Ad Hoc Networks 144 (2023) 103137

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Conditional privacy-preserving message authentication scheme for cross-domain Industrial Internet of Things

Hong Zhong [a,b], Chengdong Gu [a,b], Qingyang Zhang [a,b], Jie Cui [a,b,*], Chengjie Gu [c], Debiao He [d]

[a] School of Computer Science and Technology, Anhui University, Hefei 230039, China
[b] Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China
[c] School of Public Security and Emergency Management, Anhui University of Science and Technology, Hefei, 231131, China
[d] School of Cyber Science and Engineering, Wuhan University, 430072, China

ARTICLE INFO

Keywords:
Industrial Internet of Things (IIoT)
Authentication
Conditional privacy-preserving
Cross-domain

ABSTRACT

Industrial Internet of Things (IIoT) is a key technology for building intelligent manufacturing, optimizing industrial device management, and improving productivity. Currently, an increasing number of cross-domain interaction scenarios exist in which different industries cooperate in production. The communication of industrial devices across various domains poses additional security and privacy issues. However, most current cross-domain authentication schemes require a trusted third-party centralized authentication, which reduces system flexibility and becomes the system bottleneck in multi-domain production environments with a large number of devices. In this paper, we propose a distributed cross-domain message authentication scheme with conditional privacy-preserving for the cross-domain communication scenario in IIoT, where multiple manufacturers jointly deploy devices for collaborative production. The private key generator in each domain is only responsible for offline registration and traceability, and a set of edge gateways realize distributed authentication and token distribution to devices through secret sharing technology. In addition, we use batch authentication technology to reduce authentication latency. Security analysis indicates that the scheme satisfies the security and privacy requirements of cross-domain authentication in IIoT. Experimental analysis shows that our scheme is more computationally efficient and has lower communication costs than related schemes.

1. Introduction

Industrial Internet of Things (IIoT) [1–3] is a network of intelligent devices comprising highly connected industrial components, which help enhance the intelligent process of industrial scenarios, such as manufacturing, mining, and logistics. Through a series of tools and technology such as intelligent perception, mobile network communication [4], and intelligent data analysis, IIoT improves the supply chain management system, optimizes the production process, and achieves high productivity and low operating costs [5]. IIoT has significantly enhanced the intelligence of industrial production. However, owing to the development of productivity and continuous refinement of the social division of labor, the final product may be the result of the joint efforts of multiple sectors in different industrial fields [6]. And with frequent major disasters around the world in recent years, the demand for immediate and massive production is growing. The IIoT architecture is gradually changing from a vertical integration structure of cloud servers, edge servers, and terminals to a horizontal structure of multiple IIoT systems interaction [7]. Industrial devices belonging to different systems or factories can communicate securely and cooperate during production. For example, after a major disaster, to rapidly provide protection for the people affected, multiple industrial manufacturers need to cooperate to deploy industrial equipment to manufacture emergency housing and other necessities, where equipment from different manufacturers may be mixed together. Rescue data are shared between the industrial rescue equipment deployed by different departments to ensure rapid rescue.

Compared with single-domain device communication, cross-domain communication brings more privacy-preserving [8] and security requirements [9,10]. IIoT devices from different domains require a secure and effective authentication mechanism to ensure the secure exchange of information. If an attacker can forge or modify intercepted industrial data, it will seriously jeopardize the production stability of multiple industrial manufacturers and cause loss of life and property. Therefore, it is crucial to ensure the integrity and authenticity of industrial data, and message authentication [11,12] can satisfy this requirement. Moreover, the scheme must provide anonymity [13] to prevent attackers

[*] Corresponding author at: School of Computer Science and Technology, Anhui University, Hefei 230039, China.
E-mail addresses: cuijie@mail.ustc.edu.cn (J. Cui), gcj@ustc.edu.cn (C. Gu), hedebiao@163.com (D. He).

https://doi.org/10.1016/j.adhoc.2023.103137
Received 28 December 2022; Received in revised form 15 February 2023; Accepted 3 March 2023
Available online 8 March 2023
1570-8705/© 2023 Elsevier B.V. All rights reserved.

from obtaining source privacy from intercepted messages. However, a completely anonymous scheme cannot be used. If a compromised industrial device jeopardizes normal industrial production, a trusted agency should have the ability to trace its identity and revoke it based on the message. Group signature and pseudonym technology can be used to achieve identity privacy-preserving [14], but they both have some drawbacks. Group signature technology incurs huge computation overhead, while traditional pseudonym technology makes the length of the certificate revocation list (CRL) positively related to the number of pseudonyms owned by the device.

To address the above security issues arising from the cross-domain communication of IIoT devices, some researchers have proposed anonymous cross-domain authentication schemes [15–17]. However, most cross-domain solutions require a trusted third-party authentication server to centralize authentication. Third-party authority complicates the interaction process and becomes a system bottleneck, reducing the security and scalability of the system. Distributed authentication architecture can distribute the authentication burden to multiple authentication servers, and is more suitable for multi-domain collaborative production environments with a large number of industrial devices. Therefore, a secure and efficient cross-domain solution is required to ensure collaborative production in different industries.

1.1. Related work

In this section, we will present research progress on privacy-preserving and cross-domain authentication, respectively.

1.1.1. Privacy-preserving

In this section, we will present the progress of the group signature-based and pseudonym-based privacy-preserving schemes.

Based on the feature that the group signature can provide anonymity for group members, Lin et al. [18] combined identity-based signature (IBS) and group signature technology to achieve source anonymity and integrity of the message. Wang [19] applied the short group signature technique to propose a privacy-preserving scheme for weak identity end devices, but it has a great computation overhead. Cui et al. [20] presented an anonymous message authentication solution for semi-trusted edge IIoT nodes based on the publish–subscribe model, which ensures the confidentiality of messages through proxy re-encryption technology. Li et al. [21] proposed a hop-by-hop message authentication scheme to protect the privacy of message sources. However, Wei et al. [22] indicated that the former scheme cannot provide message integrity and proposed a new source anonymous authentication scheme, which introduced an offline computing mode to reduce latency.

Raya et al. [23] proposed a pseudonym-based scheme to protect the message integrity and source anonymity. The CA issues many pseudonyms to the device during the registration phase for subsequent authentication, and the device protects its privacy by frequently changing pseudonyms. However, when the device is revoked, all the pseudonyms are added to a revocation list, and the time to check the list is greatly increased. Sun et al. [24] and Jiang et al. [14] used a hash chain to generate pseudonyms in their schemes, thus reducing the size of the revocation list. Vijayakumar et al. [25] proposed an anonymous authentication scheme that can protect the location privacy of IoT devices. Xiong et al. [26] proposed a privacy-preserving message authentication scheme based on proxy re-signature for heterogeneous system scenarios in IIoT. The cloud server uses re-signature technology to realize message authentication between the ID-based and the certificateless-based system.

1.1.2. Cross-domain authentication

Based on public key infrastructure (PKI), some scholars have proposed several certificate-based bridging cross-domain authentication schemes. Millán et al. [27] designed a cross-authentication model for inter-domain communication based on PKI. In this model, a trusted bridging certification authority (CA) is required to share a cross-certificate with each domain CA to establish a trust relationship, reducing the number of certificate paths. Zhang et al. [15] proposed a virtual bridging CA model for distributed virtual enterprises and used secret sharing techniques to achieve effective cross-domain authentication. Yao et al. [28] presented a new bridging CA authentication model that implements authentication between the PKI and Kerberos domains, but the management of bridging CAs is complex.

Certificate management is a complex issue in certificate-based cross-domain systems, and therefore, some certificateless-based cross-domain authentication schemes have been proposed. Li et al. [29] designed a layered architecture based on a certificateless public key cryptosystem that requires only two rounds of interaction to complete the authentication. He et al. [16] presented a cross-domain handshake scheme for mobile medical social networks using hierarchical identity-based cryptography (IBC) and proved its security and practicality. Yuan et al. [17] presented a cross-domain authentication key agreement protocol for communication between the PKI and the IBC domain, but it still incurs large computation and communication costs. Liu and Ma [30] designed a heterogeneous cross-domain authentication key agreement protocol where users from two different domains can be authenticated directly without the involvement of domain trusted authorities.

