Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 9436120, 14 pages
https://doi.org/10.1155/2018/9436120

Research Article

LIP-PA: A Logistics Information Privacy Protection Scheme with Position and Attribute-Based Access Control on Mobile Devices

Qi Gao, Junwei Zhang, Jianfeng Ma, Chao Yang, Jingjing Guo, and Yinbin Miao

School of Cyber Engineering, Xidian University, Xi'an 710071, China

Correspondence should be addressed to Junwei Zhang; jwzhang@xidian.edu.cn

Received 13 April 2018; Accepted 27 June 2018; Published 15 July 2018

Academic Editor: Ding Wang

With the fast development of Logistics Internet of Things and smart devices, the security of express information processed by mobile devices in Logistics Internet of Things has attracted much attention. However, the existing secure express schemes only focus on privacy protection of personal information but do not consider the security of the logistics information against couriers with malicious mobile devices. For example, a privacy-preserving delivery path should be required in order to prevent the privacy leakage in the express delivery procedure. Therefore, besides the security of personal information, the privacy protection of logistics information and authentication of mobile devices used in express company are important to security in Logistics Internet of Things. In this paper, we propose a secure logistics information scheme LIP-PA to provide privacy protection of both personal information and logistics information. First, we define the basic requirements of Logistics Internet of Things. Then, using attribute-based encryption and position-based key exchange, we propose a logistics information privacy protection scheme with position and attribute-based access control for mobile devices. The analysis results show that our scheme satisfies the defined requirements. Finally, the performance of our scheme is evaluated and the experiment results show that our scheme is efficient and feasible for mobile devices in real parcel delivery scenario.

1. Introduction

With the rapid development of Internet of Things technology [1] and continuous optimization of the logistics operation process, the Logistics Internet of Things (LIoT) has become an indispensable pattern for modern logistics industry. Based on many network communication technologies, such as RFID [2], QR code [3], NFC [4], and D2D [5] technology, LIoT has adopted lots of mobile devices to deal with the express business.

At the same time, the fast development of modern logistics industry has also brought a lot of security issues, especially the security of mobile devices in LIoT [6]. Without security protection, the customer's private information is expressly visible on mobile devices, so that any adversary can see the private information. Besides, the adversary can easily track the parcel according to the logistics information in mobile devices and even analyze the customer's information such as personal hobbies, family members, and economic conditions [7, 8]. In addition, express delivery between different express stations can lead to data leakage and the malicious courier can analyze the flow of express station [9]. The privacy protection of express information has attracted widespread attention.

However, traditional privacy protection schemes of express information all focus on customer's personal information [10, 11], and they are unable to achieve a secure management of internal logistics staff. It is obvious that the couriers, who actually move parcels between sender and receiver, can obtain lots of express information including personal information and logistics information. Therefore, how to guarantee the express information privacy and securely manage the large-scale couriers based on mobile devices in LIoT is a focus.

As far as we know, the most popular authentication methods for couriers on mobile devices can be classified as public key authentication [12–14], password authentication [15, 16], and multifactors authentication [17–19]. However, these methods are not suitable for management of large-scale couriers on mobile devices. Group-based key exchange can

realize efficient group-based management [20, 21], but group-based methods could not provide fine-grained access control on large-scale mobile devices. As a result, attribute-based encryption with fine-grained access control can be applied to the security solutions in LIoT.

Related Work. For privacy protection in LIoT, Wei et al. [22] proposed a K-anonymous model to take the anonymous process of logistics information. This method randomly breaks the relationship between attribute values in the record to anonymous data. However, the order still retains the receiver's name and phone number, and K-anonymity will cause some loss of information. Zhang et al. [23] proposed a logistics information system privacy protection system, which can solve the contradiction between privacy protection and logistics business process by the segment encryption design. However, the disadvantage of this solution is that the two-dimensional code needs to be constantly updated at each logistics station; also the processes of encryption and decryption are repeated. Qi et al. [24] proposed a new express management system based on encrypted QR code. The real-time logistics information of goods is automatically updated through GPRS or Wi-Fi. The APP provides an optimal delivery route for couriers by employing the improved genetic algorithm. Obviously, the above works lack access control and authentication for internal logistics staff. They cannot ensure the privacy protection of logistics information.

Li et al. [25] designed a privacy-preserving express delivery system, i.e., PriExpress. This system introduces the ciphertext-policy attribute-based encryption (CP-ABE) method into the privacy protection in logistics information system (LIS). With CP-ABE [26], the parcel sender specifies an attribute-based access policy for enforcing fine-grained access control to his delivery order which contains sensitive personal information. However, the PriExpress does not separate personal information from logistics information. Customers in this scheme need abundant computation capability and remain online when they deal with the express delivery procedure.

In summary, all above schemes lack a position and attribute-based access control for both logistics information and personal information.

Privacy Protection in LIoT. Different from IoT, the security requirements of LIoT have the following characteristics.

First, privacy-preserving of logistics information should be guaranteed in LIoT. For complete logistics information, it is necessary to keep confidentiality for untrusted express staff. In traditional privacy protection schemes, logistics information is not separated from personal information. Some malicious couriers may sell the logistics information to criminals who can analyze the flow of express station according to the delivery path. Thus, privacy-preserving of logistics information is one of the required properties in LIoT.

Second, couriers who actually deliver parcels are very important to the guarantee of the security of express delivery process. But there are so large-scale couriers that it is difficult to manage them. On one hand, for some malicious couriers, they may sell privacy information to criminals. On the other hand, once the hackers get the courier's master secret, they can impersonate a valid courier to obtain the express information illegally. Therefore, it is necessary to guarantee the attribute-based access control for privacy information and ensure that the courier with specific attributes can obtain privacy information.

Due to the high turnover of couriers, it is significant to make sure that only the couriers that work online at delivery station can obtain the order information. So position-based access control is also one of the required properties of LIoT. Besides, there may be some couriers that are curious about the information which they cannot possess, so they maybe collude together and share their own attributes to obtain much more information. Therefore, it is necessary to implement the authentication of couriers. Specifically, the security requirements on couriers should guarantee anticollusion attack to attribute-based access control and anticollusion attack to position-based access control.

Third, customers always are remote and offline. Therefore, it is hard to achieve authentication of customers online [27]. A dishonest sender may deny that he (or she) has sent some harmful parcel to someone. Besides, a dishonest receiver may personate a legal receiver to take away the parcel which does not belong to himself (or herself). Therefore, it is necessary to achieve the verifiability of receiver and verifiability of parcel [28]. Last but not least, it is necessary to keep customer's unlinkability for administrator and others.

