IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 1 January 2023, accepted 31 January 2023, date of publication 9 February 2023, date of current version 15 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3243624

RESEARCH ARTICLE

Perception Layer Lightweight Certificateless Authentication Scheme for IoT-Based Emergency Logistics

JIANXI YANG[1], JINPO FAN[2], AND XIAOCHEN ZHU[3]
[1]Beijing Electronic Science and Technology Institute, Beijing 100070, China
[2]Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3]School of Communication Engineering, Xidian University, Xi'an 710071, China

Corresponding author: Jinpo Fan (fjp@bupt.edu.cn)

This work was supported in part by the Open Project Fund of Key Laboratory of Network Measurement Technology, Chinese Academy of Sciences, under Grant KFKT2019-006; and in part by the 2022 Beijing Electronic Science and Technology Institute Fundamental Research Business Fee Excellent Master Training Funding Project under Grant 328202239.

ABSTRACT Emergency logistics is of great significance for supply security in emergencies. As a crucial component of strategic material reserve and allocation, emergency logistics is characterized by high levels of safety and efficacy. The security of the IoT-based emergency logistics system cannot be overstated, considering the potential damage caused by malicious accessors. Authentication is an essential means of system security. Existing certificateless authentication protocols are mostly based on bilinear pairings, which cannot match the objectives of emergency logistics networks for lightweight deployment and fast authentication of massive nodes. In this paper, we propose a lightweight certificateless authentication protocol (CL-LAP) without bilinear pairings. The security is determined by the discrete logarithm problem on elliptic curves. Nonlinear pairings guarantee energy efficiency and minimum computation cost. In addition, we use batch verification to reduce the authentication cost and tackle the problem of quick authentication in broadcast messages. We conduct a security analysis on the proposed CL-LAP under the random oracle model to demonstrate that the proposed scheme can withstand common security threats and provide the necessary security for the perception layer. The performance analysis indicates that the suggested scheme is less complex and more efficient than similar schemes with the same level of security.

INDEX TERMS Emergency logistics, lightweight authentication, communication system security, perception layer.

I. INTRODUCTION

Frequent occurrences of natural catastrophes, accidents and calamities, public health events, and social security crises have imposed greater demands on the capacity of humans to deal with emergencies. Since the COVID-19 pandemic, many countries have declared a state of emergency. The demand for emergency supplies has spiked for a brief period, resulting in a lack of medical supplies and essentials. The significance of emergency logistics has been emphasized further and has become a global concern [1].

Emergency logistics refers to the activities that provide emergency production and living supplies to guarantee safety in response to emergencies. Unlike conventional logistics, emergency logistics encounter distinct challenges [2], [3], [4]. 1) Uncertainty of logistics activities. 2) The effectiveness and timeliness of the logistics response. 3) Limited logistics resources. 4) Communication and coordination difficulties among aid agencies. The construction of information infrastructure is a crucial component of an emergency logistics system since exchanging information and resources is vital in emergencies. It can enhance the execution capabilities of critical links such as warehousing, transportation, and distribution and ensure information sharing in emergencies. Due to

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

the rapid response of the supply chain, the effects of disasters can be mitigated.

The Internet of Things (IoT) has shown exciting application value in logistics. With its ability to acquire various data and diverse network access, the IoT empowers logistics activities to achieve visibility into the tracking and tracing of supplies throughout the logistics process [5], [6], [7]. Emergency logistics informatization is developed from the basis of military logistics and intelligent logistics, covering various fields such as wireless communication, satellite positioning, geographic information system, and cryptography. Emergency logistics activities hold a large amount of infrastructure, commercial, and demographic data, and their operations are closely related to critical information infrastructure. Meanwhile, since emergency response involves multiple organizations, such as medical care, fire protection, and police forces, information sharing brings information leakage risks. Security and privacy issues are significant challenges for the informatization construction of emergency logistics.

The perception layer in the IoT-based emergency logistics network architecture is the most fundamental data source for logistics activities. Since the perception layer is mainly composed of resource-constrained devices, its computational power and security protection capabilities are inadequate. Traditional security solutions typically demand a great deal of computational power and energy consumption and thus cannot be applied directly to the protection of the perception layer. If the perception layer lacks effective security protection mechanisms, the availability, confidentiality, integrity, controllability, and non-repudiation of information in the emergency logistics network cannot be fully guaranteed. Identity authentication-based security protection is a viable alternative to prevent perception layer devices/nodes from being illegally invaded and controlled. As the first line of defense for system security, all security measures will be useless once identity authentication is breached.

The identity authentication of the perception layer in the IoT-based emergency logistics network can uniquely identify and reliably authenticate objects [8], such as supplies, rescue equipment, vehicles, and personnel, to ensure that their physical and digital identities agree. Researchers have designed a range of security authentication protocols [9], [10], [11], [12], which are typically based on shared secrets, public key cryptography algorithms, and unique characteristics of users or devices (e.g., physical unclonable functions). Considering the computing power and security requirements in the perception layer, the lightweight authentication protocol for the perception layer in the IoT-based emergency logistics network should achieve the following objectives. 1) Two-way authentication of communication. 2) Anonymity of user identity. 3) The key generation center (KGC) cannot store all user keys. 4) The ability to update the key. 5) Resistance to common attacks. 6) Low computational complexity. 7) Low communication cost. Lightweight authentication in the perception layer has increased the network's security from the first reliance on digital identification (such as device serial number and QR code) to the authentication based on a shared secret and then to certificateless authentication. However, as we all know, security and efficiency are a pair of contradictions. Finding a balance between lightweight and security for authentication protocols is difficult in the context of limited perception layer resources.

To cover this gap, we propose a lightweight certificateless authentication protocol for the IoT-based emergency logistics network. The main contributions are as follows:

1) We propose a novel lightweight certificateless authentication protocol for perception layer authentication in emergency logistics networks.

2) Our CL-LAP authentication scheme does not use any bilinear pairing operation, thus drastically reducing computation and communication costs compared to similar certificateless authentication protocols.

3) The proposed CL-LAP is secure and robust. Under the random oracle model, we prove that CL-LAP is resistant to common attacks in the perception layer, such as adaptive chosen-message attacks and identity attacks.

4) The implementation of an anonymous identification and batch verification mechanism can satisfy the rapid verification requirements of enormous nodes in logistics activities and ensure the safety and efficacy of the emergency logistics information system.

The rest of this paper is structured as follows. Section II presents the pertinent research. Section III discusses the application scenarios of lightweight certificateless authentication schemes and the basics of the paper's comprehension. In Section IV, the suggested authentication protocol is described. The security analysis of the protocol is conducted in Section V. Section VI shows the performance evaluation. Finally, the conclusion is presented in Section VII.

II. RELATED WORK

This paper focuses on the security protection of the perception layer in IoT-based logistics networks. There are typically two implementations [13] to obtain the data of sensing nodes, aggregating data through gateway or acquiring real-time data directly from sensing nodes. The former is a typical three-level communication infrastructure (sensing nodes, gateway, and cloud server). However, this method has strict criteria for the gateway's availability. When multiple concurrent queries are executed, the gateway experiences a significant delay in obtaining data. The latter directly obtains data from sensing nodes (such as NB-IoT, LTE Cat-m), which is more real-time and flexible but requires careful design of the identity authentication protocol to accommodate the resource-constrained characteristics of sensing nodes. Numerous studies [14], [15], [16] have been conducted on the security protection of the above two types of networks, but each has its applicable scenarios. The former is more appropriate for short-distance ad hoc network scenarios, such as electronic medical care and smart home. In contrast, the latter is more appropriate for medium and long-distance communication of many devices, such as smart

metering and smart logistics. Utilizing lightweight cryptography approaches for security and privacy protection is a common concern shared by researchers despite the diversity of network architectures.

Public key cryptography is widely used for identity authentication in large-scale systems, including designing authentication protocols for the IoT, due to its significant advantages in key distribution and digital signature. According to public key cryptography, existing IoT authentication protocols can be divided into three categories, public key infrastructure and certification center (PKI/CA), identity-based certification (IBC), and certificateless public key cryptography (CL-PKC).

Traditional public key cryptography like PKI/CA rely on trusted centers and digital certificates as crucial security measures [17], [18]. A digital certificate contains the user's identity, public key, and CA's signature. CA maintains the public key of all users and authenticates users by providing digital certificates. The user's certificate and private key must be kept on an encryption chip to meet security requirements. Numerous mathematical methods, including elliptic curves [19], lattices [20], and chaotic maps [21], have been employed by researchers to build PKI/CA. However, most studies have shown the complexity of certificate generation. Overall, PKI/CA's security requires enormous complexity and cost. This is reflected in certificate generation, management, verification, and revocation phases, which makes applying PKI quite onerous. Moreover, as the number of users increases, certificates will increase exponentially, and authentication bottlenecks will appear, which cannot meet the lightweight and high-efficiency requirements of identity authentication at the perception layer in emergency logistics scenarios.

The identity-based cryptography scheme [22] effectively avoids the complexity of managing and using certificates. In IBC, the user's public key is mainly derived from its specific identity information, which has the obvious advantage of not requiring online verification and not requiring a complex management system. Reference [23] constructed a key agreement protocol based on bilinear pairings under IBC for the first time. Researchers then developed various authentication protocols based on identity signatures using bilinear pairings in IoT scenarios [24], [25], [26]. Although the IBC solution solves the problem of non-central authentication and public key binding, it also has two significant flaws. 1) Key escrow. The center generates the user's private key, and the digital signature is not individual. 2) Key update. The user's key cannot be modified since the identity and the user's key are uniquely related. Due to the rapid circulation of objects in emergency logistics activities, the life cycle of keys often changes with the links of transportation, delivery, and distribution. Unauthorized nodes may access sensitive information if the keys cannot be updated. Once a passive malicious KGC appears, the KGC with the master key will be able to decipher any message and forge any signature [27], [28], substantially reducing the security of the emergency logistics system.