Most of the above solutions require a third-party authentication server to guarantee the trust relationship. However, a third-party authentication server in centralized cross-domain authentication becomes a system bottleneck and reduces the flexibility of the system. Andersen et al. [31] proposed a decentralized authentication framework through path authentication, but the scheme does not guarantee device privacy and has low authentication efficiency. Yang et al. [32] introduced a decentralized authentication architecture in which the authentication server delegates its authentication ability to the distributed edge nodes to achieve secure and efficient authentication. In addition, some scholars have proposed some decentralized cross-domain authentication models based on blockchain [9,33,34], but the participation of domain CAs is still required in the authentication process, which inevitably increases some authentication delays.

Although the above protocols have made some progress in addressing privacy-preserving cross-domain communication of devices, most of them require the participation of a trusted third party or domain CAs during the authentication process, which increases the authentication latency. Therefore, we propose a new privacy-preserving cross-domain authentication scheme that uses a set of edge gateways to implement distributed authentication, reducing authentication latency.

1.2. Contributions

In this paper, we propose a cross-domain message authentication scheme with conditional privacy-preserving to solve cross-domain communication and privacy-preserving problem for the cross-domain communication scenario in IIoT where multiple manufacturers jointly deploy devices for collaborative production. The main contributions of this study are as follows:

- We present a distributed cross-domain message authentication model that solves the performance and flexibility problems caused by centralized authentication. The private key generator in each domain is only responsible for offline registration and device identity tracing, and a set of edge gateways playing the role of distributed CAs realize distributed authentication and token distribution to devices through (t, n)-secret sharing technology. Moreover, our solution implements batch authentication, which effectively reduces the authentication latency.

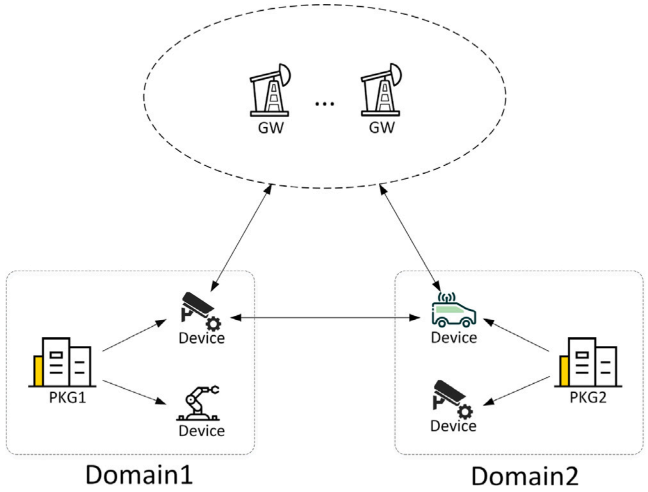


Fig. 1. System model.

- We use a one-way hash chain and identity-based signature techniques to generate pseudonyms and secret keys for devices, achieving conditional privacy-preserving while reducing the overhead associated with revoking devices.
- It is proved that the protocol meets the security and privacy requirements for the cross-domain communication of IIoT devices. In addition, a comprehensive comparison with the existing schemes shows that our scheme performs better.

1.3. Organization of the rest paper

In Section 2, we describe the preliminaries and background of the study. The details of the IIoT cross-domain authentication scheme are presented in Section 3. Sections 4 and 5 describe the security of the scheme and analyze its performance, respectively. Finally, the conclusions are summarized in Section 6.

2. Preliminaries and background

2.1. Hash chain

Assuming that $h(\cdot)$ is a secure hash function and SD is the initial seed value. Given any value S_i in a hash chain of length L, where $S_i = h^i(SD)$ ($i \in [1, L]$ and i denotes the number of hash operations), it is obvious that without knowing SD, the computation of $S_{i+1} = h(S_i)$ is easy, but not for S_{i-1}.

2.2. Threshold cryptography

A (t, n)-threshold secret sharing scheme based on the Lagrangian interpolation formula is presented by Shamir [35], in which the dealer splits the secret s into n parties and distributes them to the corresponding shareholders. Only shareholders with t or more can reconstruct the key. This can be done in the following steps. The dealer randomly chooses a polynomial with degree $t-1$ such that $s = f(0)$, where each polynomial coefficient belongs to Z_q^* and computes $s_i = f(i)$ for each shareholder. Then given any t shares $s_{i_1}, \dots, s_{i_t}$, the secret s can be reconstructed by $s = \sum_{k=1}^{t} s_k \prod_{j\neq k} \frac{i_j}{i_j - i_k}$.

2.3. Bilinear pairing

Let G and G_T be an additive and multiplicative cyclic group respectively, both with prime order q. A map $e : G * G \rightarrow G_T$ is a bilinear pairing if it satisfies the following properties:

- *Bilinear*: $e(aP, bQ) = e(P, Q)^{ab}$ for any $P, Q \in G$ and $a, b \in Z_q^*$.
- *Non-degenerate*: There exists $P \in G$, such that $e(P, P) \neq 1$.
- *Computable*: There exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G$.

2.4. Mathematical assumptions

- *Elliptic Curve Discrete Logarithm Problem (ECDLP)*: Given a point P and another point $Q = xP$ ($x \in Z_q^*$) on an elliptic curve, determining the integer x from Q is difficult.
- *Computational Diffie–Hellman Problem (CDH)*: Given the triple (P, bP, cP), where $P \in G, a \in Z_q^*$, and $b \in Z_q^*$, the computation of abP is difficult.

2.5. System model

The system architecture, as shown in Fig. 1, comprises three entities, namely the private key generator (PKG), gateway (GW), and IIoT device (DE).

- *PKG*: PKG is completely trusted and responsible for generating domain keys to which it belongs, as well as registration and secret key generation for devices and gateways. PKG is only responsible for offline entity registration and tracing device identity.
- *GW*: GWs are responsible for negotiating the master key of the system, authenticating devices, and issuing identity tokens to legitimate devices. GW is honest but can be compromised by attackers.
- *IIoT device*: IIoT device has limited computing power and small storage capacity but suffices to perform public-key cryptographic calculations and store pseudonyms, which is reasonable considering the current microcontroller unit.

Here, we briefly introduce the system workflow. First, IIoT devices and GWs in each domain register with the domain PKG for private keys, and devices also obtain pseudonyms. Then, all gateways collaborate to calculate the system master public and private keys. Devices need to get their identity tokens before collaborating with other devices for production. The device can calculate its identity token after it obtains t sub-tokens through mutual authentication with t GWs. Finally, devices with legal identity tokens can send and authenticate messages to participate in collaborative production.

2.6. Threat model

Since IIoT nodes are connected via the wireless public channel, they are potentially vulnerable to several attacks. For passive attacks, an attacker eavesdrops on the industrial data information transmitted through the wireless network to obtain confidential data or the identity of the sender. The attacker can also launch active attacks to intercept and modify transmitted industrial data information or send fake industrial data to other devices (as defined in the Dolev–Yao threat model [36]). In addition, gateways may be compromised by adversaries, and we assume that the number of gateways compromised is less than the threshold t. In short, suppose a polynomial probability time (PPT) adversary can launch the following attacks.

1. *Replay attack*: The attacker tries to disrupt normal industrial processes by replaying outdated messages.
2. *Impersonation attack*: The attacker impersonates a legal IIoT device to get an identity token from GWs or send messages over the common channel.
3. *Modification attack*: The attacker modifies intercepted legitimate messages to disrupt industrial production.
4. *Man-in-the-middle attack*: In the communication between two IIoT devices or a device and a gateway, the attacker masquerades as the communication target of two entities to manipulate the transmitted information.
5. *GW compromise attack*: The attacker attempts to compromise a group of gateways to bypass authentication mechanisms and forge identity tokens for arbitrary devices.

Table 1
Notations.