Fourth, in the real delivery scene, customers always have irregular operations such as leaving wrong addresses and phone numbers, which leads to the fact that it is difficult to manage or recover parcel. Therefore, the security requirements of LIoT should guarantee the undeniability of sender and receiver. Specifically, a sender cannot deny a parcel sent by himself (or herself), while a receiver cannot deny a parcel received by himself (or herself).

Our Contributions. Although the most popular authentication methods on mobile devices are not suitable for management of large-scale couriers [29, 30], attribute-based encryption can achieve fine-grained access control, so we need to use the ABE technology to realize position and attribute-based access control of couriers based on mobile devices in LIoT. However, this study is very challenging with the following reasons. First, it is hard to realize both attribute-based encryption and location-based access control. Second, how to securely verify the validity of a courier's claimed position is also a problem [31].

This paper proposes a logistics information privacy protection scheme with position and attribute-based access control on mobile devices. First, in order to realize fine-grained access control of encrypted logistics information, we adopt ciphertext-policy attribute-based encryption (CP-ABE) [26], which encrypts segmented logistics information in different access policies. Different couriers can only decrypt different segments of the express order in accordance with their respective attributes. Second, we apply position-based key exchange [32], which uses the courier's physical position information as credential, to realize position-based access control on couriers. Third, we utilize public key encryption

to achieve the confidentiality of personal information. At the same time, we use digital signature to ensure the verifiability of parcel and the undeniability of customers [33].

Our contributions in this paper are fourfold.

(1) We classify the required properties of our scheme including attribute-based access control, position-based access control, privacy-preserving of logistics information, confidentiality of personal information, verifiability of receiver, verifiability of parcel, anticollusion attack to attribute-based access control, anticollusion attack to position-based access control, undeniability, and unlinkability.

(2) We propose a logistics information privacy protection scheme LIP-PA. In the scheme, logistics information is divided into segments and, respectively, encrypted; administrator can prebuild access tree which contains the position attribute.

(3) We theoretically analyze the security of LIP-PA. We show that LIP-PA satisfies the above required properties.

(4) We report experimental evaluations of our scheme. Our results show that LIP-PA is efficient and feasible for mobile devices in real parcel delivery scenario.

2. Preliminaries

In this paper, some basic cryptographic algorithms are necessary. First, we will use public key encryption to protect the personal information [34] in our scheme. Second, we also need digital signature [35, 36] to realize the undeniability of customers. Third, hash functions [37] are used in generation of order information. Besides the above algorithms, ciphertext-policy attribute-based encryption and position-based key exchange are core algorithms in our scheme.

2.1. Ciphertext-Policy Attribute-Based Encryption. A ciphertext-policy attribute-based encryption scheme [26] consists of four fundamental algorithms: Setup, Encrypt, KeyGen, and Decrypt.

Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encrypt(PK, M, T): The encryption algorithm takes as input the public parameters PK, a message M, and an access tree T. The algorithm will encrypt M and produce a ciphertext CT such that only a user with a set of attributes that satisfies the access tree T will be able to decrypt CT.

Key Generation(MK, S): The key generation algorithm takes as input the master key MK and a set of attributes S. It outputs the private key SK, which is used by users to decrypt ciphertext.

Decrypt(PK, CT, SK): The decryption algorithm takes as input the public parameters PK, a ciphertext CT, and a private key SK. If the set S satisfies the access tree T then the algorithm will return a message M.

2.2. Position-Based Key Exchange. Based on the bounded storage model (BSM) and BSM pseudorandom generators (PRG), Chandran et al. construct the provable secure position-based key exchange (PBKE) protocol against colluding adversaries [32]. BSM assumes that any party including adversary can only store a part of information with high min-entropy. BSM PRG: $\{0,1\}^n \times \{0,1\}^d \longrightarrow \{0,1\}^m$ is an ε-secure BSM PRG for storage rate β and min-entropy rate α if and only if, for every αn-source X on $\{0,1\}^n$ and for every function A: $\{0,1\}^n \longrightarrow \{0,1\}^{\beta n}$, the random variable $(PRG(X,K), A(X), K)$ is ε-close to $(U_m, A(X), K)$, where $K \xleftarrow{R} \{0,1\}^d$. Different from traditional key exchange, PBKE applies the user's physical position as the unique credential to negotiate a shared key K between verifiers and a prover at a legal position P. At the end of PBKE, the shared key K and a random number are indistinguishable from the view of the colluding adversaries.

However, the previous position-based key exchange protocol is not suitable for realizing the position-based access control in ABE. Thus, an improved position-based key exchange protocol is proposed as shown in Algorithm 4.

3. Problem Formulations

3.1. System Model. As shown in Figure 1, the system model consists of following entities: customers including a sender and a receiver, couriers, and administrator with attribute authority and landmarks.

When a logistic transit process begins, as shown in Figure 1, a sender first generates an order and submits the order information to administrator. The order information consists of address information, i.e., customers' address information, and customers' personal information including the names and telephone numbers. If the administrator accepts this order, the administrator will generate a logistics information which is a delivery plan including some independent delivery steps for couriers. During the parcel delivery, every courier in one delivery step only distributes the express from one station to another station. The parcel finally arrives at the last delivery station and the receiver takes away the parcel after authenticated. More specifically, we have the following.

Customers. Customers can be divided into a sender and a receiver of parcel. They aim to absolutely protect personal information against administrator and couriers and obtain a privacy-preserving protection service for logistics information from administrator; i.e., any courier managed by administrator can only know a part of logistics information but not all the logistics information.

Administrator. Administrator, as a general management institution of logistics company, provides trusted express service for customers and completes the privacy protection of logistics information against couriers. Specifically, the administrator first employs an attribute authority (AA) to realize attribute-based management for couriers. Then, the administrator configures all the access trees for all couriers involved by the target order according to the delivery plan and encrypts the segmented logistics information with different attribute policies. If a courier delivers a parcel in some one delivery step, the courier can only decrypt the required