CL-PKC [29] provides an attractive alternative for lightweight identity authentication. Due to the following significant advantages, we decide to use certificateless public key cryptography for the identity authentication of the perception layer of the logistics network. 1) It enables efficient certification, which is crucial for emergency logistics systems. Compared with traditional public key authentication methods, certificateless authentication has lower computation and communication costs. Bilinear pairing or ECC, commonly used in certificateless authentication, has shorter keys and less computation than RSA, DSA, and EL Gammal used in traditional public key cryptography. The transmitted data packets are also shorter since digital certificates are not required to be exchanged during the authentication process. 2) It has strong non-repudiation. Since the KGC and the user jointly generate the user's private key, the user's signature cannot be forged even if there is a passive malicious KGC. 3) It avoids the additional overhead of managing and maintaining the public key certificate. The certificateless authentication approach overcomes the issue of public key authenticity. It considerably reduces the complexity of key management by calculating the receiver's complete public key based on the receiver's identity and system settings. 4) It provides flexibility and scalability. Since certificateless authentication is convenient for key updates and can adapt to dynamically changing network topology, it is compatible with emergency logistics' multi-link management and multi-participant interaction characteristics.

Recently, several proposals proposing certificateless authentication protocols in IoT were published. However, balancing lightweight, high authentication efficiency, and security is still relatively challenging. Certificateless authentication can be divided into schemes based on bilinear pairing and schemes without bilinear pairing. Several bilinear pairing-based solutions are proposed for the identity authentication of the IoT [30], [31], [32]. Despite emphasizing low-complexity design and accelerating the pairing calculation process, these schemes still have much computation costs. Researchers optimized or substituted the bilinear pairing operation and designed certificateless schemes [33], [34], [35], [36], [37], [38] without bilinear pairing. This scheme has been utilized in security and privacy design for smart grid [36], smart city monitoring [37], and healthcare [38]. However, this type of scheme is susceptible to security shortcomings. For instance, the approach described in [35] is proven unable to withstand attacks and forged signatures from hacked KGC [39]. A certificateless digital signature scheme appropriate for the Industrial IoT was proposed in reference [40]. However, this scheme could not resist public key substitution attacks [41].

Lightweight authentication for the perception layer of IoT must simultaneously take lightness, authentication efficiency, and security into account. Reference [42] proposed

a lightweight authentication protocol, using hash functions and continuous XOR functions to achieve perfect forward security, which can effectively resist internal privilege, stolen verification, and sensor node capture attacks. Reference [43] proposed a certificateless authentication protocol for IoT intelligent robots and introduced a batch verification algorithm to improve the authentication efficiency of the system. The above researches inspire lightweight identity authentication for the perception layer of the IoT-based emergency logistics network.

III. MODELS AND PROBLEMS

To accomplish reliable perception layer authentication, we first present an IoT-based emergency logistics application scenario and describe the adversaries of the system during key generation and transmission.

A. SECURITY SCENARIO

In emergency logistics, sensors, short-range wireless communication, and satellite navigation and positioning provide intelligent control of storage and transit. It is vital to have timely knowledge of the location and status of materials, containers, vehicles, and workers, as well as the logistics update. Before accessing the information, the corresponding identity must be validated to ensure security and prevent adversaries from accessing the data. The identity authentication in the perception layer discussed in this paper includes, but is not limited to, identity authentication in the WSN, consisting of wireless sensor components coupled to emergency materials, equipment, personnel, and vehicles in logistics activities, as depicted in Figure 3. All certification requirements for emergency logistics objects exist in the linkages of transportation, loading and unloading, storage, packaging, picking, and distribution, under the condition that self-organizing wireless networks can be established.

Even though the perception layer of the IoT-based logistics network is often comprised of perception nodes with limited computational capacity, limited power supply, and open communication links, distinct logistical activities have their unique characteristics. Reference [4] categorizes IoT-based logistics into twelve different categories. Emergency logistics is distinguished from chemical logistics, cold chain logistics, and green logistics by its sensitivity to time, suddenness, safety, and organizational interaction complexity. In our research, the perception layer's lightweight authentication scheme is tailored to the features of IoT-based emergency logistics.

B. SECURITY THREATS

Common attacks in the perception layer of IoT-based emergency logistics networks include eavesdropping, impersonation, forgery, information tampering, and replay assaults. Their target objects can be divided into security threats to sensing nodes, security threats to sensing networks, and security threats to core networks.

Security threats to sensing nodes. There are many logistical objects and links involved in emergency logistics. Numerous sensor nodes are dispersed, allowing attackers easy access to destroy them, unlawfully replace their hardware physically, or replace their software through local operations.

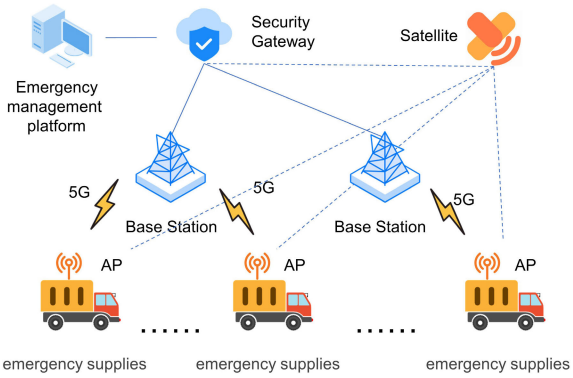

FIGURE 1. Application scenarios of emergency logistics.

Security threats to sensing networks. Due to the inherent openness of wireless channels, there are various security concerns in communication. It is impossible to establish a common security protection model for sensor networks due to the lack of a unified standard for data transmission.

Security threats to core networks. Although the core network has a relatively comprehensive security protection mechanism, its capacity to withstand denial of service (DoS) attacks is relatively weak due to the insufficient computation and communication capabilities and limited storage resources of the sensor nodes. Once the DoS attack happens, it is easy to cause network congestion, undermining the core network's availability and resulting in network paralysis.

C. SECURITY MODEL BASED ON CERTIFICATELESS AUTHENTICATION PROTOCOL

In this paper, the security of the IoT-based emergency logistics network refers to the security of the infrastructure of the logistics network, which can withstand threats and attacks from both internal and external sources. Consider the following two types of adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ (assuming $\mathcal{A}_1$ is a dishonest user and $\mathcal{A}_2$ is a passive and malicious KGC).

Type I Adversary: $\mathcal{A}_1$ is unaware of the system master key s and part of the user's private key d_{ID}, but it can replace the public key pk_{ID} of user whose identity information is ID.

Type II Adversary: $\mathcal{A}_2$ knows the system master key s and part of the user's private key d_{ID}, but cannot replace the public key pk_{ID} of user whose identity information is ID.

Definition 1: Suppose adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ cannot win the following two games with a non-negligible probability. Consequently, the certificateless authentication protocol is existentially unforgeable on adaptively certificateless signature chosen message attacks (EUF-CLS-CMA).

1) GAME 1 (EUF-CLS-CMA GAME AGAINST A TYPE I ADVERSARY)

In the system establishment stage, the challenger C runs the *Setup* algorithm to generate the system public parameters *params* and the system master key s, sends the generated

system public parameters *params* to $\mathcal{A}_1$, and secretly saves the system master key s.

In the query stage, $\mathcal{A}_1$ can adaptively perform the following polynomial order bound oracle query.

a: HASH QUERY

$\mathcal{A}_1$ can initiate a hash oracle query to all the hash values used in the scheme at any time, and C return the corresponding hash value to $\mathcal{A}_1$.

b: PARTIAL PRIVATE KEY EXTRACTION QUERY

When $\mathcal{A}_1$ performs a *Partial-Private-Key-Extract* query on the partial private key d_{ID} of the user whose identity information is ID, C generates the part private key d_{ID} of the user identity information by running the *Partial-Private-Key-Extract* algorithm, and return the value to $\mathcal{A}_1$.

c: PRIVATE KEY QUERY

In addition to the identity information ID^* of challenger C, $\mathcal{A}_1$ can initiate a *Private-Key-Extract* query on the identity information of any other user. When receiving $\mathcal{A}_1$'s *Private-Key-Extract* query for the private key sk_{ID} of the user, C runs the *Private-Key-Generate* algorithm to return the generated private key sk_{ID} to $\mathcal{A}_1$. Suppose the public key pk_{ID} of the user has been replaced, C can't calculate the correct private key unless $\mathcal{A}_1$ submits a new secret value to C.

d: PUBLIC KEY QUERY

When $\mathcal{A}_1$ makes a *Public-Key-Request* query to the user whose identity information is ID, C runs the *Secret-Value-Generate* algorithm and *Public-Key-Generate* algorithm to generate the user's public key pk_{ID} and returns it to $\mathcal{A}_1$.

e: PUBLIC KEY REPLACEMENT QUERY

When $\mathcal{A}_1$ performs the *Public-Key-Replacement* query on the user, $\mathcal{A}_1$ can use the public key $pk_{ID'}$ selected by himself to replace the public key pk_{ID} of the user.

f: SIGNATURE GENERATION QUERY

Given the message m and the user's identity information ID, when $\mathcal{A}_1$ makes a *Sign-Generate* query about the message m, C uses the ID's private key sk_{ID} to calculate the signature S and return it to $\mathcal{A}_1$. If the user's public key pk_{ID} has been replaced by $\mathcal{A}_1$ with $pk_{ID'}$, C has no corresponding secret value $x_{ID'}$, and the output of the *Sign-Generate* oracle may be wrong. So we ask $\mathcal{A}_1$ to additionally submit a new secret value $x_{ID'}$ to the *Sign-Generate* oracle.

Finally, $\mathcal{A}_1$ outputs a message/signature pair (m^*, S^*) corresponding to the challenger C's identity information ID^* and public key pk_{ID^*}.

$\mathcal{A}_1$ wins the game if and only if *Sign-Verify*$(params, ID^*, m^*, pk_{ID^*}, S^*) = 1$ is satisfied and all of the following conditions hold.

(1)ID^* is never submitted to the *Private-Key-Extract* oracle.

(2)ID^* is never submitted to both the *Public-Key-Replacement* oracle and the *Partial-Private-Key-Extract* oracle at the same time.

(3)$(m^*, S^*, ID^*, pk_{ID^*})$ is not obtained by the *Sign-Generate* oracle.

2) GAME 2 (EUF-CLS-CMA GAME AGAINST A TYPE II ADVERSARY)

In the system establishment stage, challenger C inputs security parameter k, runs *Setup* algorithm to generate system public parameter *params* and system master key s, and sends the generated system parameter *params* and system master key s to $\mathcal{A}_2$.