PKG	Private key generator
GW	Gateway
DE_i	The ith IIoT device
D_i	The ith domain
TS_j	The jth time slot
$PID_{i,j}$	The pseudonym of DE_i at TS_j
k_i	Secret key of PKG_i
P_{PKG_i}	Public key of PKG_i
s	System master secret key
P_{pub}	System master public key
$Sign(SK, M)$	Sign the message M by private key SK
$Cert_{GW_i}$	GW_i's certificate from PKG
$Ver(PK, M, \sigma)$	Verify the signature σ of M by PK
$\|\|$	The concatenation operation

2.7. Security objectives

For the above threat model, assuming that all industrial data information is encrypted, our scheme mainly focuses on the following security objectives.

1. *Message integrity and authentication*: The receiver can use message authentication to ensure that the message is legitimate and has not been modified or forged.
2. *Identity privacy-preserving*: Except for the PKG of the domain where the device belongs, no entity can obtain the private information of the device from the intercepted message.
3. *Traceability and identity revocation*: When the damaged device sends false industrial data to affect normal industrial production, the PKG of the domain to which it belongs can obtain its real identity and revoke it to prevent it from causing greater harm.
4. *Unlinkability*: Neither the GW nor the malicious device can link any two messages sent by the same device with a time interval exceeding Δt.

3. Proposed scheme

In this section, we will describe our scheme from the following stages: system setup, IIoT device's pseudonyms and private keys generation, GW's registration, system master key generation, token generation, message authentication, and update of GWs. First, all PKGs negotiate the public parameters of the system and generate their own public and private keys. Then GWs registered in all domains collaborate to generate the master secret key of the system and obtain their own shares through secret sharing techniques. Finally, the successfully registered IIoT devices need to be authenticated by t GWs to obtain their identity token before sending messages, and the identity token is used to sign the sent messages to indicate their legitimacy. In our scheme, due to the division of time slots, both the pseudonym and the identity token of the device are valid in only one time slot. The updated secret shares of GWs will take effect at the next time slot, while in the current time slot, GWs still use the old secret shares to generate subtokens for devices. In this way, devices can communicate with each other during the dynamic update of GWs. Table 1 lists the symbols used in this paper.

3.1. System setup

Given the security parameter θ, the PKG in each domain collaborates to generate the public parameters $\{q, P, Q, Q', G, G_T, e, H, H_1, H_2, H_3, t, n\}$, where G is an additive group of order q, P, Q, and Q' are three different generators of G, $e : G \times G \rightarrow G_T$ is a bilinear mapping, $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$, $H_3 : \{0,1\}^* \times \{0,1\}^* \times G \times G \rightarrow Z_q^*$, $H : \{0,1\}^* \rightarrow G$ are secure hash functions, n and t represent the number of domains and the threshold, respectively. And the PKG_i in domain D_i generates the domain's private key k_i and public key $P_{PKG_i} = k_i P$.

3.2. DE's pseudonyms and private keys generation

In this phase, the PKG in each domain generates a series of pseudonyms and the corresponding private keys pre-stored in each IIoT device within the domain. We assume the PKG assigns C pseudonyms to each device, and each pseudonym has a valid duration of ΔT. The valid time range of the pseudonym $PID_{i,j}$ of device DE_i at the jth time slot TS_j is $[j \cdot \Delta T, (j+1) \cdot \Delta T]$ $(j \in [1, C])$. After receiving the real identity ID_i of device DE_i to be registered, PKG_ϵ selects two random seeds $SD_{i,1}$ and $SD_{i,2}$, and computes pseudonyms for DE_i through two hash chains according to the following equation, where k_ϵ is the private key of PKG_ϵ.

$$\begin{cases} S_{1,j} = H_1^j(SD_{i,1}) \\ S_{2,C-j+1} = H_1^{C-j+1}(SD_{i,2}) \\ PID_{i,j,1} = H_1(S_{1,j} \oplus S_{2,C-j+1}) \\ PID_{i,j,2} = ID_i \oplus H_2(k_\epsilon PID_{i,j,1}, PID_{i,j,1}, P_{PKG_\epsilon}) \end{cases}$$

For each pseudonym $PID_{i,j} = (PID_{i,j,1}, PID_{i,j,2})$, PKG_ϵ uses the KIBS scheme [37] to compute the corresponding private key $SK_{i,j}$ as following: PKG_ϵ randomly chooses $t_{i,j} \in Z_q^*$ and computes $T_{i,j} = t_{i,j}P, h_{i,j} = H_2(PID_{i,j}, TS_j, T_{i,j})$, and $S_{i,j} = (k_\epsilon + h_{i,j} \cdot t_{i,j}) \cdot Q$. Then PKG_ϵ sets $SK_{i,j} = (T_{i,j}, S_{i,j})$ and securely sends $(PID_{i,j}, SK_{i,j})$ to DE_i. In addition, for each IIoT device, PKG_k saves the information $(ID_i, SD_{i,1}, SD_{i,2})$ in the database, which is used to reveal all pseudonyms of the illegal device.

3.3. GW's registration

For GW_i from the domain D_j, PKG_j generates its certificate $Cert_{GW_i}$ as following steps:

(1) PKG_j randomly chooses $v_i \in Z_q^*$ as GW_i's private key and computes $P_{GW_i} = v_i P$ as its public key.
(2) PKG_j computes the signature S_{GW_i} on P_{GW_i}, where $S_{GW_i} = Sign(k_j, P_{GW_i} \| D_j)$ and $\|$ is connect operation.
(3) PKG_j sends v_i, P_{GW_i}, and $Cert_{GW_i}$ to GW_i over a secure channel, where $Cert_{GW_i} = (P_{GW_i}, D_j, S_{GW_i})$.

In this step, the gateway stores the domain names and domain public keys of all cooperative domains obtained from the PKG. In addition, the number of gateways deployed by each domain does not exceed the threshold t.

3.4. System master key generation

In this section, GWs collaborate to generate the master public and private key pairs (s, P_{pub}) of the system and their respective share s_i and P_{s_i} through secret sharing technology.

(1) GW_i randomly selects a secret $a_{i,0} \in Z_q^*$ and a polynomial function $f_i(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + \cdots + a_{i,t-1}x^{t-1} \mod q$ with degree $t-1$, where $a_{i,1}, \ldots, a_{i,t-1} \in Z_q^*$.
(2) For $j \in [0, t-1]$, GW_i calculates and publishes $a_{i,j}P$ to other GWs, as well as sends $f_i(k)$ secretly to GW_k $(k \in [1,n], k \neq i)$.
(3) Upon receiving $f_k(i)$ from GW_k $(k \in [1,n], k \neq i)$, GW_i checks if $f_k(i)P = \sum_{j=0}^{t-1} i^j \cdot a_{k,j}P$ holds. If the check fails, GW_i rejects $f_k(i)$.
(4) GW_i calculates its own secret share $s_i = \sum_{\epsilon=1}^{n} f_\epsilon(i)$, and the corresponding public share $P_{s_i} = s_i P$.
(5) GW_i computes the system's master public key $P_{pub} = \sum_{i=1}^{n} a_{i,0}P$, and broadcasts $\{P_{s_i}, P_{pub}\}$.
(6) Now, the system's master private key $s = \sum_{i=1}^{n} a_{i,0}$ is distributed to all GWs and no GW alone knows the exact secret value s.

3.5. Token generation

An IIoT device DE_i from domain D_ϵ is first authenticated by a group of GWs and gets the corresponding sub-tokens. Then DE_i computes its identity token through these sub-tokens. In this step, the mutual authentication between the gateway and the device is realized. The detailed steps are as follows.

Step 1: First, the device performs the following steps to initiate an authentication request.

(1) DE_i generates an access control information ACI_i, which may include its domain information D_ϵ, pseudonym $PID_{i,j}$, and expiration time.
(2) DE_i selects a random number $r_{i,j} \in Z_q^*$, and computes $R_{i,j} = r_{i,j}P$, $h'_{i,j} = H_3(ACI_i, tt_i, T_{i,j}, R_{i,j})$, and $W_{i,j} = h'_{i,j}S_{i,j} + r_{i,j}Q'$, where $tt_i \in [TS_j \cdot \Delta T, TS_{j+1} \cdot \Delta T]$ is the timestamp.
(3) DE_i sends the request $(ACI_i, tt_i, T_{i,j}, R_{i,j}, W_{i,j})$ to t GWs.