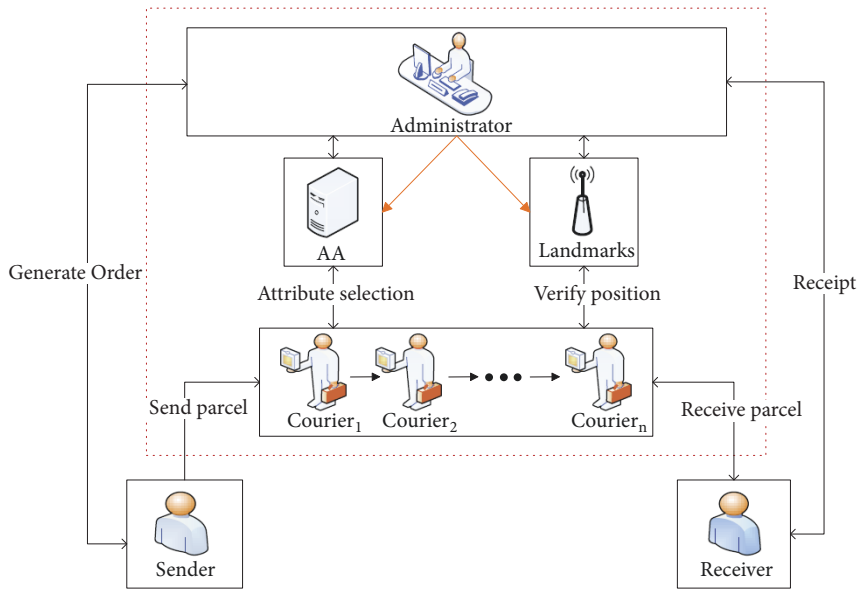

Figure 1: The system model.

information segment (i.e., the next station information of the current delivery step). At the same time, the administrator employs some landmarks to verify the location of the courier in order to guarantee that the courier from a legal station in a valid time slot can get the required information segment to perform the delivery task.

Couriers. Couriers are employed by express company. They are the entities that actually deliver parcels between a sender and a receiver. A courier is only responsible for delivering the parcels from one station to another station in a delivery step. The courier just needs to obtain the required information segment (e.g., the next station) with position and attribute-based access control. In this way, a parcel delivery process consists of multiple delivery steps performed by multiple couriers.

3.2. Threat Model

Administrator. Administrator, as a manager of an express company, is honest but curious. On one hand, the administrator is responsible for privacy protection on customers' address information and logistics information against couriers. For such a service, the administrator is in charge of securely encrypting the logistics information and building suitable access policy to couriers. AA and landmarks are employed by administrator to guarantee position and attribute-based access control. On the other hand, in order to obtain more potential benefits, the administrator is also very interested in customers' personal information, such as name and telephone number.

Customers. A customer of the parcel (i.e., sender or receiver) may have the following dishonest behaviors. First, a dishonest sender may deny that he (or she) has sent some harmful parcels to someone. Second, a dishonest receiver may personate a legal receiver to take away the parcel which does not belong to himself (or herself).

Couriers. Couriers, as the entities that actually deliver parcels, are very important for the guarantee of the security of the express delivery process. However, in order to obtain illegal individual benefit, some couriers may have four dishonest behaviors: First, couriers are curious about the customers' address and personal information; they may sell them to obtain economic benefit. Second, some colluding couriers may attempt to steal the logistics information even if they are not located at the valid delivery station at work time. Third, some couriers with different attributes may collude with others in order to decrypt the extra information which they could not know originally. Fourth, couriers may modify the order information in order to disturb the express delivery process, such as changing the valid receiver information into an illegal receiver.

3.3. Design Goals. According to the requirements and the adversary model, the proposed scheme should satisfy the following properties:

(1) Attribute-based access control (ABAC): Our scheme should achieve a fine-grained access control of encrypted logistics information based on the attributes of couriers. The required part of logistics information could only be decrypted by a valid courier whose attributes satisfy the access policy. Apart from this, there is no way to obtain the other parts of logistic information for valid couriers.

(2) Position-based access control (PBAC): Our scheme should ensure that a courier that is going to obtain the

Table 1: Comparison with related work.

	LIPPS	NEMS	PriExpress	Our scheme
ABAC	×	×	√	√
PBAC	×	×	×	√
PPLI	√	×	√	√
CPI	×	√	×	√
VR	√	√	√	√
VP	×	×	×	√
ACA-A	-	-	√	√
ACA-P	-	-	-	√
UD	×	×	×	√
UL	×	×	√	√

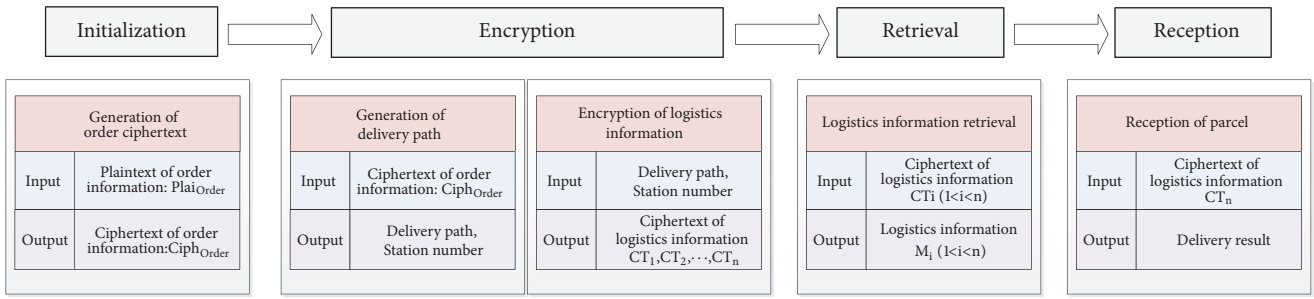

Figure 2: The LIP-PA framework.

required part of logistics information must be at a valid delivery station at the expected work time.

(3) Privacy-preserving of logistics information (PPLI): First and foremost, our scheme should guarantee confidentiality of logistics information. For logistics company, the whole delivery path should only be known by administrator, so a valid courier can only decrypt the partial logistics information which is necessary for the delivery process. The complete logistics information keeps privacy protection to all couriers.

(4) Confidentiality of personal information (CPI): Our scheme should ensure the confidentiality of personal information even to administrator. Customers' personal information contains sender's and receiver's names, phone numbers, etc. It is only visible among the sender and the receiver.

(5) Verifiability of receiver (VR): Our scheme should provide the verifiability of receiver. Only when the receiver of parcel is the expected one according to the order information, can receiver take away the parcel from the final courier.

(6) Verifiability of parcel (VP): A receiver in our scheme should ensure that the order information of the parcel is the correct and unforged during the express delivery process, and then he (or she) will receive this parcel.

(7) Anticollusion attack to attribute-based access control (ACA-A): Our scheme should ensure that the colluding couriers with different attributes cannot obtain the additional logistics information under the colluding attribute sets.

(8) Anticollusion attack to position-based access control (ACA-P). Our scheme should achieve that the colluding couriers that are not located at the valid station cannot obtain the logistics information according to the position-based access control policy.

(9) Undeniability (UD): A sender cannot deny a parcel sent by himself (or herself), while a receiver cannot deny a parcel received by himself (or herself).

(10) Unlinkability (UL): Although the same sender sends lots of parcels to a receiver, the administrator and others cannot distinguish whether the encrypted order information in the many delivery processes originates from the same sender.