In the query stage, $\mathcal{A}_2$ can adaptively perform the following polynomial order bound oracle query.

a: HASH QUERY

$\mathcal{A}_2$ can access all the hash oracles used in the scheme and get the corresponding hash value.

b: PRIVATE KEY QUERY

In addition to the identity information of challenger C, $\mathcal{A}_2$ initiates a *Private-Key-Extract* query on the identity information of any other user. When receiving $\mathcal{A}_2$'s *Private-Key-Extract* query for the private key sk of the user, C runs the *Private-Key-Generate* algorithm to return the generated private key sk to $\mathcal{A}_2$.

c: PUBLIC KEY QUERY

When $\mathcal{A}_2$ performs a *Public-Key-Request* query on the public key pk_{ID} of the user, C runs the *Secret-Value-Generate* algorithm and the *Public-Key-Generate* algorithm to generate the user's public key pk_{ID} and return it to $\mathcal{A}_2$.

d: SIGNATURE GENERATION QUERY

Given message m and user's identity information ID, when $\mathcal{A}_2$ performs a *Sign-Generate* query about message m, C uses ID's private key sk_{ID} to calculate signature S and return it to $\mathcal{A}_2$.

Finally, $\mathcal{A}_2$ outputs a message/signature pair (m^*, S^*) corresponding to the challenger C's identity information ID^* and public key pk_{ID^*}.

$\mathcal{A}_2$ wins the game if and only if *Sign-Verify*$(params, ID^*, m^*, pk_{ID^*}, S^*) = 1$ is satisfied and both of the following conditions hold.

(1)ID^* is never submitted to the *Private-Key-Extract* oracle.

(2)$(m^*, S^*, ID^*, pk_{ID^*})$ is not obtained by the *Sign-Generate* oracle.

IV. EMERGENCY LOGISTICS LIGHTWEIGHT AUTHENTICATION PROTOCOL

This section first proposes the communication model of CL-LAP, a lightweight authentication protocol based on certificateless signature, which corresponds to the design of perception layer authentication for IoT-based emergency

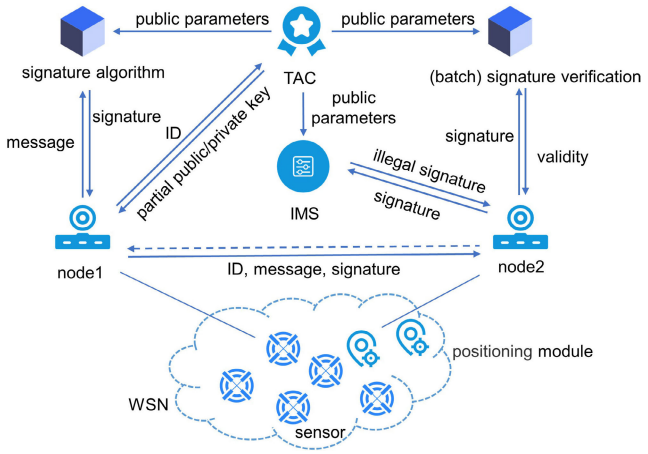

FIGURE 2. Communication model of CL-LAP.

logistics networks. Then the specific algorithm design of the protocol is developed, and the particular process of protocol authentication is described in detail.

A. PROTOCOL COMMUNICATION MODEL

The system model of the lightweight authentication protocol CL-LAP is shown in Figure 3. The communication model mainly includes

1) TRUSTED CERTIFICATION CENTER (TAC)

The emergency logistics management department or a trusted third party can construct the TAC. Assume TAC is wholly trustworthy and impenetrable. It is primarily accountable for the following three duties.

(1)The TAC randomly assigns unique and legitimate anonymous identity information for communication in the sensing network, including a signature of the TAC to prove that the TAC indeed assigns the identity.

(2)The public parameters and the master key are generated in the system parameter establishment stage.

(3)The TAC creates a partial key in response to a request from a sensing node. It then transmits it to the sensing node through the secure channel, and the node verifies the validity of the received partial key.

2) SENSING NODES

Since emergency materials usually do not have communication functions, various sensing nodes are attached to the materials or deployed in storage and transportation environments. These sensing nodes establish a sensing network through wireless self-organization and exchange broadcast signals for communication. Each node can be considered a router and can locate and restore connections.

3) SINK NODE

The sink node's primary responsibility is to receive and transmit the sensing data from the sensing node.

In addition to the above communication entities, the communication model of CL-LAP incorporates signature, batch signature verification, and invalid message search algorithms. These algorithms and keys are used to realize the efficient and secure certification of sensing nodes' identity and broadcast messages in the sensing network.

TABLE 1. Notations and meanings.

No.	Notations	Meanings
1	p, q	prime number
2	F_q	Finite fields of characteristic q
3	Z_q^*	finite fields of order q
4	e	bilinear mapping
5	G_1	multiplicative cyclic group
6	G	additive cyclic group
7	P	The generating element of G
8	$k, 1^k$	Security parameters
9	H_i, h_i	One-way Hash function
10	$params$	System public parameters
11	s	System master key
12	s_T	KGC's private key
13	P_T	KGC's public key
14	P_pub	System public key
15	D_i, d_{ID}	The user's partial private key
16	R_i	The user's partial public key
17	x_i, x_{ID}	Secret value
18	d_i, sk_{ID}, sk_i	The user's private key
19	pk_{ID}, pk_i	The user's public key
20	$\sigma, \sigma_i, S, S_i, K_i$	Signature
21	L_{SK}	List of user's private key
22	L_S	List of user's signature
23	L_{PSK}	List of user's partial private key
24	L_{PK}	List of user's public key

B. LIGHTWEIGHT AUTHENTICATION PROTOCOL CL-LAP

This section proposes a lightweight authentication protocol CL-LAP without bilinear pairings. The authentication protocol is mainly composed of system parameter establishment algorithm (*Setup*), secret value generation algorithm, partial private key extract algorithm, signature generation algorithm (*Sign-Generate*), signature verification algorithm (*Sign-Verify*), and batch signature verification algorithm. The specific process is shown in Figure 3. The detailed operation process of the algorithm is described as follows.

1) SYSTEM PARAMETER ESTABLISHMENT ALGORITHM

Randomly select a large prime number q ($q > 2^k$, k is a security parameter), the elliptic curve $y^2 \equiv x^3 + ax + b \,(\mathrm{mod} q)$ on the finite field, where $a, b \in Z_q^*$, satisfy $4a^3 + 27b^2 \neq 0 \bmod q$. G is an additive cyclic group of elliptic curves and P is the generator of G.

Select four collision-resistant and safe hash functions,

$$\begin{aligned} &H_1 : \{0,1\}^* \to Z_q^* \\ &H_2 : G \times G \times G \to Z_q^* \\ &H_3 : \{0,1\}^* \times G \times G \times \{0,1\}^* \to Z_q^* \\ &H_4 : G \times G \times G \times \{0,1\}^* \to Z_q^*. \end{aligned} \tag{1}$$

Randomly select a system master key $s \in Z_q^*$, keep it secret, and calculate the system public key $P_{pub} = sP$.

KGC public system public parameters $params = \{q, P, G, P_{pub}, H_1, H_2, H_3, H_4\}$. H_3 and H_4 introduce anonymity protection for the entity identity information of sensing nodes.

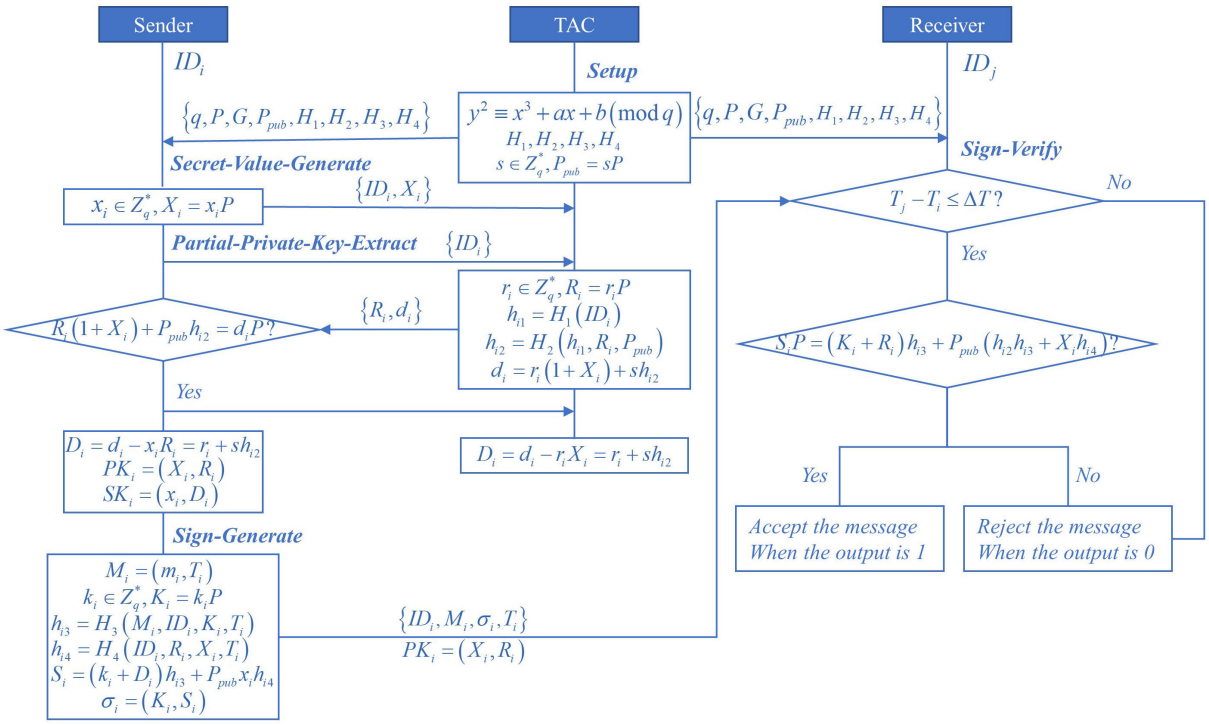

FIGURE 3. Process of certificateless authentication protocols without bilinear pairings.

In order to achieve the anonymity protection of the node entity identity information, TAC selects two random numbers $u, v \in Z_q^*$, keeps them secret and calculates $ID_i = \left(h_{i1}, uEID_i \oplus vP_{pub}\right)$ as its identity information for communication in the sensing network, where $h_{i1} = H_1(EID_i)$. The entity identity information of the sensing node is $EID_i \in \{0, 1\}^*$. Only TAC can calculate the entity identity information EID_i of the node based on h_{i1}.