Step 2: After receiving the request information, GW_k $(k = 1, 2, \dots, t)$ will do the following.

(1) GW_k checks the legitimacy of $PID_{i,j}$ and ACI_i. If $PID_{i,j,1}$ is in CRL or ACI_i not compliant, it will reject the request.
(2) GW_k computes the time slot TS_j by tt_i, and then computes $h_{i,j} = H_2(PID_{i,j}, TS_j, T_{i,j})$ and $h'_{i,j} = H_3(ACI_i, tt_i, T_{i,j}, R_{i,j})$.
(3) GW_k checks the legitimacy of DE_i by verifying Eq. (1). Reject DE_i if verification fails.

$$e(h'_{i,j}P_{PKG_\epsilon} + h_{i,j}h'_{i,j}T_{i,j}, Q) \cdot e(R_{i,j}, Q') = e(W_{i,j}, P) \tag{1}$$

(4) GW_k computes the sub-token $\sigma_{i,k} = s_k \cdot H(ACI_i)$ and $SG_k = \sigma_{i,k} \oplus \upsilon_i R_{i,j}$, then sends $(SG_k, Cert_{GW_k})$ to DE_i.

Step 3: Upon receiving $(SG_k, Cert_{GW_k})$ $(k = 1, 2, \dots, t)$ from t GWs, DE_i will do the following.

(1) DE_i first checks the legitimacy of GW_k by performing $Verify(P_{PKG_k}, P_{GW_k} \| D_k, S_{GW_k})$. Then it recovers $\sigma_{i,k} = SG_k \oplus r_{i,j}P_{GW_k}$, where P_{GW_k} is included in $Cert_{GW_k}$.
(2) DE_i authenticates GWs in batches by checking Eq. (2). If for some $l \in [1, t]$, the sub-token $\sigma_{i,l}$ cannot be authenticated, it means GW_l is illegitimate. Then DE_i reports the illegitimate GW_l to the corresponding PKG and requests another GW for the sub-token.

$$e(\sum_{k=1}^{t} \sigma_{i,k}, P) = e(H(ACI_i), \sum_{k=1}^{t} P_{s_i}). \tag{2}$$

(3) It computes $\sigma_i = \sum_{k=1}^{t} \omega_k \sigma_{i,k} = \sum_{k=1}^{t} \omega_k s_k H(ACI_i) = sH(ACI_i)$, where $\omega_k = \prod_{l=1}^{t} \frac{l}{l-k} (l \neq k)$. The identity token σ_i is a BLS signature and is valid for only one time slot. Once the token σ_i is obtained, DE_i can participate in the following message authentication.

3.6. Message authentication

When an IIoT device DE_i needs to send a message M_i, it selects a random u_i from Z_q^* and computes $U_i = u_i P$, $c_i = H_2(ACI_i, M_i \| tt_i, U_i)$, and $\alpha_i = c_i\sigma_i + u_i Q$, where tt_i is a timestamp. Then DE_i sends $(M_i, ACI_i, U_i, tt_i, \alpha_i)$ to the receiver.

Upon receiving the message $(M_i, ACI_i, U_i, tt_i, \alpha_i)$ from DE_i, the receiver first checks the validity of tt_i and ACI_i. Refuse to receive if either is invalid. Then compute $c_i = H_2(ACI_i, M_i \| tt_i, U_i)$ and determine whether the message is valid by verifying Eq. (3).

$$e(\alpha_i, P) \overset{?}{=} e(c_i H(ACI_i), P_{pub}) \cdot e(Q, U_i) \tag{3}$$

If sufficient messages are awaiting authentication, it will take a lot of time for the receiver to authenticate them. To reduce the authentication overhead, we use batch authentication to reduce pairing operations. Assume that there are m signatures to verify. For $(M_\epsilon, ACI_\epsilon, tt_\epsilon, U_\epsilon, \alpha_\epsilon)$ $(\epsilon \in [1, m])$, batch authentication is done by applying Eq. (4).

$$e(\sum_{\epsilon=1}^{m} \alpha_\epsilon, P) \overset{?}{=} e(\sum_{\epsilon=1}^{m} c_\epsilon H(ACI_\epsilon), P_{pub}) \cdot e(Q, \sum_{\epsilon=1}^{m} U_\epsilon) \tag{4}$$

3.7. Update of GWs

3.7.1. Joining of a GW

When a new gateway GW_ζ is added to the system, GW_ζ requires to obtain its private share of s. The number of gateways will be changed to $n+1$ and the threshold to t'. The update process of the secret share is as follows.

1. GW_i $(i \in [1, n])$ randomly generates a polynomial function $f_i(x) = s_i + a_{i,1}x + a_{i,2}x^2 + \cdots + a_{i,t'-1}x^{t'-1} \mod q$ with degree $t'-1$, where $a_{i,1}, \dots, a_{i,t'-1} \in Z_q^*$.
2. For $j \in [1, t'-1]$, GW_i calculates and publishes $s_i P$ and $a_{i,j}P$ to other gateways, as well as sends $f_i(k)$ secretly to GW_k $(k \in [1, n+1], k \neq i)$.
3. Upon receiving $f_k(i)$ from GW_k $(k \in [1, n+1], k \neq i)$, GW_i checks if $f_k(i)P = \sum_{j=0}^{t'-1} i^j \cdot a_{k,j}P$ holds. If the check fails, GW_i rejects $f_k(i)$.
4. GW_i calculates its new secret share $s'_i = \sum_{\epsilon=1}^{n} f_\epsilon(i)$ and the corresponding public share $P'_{s_i} = s'_i P$. Finally, GW_i broadcasts $\{P'_{s_i}, P_{pub}\}$.

3.7.2. Revocation of a GW

When the gateway GW_ζ is revoked, other gateways should update the secret share so that GW_ζ cannot participate in the subsequent collaborative authentication. At this time, the number of gateways will be changed to $n-1$ and the threshold to t'. The update process of the secret share is as follows.

1. GW_i $(i \in [1, n-1])$ randomly generates a polynomial function $f_i(x) = s_i + a_{i,1}x + a_{i,2}x^2 + \cdots + a_{i,t'-1}x^{t'-1} \mod q$ with degree $t'-1$, where $a_{i,1}, \dots, a_{i,t'-1} \in Z_q^*$.
2. For $j \in [1, t'-1]$, GW_i calculates and publishes $s_i P$ and $a_{i,j}P$ to other gateways, as well as sends $f_i(k)$ secretly to GW_k $(k \in [1, n-1], k \neq i)$.
3. Upon receiving $f_k(i)$ from GW_k $(k \in [1, n-1], k \neq i)$, GW_i checks if $f_k(i)P = \sum_{j=0}^{t'-1} i^j \cdot a_{k,j}P$ holds. If the check fails, GW_i rejects $f_k(i)$.
4. GW_i calculates its new secret share $s'_i = \sum_{\epsilon=1}^{n} f_\epsilon(i)$ and the corresponding public share $P'_{s_i} = s'_i P$. Finally, GW_i broadcasts $\{P'_{s_i}, P_{pub}\}$.

4. Security proof and analysis

In this section, we present the security of the proposed scheme and show that the scheme satisfies the security objectives described in Section 2.

4.1. Security proof

The security model of our scheme can be described by the following game between the adversary $\mathcal{A}$ and the challenger $\mathcal{S}$:

Setup: The challenger $\mathcal{S}$ inputs the security parameter k, obtains the system parameters and returns them to $\mathcal{A}$.

Queries: The adversary $\mathcal{A}$ can make the following queries:

- *Hash Query*: $\mathcal{A}$ can request the hash function and the challenger $\mathcal{S}$ stores and returns the corresponding hash value.

Table 2
Execution time.