3.4. Comparison with Related Work. In this section, we compare our scheme with the related schemes including LIPPS [23], NEMS [24], and PriExpress [25]. Table 1 shows the comparison results, where "√" means satisfied, "×" means dissatisfied, and "–" means uninvolved.

From the Table 1, we can see that both LIPPS and NEMS cannot provide ABAC. It is obvious that all the related schemes including LIPPS, NEMS, and PriExpress cannot guarantee PBAC, VP, and UD. Meanwhile PriExpress cannot provide totally CPI. Our scheme can satisfy all the properties in Table 1.

4. The Proposed Scheme

4.1. Overview of Scheme LIP-PA. The scheme LIP-PA consists of four phase: initialization, encryption, retrieval, and reception as shown in Figure 2.

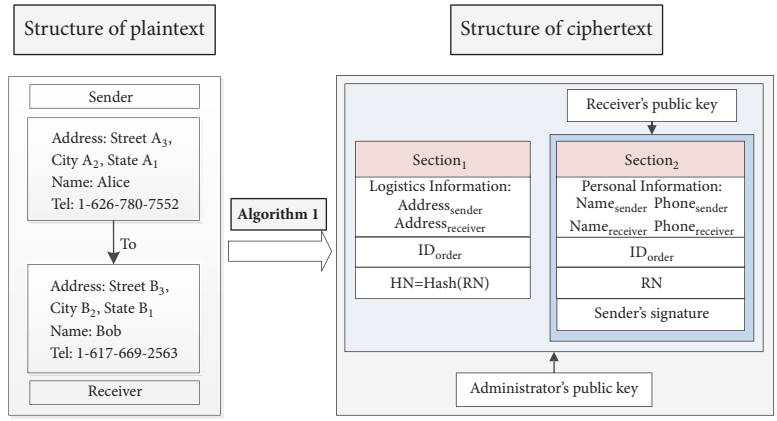

Figure 3: Initialization of order information.

Input: plaintext of order information $Plai_{Order}$
Output: ciphertext of order information $Ciph_{Order}$
1: generate random number ID_{Order}, RN
2: $HN \longleftarrow Hash(RN)$
3: $signature_{Sen} \longleftarrow E(PRI_{Sen}, [ID_{Order}||Plai_{Order}])$
4: $Section_1 \longleftarrow Add_{Sen}||Add_{Rec}||ID_{Order}||HN$
5: $Section_2 \longleftarrow Nam_{Sen}||Nam_{Rec}||Pho_{Sen}||Pho_{Rec}||ID_{Order}||RN||signature_{Sen}$
6: $Ciph_{Section_2} \longleftarrow E(PUB_{Rec}, [Section_2])$
7: $Ciph_{Order} \longleftarrow E(PUB_{Adm}, [Ciph_{Section_2}||Section_1])$
8: **return** $Ciph_{Order}$

Algorithm 1: Generation of order ciphertext.

In the initialization phase, a sender will generate an encrypted order and launch an order request to administrator. The encrypted order information consists of customers' address information and personal information like names, telephone numbers, etc.

Upon receiving the order request from sender, the administrator constructs logistics information based on the planned delivery path in the encryption phase. Then, the administrator formulates the position and attribute-based access control and encrypts different segments of logistics information with different access control policies.

In the retrieval phase, a courier located at a valid station at work time can run a position-based key exchange protocol to obtain a secret key about position attribute. Based on the position-based key, the courier who satisfies the desired attribute policy can retrieve required logistics information in order to transmit the parcel from one station to next station.

When the parcel arrives at last station, the courier will transmit the parcel to target receiver in the reception phase. In this phase, the courier should verify the authenticity of receiver. The receiver would also verify the correctness of order information on parcel. If both authentication of receiver and validity of parcel are verified, the parcel will be delivered to receiver successfully.

4.2. Initialization. We assume that sender, receiver, administrator, and courier must be registered and have a certified public/private key pair, respectively, before initialization.

In our scheme, order information can be divided into two types: logistics information and personal information. Logistics information including sender's address (Add_{Sen}) and receiver's address (Add_{Rec}) should be encrypted using public key of administrator to provide the property of secrecy against adversarial couriers. Personal information, such as sender's name (Nam_{Sen}), receiver's name (Nam_{Rec}), sender's phone number (Pho_{Sen}), and receiver's phone number (Pho_{Rec}), should be always secret during the express delivery process considering the confidentiality. Figure 3 illustrates the structure of encrypted order information sent from sender to administrator. Algorithm 1 shows the detailed generation process of order ciphertext, where $E()$ is the public key encryption algorithm, PRI_{user} means the user's private key, and PUB_{user} means the user's public key.

As we can see, the ciphertext mainly contains two sections: $Section_1$; $Section_2$. $Section_1$ contains logistics information and $Section_2$ contains personal information. Note that, in line 2 of Algorithm 1, a random number ID_{Order} is unique identity of parcel. In addition, the sender generates a random number RN in $Section_2$. At the same time, the

Input: ciphertext of order information $Ciph_{Order}$
Output: delivery path $Optimalpath$, station number $Num_{station}$
1: $D(PRI_{Adm}, [Ciph_{Order}]) \longrightarrow Ciph_{Section_2}||Section_1$
2: **if** $A_2 = B_2$ **then**
3: $Num_{station} = 3$
4: $A_3A_2B_3 \longrightarrow Optimalpath$
5: **else**
6: **if** $A_1 = B_1$ **then**
7: $Num_{station} = 5$
8: $A_3A_2A_1B_2B_3 \longrightarrow Optimalpath$
9: **else**
10: $Num_{station} = 6$
11: $A_3A_2A_1B_1B_2B_3 \longrightarrow Optimalpath$
12: **end if**
13: **end if**
14: **return** $Optimalpath$, $Num_{station}$

Algorithm 2: Generation of delivery path.