2) SECRET VALUE GENERATION ALGORITHM

This algorithm is run by the sensing node N_i (the node's identity information is ID_i). The sensing node N_i picks a random secret value $x_i \in Z_q^*$, calculates $X_i = x_iP$, saves x_i secretly and sends the (ID_i, X_i) to the TAC.

3) PARTIAL PRIVATE KEY EXTRACT ALGORITHM

This algorithm is run jointly by the TAC and the sensing node N_i. When the sensing node N_i requests TAC to generate a partial key, TAC picks a random number $r_i \in Z_q^*$, and calculates $R_i = r_iP$, $h_{i2} = H_2\left(h_{i1}, R_i, P_{pub}\right)$, $d_i = r_i(1 + X_i) + sh_{i2}$, where R_i is the partial public key of node N_i.

TAC sends (R_i, d_i) to node N_i. To check the legitimacy of (R_i, d_i), node N_i checks the legitimacy by calculating whether the following equation holds,

$$R_i(1 + X_i) + P_{pub}h_{i2} = d_iP. \tag{2}$$

If it holds, compute $D_i = d_i - x_iR_i = r_i + sh_{i2}$ as its partial private key. At the same time, TAC can also calculate the partial private key D_i of node N_i.

The public key of node N_i is $PK_i = (X_i, R_i)$ and the private key is $SK_i = (x_i, D_i)$.

4) SIGNATURE GENERATION ALGORITHM

This algorithm is run by the sensing node N_i (signer). The process of signing the message m_i by the sensing node consists of four main steps as follows.

Computing $M_i = (m_i, T_i)$, where T_i is the timestamp and $m_i, M_i \in \{0, 1\}^*$.

Selecting a random number $k_i \in Z_q^*$ and computing $K_i = k_iP$.

Computing $h_{i3} = H_3(M_i, ID_i, K_i, T_i)$, $h_{i4} = H_4(ID_i, R_i, X_i, T_i)$.

Generating the signature $\sigma_i = (K_i, S_i)$ about the message M_i, where $S_i = (k_i + D_i)h_{i3} + P_{pub}x_ih_{i4}$.

The broadcast message sent by the sensing node N_i in the sensing network is $\{ID_i, M_i, \sigma_i, T_i\}$.

5) SIGNATURE VERIFICATION ALGORITHM

This algorithm is run by the sensing node N_j (receiver). When sensing node N_j receives a broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ from sensing node N_i, sensing node N_j verifies the legitimacy of signature σ_i in message M_i, thus determine the authenticity and integrity of the source of message M_i. It realizes authentication of broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ in the sensing network and prevents sensing nodes from sending fake broadcast messages.

Calculating whether $T_j - T_i \le \Delta T$ holds. If it holds, run the following step to verify the legitimacy of the message M_i's signature σ_i. Otherwise, reject the message. T_j is the current

Algorithm 1 Single Signature Verification Process in CL-LAP

Input: $params$, $\{ID_i, M_i, \sigma_i, T_i\}$.
Output: $1 or 0$
if T_i is not expired and $T_j - T_i \leq \Delta T$ **then**
  do $h_{i3} = H_3(M_i, ID_i, K_i, T_i)$,
    $h_{i4} = H_4(ID_i, R_i, X_i, T_i)$
  if $S_iP = (K_i + R_i)\, h_{i3} + P_{pub}\,(h_{i2}h_{i3} + X_i h_{i4})$ **then**
    return 1
  else
    return 0
  end if
end if

timestamp representing the time when the receiver received the message.

Inputting the message/signature pair (M_i, σ_i) corresponding to the message M_i. The receiver verifies the legitimacy of the signature S_i in the message M_i by equation (3),

$$S_iP = (K_i + R_i)\, h_{i3} + P_{pub}\,(h_{i2}h_{i3} + X_i h_{i4}). \tag{3}$$

If it holds, it means that the single signature S_i of message M_i is legitimate and thus accepts the message sent by node N_i. Otherwise, rejects the message.

The specific process of signature verification in CL-LAP is shown in Algorithm 1.

6) BATCH SIGNATURE VERIFICATION ALGORITHM

This algorithm is executed by sensing node N_j (receiver). When a large number of broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ $(i = 1, 2, \cdots, n)$ are clustered at sensing node N_j, a batch verification algorithm is introduced to improve the authentication efficiency of the signature σ_i $(i = 1, 2, \cdots, n)$ in the batch message M_i $(i = 1, 2, \cdots, n)$. The authenticity and integrity of the message M_i are checked to achieve authentication of broadcast messages $\{ID_i, M_i, \sigma_i, T_i\}$ in the sensing network and prevent sensing nodes from sending fake broadcast messages.

Calculating whether $T_j - T_i \leq \Delta T$ holds. If it holds, run the following step to verify the legitimacy about the message M_i's signature σ_i. Otherwise, reject the message. T_i is the current timestamp representing the time when the receiver received the message.

Inputting n message/signature pairs (M_i, σ_i) corresponding to n messages M_i, and the receiver verifies the legitimacy of S_i in n signatures by equation (4),

$$\sum_{i=1}^{n} a_i S_i P = \sum_{i=1}^{n} a_i\,(K_i + R_i) h_{i3} + P_{pub} \sum_{i=1}^{n} a_i\,(h_{i2}h_{i3} + X_i h_{i4}), \tag{4}$$

where $\vec{a} = (a_1, a_2, \cdots, a_n)$ is a small exponential vector.

Algorithm 2 IMS Algorithm for Batch Signature Verification in CL-LAP

Input: $ML = \{ID_i, M_i, \sigma_i, T_i\}$
Output: $IML = \{ID_1, ID_2, \cdots, ID_m\}$
Function
  invalidMessageSearch (ML,IML,MI,low,high)
    else
if *batchVerify (ML,MI,low,high)* **then**
  return *TRUE*
  else if *(low = = high)*
    IML.append (ML [low])
    return *IML*
    mid $= (low + high)/2$
    else if $(MI < mid)$
      invalidMessageSearch (ML,IML,MI,low,mid)
    else
      invalidMessageSearch (ML,IML,MI,mid+1,high)
    end if
  end if
  return *IML*
end if
end Function
for *i:=1 to n* **do**
  invalidMessageSearch (ML,IML,i,1,n)
end for

If equation (4) holds, all the n messages corresponding to n signatures are legitimate and thus accept all of the messages sent by these nodes. Otherwise, there are illegitimate signatures among the messages corresponding to n signatures.

The IMS algorithm is introduced in CL-LAP to improve authentication efficiency and prevent missing significant messages. We implement the search for illegal signatures in batch signatures and the search for invalid broadcast messages in batch broadcast messages. The detailed implementation process is shown in Algorithm 2. When the signature S_i $(i = 1, 2, \cdots, n)$ in the broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ $(i = 1, 2, \cdots, n)$ does not satisfy equation (4), the search for invalid broadcast messages is achieved by running the IMS algorithm, whose input is the list of messages and output is the list of invalid messages. *batchVerify*$(ML, MI, low, high)$ indicates to verify the signatures with subscript between $[low, high]$, returning *TRUE* for successful verification and *FALSE* for failure. Accepting valid broadcast messages and discarding invalid ones after the verification. In this way, it is not necessary to discard all the n broadcast messages that do not satisfy equation (4).

V. PROTOCOL SECURITY ANALYSIS

This section first gives the proposed protocol's correctness analysis and security proof. Second, it demonstrates that CL-LAP can withstand common assaults in the IoT perception layer using a random oracle model based on the assumption of the difficulty of DLP on elliptic curves.

A. CORRECTNESS ANALYSIS

1) CORRECTNESS OF SIGNATURE VERIFICATION ALGORITHM

After receiving the broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$, the user U_i (receiver) verifies the correctness of S_i by equation (5),

$$\begin{aligned} S_iP &= \left[(k_i + D_i)\, h_{i3} + P_{pub} x_i h_{i4}\right] P \\ &= \left[k_i h_{i3} + (r_i + sh_{i2})\, h_{i3} + P_{pub} x_i h_{i4}\right] P \\ &= K_i h_{i3} + (r_i h_{i3} + sh_{i2} h_{i3})\, P + P_{pub} X_i h_{i4} \\ &= K_i h_{i3} + R_i h_{i3} + P_{pub} h_{i2} h_{i3} + P_{pub} X_i h_{i4}. \end{aligned} \quad (5)$$

If it holds, the signature S_i generated in the broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ sent by user U_i (the signer) is correct. Otherwise, the generation process of user U_i's signature S_i is illegitimate or the broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ has been tampered during transmission.

2) CORRECTNESS OF BATCH SIGNATURE VERIFICATION ALGORITHM

After receiving the broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$, the sensing node verifies the correctness of S_i by equation (6),

$$\begin{aligned} SP &= \sum_{i=1}^{n} a_i S_i P \\ &= \sum_{i=1}^{n} a_i \left[(k_i + D_i)\, h_{i3} + P_{pub} x_i h_{i4}\right] P \\ &= \sum_{i=1}^{n} a_i \left[k_i h_{i3} + (r_i + sh_{i2})\, h_{i3} + P_{pub} x_i h_{i4}\right] P \\ &= \sum_{i=1}^{n} a_i (K_i + R_i) h_{i3} + P_{pub} \sum_{i=1}^{n} a_i (h_{i2} h_{i3} + X_i h_{i4}). \end{aligned} \quad (6)$$

If it holds, the signatures S_i generated in the broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ are correct. Otherwise, the generation process of signatures is illegitimate, or tampering occurs during the broadcast message's transmission.

B. PROOF OF SECURITY

1) NON-FALSIFIABILITY

Theorem 1: In the random oracle model, CL-LAP is EUF-CLS-CMA in the case of DLP intractable on elliptic curves.

Proof: Theorem 1 can be derived from Lemma 1 and Lemma 2. □

Lemma 1: Under the random oracle model, suppose an adversary $\mathcal{A}_1$ with probabilistic polynomial time capability can successfully forge a legitimate signature with non-negligible probability through the interaction process with challenger C. *Challenger* C *can find an instance that solves the DLP on the elliptic curve.*

Proof: Suppose $\langle P, Q\rangle$ is a random instance of the DLP difficulty assumption on an elliptic curve. P, Q is a generating element of the cyclic group G, where $Q = aP$ and $a \in Z_q^*$. The objective of C is to find a after completing the interaction with $\mathcal{A}_1$.