Symbol	Description	Time (ms)
T_{bp}	Bilinear pairing	0.699
T_{mtp}	Hash map to G	3.141
T_{sm}	Scale multiplication	1.651
T_e	Exponentiation operation over G_T	0.109

- *Extract Query*: $\mathcal{A}$ can request a private key corresponding to an identity ACI of its choice. Then, $\mathcal{S}$ return the corresponding private key σ to $\mathcal{A}$.
- *Sign Query*: $\mathcal{A}$ can request the signature of a message M of its choice. Then, $\mathcal{S}$ responds to $\mathcal{A}$ with δ.

Output: $\mathcal{A}$ outputs a signature δ on M and ACI. $\mathcal{A}$ is deemed to win in the game if i) δ is a valid signature, ii) ACI has not been queried from the extract oracle, and iii) the tuple (M, ACI) has not been requested to the sign oracle.

Theorem 1. *If the BLS scheme is $(t', q_H, q_E, \epsilon')$-secure against existential forgery on the adaptive chosen-message attack, the proposed scheme is $(t, q_H, q_{H_2}, q_E, q_S, \epsilon)$-secure against existential forgery under the adaptive chosen-message attack, for any t and ϵ satisfying $\epsilon \approx \epsilon'$ and $t = t' + O(q_S)$.*

Proof. Suppose that the adversary $\mathcal{A}$ can break the proposed scheme. Now, we construct a simulator $\mathcal{S}$ that can break the BLS scheme in GDH group based on $\mathcal{A}$. $\mathcal{S}$ is given a tuple $(P, P_{pub} = sP)$, where $s \in Z_q^*$. The simulator $\mathcal{S}$ interacts with $\mathcal{A}$ to simulate as follows.

Setup: The simulator $\mathcal{S}$ chooses a random $y \in Z_q^*$ and computes $Q = yP$. Then $\mathcal{S}$ sends the public system parameters $Params = (P, Q, P_{pub}, H, H_2)$ to $\mathcal{A}$.

H Query: When $\mathcal{A}$ makes an *H Query* with the message ACI, $\mathcal{S}$ checks whether the tuple (ACI, X) already appears on the hash list *H-list*. If so, $\mathcal{S}$ returns $X = H(ACI)$ to $\mathcal{A}$. Otherwise, $\mathcal{S}$ forwards the query to the H oracle of the BLS scheme to get an $X = H(ACI) \in G$. At last, $\mathcal{S}$ returns X to $\mathcal{A}$ and adds (ACI, X) to the *H-list*.

H_2 Query: When $\mathcal{A}$ makes an *H_2 Query* with a message tuple (ACI, M, σ), $\mathcal{S}$ checks whether the tuple (ACI, M, σ) already appears on the hash list *H_2-list*. If so, $\mathcal{S}$ returns $h = H_2(ACI, M, \sigma)$ to $\mathcal{A}$. Otherwise, $\mathcal{S}$ chooses a random $h \in Z_q^*$ and adds the tuple (ACI, M, σ, h) into the *H_2-list*. At last, $\mathcal{S}$ returns $h = H_2(ACI, M, \sigma)$ to $\mathcal{A}$.

Extract Query: When $\mathcal{A}$ makes an *Extract Query* for the corresponding private key of ACI, $\mathcal{S}$ forwards the query to the signature oracle of the BLS to get a signature $\sigma = s \cdot H(ACI)$ on ACI under P_{pub}. At last, $\mathcal{S}$ returns σ to $\mathcal{A}$ and stores (ACI, σ) to the *Extract-list*.

Sign Query: When $\mathcal{A}$ makes a *Sign Query* on M and ACI, $\mathcal{S}$ finds whether the corresponding tuple (ACI, σ) from the *Extract-list*.

- If (ACI, σ) exists on the *Extract-list*, $\mathcal{S}$ chooses a random $r \in Z_q^*$, and computes $U = rP, h = H_2(ACI, M, U)$, and $\alpha = h\sigma + rQ$. Then, $\mathcal{S}$ returns $\delta = (U, \alpha)$ to $\mathcal{A}$ and stores (ACI, M, U, h) on the *H_2-list*.
- Otherwise, $\mathcal{S}$ makes an *Extract Query* to get the corresponding private key σ and stores (ACI, σ) to the *Extract-list*. Then, $\mathcal{S}$ calculates the signature $\delta = (U, \alpha)$ on M and ACI by σ, returns δ to $\mathcal{A}$ and stores (ACI, M, U, h) on the *H_1-list*.

Output: Ultimately, $\mathcal{A}$ outputs a forgery signature $\delta^* = (U^*, \alpha^*)$ on M^* and ACI^* where ACI^* has not been stored on the *Extract-list* and the tuple (M^*, ACI^*) has not been requested to the sign oracle. According to $\alpha^* = h^* \cdot \sigma^* + rQ$ and $U^* = uP$, $\mathcal{S}$ computes $h^{*(-1)}(\alpha^* - yU^*) = \sigma^*$. Then σ^* is a valid signature on ACI^* under P_{pub} of the BLS scheme. Finally, $\mathcal{S}$ outputs σ^* as a solution to the BLS scheme. □

4.2. Security analysis

4.2.1. Message integrity and authentication

According to Theorem 1, we can get that as long as the BLS scheme is unforgeable, our scheme is secure against existential forgery under the adaptive chosen message attack in the random oracle model. Therefore, no PPT adversary can forge a valid message signature $(M_i, ACI_i, U_i, tt_i, \alpha_i)$ that can make the equation $e(\alpha_i, P) \overset{?}{=} e(c_i H(ACI_i), P_{pub}) \cdot e(Q, U_i)$ hold. Therefore, the scheme can achieve authentication and message integrity.

4.2.2. Identity privacy-preserving

In the scheme, the part of the pseudonym $PID_{i,j,2}$ that contains the real identity of the device is calculated from the PKG_ϵ's master key k_ϵ. The adversary can only get the true identity of the device by calculating the equation $ID_i = PID_{i,j,2} \oplus H_2(k_\epsilon PID_{i,j,1}, PID_{i,j,1}, P_{PKG_\epsilon})$. Due to the intractability of the ECDLP problem, the adversary cannot obtain the real identity without knowing k_ϵ. As a result, the adversary cannot acquire any privacy about the device's identity from the public message.

4.2.3. Traceability and identity revocation

The PKG of each domain can reveal the real identity ID_i of the malicious device DE_i under its domain from the device's pseudonym $PID_{i,j}$. PKG_ϵ computes $ID_i = PID_{i,j,2} \oplus H_2(k_\epsilon PID_{i,j,1}, PID_{i,j,1}, P_{PKG_\epsilon})$ by its master secrets k_ϵ. Then PKG_ϵ queries the database to obtain the corresponding hash seeds $SD_{i,1}$ and $SD_{i,2}$ according to ID_i, and discloses them to revoke all pseudonyms of the device. The unique pseudonym available for the device at each time slot can be calculated based on the two hash seeds, so at the jth time slot, only the $PID_{i,j,1}$ of the device DE_i is stored in the CRL.

4.2.4. Unlinkability

Devices frequently change pseudonyms to ensure privacy, where $PID_{i,j}$ is generated by two hash seeds $SD_{i,1}$ and $SD_{i,2}$. If the time interval between two messages M_i and M_j sent by a device exceeds Δt, the adversary cannot determine whether the two messages are from the same device without the knowledge of the $SD_{i,1}$ and $SD_{i,2}$. Therefore, our scheme supports long-term unlinkability. In addition, our scheme achieves short-term linkability, which can resist the Sybil attacks launched by a malicious device.