Input: $Optimalpath$, $Num_{station}$
Output: ciphertext of logistics information $(CT_1, CT_2, \ldots, CT_n)$
1: $n = Num_{station}$
2: **for** $i = 1; i \leq n; i++$ **do**
3: $Position_i \longleftarrow delivery\ station\ on\ Optimalpath[i]$
4: picks $K_{i6} \overset{R}{\leftarrow} \{0,1\}^m$
5: $\mathcal{S}_{iSpatial} \longleftarrow \{Position_i, T_i\}$
6: $attr(\mathcal{S}_{iSpatial}) \longleftarrow K_{i6}$
7: **end for**
8: **for** $i = 1; i \leq n-1; i++$ **do**
9: $M_i \longleftarrow Optimalpath[i]$
10: **end for**
11: $M_n \longleftarrow Ciph_{Section_2}||HN$
12: Setup $\longrightarrow (PK, MK)$
13: Key Generation$(PK, MK, \mathcal{S}) \longrightarrow (SK)$
14: **for** $j = 1; j \leq n; j++$ **do**
15: Encrypt $(PK, M_j, T_j) \longrightarrow (CT_j)$
16: **end for**
17: **return** $(CT_1, CT_2, \ldots, CT_n)$

Algorithm 3: Encryption of logistics information.

sender computes $HN = Hash(RN)$ in $Section_1$. In line 5 of Algorithm 1, the sender's digital signature is added to $Section_2$ for the verifiability of parcel. Finally, Algorithm 1 outputs the ciphertext of order information, which will be submitted to administrator.

4.3. Encryption. The encryption phase contains two steps which administrator needs to complete. First, the administrator runs the delivery path generation algorithm (i.e., Algorithm 2) and generates the logistics information according to sender's and receiver's addresses in $Ciph_{Order}$. Second, based on the delivery path, the administrator formulates the position and attribute policies $(T_1, T_2, \ldots, T_n)$ and encrypts segments of logistics information using CP-ABE with related policies. Algorithm 3 shows the detailed encryption process of logistics information.

In line 1 of Algorithm 2, the administrator conducts $D(PRI_{Adm}, [Ciph_{Order}])$, where $D()$ is a public key decryption algorithm, and obtains Add_{Sen}, Add_{Rec}, ID_{Order}, HN, and $Ciph_{Section_2}$. Because address can be divided into three sections, street, city, and state, all address structures can be combined to form multiple tree structures. According to sender's and receiver's addresses, the administrator will generate an optimal path, as shown in Figure 4.

Obviously, the sender's address is different from receiver's address. In other words, the street $A_3 \neq B_3$. There are three types of paths according to addresses of sender and receiver. The parcel will be distributed according to the optimal path.

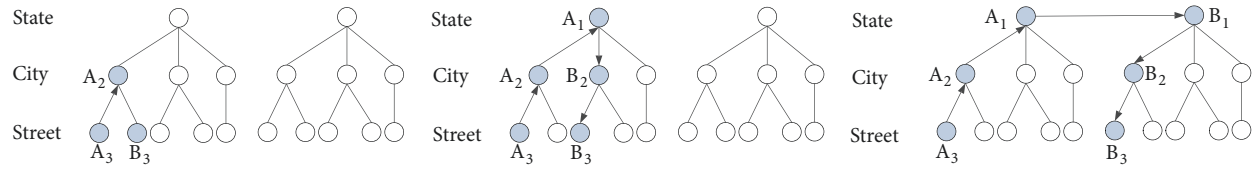

Figure 4: Delivery path.

So the number of delivery stations can be divided into three types:

(1) When $A_2 = B_2$, as shown in Figure 4(a), the optimal path is $A_3A_2B_3$, so there are three delivery stations on the optimal path.

(2) When $A_1 = B_1$ *and* $A_2 \neq B_2$, as shown in Figure 4(b), the optimal path is $A_3A_2A_1B_2B_3$, so there are five delivery stations on the optimal path.

(3) When $A_1 \neq B_1$, as shown in Figure 4(c), the optimal path is $A_3A_2A_1B_1B_2B_3$, so there are six delivery stations on the optimal path.

It is worth noting that, in real parcel delivery scenario, the numbers of delivery stations may be changed, such as wrong delivery or route change. The alternative solutions are as follows.

When the administrator has encrypted multiple paths and made the ciphertext into a QR code, the courier can decrypt multiple optional station addresses. He (or she) needs to choose a suitable station according to actual situation. When the existing optional paths are all unavailable, the administrator will encrypt a new path and send the new ciphertext to courier. If the parcel is wrongly transmitted, the solution is different. For example, the original path is $A_3A_2B_3$, as shown in Figure 4(a); the real path becomes $A_3A_2CB_3$. It means the courier at A_2 transmits the parcel to the wrong station C; at the same time, the courier at C cannot decrypt the logistics information. So he (or she) will return the parcel to station A_2. The courier at A_2 needs to tell the event to administrator. Then administrator will adjust the access policy of logistics information.

In lines 2-7 of Algorithm 3, the administrator predetermines the position attribute according to delivery stations on delivery path for couriers, where $attr(\mathcal{S})$ means the attribute $\mathcal{S}$'s value. Our scheme guarantees that the courier needs to arrive at the correct delivery position, so that he (or she) can obtain a secret key about the policy of position-based access control.

In lines 8-11 of Algorithm 3, the administrator divides the path into segments according to delivery station nodes and obtains segments $M_1, M_2, \ldots, M_n$. In lines 12-15 of Algorithm 3, the administrator, respectively, encrypts the segments $M_1, M_2, \ldots, M_n$ under CP-ABE. This method guarantees a fine-grained access control of encrypted logistics information. Besides, the position attribute $\mathcal{S}_{Spatial}$ is added to leaf nodes of access tree. So our scheme achieves a position-based access control.

After completing Algorithm 3, the administrator makes the ciphertext $CT_1, CT_2, \ldots, CT_n$ combined with ID_{Order}. At the same time, he (or she) sends encrypted PK and SK to couriers using his (or her) public key. When the sender drops off the parcel at local delivery station to courier, the courier can inquire about the ciphertext according to ID_{Order}. Then he (or she) makes the ciphertext into a QR code, which will be pasted on the parcel.

4.4. Retrieval. When the parcel arrives at the delivery station, the courier at this station scans QR code to get ciphertext CT_i and decrypts logistics information M_i; then he (or she) transmits the parcel to next station.

Before logistics information retrieval, the courier can decrypt and obtain PK and SK sent by administrator. In the retrieval phase, the courier who is located at a valid station at work time needs to run an improved position-based key exchange protocol to obtain the secret key about policy of position-based access control. In Algorithm 4, the courier performs the improved position-based key exchange (I-PBKE) with landmarks to obtain $\mathcal{S}_{Spatial}$, where $F(X_i, K_j)$ means the BSM PRG function.

In the previous position-based key exchange protocol (PBKE) [32], it assumes that landmarks must store $\{X_i\}$ in order to compute the expected response from courier. However, this position-based key exchange protocol is not suitable for realizing the position-based access control with ABE in our scheme. There are two reasons. First, X_i is a long string which is drawn from the landmark's reverse block entropy source. Thus the landmark's storage capacity needs to be large enough. What is more, the landmark generates X_i randomly along with the protocol execution. It means the final exchange key K_6 is determined by all landmarks after protocol execution, so that the administrator cannot prebuild access tree for couriers.