In the system parameter building phase, C runs the *Setup* algorithm to generate the system public parameter $params\{q, P, G, P_{pub} H_1, H_2, H_3, H_4\}$, where $P_{pub} = aP$. C sends the generated system public parameter *params* to $\mathcal{A}_1$ and secretly saves the system master key a. C selects the identity information ID_1 as its challenge identity.

In the interrogation phase, $\mathcal{A}_1$ adaptively performs the following polynomial order of magnitude bounded prophecy machine interrogation. C maintains the following lists $\{L_1, L_2, L_3, L_4, L_{PSK}, L_{PK}\}$, all initialized to be empty, to record the interrogation data of $\mathcal{A}_1$ to the prophecy machine H_1, H_2, H_3, H_4, the private key, and the public key of the user, respectively.

a: HASH INTERROGATION

All hash functions $H_i\,(i = 1 \sim 4)$ are treated as random oracle. C maintains lists $\{L_1, L_2, L_3, L_4\}$, where $L_1 = \{ID_l, h_{l1}\}$, $L_2 = \{h_{l1}, R_l, P_{pub}, h_{l2}\}$, $L_3 = \{M_l, ID_l, K_l, T_l, h_{l3}\}$, $L_4 = \{ID_l, R_l, X_l, T_l, h_{l4}\}$. When $\mathcal{A}_1$ makes a $H_i\,(i = 1 \sim 4)$ query, C gives the following answer. If the query for ID_i is found in the list L_i, then the corresponding $h_{ij}\,(j = 1 \sim 4)$ is returned to $\mathcal{A}_1$. Otherwise, C randomly selects $h_{ij}\,(j = 1 \sim 4)$, adds it to the list L_i and returns h_{ij} to $\mathcal{A}_1$.

b: PARTIAL PRIVATE KEY EXTRACT QUERY

When $\mathcal{A}_1$ makes a *Partial-Private-Key-Extract*(ID_i) query to ID_i, C gives the following answer, if $ID_i = ID_I$, C terminates the game. If $ID_i \neq ID_I$, find the query to (ID_i, R_i, D_i) in list L_{PSK}, then return the corresponding partial private key D_i to $\mathcal{A}_1$. Otherwise, C randomly selects $a_i \in Z_q^*$, makes $D_i = a_i$, adds (ID_i, R_i, D_i) to the list $L_{PSK} = \{ID_i, R_i, D_i\}$ and returns a to $\mathcal{A}_1$.

c: PUBLIC KEY QUERY

C maintains the list $L_{PK} = \{ID_l, x_l, X_l\}$. When $\mathcal{A}_1$ makes a *Request-Public-Key*(ID_i) query to ID_i, C gives the following answer, if the query to (ID_i, x_i, X_i) is found in the list L_{PK}, then the corresponding X_i is returned to $\mathcal{A}_1$. Otherwise, it is divided into the following two cases. If $ID_i = ID_I$, C randomly selects $x_i, a_i, b_i \in Z_q^*$, such that $X_i = x_iP$, $H_2\left(h_{i1}, R_i, P_{pub}\right) = a_i$, $R_i = b_iP - a_iP_{pub}$, adds $\left(h_{i1}, R_i, P_{pub}, a_i\right)$ and (ID_i, x_i, X_i) to the lists L_2 and L_{PK}, and returns X_i to $\mathcal{A}_1$. Otherwise, C randomly picks $x_i, a_i, b_i \in Z_q^*$ such that $X_i = x_iP$, $H_2\left(h_{i1}, R_i, P_{pub}\right) = a_i$, $R_i = b_iP$, adds $\left(h_{i1}, R_i, P_{pub}, a_i\right)$ and (ID_i, x_i, X_i) to lists L_2 and L_{PK} and returns X_i to $\mathcal{A}_1$.

d: SECRET VALUE QUERY

When $\mathcal{A}_1$ makes a *Request-Secret-Value*(ID_i) query to ID_i, C gives the following answer, if $ID_i = ID_I$, C terminates the game. If $ID_i \neq ID_I$, if the query to (ID_i, R_i, D_i) is found in the list L_{PK}, then the corresponding secret value x_i is returned to $\mathcal{A}_1$. Otherwise, C runs the *Request-Public-*

Key(ID_i) algorithm to generate (x_i, X_i) and returns the generated secret value x_i to $\mathcal{A}_1$.

e: PUBLIC KEY REPLACEMENT QUERY

When $\mathcal{A}_1$ makes an *Replace-Public-Key*(ID_i, PK_i') query on ID_i, C gives the following answer, if the query on (ID_i, x_i, X_i) is found in the list L_{PK}, then X_i is replaced by X_i' selected by $\mathcal{A}_1$ and $x_i = \perp$. Otherwise, C runs the *Request-Public-Key*(ID_i) algorithm to make a public key query on ID_i.

f: SIGNATURE GENERATION QUERY

When $\mathcal{A}_1$ makes a *Sign-Generate*(ID_i, M_i) query to ID_i about message M_i, C recovers h_{i1}, $\left(h_{i1}, R_i, P_{pub}, h_{i2}\right)$, $(M_i, ID_i, K_i, T, h_{i3})$, $(ID_i, R_i, X_i, T_i, h_{i4})$, (ID_i, R_i, D_i) and (ID_i, x_i, X_i) from list $\{L_1, L_2, L_3, L_4, L_{PSK}, L_{PK}\}$. C randomly selects $S_i \in Z_q^*$, makes $K_i = h_{i3}^{-1}[S_iP - P_{pub}(h_{i2}h_{i3} + X_ih_{i4})] - R_i$, adds $\left(h_{i1}, R_i, P_{pub}, h_{i2}\right)$, $(M_i, ID_i, K_i, T_i, h_{i3})$ and $(ID_i, R_i, X_i, T_i, h_{i4})$ to lists L_2, L_3 and L_4 and returns signature S_i to $\mathcal{A}_1$. Since $S_iP = (K_i + R_i)\, h_{i3} + P_{pub}\,(h_{i2}h_{i3} + X_ih_{i4})$ satisfies equation (3), the generated signature S_i is a legitimate signature.

g: FORGERY

$\mathcal{A}_1$ Outputs the forged signature (ID^*, M, K^*, S^*). where ID^* is never submitted both to the *Partial-Private-Key-Extract*(ID_i) oracle machine and to the *Request-Secret-Value*(ID_i) oracle machine at the same time. The (ID^*, M) is never submitted to the *Sign-Generate*(ID_i, M_i) oracle machine. If $ID_i \neq ID^*$, then C fails. Otherwise, it follows from the forking lemma that C can find the L_{PSK} and L_{PK} lists through the oracle replay attack, and obtain two sets of valid signature (ID_i, M_i, K_i, S_i) and (ID^*, M, K^*, S^*) by repeating the above interaction process.

$$\begin{aligned} S_i &= (k_i + D_i)\, h_{i3} + P_{pub}x_ih_{i4}, \\ S_i^* &= (k_i + D_i)\, h_{i3}^* + P_{pub}x_ih_{i4}, \end{aligned} \tag{7}$$

where $h_{i3} \neq h_{i3}^*$.

Utilizing $X_i = x_iP$, $P_{pub} = aP$, $R_i = b_iP$, according to equation (7), it can be found that

$$a = h_{i2}^{-1}\left(S_i - S_i^*\right) / \left(h_{i3} - h_{i3}^*\right) - k_ih_{i2}^{-1} - a_ih_{i2}^{-1}. \tag{8}$$

That is, C solves an instance of the DLP hardship assumption.

□

Lemma 2: Under the random oracle model, if an adversary $\mathcal{A}_2$ with probabilistic polynomial time capability can successfully forge a legitimate signature with non-negligible probability through the interaction process with challenger C, *challenger* C *can find an instance that solves the DLP on the elliptic curve.*

Proof: Suppose that $\langle P, Q\rangle$ is a random instance of the DLP difficulty assumption on an elliptic curve, where P, Q are generators of the cyclic group G, $Q = bP$, $b \in Z_q^*$. The goal of C is to find b after completing the interaction with $\mathcal{A}_2$.

In the system parameter establishment phase, C runs the *Setup* algorithm to generate the system public parameter *params* $\left\{q, P, G, P_{pub}, H_1, H_2, H_3, H_4\right\}$, where $P_{pub} = sP$. C sends the generated system public parameter *params* to $\mathcal{A}_2$ and secretly saves the system master key s. C selects the identity information ID_I as its identity information.

In the interrogation phase, $\mathcal{A}_2$ adaptively performs the following polynomial order-of-magnitude bounded prophecy machine interrogation. C maintains the following lists $\{L_2, L_3, L_4, L_{PK}\}$initialized all empty to record the interrogation data of $\mathcal{A}_2$ to the prophecy machine H_2, H_3, H_4, and the user public key, respectively. All are the same as Lemma1 except for public key interrogation and signature interrogation.

h: PUBLIC KEY QUERY

C maintains the list $L_{PK} = \{ID_I, x_I, X_I\}$. When $\mathcal{A}_2$ makes a *Request-Public-Key*(ID_i) query to ID_i, C gives the following answer, if the query to (ID_i, x_i, X_i) is found in the list L_{PK}, then the corresponding X_i is returned to $\mathcal{A}_2$. Otherwise, it is divided into the following two cases. If $ID_i = ID_I$, C randomly selects $x_i, b_i, r_i \in Z_q^*$, such that $X_i = x_ibP$, $H_2\left(h_{i1}, R_i, P_{pub}\right) = a_i$, $R_i = r_iP$, adds $\left(h_{i1}, R_i, P_{pub}, a_i\right)$ and ($ID_i, \perp, x_ibP$) to the lists L_2 and L_{PK}, and returns X_i to $\mathcal{A}_2$. Otherwise, C randomly picks $x_i, b_i, r_i \in Z_q^*$ such that $X_i = x_iP$, $H_2\left(h_{i1}, R_i, P_{pub}\right) = a_i$, $R_i = b_iP$, adds $\left(h_{i1}, R_i, P_{pub}, a_i\right)$ and ($ID_i, \perp, X_i$) to lists L_2 and L_{PK} and returns X_i to $\mathcal{A}_2$.

