$, where $\hat{P}, \hat{Q} \in G_0$	T_{PA}	0.0146
Related to ECC	xP, where$P \in G, x \in Z_q^*$	T_{EM}	0.7538
	$P + Q$, where $P, Q \in G$	T_{EA}	0.0040
MapToPoint function		T_H	1.3277
One-way Hash function		T_h	0.0002

According to the definitions of these cryptographic operations, the size of $\hat{p}$ is 64 bytes and p is 20 bytes. Therefore, the element in G_0 is 128 bytes and the element in G is 40 bytes. We define the sizes of an identity of node and a one-way hash function result as 10 bytes and 20 bytes respectively.

7.1 Computation cost comparison

In this subsection, EIAS is compared with SE-IAS scheme in terms of computation cost. For simplicity, let Identity Key Generation Phase, Message Signing Phase, Message Aggregation phase and Aggregation Verification Phase be abbreviated as *IKP*, *MSP*, *MAP* and *AVP* respectively during later analysis.

As far as Shen et al.'s SE-IAS, the computation cost in *IKP* consists of one Map-To-Point function operation and one scalar multiplication operation related to the bilinear pairing, therefore the total execution time of *IKP* is $1T_H + 1T_{PM}$; the computation cost in *MSP* consists of two scalar multiplication operations related to the bilinear pairing, one point addition operation related to the bilinear pairing and one Map-To-Point function operation, therefore the total execution time of *MSP* is $2T_{PM} + T_{PA} + T_H$; the computation cost for n messages in *MAP* consists of $4n$ pairing operations, n MapToPoint function operations, one scalar multiplication operation related to the bilinear pairing, $(n-1)$ point addition operations related to the bilinear pairing, and one one-way hash function operation, therefore the total execution time of *MAP* is $4nT_{BP} + nT_H + (n-1)T_{PA} + 1T_{PM} + 1T_h$; the computation cost for n messages in *AVP* consists of $(2n+1)$ pairing operations, n MapToPoint function operations, $4n$ scalar multiplication operation related to the bilinear pairing, n point addition operations related to the bilinear pairing, and one one-way hash function operation, therefore the total execution time of *AVP* is $(2n{+}1)T_{BP} + 4nT_{PM} + nT_H + 1T_h$.

As far as EIAS, the computation cost in *IKP* consists of one scalar multiplication operation related to the ECC and one one-way hash function operation, therefore the total execution time of *IKP* is $T_{EM} + T_h$; the computation cost in *MSP* also consists of one scalar multiplication operation related to the ECC and one one-way hash function operation, therefore the total execution time of *MSP* is $T_{EM} + T_h$; the computation cost for n messages in *MAP* consists of $3n$ scalar multiplication operations related to the ECC, $(3n-1)$ point addition operations related to the ECC, and $(n+1)$ one-way hash function operations, therefore the total execution time of *MAP* is $3nT_{EM} + (3n-1)T_{EA} + (n+1)T_h$; the computation cost for n messages in *AVP* consists of $(n+5)$ scalar multiplication operation related to the ECC, $(2n+2)$ point addition operations related to the ECC, and $(n+1)$ one-way hash function operations, therefore the total execution time of *AVP* is $(n+5)T_{EM} + (n+1)T_h + (2n+2)T_{EA}$.

The total execution time of *IKP*, *MSP*, *MAP* and *AVP* in SE-IAS and EIAS can be calculated according to Tab. 2. The results are shown in Tab. 3.

As shown in Tab. 3, the computation cost time of SE-IAS in *IKP* and*MSP* are 3.975 ms and 6.630 ms. However, the computation cost time of EIAS in *IKP* and *MSP* are both 0.754 ms, which can decrease by 81% and 88% when compared with the time of SE-IAS. The computation cost comparisons in *IKP*, *MSP*,*MAP* (aggregating 50 messages) and *AVP* (verifying aggregate signature with 50 messages) illustrated in Fig. 2 and Fig. 3, which can vividly show that our proposed scheme takes a large advantage on computation cost over SE-IAS scheme.