4.2.5. Replay attack

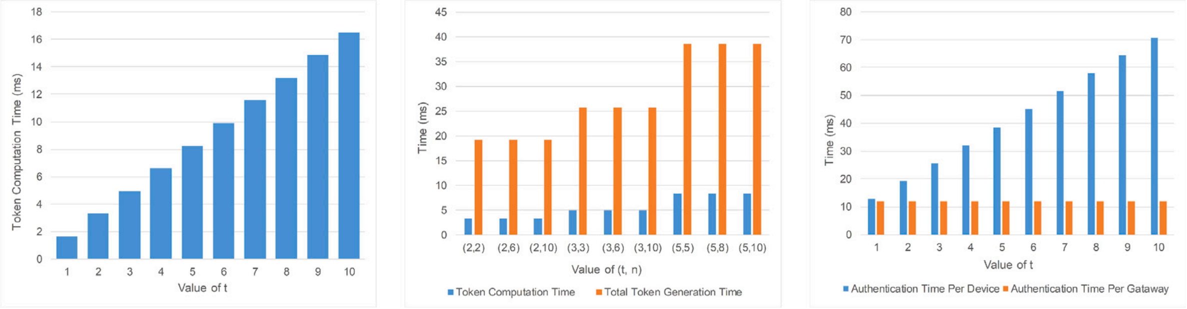
For each message $(M_i, ACI_i, U_i, tt_i, \alpha_i)$ sent by the device, the receiver determines whether the message has expired by checking the validity of the timestamp tt_i. Since the signature α_i is relevant on tt_i, when the adversary changes the old timestamp tt_i to tt'_i, the new message $(M_i, ACI_i, U_i, tt'_i, \alpha_i)$ cannot pass the verification. Therefore, replay attacks can be detected in our scheme.

4.2.6. Impersonation attack

From Theorem 1, we know that an adversary who wants to pretend to be a legitimate device to send a valid message that passes the equation $e(\alpha_i, P) \overset{?}{=} e(c_i H(ACI_i), P_{pub}) \cdot e(Q, U_i)$ check must have the corresponding identity token σ_i. But σ_i is a BLS signature, and only the authenticated devices can get it. Therefore, our scheme can resist impersonation attacks.

4.2.7. Man-in-the-middle attack

For the token generation phase, mutual authentication is achieved between the IIoT device and the gateway, so that an adversary cannot successfully launch a man-in-the-middle attack at this point. For the message authentication phase, the receiver needs to authenticate each industrial data message. According to Theorem 1, an adversary cannot modify or forge a legitimate message from an intercepted message. Therefore, our scheme can tolerate man-in-the-middle attacks.



(a) The Cost of Computing a Token

(b) The Cost in Token Generation Phase with Different Security Parameters

(c) The Cost of Devices and Gateways with Different Thresholds

Fig. 2. Computation cost in token generation phase.

4.2.8. *GW compromise attack*

If a PPT adversary cannot break the BLS signature with non-negligible probability, then even if t' ($t' \in [0, t-1]$) gateways are compromised, it cannot generate a valid identity token. In the worst case, the adversary compromises $t-1$ gateways, i.e., it has $t-1$ secret shares $s_1, \ldots, s_{t-1}$. Then it can compute $t-1$ sub-tokens $\sigma_i = s_i H(ACI)$ ($i \in [0, t-1]$). Assuming that the adversary can generate a valid identity token $\sigma^* = \sum_{i=1}^{t} \varsigma_i \sigma_i$, it can calculate the sub-token $\sigma_t^* = (\sigma^* - \sum_{i=1}^{t-1} \varsigma_i \sigma_i) \cdot \varsigma^{-1}$, i.e. it can forge a BLS signature $\sigma_t = s_t H(ACI)$ without the secret share s_t. Therefore, the attacker cannot compute a valid identity token even with $t-1$ gateways compromised.

5. Performance analysis and comparison

In this section, we first introduce the experimental environment, and then we analyze and evaluate the performance of the proposed scheme in terms of computation cost and communication cost. We also compare the performance of the proposed protocol with [19,32], and [26]. We perform the cryptographic operation using the charm 0.50 library on a host running Ubuntu 20.04 TLS with an Intel Core i5-7500 CPU @3.4 GHz and 16 GB memory. The bilinear pairing $e : G \times G \rightarrow G_T$ is constructed on the curve $y^2 = x^3 + x$ with embedding degree 2 over a 512 bits finite field, $|G| = 1024$ bits and $|Z_q^*| = 160$ bits. Table 2 recodes the execution time of the major cryptographic operations.

5.1. *Computation cost*

5.1.1. *Cost in token generation*

We evaluate the computation cost of the token generation phase. The device needs to be authenticated by at least t GWs and obtain the corresponding sub-tokens to calculate its identity token. The computation cost of the device is $2T_{bp} + t \cdot T_{mpt} + (2t+3)T_{sm}$, while each gateway is $3T_{bp} + T_{mpt} + 4T_{sm}$. We evaluate the time for the device to compute the token when different numbers of GWs cooperate on authentication, that is, we evaluate the time to compute the token for different values of t when the value of n is fixed to 10 in the (t, n)-secret sharing scheme. The result is shown in Fig. 2(a). Even with $t = 10$, it only takes 17 ms to compute the token. Furthermore, we also investigate the effect of different values of t and n on the computation overhead of the token generation stage. As shown in Fig. 2(b), when the threshold t is the same, the computation cost is roughly the same even if the value of n varies, which is a reasonable result. Finally, we evaluate the authentication cost for IIoT devices and GWs separately. As shown in Fig. 2(c), as threshold t increases, the computation overhead of each device also increases, but not proportionally, because our scheme supports the batch authentication of gateways by the device. Also, the computation time for each GW is roughly the same because the GW authenticates each request only once.

5.1.2. *Cost in message authentication*

IIoT devices can participate in the message authentication process after getting the identity token. The computation cost for the sender to send a message is $3T_{sm}$, and the overhead for the receiver to authenticate the message is $3T_{bp} + T_{mpt} + T_{sm}$. In addition, our scheme supports batch authentication, and the overhead for batch authentication of m messages is $3T_{bp} + nT_{mpt} + nT_{sm}$, effectively reducing the number of pairing operations.

5.1.3. *Overall computation cost*

Table 3 shows a comparison between our scheme and related schemes in terms of computation cost. Since our scheme can perform multiple message authentication after obtaining an identity token, we will compare the total computation overhead of multiple message authentication. Here we assume $t = 5$, i.e. the IIoT device is authenticated by at least 5 gateways to obtain the token. Fig. 3 depicts the overall computation overhead for one token generation and m messages authentication, and the results illustrate the low overall overhead of our scheme.

5.2. *Communication cost*

In this section, we focus on the communication cost caused by the pseudonym, signature, and timestamp. As mentioned previously, $|G| = 128$ bytes and $|Z_q^*| = 20$ bytes. In addition, we set the pseudonym (ID) to 20 bytes and the timestamp to 4 bytes, respectively. Table 4 presents the communication cost of our scheme and related schemes for one token generation and m message authentication. Since the token generation stage requires multiple gateways to cooperate to authenticate devices, the communication cost of our token generation stage is relatively large. However, our scheme has less overhead in the message authentication phase. As shown in Fig. 4, when m is greater than 10, the communication cost of the proposed scheme is significantly better than other schemes.

6. Conclusion

In this paper, we proposed a privacy-preserving message authentication scheme to protect cross-domain communication of IIoT devices. We achieved distributed authentication without a trusted third-party using secret sharing and IBS technology, and the authentication process between the IIoT device and gateway required only one round of interaction. The pseudonyms of devices were generated using hash chain technology, which effectively reduces the size of the CRL. Our scheme implemented batch authentication, reducing the authentication latency. The security of our scheme was proven, and experimental analysis showed that our scheme could be applied to practical cross-domain industrial production. The overhead required by most existing cross-domain authentication schemes is still a large burden for

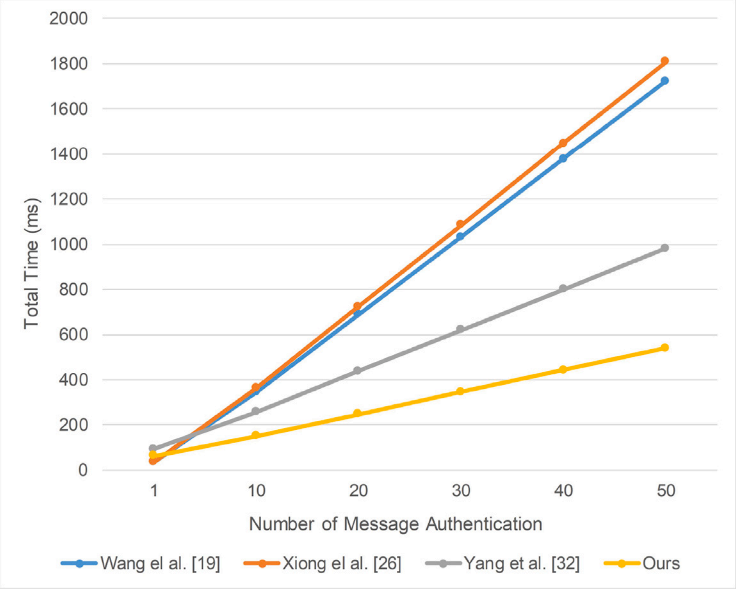


Fig. 3. Computation cost.