i: SIGNATURE GENERATION QUERY

When $\mathcal{A}_2$ makes a *Sign-Generate*(ID_i, M_i) query to ID_i about message M_i, C recovers $\left(h_{i1}, R_i, P_{pub}, h_{i2}\right)$, $(M_i, ID_i, K_i, T_i, h_{i3})$, $(ID_i, R_i, X_i, T_i, h_{i4})$ and (ID_i, x_i, X_i) from list $\{L_2, L_3, L_4, L_{PK}\}$. If $ID_i = ID_I$, C randomly selects $b_i \in Z_q^*$, such that $K_i = k_iP - b_iX_i$, it can solve $S_i = (R_i\, h_{i3} + K_ih_{i3} - b_iX_ih_{i3})\, P^{-1} + h_{i2}h_{i3}s + X_ih_{i4}s$, and return the generated signature S_i to $\mathcal{A}_2$. The signature S_i can be verified as a legitimate signature by equation (3). If $ID_i \neq ID_I$, the signature is completed normally.

j: FORGERY

$\mathcal{A}_2$ outputs the forged signature (ID^*, M, K^*, S^*), where ID^* is never submitted to the *Request-Secret-Value*(ID_i) random oracle. At the same time, the (ID^*, M) is never submitted to the *Sign-Generate*(ID_i, M_i) random oracle. If $ID_i \neq ID^*$, then C fails. Otherwise, it follows from the forking lemma that C can find the L_{PSK} and L_{PK} lists through the oracle replay attack, and obtain two sets of valid signature (ID_i, M_i, K_i, S_i) and (ID^*, M, K, S^*) by repeating the above interaction process.

$$\begin{aligned} S_i &= (k_i + D_i)\, h_{i3} + P_{pub}x_ih_{i4}, \\ S_i^* &= (k_i + D_i)\, h_{i3}^* + P_{pub}x_ih_{i4}, \end{aligned} \tag{9}$$

where $h_{i3} \neq h_{i3}^*$.

Utilizing $X_i = x_i bP, P_{pub} = sP, R_i = r_i P$, according to equation (9), it can be found that

$$\begin{aligned}\frac{h_{i3}^* S_i - h_{i3} S_i^*}{h_{i3}^* - h_{i3}} &= \frac{P_{pub} h_{i3}^* x_i h_{i4} - P_{pub} h_{i3} x_i h_{i4}}{h_{i3}^* - h_{i3}} \\ &= P_{pub} x_i h_{i4} \\ &= b^{-1} X_i h_{i4} s. \end{aligned} \tag{10}$$

According to equation (10), it can be found that

$$b = \left(h_{i3}^* S_i - h_{i3} S_i^*\right)^{-1} \left(h_{i3}^* - h_{i3}\right) X_i h_{i4} s. \tag{11}$$

That is, C solves an instance of the DLP hardship assumption.

However, this contradicts the assumption that DLP on elliptic curves is difficult to solve. Therefore, the likelihood that an adversary of the above two types succeeds in forging a legitimate signature is negligible. An adversary cannot forge a legitimate identity message or generate a legitimate signature satisfying equation (3) to send a forged broadcast message to other users. The protocol is existentially unforgeable under adaptive choice message attacks and identity attacks.

□

2) ANONYMOUS

The sensing node will request TAC to register its identity information when it enters the sensing network. TAC will assign a unique and legal anonymous identity information ID_i to the node based on its entity identity information EID_i and attach TAC's signature to ensure that the identity signature is indeed assigned by the TAC, as $h_{i1} = H_1(EID_i)$, $ID_i = \left(h_{i1}, uEID_i \oplus vP_{pub}\right)$. Sensing nodes use the anonymous identity information ID_i to communicate in the sensing network. Only the TAC and the sensing node know the entity identity information EID_i. Therefore, CL-LAP has anonymity and achieves anonymous communication of the sensing node in the sensing network.

3) UNDENIABILITY

The sensing node whose identity information is ID_i uses its private key SK_i to sign the broadcast message M_i, where the signatures $\sigma_i = (K_i, S_i), K_i = k_i P, S_i = (k_i + D_i) h_{i3} + P_{pub} x_i h_{i4}$. After receiving the broadcast message, the public key PK of the signer and the signature σ_i in message M_i are utilized in equation 3 to verify the signature's legitimacy. Theorem 2 demonstrates that CL-LAP is unforgeable under the random oracle model based on the difficulty assumption of DLP on elliptic curves, meaning that an attacker cannot forge a legal identity message or signature. The signer's private key $SK_i = (x_i, D_i)$ is defined by both the secret value x_i and the partial private key D_i, where the secret value is kept secretly by the signer, and the partial private key D_i is only known to the TAC and the signer. By confirming that the signature in the broadcast message satisfies equations (3) and (4) with the signer's public key, it is possible to ensure that the signer sends the broadcast message and verify that CL-LAP has non-repudiation.

4) MESSAGE INTEGRITY

Each broadcast message sent by a sensing node is signed using a one-way hash function. According to the characteristics of the one-way hash function, different hash values must correspond to separate inputs for the same hash function. Therefore, the resulting hash value and signature will change if the message is altered. Upon receiving the message, the receiver verifies the signature to determine whether the message has been changed. Therefore, with CL-LAP, the receiver must receive the message without tampering, indicating that CL-LAP ensures the message's integrity.

C. SECURITY ANALYSIS

1) COUNTERFEIT ATTACKS

Each broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ sent by a sensing node needs to be accompanied by a signature $\sigma_i = (K_i, S_i)$. According to Theorem 1, the probability that an adversary (attacker) wants to impersonate a valid sensing node in the sensing network to generate a legitimate signature is negligible. An attacker cannot produce a valid signature that satisfies equations (3) and (4) to send a forged broadcast message to other authorized sensing nodes. Therefore, CL-LAP can resist counterfeit attacks.

2) FORGERY ATTACKS

A sensing node can only register its identity through TAC when it joints the sensing network. Every broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$ sent by a sensing node must be accompanied by a signature $\sigma_i = (K_i, S_i)$. Based on Theorem 1, the probability that an attacker will attempt to forge a legitimate identity message or signature is negligible. An attacker cannot forge a legitimate identity message or generate a signature meeting equations (3) and (4) to send a forged message to other legitimate sensing nodes. Therefore, CL-LAP is resistant to forgery attacks.

3) INFORMATION FALSIFICATION

In CL-LAP, each message M_i delivered by a sensing node is accompanied by a signature σ_i, and the broadcast message is sent in the format $\{ID_i, M_i, \sigma_i, T_i\}$. If an attacker modifies the broadcast message $\{ID_i, M_i, \sigma_i, T_i\}$, the signature σ_i will change correspondingly. On the one hand, the receiver gets the message and validates whether the signature σ_i in the broadcast message is legitimate by equations (3) and (4). On the other hand, Theorem 1 demonstrates that the signature σ_i is existentially unforgeable. In conclusion, CL-LAP is resistant to message tampering.

4) REPLAY ATTACKS

The lightweight authentication protocol CL-LAP proposed in this section eliminates the replay attack by appending a timestamp T_i to the message m_i. When the receiver receives the message, the freshness of the message is determined by calculating whether $T_j - T_i \leq \Delta T$ holds. T_i is the time the signer sends the message, T_j is the time the receiver gets the

message, and ΔT is the maximum time interval the system will accept to achieve resistance to replay attacks.

VI. PERFORMANCE ANALYSIS

This section simulates the performance of CL-LAP in terms of computation and communication costs in conjunction with the response requirements of emergency logistics systems. In addition, the performance is compared to existing authentication protocols of the same type. The scheme's lightness is mainly reflected in the lower computation cost, while its efficiency is reflected primarily in the lower communication cost.

The simulation of the authentication protocol is implemented on a computer with an Intel CORE i5 (2.3 GHz) processor, a 64-bit Win10 operating system, and Visual C 6.0 with the Miracle emulation library. The elliptic curve based on bilinear mapping $e : G_1 \times G_1 \rightarrow G_T$ in the authentication protocol is implemented using the additive cyclic group G_1 on the supersingular elliptic curve $E_1 : y^2 \equiv x^3 + x \,(\mathrm{mod} q)$ with embedding degree two in Miracle library, where q is a prime number of 160 bits and the generator P_1 of the cyclic group G_1 is a prime number of 512 bits. The elliptic curve without bilinear pairings is implemented with the additive cyclic group G on the supersingular elliptic curve $E_2 : y^2 \equiv x^3 + ax + b \,(\mathrm{mod} q)$ with embedding degree two. This is done with the Miracle library, where $a, b \in Z_q^*$, P is the generator of the cyclic group G of order q, and q is a prime number of 160 bits, as shown in Table 5. In the Miracle library, the elements of the cyclic group G on the elliptic curve are 32 bytes. Compared to this, the elements of the cyclic group G_1 on the elliptic curve are 64 bytes after the bilinear pairings.

A. COMPUTATION COST

CL-LAP is a lightweight authentication scheme for the perception layer of IoT-based emergency logistics networks, which reduces computational complexity. This certificateless digital signature scheme does not utilize bilinear pairings and reduces the high computation cost. We compare the computation cost of the proposed CL-LAP with the performance of the latest lightweight certificateless authentication protocols [31], [43], [44], [45]. The computation cost is separated into three categories for comparative purposes, signature generation cost, single message authentication cost, and batch message authentication cost. Table 5 depicts the ECC operations involved in the authentication process and the time required for their execution.

The generation of sensing node signature in CL-LAP consists of two scalar multiplication operations on the cyclic group G, two dot-add operations, and two Hash operations. The computation cost of generating a single signature is $2T_{mul-G} + 2T_{plus-G} + 2T_h$ or 0.8878 ms. Verifying a single signature contains two scalar multiplication operations on the cyclic group G, two dot-add operations, and three hash operations. Therefore, the computation cost for individual signature verification is $2T_{mul-G} + 3T_{plus-G} + 3T_h$ or 0.8897 ms,

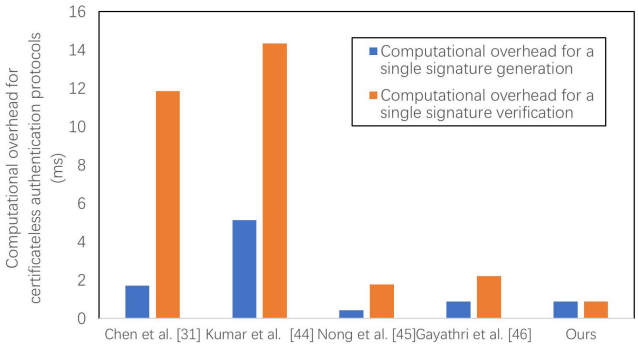

FIGURE 4. Computation cost comparison of certificateless authentication protocols.

and the computation cost for individual signature generation and signature verification is $4T_{mul-G} + 5T_{plus-G} + 5T_h$ or 1.7775 ms. The batch verification of n signatures consists of $2n + 2$ scalar multiplication operations on the cyclic group G, $2n + 1$ dot-add operations on the cyclic group G, and $3n$ Hash operations. The computation cost of bulk signature verification is $(2n + 2)\, T_{mul-G} + (2n + 1)\, T_{plus-G} + (3n)\, T_h$ or 0.4477n +0.4456 ms.