Table 3: The computation cost comparison of the two schemes

	SE-IAS	EIAS
IKP	$T_H + T_{PM}$ ≈3.975 *ms*	$T_{EM} + T_h$ ≈0.754 *ms*
MSP	$2T_{PM} + T_{PA} + T_H$ ≈6.630 *ms*	$T_{EM} + T_h$ ≈0.754 *ms*
MAP	$4nT_{BP} + nT_H$ $+(n-1)T_{PA}$ $+1T_{PM} + 1T_h$ ≈ 27.008n +2.629 *ms*	$3nT_{EM} + (3n-1)T_{EA}$ $+(n+1)T_h$ ≈ 2.274n- 0.004 *ms*
AVP	$(2n+1)T_{BP} + 4nT_{PM}$ $+nT_H + 1T_h$ ≈24.736n +6.417 *ms*	$(n+5)T_{EM} + (n+1)T_h$ $+(2n+2)T_{EA}$ ≈ 0.762n +3.777 *ms*

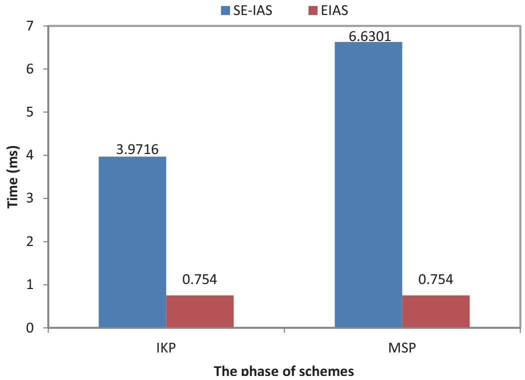

Figure 2: The computation costs of the *IKP* and *MSP* phase in the two schemes

The Fig. 4 demonstrates the computation costs for aggregating or verifying different number of messages in MAP and *AVP*. Where, MAP of SE-IAS demonstrates the computation cost for aggregating different number of messages in *MAP* of the SE-IAS scheme, *AVP* of SE-IAS demonstrates the computation cost for the data center to verify different number of messages in *AVP* of the SE-IAS scheme, *MAP* of EIAS and AVP-IAS have similar meaning with the former two. As shown in Fig. 4, EIAS is more efficient than SE-IAS scheme regardless of the number of messages.

In summary, compared with SE-IAS scheme, EIAS has much lower computation cost in each phase than AVP-IAS.

7.2 Communication cost comparison

Next, the communication cost is analyzed between EIAS and Shen et al.'s SE-IAS in this subsection.

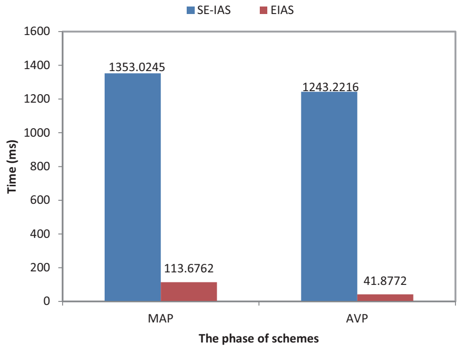

Figure 3: The computation costs of the *MAP* and *AVP* phase in the two schemes

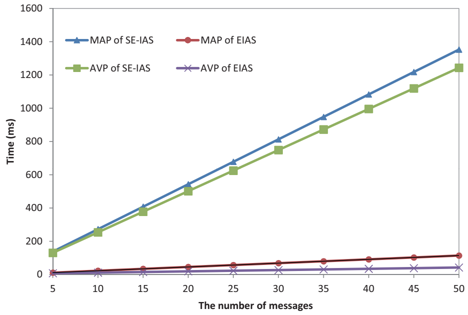

Figure 4: The computation costs of MAP and AVP for different number of messages

According the previous analysis, the sizes of $\hat{p}$, p, G_0, G and one-way hash function result have been defined as 64 bytes, 20 bytes, 128 bytes, 40 bytes and 20 bytes respectively. We define the sizes of an identity of node and a one-way hash function result as 10 bytes and 20 bytes respectively. For simplicity, the data in messages is not considered in the communication cost comparison because it is the same to every scheme.