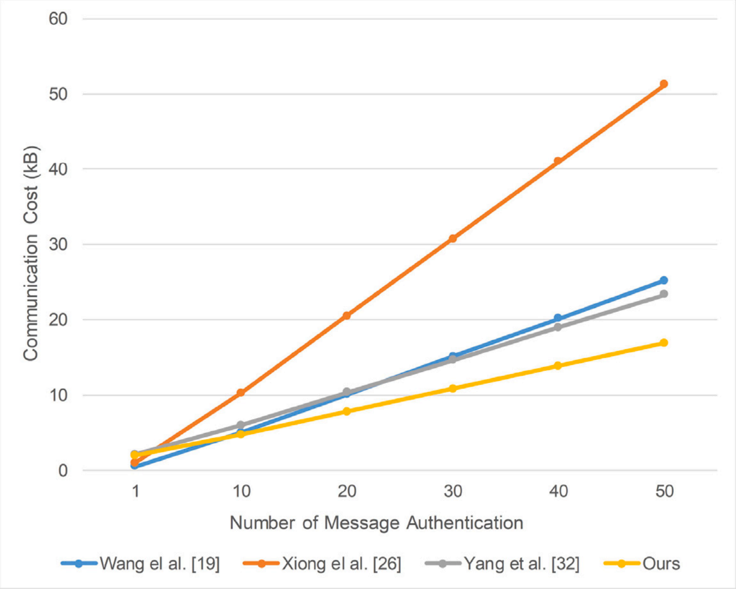


Fig. 4. Communication cost.

Table 3
The performance comparison in computation cost.

	TokenGen	Signing	Verification	Batch verification
Wang et al. [19]	–	$3T_{bp}+9T_{sm}+3T_e$	$5T_{bp}+8T_{sm}+4T_e$	$5nT_{bp}+8nT_{sm}+4nT_e$
Xiong et al. [26]	–	$2T_{bp}+2T_{mtp}+7T_{sm}$	$6T_{bp}+3T_{mtp}+2T_{sm}$	$6nT_{bp}+3nT_{mpt}+2nT_{sm}$
Yang et al. [32]	$(t+7)T_{bp}+(2t+6)T_{mpt}+\ (t+5)T_{sm}+T_e$	$2T_{mpt}+3T_{sm}$	$3T_{bp}+T_{mpt}+T_{sm}$	$3nT_{bp}+nT_{mpt}+nT_{sm}$
Ours	$5T_{bp}+(t+1)T_{mpt}+(2t+7)T_{sm}$	$3T_{sm}$	$3T_{bp}+T_{mpt}+T_{sm}$	$3T_{bp}+nT_{mpt}+nT_{sm}$

Table 4
The performance comparison in communication cost.

	TokenGen	Message authentication	Total
Wang et al. [19]	–	$3\vert G\vert+6\vert Z_q^*\vert$	$3m\vert G\vert+6m\vert Z_q^*\vert$
Xiong et al. [26]	–	$8\vert G\vert$	$8m\vert G\vert$
Yang et al. [32]	$(2t+3)\vert G\vert+\vert Z_q^*\vert+2\vert TS\vert$	$3\vert G\vert+2\vert Z_q^*\vert+2\vert TS\vert$	$(3m+2t+3)\vert G\vert+(2m+1)\vert Z_q^*\vert+(2m+2)\vert TS\vert$
Ours	$(2t+3)\vert G\vert+2\vert Z_q^*\vert+2\vert TS\vert$	$2\vert G\vert+2\vert Z_q^*\vert+2\vert TS\vert$	$(L2m+2t+3)\vert G\vert+(2m+2)\vert Z_q^*\vert+(2m+2)\vert TS\vert$

resource-constrained devices, such as sensors in industrial environments. Therefore, future work in this study is to design a lightweight cross-domain message authentication scheme for resource-constrained devices.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

The work was supported in part by the National Natural Science Foundation of China under Grant 62272002, Grant 62202005 and Grant U1936220, in part by the Excellent Youth Foundation of Anhui Scientific Committee under Grant 2108085J31, in part by the Natural Science Foundation of Anhui Province, China under Grant 2208085QF198, in part by the University Synergy Innovation Program of Anhui Province under Grant GXXT-2022-049 and in part by the Special Fund for Key Program of Science and Technology of Anhui Province, China under Grant 202003A05020043. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

References

[1] Jian-Qiang Li, F Richard Yu, Genqiang Deng, Chengwen Luo, Zhong Ming, Qiao Yan, Industrial Internet: A survey on the enabling technologies, applications, and challenges, IEEE Commun. Surv. Tutor. 19 (3) (2017) 1504–1526.

[2] Prosanta Gope, Ashok Kumar Das, Neeraj Kumar, Yongqiang Cheng, Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inform. 15 (9) (2019) 4957–4968.

[3] Dongyang Xu, Keping Yu, James A. Ritcey, Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0, IEEE Trans. Ind. Inform. (2021).

[4] Malvin Nkomo, Gerhard P Hancke, Adnan M Abu-Mahfouz, Saurabh Sinha, Adeiza J Onumanyi, Overlay virtualized wireless sensor networks for application in industrial Internet of things: A review, Sensors 18 (10) (2018) 3215.

[5] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, Mikael Gidlund, Industrial Internet of things: Challenges, opportunities, and directions, IEEE Trans. Ind. Inform. 14 (11) (2018) 4724–4734.

[6] Parminder Singh, Mehedi Masud, M Shamim Hossain, Avinash Kaur, Cross-domain secure data sharing using blockchain for industrial IoT, J. Parallel Distrib. Comput. 156 (2021) 176–184.

[7] Shaoyong Guo, Fengning Wang, Neng Zhang, Feng Qi, Xuesong Qiu, Master-slave chain based trusted cross-domain authentication mechanism in IoT, J. Netw. Comput. Appl. 172 (2020) 102812.

[8] Jing Chen, Zeyi Zhan, Kun He, Ruiying Du, Donghui Wang, Fei Liu, XAuth: Efficient privacy-preserving cross-domain authentication, IEEE Trans. Dependable Secure Comput. (2021).

[9] Meng Shen, Huisen Liu, Liehuang Zhu, Ke Xu, Hongbo Yu, Xiaojiang Du, Mohsen Guizani, Blockchain-assisted secure device authentication for cross-domain industrial IoT, IEEE J. Sel. Areas Commun. 38 (5) (2020) 942–954.

[10] Lu Zhou, Kuo-Hui Yeh, Gerhard Hancke, Zhe Liu, Chunhua Su, Security and privacy for the industrial Internet of things: An overview of approaches to safeguarding endpoints, IEEE Signal Process. Mag. 35 (5) (2018) 76–87.

[11] Jing Zhang, Jie Cui, Hong Zhong, Zhili Chen, Lu Liu, PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular Ad-hoc networks, IEEE Trans. Dependable Secure Comput. 18 (2) (2019) 722–735.

[12] Lu Wei, Jie Cui, Yan Xu, Jiujun Cheng, Hong Zhong, Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs, IEEE Trans. Inf. Forensics Secur. 16 (2020) 1681–1695.