Table 5 compares the theoretical and practical simulation computation cost in researches [31], [43], [44], [45] with the proposed lightweight authentication protocol CL-LAP in a clear way. The authentication protocols in the covered research are ECC-based certificateless authentication protocols applied to IoT. Researches [31] and [44] is a certificateless authentication protocol based on bilinear pairings, and researches [43], [45] and CL-LAP are certificateless authentication protocols without bilinear pairings. In the signature generation phase, the efficiency of CL-LAP is 82.7% higher than the authentication protocol proposed in [44]. Similarly, it can be computed that CL-LAP is 48.1% and 21.4% more efficient than the authentication protocols proposed in researches [31] and [45] during the signature creation phase. The efficiency of CL-LAP in the signature verification phase is 92.5%, 93.8%, 49.8%, and 59.8% higher than that of the authentication protocols proposed in researches [31], [43], [44], [45], respectively. The CL-LAP signature generation phase and the signature verification phase are 86.9%, 90.9%, 19.8%, and 42.8% more efficient than the authentication protocols proposed in researches [31], [43], [44], [45], respectively. In addition, although the computation cost of the authentication protocol proposed in [43] in the signature generation phase is smaller than that of CL-LAP, the computation cost of signature verification is 49.8% higher than that of CL-LAP. The total computation cost obtained by adding signature generation and signature verification is 19.8% higher than that of CL-LAP.

Figure 4 compares the computational cost for a single signature generation and single signature verification in a CL-PKC-based authentication protocol. It is the same as the conclusion drawn from the data analysis above. Figure 4 shows that less computational cost is needed to generate a single signature in this paper's lightweight authentication

TABLE 2. Two types of elliptic curves involved in authentication protocols.

The elliptic curve equation	Bilinear mapping	Cyclic group order	Generating element order	Length of elements in cyclic group
$E_1 : y^2 \equiv x^3 + x \,(\mathrm{mod} q)$	$e : G_1 \times G_1 \rightarrow G_T$	160 bits	512 bits	1024 bits
$E_2 : y^2 \equiv x^3 + ax + b \,(\mathrm{mod} q)$	F_q	/	160 bits	160 bits

TABLE 3. Actual computation cost of different operations in ECC.

Operations involved	Running time (ms)
Bilinear pairs:$e\,(P, Q)$, where $P, Q \in G_1$.	$T_{bp} = 4.2110$
Scalar multiplication operation on G_1:xP, where $x \in Z_q^*, P \in G_1$.	$T_{mul-G_1} = 1.7090$
Point addition operation on G_1:$P + Q$, where $P, Q \in G_1$.	$T_{plus-G_1} = 0.0071$
Scalar multiplication operation on G:xP, where $x \in Z_q^*, P \in G$.	$T_{mul-G} = 0.4420$
Point addition operation on G:$P + Q$, where $P, Q \in G$.	$T_{plus-G} = 0.0018$
Hash operations	$T_h = 0.0001$
MapToPoint Hash Operation	$T_{mtph} = 4.4060$

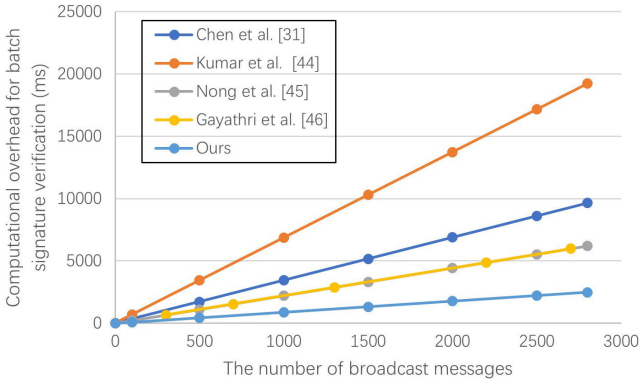

FIGURE 5. Comparing computation costs of batch signature verification in CL-PKC-based authentication protocols.

protocol than schemes in Chen et al. [31], Kumar et al. [44], and Gayathri et al. [45]. The computation cost for single signature verification is much lower than the authentication protocols proposed in [31], [43], [44], and [45].

Figure 5 compares the computation cost for n broadcast messages' signatures to be verified in one-time batch signature verification using the CL-PKC authentication protocols. The computation cost for batch signature verification of CL-LAP authentication protocol is much lower than authentication protocols proposed in [31], [43], [44], and [45]. Moreover, the computation cost for batch signature verification of CL-LAP will also differ significantly from that needed for other authentication protocols as the number of broadcast messages rapidly rises.

B. COMMUNICATION COST

Due to the fading and interference of wireless channels, for sensing nodes with limited transmit power, lower communication costs can improve the correct reception of a single message, shorten the authentication time and improve the authentication efficiency at the same level of hardware signal processing. In the configuration specification of emergency logistics storage facilities and equipment established

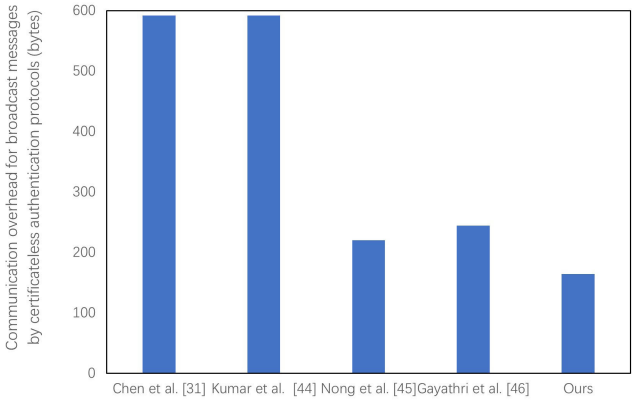

FIGURE 6. Comparison of the communication cost for sending a broadcast message based on CL-PKC authentication protocols.

in China [46], the A-level emergency response time should be within thirty minutes, and the capacity of comprehensive processing emergency materials for sorting, packaging, and marking should be 60 m^3/h. The decreased communication cost can effectively reduce the response time of emergency logistics and improve the operation efficiency to respond to emergencies effectively.

The communication cost generated by the partial private key, public key, signature, and timestamp is mainly considered. Assume that the bit length of the hash output is 20 bytes, the timestamp T_i is 4 bytes, the length of each element in the cyclic group G_1 is 128 bytes, and the corresponding element in Z_q^* is 40 bytes. Each element in the cyclic group G has a length of 40 bytes, and the corresponding element in Z_q^* is 20 bytes.

This paper proposes a lightweight authentication protocol CL-LAP with partial private key $D_i \in Z_q^*$, public key $X_i \in G$, and a broadcast message sent by the sensing node as $\{ID_i, M_i, \sigma_i, T_i\}$. The signatures $\sigma_i = (K_i, S_i)$, $K_i \in G$, $S_i \in Z_q^*$, $ID_i \in G$. Therefore, the communication cost of a sensing node sending one broadcast message is 164 bytes, and the communication cost of sending n broadcast messages is $164n$ bytes. The comparison results of the communication cost of different authentication protocols are shown in Table 5.

From Table 5, it can be visualized that the communication cost required to send a broadcast message by the CL-LAP protocol is significantly smaller than the communication cost required by the authentication protocol proposed in the researches [31], [43], [44], [45].

Figure 6 compares the communication cost of the CL-PKC-based authentication protocol to send a broadcast message. The conclusion is the same as the data analysis in Table 5. It can be seen intuitively from Figure 6 that the communication cost to send a broadcast message by CL-LAP is significantly less than that in [31], [43], [44], and [45].

TABLE 4. Comparison of the computation cost of certificateless based authentication protocols.

Authentication protocol name	Signature generation cost (ms)	Single signature verification cost (ms)	Batch signature verification cost (ms)
Chen et al. [31]	$T_{mul-G_1} + 2T_h = 1.7092$	$2T_{bp} + 2T_{mul-G_1} + 2T_{plus-G_1} + 3T_h = 11.8545$	$2T_{bp} + (2n+1)\,T_{mul-G_1} + (4n-2)\,T_{plus-G_1} + (3n)\,T_h = 3.4467n + 10.1168$
Kumar et al. [44]	$3T_{mul-G_1} + 2T_{mul-G_1} + 2T_h = 5.1414$	$3T_{bp} + T_{mul-G_1} + T_{plus-G_1} + 3T_h = 14.3494$	$3T_{bp} + (4n)\,T_{mul-G_1} + (4n-3)\,T_{plus-G_1} + (2n)\,T_h = 6.8646n + 12.6117$
Nong et al. [43]	$T_{mul-G} + 2T_h = 0.4422$	$4T_{mul-G} + 3T_{plus-G} + 3T_h = 1.7737$	$(5n)\,T_{mul-G} + (3n)\,T_{plus-G} + (3n+2)\,T_h = 2.2157n + 0.0002$
Gayathri et al. [45]	$2T_{mul-G} + 3T_{plus-G} + 3T_h = 0.8897$	$5T_{mul-G} + 3T_{plus-G} + 5T_h = 2.2157$	$(5n+3)\,T_{mul-G} + (3n)\,T_{plus-G} + (2n+3)\,T_h = 2.2156n + 1.3263$
CL-LAP	$2T_{mul-G} + 2T_{plus-G} + 2T_h = 0.8878$	$2T_{mul-G} + 3T_{plus-G} + 3T_h = 0.8897$	$(2n+2)\,T_{mul-G} + (2n+1)\,T_{plus-G} + (3n)\,T_h = 0.8879n + 0.8858$

TABLE 5. Comparison of communication cost of different authentication protocols.