As far as EIAS: The message sent by sensor node to cluster node consists of $\{\sigma_i, R_i, U_i, ID_i,$
$data_i\}$, which includes two elements in G ($R_i, U_i \in G$, 40×2 bytes), one identity (ID_i, 10 bytes) and one hash function's output ($\sigma_i \in Z_q$, 20 bytes). Therefore, the size of message is 110 bytes; The aggregated message (Assume aggregate k messages) sent by cluster node to the data center consists of $\{\sigma, \underbrace{\{R_i, U_i, ID_i, data_i\}}_{k}\}$, which includes $2 \times k$ elements in G ($R_i, U_i \in G$, 40×2×k bytes), k identities (ID_i, $10 \times k$ bytes) and one hash function's output ($\sigma_i \in Z_q$, 20 bytes), therefore, the size of aggregated message is $90 \times k + 20$ bytes.

As far as SE-IAS: The message sent by sensor node to cluster node consists of $\{U_i, T_i, ID_i, data_i\}$, which includes two elements in G_0 ($T_i, U_i \in G_0$, 128×2 bytes) and one identity (ID_i, 10 bytes), therefore, the size of message is 266 bytes; The aggregated message (Assume aggregate k messages) sent by cluster node to the data center consists of $\{U, \underbrace{\{T_i, ID_i, data_i\}}_{k}\}$, which includes k elements in G_0 ($T_i \in G_0$, 128×k bytes), k identities (ID_i, 10 bytes) and one elements in G($U \in G_0$,128×1 bytes). Therefore, the size of aggregated message is $138 \times k + 128$ bytes. Tab. 4 shows the communication cost comparison results of a message sent by a sensor node to a cluster node and a aggregate message (50 messages are aggregated) sent by a cluster node to the data center. In the former process, EIAS has decreased by 43% compared with SE-IAS. In addition, EIAS has decreased by 35% compared with SE-IAS during the later process. The communication cost of the aggregate message in the two schemes (EIAS and SE-IAS) can be illustrated in the Fig. 5 as the k changes. It vivid shows that EIAS has very obvious advantages than SE-IAS in decreasing communication cost. As a result, EIAS incurs much lower computation and communication cost than SE-IAS, and is more suit for the WSNs environment.

Table 4: The comparison of communication cost

	Sensor node→Cluster node	
	Component	Size
SE-IAS	$\{U_i, T_i, ID_i, data_i\}$	266 bytes
EIAS	$\{\sigma_i, R_i, U_i, ID_i, data_i\}$	110 bytes
	Cluster node→Data center	
	Component	Size
SE-IAS	$\{U, \{T_k, ID_k, data_k\}_{\times 50}\}$	7028 bytes
EIAS	$\{\sigma^j, \{R_i, U_i, ID_i, data_i\}_{\times 50}\}$	4520 bytes

Tip: The size of $data_i$ is excluded in the comparison.