The improved position-based key exchange protocol is shown in Algorithm 4. The landmarks predetermine the keys $K_1, K_2, K_3, K_4, K_5, K_6$ that are to be used at every iteration of the application of the PRG. Now, the expected exchange key K_6 is known before protocol execution to all landmarks.

Obviously, there are two advantages of the improved position-based key exchange (I-PBKE) compared with the previous PBKE [32]:

(1) The expected exchange key K_6 is known by all landmarks before protocol execution. In other words, the position attribute's value is already determined, so the administrator can prebuild the access tree T which contains the position

1: Landmarks$\{L_1, L_2, L_3, L_4\}$ executes:
2: pick keys K_1,K_2,K_3,K_4,$K_5 \overset{R}{\leftarrow} \{0,1\}^m$
3: broadcast K_1,K_2,K_3,K_4,K_5 over their private channel.
4: At time $T - T_1$, L_1 picks large string X_4, computes $K_5' = F(X_4, K_4) \oplus K_5$, and broadcasts (X_4, K_1, K_5')
5: At time $T - T_2$, L_2 picks large string X_1,X_5, computes $K_2' = F(X_1, K_1) \oplus K_2$, $K_6' = F(X_5, K_5) \oplus K_6$, and broadcasts (X_1, X_5, K_2', K_6')
6: At time $T - T_3$, L_3 picks large string X_2, computes $K_3' = F(X_2, K_2) \oplus K_3$, and broadcasts (X_2, K_3')
7: At time $T - T_4$, L_4 picks large string X_3, computes $K_4' = F(X_3, K_3) \oplus K_4$, and broadcasts (X_3, K_4')
8: Courier executes:
9: At time T, the courier receives all of the strings
10: **for** $i = 1$; $i < 6$; $i++$ **do**
11: compute $K_{i+1} = F(X_i, K_i) \oplus K_{i+1}'$
12: end for
13: **return** exchange key K_6

Algorithm 4: Improved position-based key exchange.

Input: ciphertext CT_i
Output: logistics information M_i
1: Courier executes:
2: $K_{i6} \longleftarrow$ I-PBKE
3: $attr(\mathcal{S}_{Spatial}) \longleftarrow K_{i6}$
4: $CT_i = (T_i, \widetilde{C}_i, C_i)$
5: **if** $\mathcal{S}$ satisfies T_i **then**
6: $r \longleftarrow$ node of access tree T_i
7: $A \longleftarrow DecryptNode(CT_i, SK, r)$
8: $M_i \longleftarrow \widetilde{C}_i / (e(C_i, SK)/A)$
9: end if
10: **return** logistics information M_i

Algorithm 5: Logistics information retrieval.

attribute, instead of waiting for the courier's response when the parcel arrives at delivery station.

(2) The landmarks need not store long strings $\{X_i\}$.

In line 2 of Algorithm 5, the courier obtains the secret key K_6 according to Algorithm 4 (I-PBKE); thus the courier possesses suitable attribute set $\mathcal{S}$. Since the courier has got PK and SK sent by administrator and he (or she) satisfies the desired access tree T, the courier can retrieve required logistics information M_i, as shown in lines 5-9 of Algorithm 5. After decrypting the logistics information M_i, the courier will transmit parcel to next station. Multiple couriers collaborate to complete the express delivery process.

4.5. Reception. When the parcel arrives at last station, the final courier gets ciphertext CT_n; then he (or she) decrypts logistics information and transmits the parcel to target receiver.

Note that, in line 2 of Algorithm 6, the courier decrypts M_n according to Algorithm 5 (LIR). Specifically, the courier obtains the secret key about the position attribute, decrypts the ciphertext CT_n, and gets $Ciph_{Section_2}$ and HN.

When the receiver comes to pick up parcel, he (or she) should verify the correctness of order information on parcel and the courier should verify the authenticity of receiver. After mutual verification between courier and receiver, the receiver will get the parcel from courier successfully.

The details of reception of parcel are illustrated in Algorithm 6. Firstly, the receiver can get $E(PUB_{Rec}, [Section_2])$ from courier and decrypt it using his (or her) private key. Then the receiver obtains the following information: ID_{Order}, RN, $signature_{Sen}$, and personal information: Nam_{Sen}, Nam_{Rec}, Pho_{Sen}, and Pho_{Rec}. By verifying $signature_{Sen}$, he (or she) can confirm the integrity of parcel information. In addition, the receiver can compute $HN_1 = Hash(RN)$. By comparing the string HN_1 shown by receiver with the information HN which courier possesses, the courier can verify the validity of receiver. Then the receiver conducts $E(PUB_{Adm}, [ID_{Order} || RN])$ and sends it to administrator. The administrator can compute $HN_2 = Hash(RN)$ and check $HN_2 = HN$, in order to verify that the receiver has received the parcel.

5. Analysis of Scheme

In this section, we demonstrate that our scheme satisfies all the required properties.

5.1. Attribute-Based Access Control (ABAC). In our scheme, the logistics information is encrypted under CP-ABE. With

Input: ciphertext CT_n
Output: delivery result
1: courier executes:
2: $M_n \longleftarrow LIR(CT_n)$
3: $Ciph_{Section_2}||HN \longleftarrow M_n$
4: send $Ciph_{Section_2}$ to receiver
5: send $E(PUB_{Adm}, [HN])$ to administrator
6: receiver executes:
7: $Section_2 \longleftarrow D(PRI_{Rec}, [Ciph_{Section_2}])$
8: $HN_1 \longleftarrow Hash(RN)$
9: **if** $D(PUB_{Sen}, [signature_{Sen}]) = ID_{Order}||Plai_{Order}$ **then**
10: $Ciph_{FSC} \longleftarrow E(PUB_{Cou}, [ID_{Order}||HN_1])$
11: send $Ciph_{FSC}$ to courier
12: courier executes:
13: $ID_{Order}||HN_1 \longleftarrow D(PRI_{Cou}, [Ciph_{FSC}])$
14: **if** $HN_1 = HN$ **then**
15: receiver executes:
16: $Ciph_{FSA} \longleftarrow E(PUB_{Adm}, [ID_{Order}||RN])$
17: send $Ciph_{FSA}$ to administrator
18: administrator executes:
19: $ID_{Order}||RN \longleftarrow D(PRI_{Adm}, [Ciph_{FSA}])$
20: $HN \longleftarrow D(PRI_{Adm}, [E(PUB_{Adm}, [HN])])$
21: $HN_2 \longleftarrow Hash(RN)$
22: **if** $HN_2 = HN$ **then**
23: delivery result ⟵ Success
24: end if
25: **else**
26: delivery result ⟵ Receiver Wrong
27: end if
28: **else**
29: delivery result ⟵ Parcel Wrong
30: end if
31: **return** delivery result

Algorithm 6: Reception of parcel.