Authentication protocol name	Send a broadcast message (bytes)	Send n broadcast messages (bytes)
Chen et al. [31]	592	592n
Kumar et al. [44]	592	592n
Nong et al. [43]	220	220n
Gayathri et al. [45]	244	244n
CL-LAP	164	164n

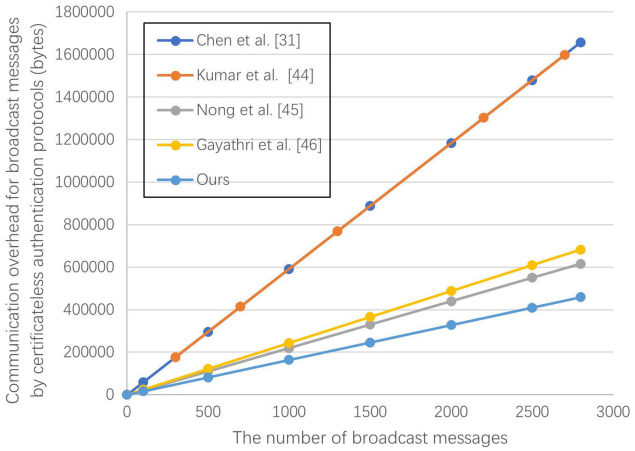

FIGURE 7. Comparison of communication cost for sending *n* broadcast messages based on CL-PKC authentication protocols.

The communication cost to send a broadcast message by the authentication protocols based on CL-PKC is depicted in Figure 7. The communication cost to send broadcast messages by CL-LAP and the authentication protocols proposed in [31], [43], [44], and [45] will gradually diverge as the number of broadcast messages rises.

VII. CONCLUSION

There has been a recent uptick in the development of emergency logistics based on the IoT. In this paper, we assess the necessity for lightweight authentication in the IoT-based emergency logistics networks and give application scenarios. Then, we propose a lightweight certificateless authentication protocol for the perception layer that provides quick authentication between sensing nodes and batch authentication. Security and performance analyses show that the proposed protocol can effectively meet data security requirements in emergency logistics systems and improve the authentication efficiency between nodes while providing the same security. In addition, our protocol can be applied to authentication in IoT-based emergency logistics networks. Future work may achieve overall security protection for the emergency logistics system by introducing the security design of the network layer and application layer to improve the overall security of the emergency logistics system.

REFERENCES

[1] Y. Wang, S. Peng, and M. Xu, "Emergency logistics network design based on space–time resource configuration," *Knowl.-Based Syst.*, vol. 223, Jul. 2021, Art. no. 107041.

[2] B. Balcik and B. M. Beamon, "Facility location in humanitarian relief," *Int. J. Logistics Res. Appl.*, vol. 11, no. 2, pp. 101–121, Apr. 2008.

[3] A. M. Caunhye, X. Nie, and S. Pokharel, "Optimization models in emergency logistics: A literature review," *Socio-Economic Planning Sci.*, vol. 46, no. 1, pp. 4–13, Mar. 2012.

[4] H. Golpira, S. A. R. Khan, and S. Safaeipour, "A review of logistics Internet-of-Things: Current trends and scope for future research," *J. Ind. Inf. Integr.*, vol. 22, Jun. 2021, Art. no. 100194.

[5] H. Yang, L. Yang, and S.-H. Yang, "Hybrid ZigBee RFID sensor network for humanitarian logistics centre management," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 938–948, May 2011.

[6] M. Tajima, "Strategic value of RFID in supply chain management," *J. Purchasing Supply Manag.*, vol. 13, no. 4, pp. 261–273, Dec. 2007.

[7] L. Yang, S. H. Yang, and L. Plotnick, "How the Internet of Things technology enhances emergency response operations," *Technol. Forecasting Social Change*, vol. 80, no. 9, pp. 1854–1867, Nov. 2013.

[8] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the Internet of Things," *J. Cyber Secur. Mobility*, vol. 1, no. 4, pp. 309–348, Oct. 2014.

[9] H.-Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 337–340, Oct./Dec. 2007.

[10] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-Peer Netw. Appl.*, vol. 9, no. 5, pp. 824–840, 2016.

[11] S. Anandhi, R. Anitha, and V. Sureshkumar, "IoT enabled RFID authentication and secure object tracking system for smart logistics," *Wireless Pers. Commun.*, vol. 104, pp. 543–560, Oct. 2018.

[12] C.-M. Chen, X. Li, S. Liu, M.-E. Wu, and S. Kumari, "Enhanced authentication protocol for the Internet of Things environment," *Secur. Commun. Netw.*, vol. 2022, pp. 1–13, Mar. 2022.

[13] L. Kou, Y. Shi, L. Zhang, D. Liu, and Q. Yang, "A lightweight three-factor user authentication protocol for the information perception of IoT," *Comput., Mater. Continua*, vol. 58, no. 2, pp. 545–565, 2019.

[14] C.-M. Chen, Z. Chen, S. Kumari, and M.-C. Lin, "LAP-IoHT: A lightweight authentication protocol for the Internet of Health Things," *Sensors*, vol. 22, no. 14, p. 5401, Jul. 2022.

[15] R. Pothumarti, K. Jain, and P. Krishnan, "A lightweight authentication scheme for 5G mobile communications: A dynamic key approach," *J. Ambient Intell. Humanized Comput.*, vol. 12, pp. 1–19, Jan. 2021.

[16] S. Sankaran, "Lightweight security framework for IoTs using identity based cryptography," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2016, pp. 880–886.

[17] S. A. Çamtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 15, no. 2, pp. 346–358, Apr. 2007.
[18] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *Proc. 37th Annu. IEEE Conf. Local Comput. Netw.*, Oct. 2012, pp. 956–963.
[19] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for Industry 4.0," *Sci. China Inf. Sci.*, vol. 65, no. 1, pp. 1–15, Jan. 2022.
[20] Q. Wang, D. Wang, C. Cheng, and D. He, "Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 193–208, Jan. 2023.
[21] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 1338–1351, Mar./Apr. 2022.
[22] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1984, pp. 47–53.
[23] A. Joux, "A one round protocol for tripartite Diffie–Hellman," in *Proc. Int. Algorithmic Number Theory Symp.* Cham, Switzerland: Springer, 2000, pp. 385–393.
[24] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, Jul. 2015.
[25] K. G. Paterson, "ID-based signatures from pairingson elliptic curves," *Electron. Lett.*, vol. 38, no. 18, p. 1025, 2002.
[26] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proc. Int. Workshop Sel. Areas Cryptogr.* Cham, Switzerland: Springer, 2002, pp. 310–324.
[27] H. Al Housani, J. Baek, and C. Y. Yeun, "Survey on certificateless public key cryptography," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, 2011, pp. 53–58.
[28] P. Nayak and G. Swapna, "Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100641.
[29] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Cham, Switzerland: Springer, 2003, pp. 452–473.
[30] J. Liu, H. Cao, Q. Li, F. Cai, X. Du, and M. Guizani, "A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1321–1330, Apr. 2019.
[31] Y. Chen, W. Xu, L. Peng, and H. Zhang, "Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT," *IEEE Access*, vol. 7, pp. 15210–15221, 2019.
[32] J. Li and Y. Zhang, "Cryptanalysis and improvement of batch verification certificateless signature scheme for VANETs," *Wireless Pers. Commun.*, vol. 111, no. 2, pp. 1255–1269, Mar. 2020.
[33] D. He, J. Chen, and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings," *Int. J. Commun. Syst.*, vol. 25, no. 11, pp. 1432–1442, Nov. 2012.
[34] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings," *Int. J. Commun. Syst.*, vol. 27, no. 7, pp. 1083–1090, 2014.
[35] K.-H. Yeh, C. Su, K.-K. R. Choo, and W. Chiu, "A novel certificateless signature scheme for smart objects in the Internet-of-Things," *Sensors*, vol. 17, no. 5, p. 1001, 2017.
[36] W. Baoyi, L. Li, Z. Shaomin, and H. Jing, "Research on privacy protection scheme based on certificateless aggregation signcryption in AMI," *Internet Things (IoT) Eng. Appl.*, vol. 4, no. 1, pp. 7–12, 2019.
[37] M. Cui, D. Han, and J. Wang, "An efficient and safe road condition monitoring authentication scheme based on fog computing," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9076–9084, Oct. 2019.
[38] B. Zhang, "A lightweight data aggregation protocol with privacy-preserving for healthcare wireless sensor networks," *IEEE Syst. J.*, vol. 15, no. 2, pp. 1705–1716, Jun. 2021.
[39] X. Jia, D. He, Q. Liu, and K. K. R. Choo, "An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment," *Ad Hoc Netw.*, vol. 71, pp. 78–87, Mar. 2018.
[40] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018.
[41] H. Xiong, Q. Mei, and Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," *IEEE Syst. J.*, vol. 14, no. 1, pp. 310–320, Mar. 2020.
[42] C.-M. Chen, S. Liu, S. A. Chaudhry, Y.-C. Chen, and M. A. Khan, "A lightweight and robust user authentication protocol with user anonymity for IoT-based healthcare," *Comput. Model. Eng. Sci.*, vol. 131, no. 1, pp. 307–329, 2022.
[43] Q. Nong, "Practical secure certificateless cryptographic protocol with batch verification for intelligent robot authentication," in *Proc. Int. Conf. Mechatronics Intell. Robot.* Cham, Switzerland: Springer, 2018, pp. 483–488.
[44] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustain. Comput., Inform. Syst.*, vol. 18, pp. 80–89, Jun. 2018.
[45] N. B. Gayathri, G. Thumbur, P. V. Reddy, and Z. U. R. Muhammad, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31808–31819, 2018.
[46] *Disposition Specification of Emergency Logistics Facilities and Equipment*, China Federation of Logistics & Purchasing, Beijing, China, Jul. 2018.

JIANXI YANG received the Ph.D. degree from the Beijing University of Technology, Beijing, China, in 2006. He is currently an Associate Professor with the Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute. He has published more than 30 articles and more than ten inventions. His research interests include future network security, communication anti-jamming, and electronic countermeasures.

JINPO FAN received the B.S. degree in communication engineering and the M.S. degree in electronic and communication engineering from the Beijing Electronic Science and Technology Institute, Beijing, China, in 2015 and 2020, respectively. He is currently pursuing the Ph.D. degree in information and communication engineering with the Beijing University of Posts and Telecommunications, Beijing. His research interests include machine learning and signal recognition, cryptography, and wireless sensor network security.

XIAOCHEN ZHU received the B.Eng. degree in electronic information engineering from the Hebei University of Technology, in 2018, and the M.Eng. degree in army command studies from Xidian University, in 2021. Her research interests include cryptography and the IoT security.