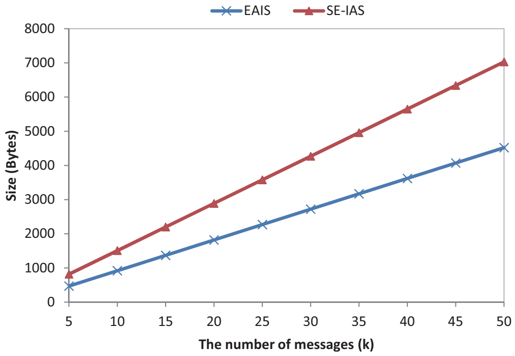

Figure 5: The computation costs of MAP and AVP for different number of messages

8 Conclusion and future work

WSNs are the major contributors to big data acquisition, but data acquisition cannot be played optimally because nodes are limited in computation and power. Therefore, to design secure and efficient signature schemes for data collection and aggregation in WSNs is very urgent. To solve this issue, we propose a new and efficient identity-based data aggregation authentication scheme in this paper. The proposed scheme constructs data aggregation signature using ECC, and it decreases the computation costs in message signing phase, message aggregation phase and aggregation verification phase and does not use any complex bilinear pairing operation, which is very suitable for resource-restricted WSNs environment. The security proof and analysis show that our proposed scheme meets the security requirements for WSNs data integrity protection, and is secure against forgery attack, coalition attack and other security attacks with hiding feature and subjective fraudulence. The performance comparison demonstrates EIAS has clear advantages in term of computation cost and communication cost when compared with similar data aggregation scheme for WSNs.

Although EIAS is more efficient and secure than similar schemes, lightweight signature scheme is more favored. Therefore, to design secure lightweight signature aggregation scheme is our next work.

Acknowledgement: The work was supported in part by the National Natural Science Foundation of China (61572370), and the National Natural Science Function of Qinghai Province (2019-ZJ-7065, 2017-ZJ-959Q), the MOE (Ministry of Education in China) Project of Humanities and Social Sciences (17YJCZH203) and the Natural Science Foundation of Hubei Province in China (2016CFB652).

References

Amin, R.; Biswas, G. (2016): A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, vol. 36, pp. 58-80.

Bellare, M.; Micciancio, D.; Warinschi, B. (2003): Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions. *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 614-629.

Boneh, D.; Gentry, C.; Lynn, B.; Shacham, H. (2003): Aggregate and verifiably encrypted signatures from bilinear maps. *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 416-432.

Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. (2016): Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, vol. 56, pp. 684-700.

Chang, C. C.; Le, H. D. (2016): A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357-366.

Chen, T. H.; Shih, W. K. (2010): A robust mutual authentication protocol for wireless sensor networks. *ETRI Journal*, vol. 32, no. 5, pp. 704-712.

Das, A. K. (2016): A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 223-244.

Das, A. K.; Sharma, P.; Chatterjee, S.; Sing, J. K. (2012): A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646-1656.

Das, M. L. (2009): Two-factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086-1090.

Di Pietro, R.; Guarino, S.; Verde, N. V.; Domingo-Ferrer, J. (2014): Security in wireless ad-hoc networks-a survey. *Computer Communications*, vol. 51, pp. 1-20.

Hartung, G.; Kaidel, B.; Koch, A.; Koch, J.; Rupp, A. (2016): Fault-tolerant aggregate signatures. *Public-Key Cryptography-PKC 2016*, pp. 331-356.

He, D.; Kumar, N.; Chilamkurti, N. (2015): A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Information Sciences*, vol. 321, pp. 263-277.

He, D.; Zeadally, S.; Kumar, N.; Lee, J. H. (2017): Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590-2601.

He, H.; Zhang, J.; Gu, J.; Hu, Y.; Xu, F. (2017): A fine-grained and lightweight data access control scheme for wsn-integrated cloud computing. *Cluster Computing*, vol. 20, no. 2, pp. 1457-1472.

Jiang, Q.; Ma, J.; Lu, X.; Tian, Y. (2015): An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1070-1081.

Jiang, Q.; Zeadally, S.; Ma, J.; He, D. (2017): Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access*, vol. 5, pp. 3376-3392.

Koblitz, N. (1987): Elliptic curve cryptosystems. *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209.

Kumari, S.; Khan, M. K.; Atiquzzaman, M. (2015): User authentication schemes for wireless sensor networks: a review. *Ad Hoc Networks*, vol. 27, pp. 159-194.

Li, C. T.; Weng, C. Y.; Lee, C. C. (2013): An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. *Sensors*, vol. 13, no. 8, pp. 9589-9603.