CP-ABE, the courier is specified with an attribute-based access policy for fine-grained access control of logistics address.

Specifically, the administrator selects attributes $\mathcal{S}$ and builds access tree T for couriers. The required logistics information M_i can only be decrypted by the valid courier whose attributes satisfy the access policy T_i. Different courier can only decrypt different segments of logistics information in accordance with their respective private keys, which correspond to different attributes sets $\{\mathcal{S}_i\}$ satisfying the access policy.

5.2. Position-Based Access Control (PBAC). Different from traditional cryptography, position-based cryptography uses the user's spatial position information as the only credential for user. In our scheme, the courier's position of valid delivery station at the expected work time is considered as one of the indispensable attributes. Specifically, the courier needs to obtain a secret key K_6 about position attribute $\mathcal{S}_{Spatial}$, so that he can continue the decryption process.

In addition, landmarks predetermine the keys K_6. It means that the expected value of position attribute is already known by all landmarks before protocol execution. Then the position attribute $\mathcal{S}_{Spatial}$ will be added to leaf nodes of access tree, so that the administrator can prebuild the access tree T.

5.3. Privacy-Preserving of Logistics Information (PPLI). In our scheme, besides sender and receiver, the whole delivery path is only known by administrator. The sender submits encrypted order information $Ciph_{Order}$ to administrator; then the administrator, respectively, encrypts the segmented logistics information $\{M_i\}$ under CP-ABE, as shown in Algorithm 3.

On the one hand, for general people who do not have the correct attributes, the only information they can get is ID_{Order}, which is used to uniquely identify the parcel. Apart from this, they cannot obtain anything about the plaintext of logistics information, i.e., Add_{Sen} and Add_{Rec}. On the other hand, the courier who actually moves parcel can only decrypt partial address information M_i according to attributes. M_i is the next delivery station address, which is necessary for the courier's delivery process.

5.4. Confidentiality of Personal Information(CPI). In initialization phase, customer's personal information which contains Nam_{Sen}, Nam_{Rec}, Pho_{Sen}, and Pho_{Rec} is encrypted by

receiver's public key PUB_{Rec}. In last phase, the parcel arrives at the final delivery station and the receiver obtains $Ciph_{Section_2}$ from the final courier and executes $D(PRI_{Rec}, [Ciph_{Section_2}])$, so that the receiver gets the personal information which is included in $Section_2$. In the whole parcel transit process, only the target receiver can decrypt the personal information. For other people including administrator and couriers, the probability of obtaining $Section_2$ is negligible even if they have $Ciph_{Section_2}$.

5.5. Verifiability of Receiver (VR). The courier can verify the correctness of receiver. In the phase of reception, the final courier can obtain HN using $LIR(CT_n)$. At the same time, the target receiver can get $Section_2$ using $D(PRI_{Rec}, [Ciph_{Section_2}])$, where RN is included in $Section_2$. Then the receiver computes $HN_1 = Hash(RN)$. By comparing the hash value HN_1 which receiver shows with HN, the courier can verify the correctness of receiver. For the adversary who wants to simulate the receiver, he (or she) must obtain RN. Because hash function is noninvertible and collision resistant and $Section_2$ cannot be decrypted without PRI_{Rec} which is kept secretly by receiver, the adversary has a negligible probability to obtain RN and HN. Consequently, our scheme can prevent forging identity by adversary to take away the parcel which does not belong to himself (or herself).

5.6. Verifiability of Parcel (VP). The digital signature guarantees the origin and integrity of parcel. The sender generates digital signature $signature_{Sen}$ by $E(PRI_{Sen}, [ID_{Order}||Plai_{Order}])$ and adds it into $Section_2$. Then $Section_2$ is encrypted using receiver's public key Pub_{Rec}. In the reception phase, the receiver can decrypt $Section_2$ and obtain $signature_{Sen}$. He (or she) can decrypt $E(PRI_{Sen}, [ID_{Order}||Plai_{Order}])$ using sender's public key and get $Plai_{Order}$, ID_{Order}. $Plai_{Order}$ contains receiver's personal information and address information, so that the receiver can confirm that the parcel is not forged. As a result, our scheme can prevent parcel forgery by malicious couriers during the express delivery process.

5.7. Anticollusion Attack to Attribute-Based Access Control (ACA-A). In the retrieval phase, the courier with appropriate attributes can only decrypt a segment M_i. However, couriers are so curious about other information that they may collude with others in order to enlarge their privileges. Our scheme ensures the courier only can decrypt the specific information according to his (or her) attributes.

For example, assuming that couriers C_1, C_2 have the attribute set $\mathcal{S}_1, \mathcal{S}_2$. Couriers C_1 and C_2 want to collude together. There is a courier C_3 who has the attribute set $\mathcal{S}_3$; let $\mathcal{S}_3 = S_1 \cup \mathcal{S}_2$. So C_1, C_2 want to obtain C_3's secret key and decrypt C_3's information. In our scheme, C_1 and C_2 must recover $e(g, g)^{\alpha s}$ in order to obtain C_3's secret key. In the phase of encryption, the string s from different couriers is randomized, so C_1 and C_2 cannot recover $e(g, g)^{\alpha s}$. It means C_3's ciphertext cannot be decrypted even if C_1 and C_2 collude. In other words, the collusion of multiple couriers is useless for decryption of addition logistics information.

5.8. Anticollusion Attack to Position-Based Access Control (ACA-P). The improved position-based key exchange (I-PBKE) which we propose is shown in Algorithm 4. It achieves that the colluding couriers who are not located at the valid station cannot obtain the logistics information. In other words, the position attribute's value K_6 cannot be distinguished with other random strings for colluding couriers.

Suppose there exists a set of malicious couriers. Let C_j be the malicious couriers between the honest courier at position P and landmarks $\{L_j \mid (1 \leq j \leq 4)\}$. At time T, C_1 can store$(K_1, K_5', A(X_4, K_1, K_5'))$, C_2 can store $(K_2', K_6', A(X_1, X_5, K_2', K_6'))$, C_3 can store $(K_3', A(X_2, K_3'))$, and C_4 can store $(K_4', A(X_3, K_4'))$, where $A(X_i, K_j)$ is any arbitrary adversarial algorithm.