[13] Ling Xiong, Naixue Xiong, Changyuan Wang, Xinqiao Yu, Mengxia Shuai, An efficient lightweight authentication scheme with adaptive resilience of asynchronization attacks for wireless sensor networks, IEEE Trans. Syst. Man Cybern. Syst. 51 (9) (2019) 5626–5638.

[14] Shunrong Jiang, Xiaoyan Zhu, Liangmin Wang, An efficient anonymous batch authentication scheme based on HMAC for VANETs, IEEE Trans. Intell. Transp. Syst. 17 (8) (2016) 2193–2204.

[15] Wenfang Zhang, Xiaomin Wang, Muhammad Khurram Khan, A virtual bridge certificate authority-based cross-domain authentication mechanism for distributed collaborative manufacturing systems, Secur. Commun. Netw. 8 (6) (2015) 937–951.

[16] Debiao He, Neeraj Kumar, Huaqun Wang, Lina Wang, Kim-Kwang Raymond Choo, Alexey Vinel, A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network, IEEE Trans. Dependable Secure Comput. 15 (4) (2016) 633–645.

[17] Chao Yuan, Wenfang Zhang, Xiaomin Wang, EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system, Arab. J. Sci. Eng. 42 (8) (2017) 3275–3287.

[18] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, Xuemin Shen, GSIS: A secure and privacy-preserving protocol for vehicular communications, IEEE Trans. Veh. Technol. 56 (6) (2007) 3442–3456.

[19] Zhiwei Wang, A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity, Future Gener. Comput. Syst. 82 (2018) 342–348.

[20] Jie Cui, Fengqun Wang, Qingyang Zhang, Yan Xu, Hong Zhong, Anonymous message authentication scheme for semitrusted edge-enabled iIoT, IEEE Trans. Ind. Electron. 68 (12) (2020) 12921–12929.

[21] Jian Li, Yun Li, Jian Ren, Jie Wu, Hop-by-hop message authenticationand source privacy in wirelesssensor networks, IEEE Trans. Parallel Distrib. Syst. 25 (5) (2013) 1223–1232.

[22] Jiannan Wei, Tran Viet Xuan Phuong, Guomin Yang, An efficient privacy preserving message authentication scheme for Internet-of-things, IEEE Trans. Ind. Inform. 17 (1) (2020) 617–626.

[23] Maxim Raya, Jean-Pierre Hubaux, Securing vehicular Ad hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.

[24] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin Shen, Jinshu Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, IEEE Trans. Veh. Technol. 59 (7) (2010) 3589–3603.

[25] Pandi Vijayakumar, Mohammad S Obaidat, Maria Azees, SK Hafizul Islam, Neeraj Kumar, Efficient and secure anonymous authentication with location privacy for IoT-based WBANs, IEEE Trans. Ind. Inform. 16 (4) (2019) 2603–2611.

[26] Hu Xiong, Yan Wu, Chuanjie Jin, Saru Kumari, Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT, IEEE Internet Things J. 7 (12) (2020) 11713–11724.

[27] Gabriel López Millán, Manuel Gil Pérez, Gregorio Martínez Pérez, Antonio F Gómez Skarmeta, PKI-based trust management in inter-domain scenarios, Comput. Secur. 29 (2) (2010) 278–290.

[28] Yao Yao, Wang Xingwei, Sun Xiaoguang, A cross heterogeneous domain authentication model based on PKI, in: 2011 Fourth International Symposium on Parallel Architectures, Algorithms and Programming, IEEE, 2011, pp. 325–329.

[29] Yanping Li, Weifeng Chen, Zhiping Cai, Yuguang Fang, CAKA: A novel certificateless-based cross-domain authenticated key agreement protocol for wireless mesh networks, Wirel. Netw. 22 (8) (2016) 2523–2535.

[30] Xiaoxue Liu, Wenping Ma, CDAKA: A provably-secure heterogeneous cross-domain authenticated key agreement protocol with symptoms-matching in TMIS, J. Med. Syst. 42 (8) (2018) 1–15.

[31] Michael P Andersen, Sam Kumar, Moustafa AbdelBaky, Gabe Fierro, John Kolb, Hyung-Sin Kim, David E Culler, Raluca Ada Popa, $\{WAVE\}$: A decentralized authorization framework with transitive delegation, in: 28th USENIX Security Symposium, USENIX Security 19, 2019, pp. 1375–1392.

[32] Anjia Yang, Jian Weng, Kan Yang, Cheng Huang, Xuemin Shen, Delegating authentication to edge: A decentralized authentication architecture for vehicular networks, IEEE Trans. Intell. Transp. Syst. (2020).

[33] Chaosheng Feng, Bin Liu, Zhen Guo, Keping Yu, Zhiguang Qin, Kim-Kwang Raymond Choo, Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of drones, IEEE Internet Things J. 9 (8) (2021) 6224–6238.

[34] Fei Tong, Xing Chen, Kaiming Wang, Yujian Zhang, CCAP: A complete cross-domain authentication based on blockchain for Internet of things, IEEE Trans. Inf. Forensics Secur. 17 (2022) 3789–3800.

[35] Adi Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.

[36] Danny Dolev, Andrew Yao, On the security of public key protocols, IEEE Trans. Inform. Theory 29 (2) (1983) 198–208.

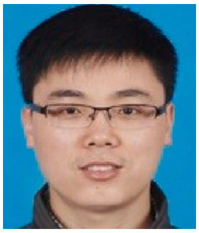
[37] Kyung-Ah Shim, CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. 61 (4) (2012) 1874–1883, http://dx.doi.org/10.1109/TVT.2012.2186992.

Hong Zhong was born in Anhui Province, China, in 1965. She received her Ph.D. degree in computer science from University of Science and Technology of China in 2005. She is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). She has over 200 scientific publications in reputable journals (e.g. IEEE Journal on Selected Areas in Communications, IEEE

Transactions on Parallel and Distributed Systems, IEEE Transactions on Mobile Computing, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Multimedia, IEEE Transactions on Vehicular Technology, IEEE Transactions on Network and Service Management, IEEE Transactions on Cloud Computing, IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics and IEEE Transactions on Big Data), academic books and international conferences.

Chengdong Gu is now a research student in the School of Computer Science and Technology, Anhui University. His research focuses on the security of Industrial Internet of Things.

Qingyang Zhang was born in Anhui Province, China, in 1992. He received his B. Eng. degree and Ph.D. degree in computer science from Anhui University in 2021. He is currently a lecture of School of Computer Science and Technology at Anhui University. His research interest includes edge computing, computer systems, and security.



Jie Cui (Senior Member, IEEE) was born in Henan Province, China, in 1980. He received his Ph.D. degree in University of Science and Technology of China in 2012. He is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). He has over 150 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Mobile Computing, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Computers, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics, IEEE Transactions on Cloud Computing and IEEE Transactions on Multimedia), academic books and international conferences. He is in the Editorial Board of several international journals, such as IET Communications, Security and Communication Networks, and Sensors.

Chengjie Gu received his Ph.D. degree in Nanjing University of Posts and Telecommunications in 2012. From 2012 to 2017, he was an innovation team leader in the 38th Research Institute of CETC and conducted research and development in the communication and networking sector. Currently he is a dean of school of public security and emergency of Anhui university of science and technology. He has completed postdoctoral research at the USTC. He is a high-level innovation leader of Anhui province and a cybersecurity expert of Zhejiang province in China. His research interest includes network security and trusted network architecture, etc.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University, Wuhan, China in 2009. He is currently a professor of the School of Cyber Science and Engineering, Wuhan University, Wuhan, China and the Shanghai Key Laboratory of Privacy Preserving Computation, MatrixElements Technologies, Shanghai 201204, China. His main research interests include cryptography and information security, in particular, cryptographic protocols. He has published over 100 research papers in refereed international journals and conferences, such as IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Security and Forensic, and Usenix Security Symposium. He is the recipient of the 2018 IEEE Systems Journal Best Paper Award and the 2019 IET Information Security Best Paper Award. His work has been cited more than 10000 times at Google Scholar. He is in the Editorial Board of several international journals, such as Journal of Information Security and Applications, Frontiers of Computer Science, and Human-centric Computing & Information Sciences.