Li, S.; Tryfonas, T.; Li, H. (2016): The internet of things: a security point of view. *Internet Research*, vol. 26, no. 2, pp. 337-359.

Liu, X.; Zhu, H.; Ma, J.; Li, Q.; Xiong, J. (2014): Efficient attribute based sequential aggregate signature for wireless sensor networks. *International Journal of Sensor Networks*, vol. 16, no. 3, pp. 172-184.

Liu, Y.; Guo, W.; Fan, C. I.; Chang, L.; Cheng, C. (2018): A practical privacy-preserving data aggregation (3pda) scheme for smart grid. *IEEE Transactions on Industrial Informatics*.

Liu, Y.; Zhong, Q.; Chang, L.; Xia, Z.; He, D. (2016): A secure data backup scheme using multi-factor authentication. *IET Information Security*, vol. 11, no. 5, pp. 250-255.

Mahmood, M. A.; Seah, W. K.; Welch, I. (2015): Reliability in wireless sensor networks: A survey and challenges ahead. *Computer Networks*, vol. 79, pp. 166-187.

Miller, J. G. (1984): Culture and the development of everyday social explanation. *Journal of Personality and Social Psychology*, vol. 46, no. 5, pp. 961.

Pointcheval, D.; Stern, J. (1996): Security proofs for signature schemes. *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 387-398.

Rashid, B.; Rehmani, M. H. (2016): Applications of wireless sensor networks for urban areas: a survey. *Journal of Network and Computer Applications*, vol. 60, pp. 192-219.

Shamir, A. (1984): Identity-based cryptosystems and signature schemes. *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47-53.

Shen, L.; Ma, J.; Liu, X.; Miao, M. (2016): A provably secure aggregate signature scheme for healthcare wireless sensor networks. *Journal of Medical Systems*, vol. 40, no. 11, pp. 244.

Sookhak, M.; Gani, A.; Khan, M. K.; Buyya, R. (2017): Dynamic remote data auditing for securing big data storage in cloud computing. *Information Sciences*, vol. 380, pp. 101-116.

Su, Z.; Xu, Q.; Qi, Q. (2016): Big data in mobile social networks: a qoe-oriented framework. *IEEE Network*, vol. 30, no. 1, pp. 52-57.

Sun, Y.; Song, H.; Jara, A. J.; Bie, R. (2016): Internet of things and big data analytics for smart and connected communities. *IEEE Access*, vol. 4, pp. 766-773.

Tang, J.; Liu, A.; Zhao, M.; Wang, T. (2018): An aggregate signature based trust routing for data gathering in sensor networks. *Security and Communication Networks*, vol. 2018.

Turkanović, M.; Brumen, B.; Hölbl, M. (2014): A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Networks*, vol. 20, pp. 96-112.

Turkanovic, M.; Holbl, M. (2013): An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Elektronika ir Elektrotechnika*, vol. 19, no. 6, pp. 109-116.

Wen, Y.; Ma, J.; Huang, H. (2011): An aggregate signature scheme with specified verifier. *Chinese Journal of Electronics*, vol. 20, no. 2, pp. 333-336.

Xue, K.; Ma, C.; Hong, P.; Ding, R. (2013): A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316-323.

Yuan, J. J. (2014): An enhanced two-factor user authentication in wireless sensor networks. *Telecommunication Systems*, vol. 55, no. 1, pp. 105-113.

Zhang, L.; Hu, C.; Wu, Q.; Domingo-Ferrer, J.; Qin, B. (2016): Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562-2574.

Zhang, L.; Wu, Q.; Domingo-Ferrer, J.; Qin, B.; Hu, C. (2017): Distributed aggregate privacy-preserving authentication in vanets. *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516-526.

Zhang, L.; Zhang, F. (2009): A new certificateless aggregate signature scheme. *Computer Communications*, vol. 32, no. 6, pp. 1079-1085.