After time T, the sequence of string reaching at adversary is different. Particularly, as for C_1, the string (X_1, X_5, K_2', K_6') first arrives and C_1 computes $K_2 = F(X_1, K_1) \oplus K_2'$. Later, the string (X_2, K_3') arrives and C_1 computes $K_3 = F(X_2, K_2) \oplus K_3'$. Finally, the string (X_3, K_4') arrives and C_1 computes $K_4 = F(X_3, K_3) \oplus K_4'$. Even if the malicious couriers collude together, according to properties of the ε-secure BSM PRG, the probability of the malicious couriers correctly guessing $K_5 = F(A(X_4), K_4) = F(X_4, K_4) \oplus K_5'$ is $\varepsilon + 2^{-\varphi}$, which is negligible in security parameter by choice of κ and r; thus $r \geq (2/\sigma)\kappa lb(n)$. So K_5 is still a random string to adversaries; thus they cannot find anything about K_6. Similarly, as for other possible reaching sequences, even if the malicious couriers collude together, they cannot find anything about final key K_6.

5.9. Undeniability (UD). Specifically, the sender cannot deny a parcel sent by himself (or herself), while the receiver cannot deny a parcel received by himself (or herself). In the step of initialization, the sender generates digital signature $signature_{Sen}$ which uses his (or her) private key PRI_{Sen} and then adds the signature $signature_{Sen}$ to $Section_2$. So, after decrypting $Section_2$, the receiver can confirm that the parcel was sent by sender. In the step of reception, when the receiver wants to take away the parcel, he (or she) should conduct $E(PUB_{Adm}, [ID_{Order}||RN])]$ and send it to administrator. Then the administrator can decrypt $E(PUB_{Adm}, [ID_{Order}||RN])]$ using Pri_{Adm}. At the same time, the administrator can receive HN sent by courier. By computing $HN_2 = Hash(RN)$ and checking $HN_2 = HN$, the administrator can verify that the receiver has received the parcel.

5.10. Unlinkability (UL). In the initialization phase, the sender's encrypted order information $Ciph_{Order}$ which contains Nam_{Sen}, Nam_{Rec}, Pho_{Sen}, Pho_{Rec}, Add_{Sen}, and Add_{Rec} and is transmitted to receiver. It is impossible for administrator and couriers to reveal the identity of customers from the encrypted order information.

As shown in Algorithm 1, a different random number RN is used in each generation of order ciphertext. $Section_2$ contains RN and $Section_1$ contains $HN(HN = Hash(RN))$, so each order information is different even if it is sent by the same sender. Since RN is random, the administrator and

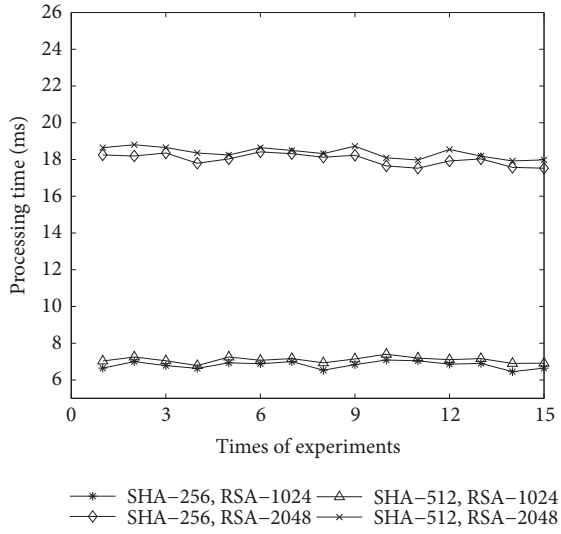

Figure 5: Computation overhead in initialization phase.

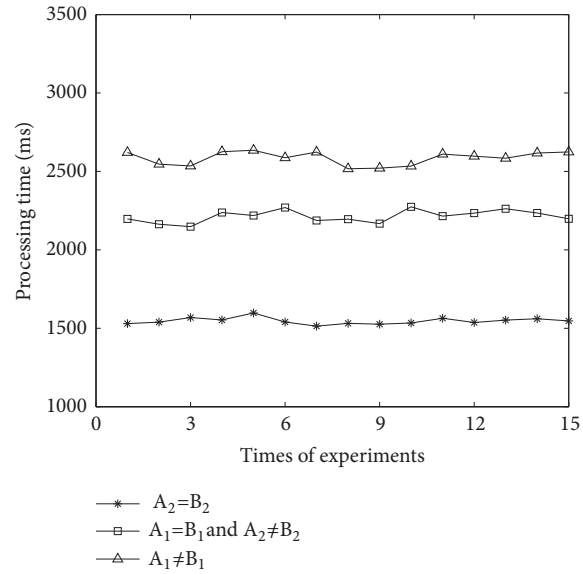

Figure 6: Computation overhead in encryption phase.

others are unable to tell whether these encrypted orders have the same logistics information (Add_{Sen}, Add_{Rec}) and personal information (Nam_{Sen}, Nam_{Rec}, Pho_{Sen}, and Pho_{Rec}). In other words, except customers, other people cannot distinguish whether the encrypted order information $Ciph_{Order}$ in many delivery processes originates from the same sender.

6. Performance Evaluation

In this section, we mainly focus on evaluation of computation overhead of our proposed scheme. The performance evaluation consists of four parts according to LIPPA, i.e., initialization, encryption, retrieval, and reception. The experiments are implemented on an Android phone (Band: Samsung Galaxy S7 Edge, CPU: Quad Core 2.15GHz, Operating System: Android 6.0, ROM:32G, RAM:4G). Our implementation is based on Java Pairing-Based Cryptography Library (JPBC).

Initialization. In the initialization phase, a sender wants to submit an encrypted order to administrator. Specifically, the sender needs to complete $Hash(RN)$, $E(PUB_{Rec}, [Section_2])$, $E(PUB_{Adm}, [Ciph_{Section_2}||Section_1])$, and $signature_{Sen}$. In Figure 5, we adopt hash function and RSA algorithm with different parameters to evaluate the sender's computation overhead. From Figure 5, we notice that the hash functions with different parameters lead to slightly different computation overhead. RSA algorithm with different parameters has greater impact on computational cost. When the hash function is SHA-512 and RSA algorithm is RSA-2048, the computation cost is still lower than 20ms. In general, the computation overhead of initialization is low for sender.

Encryption. In this phase, the computational cost of administrator mainly reflects on encryption of logistics information. In Figure 6, we compare the administrator's computation overhead under three types of delivery paths. The administrator, respectively, encrypts the segmented logistics information $M_1, M_2, \ldots, M_n$ (where $n = 3$ if $A_2 = B_2$; $n = 5$ if $A_2 \neq B_2$ and $A_1 = B_1$; $n = 6$ if $A_1 \neq B_1$) under CP-ABE. We set that the number of attributes in private key is fixed to 10, the number of leaf nodes in policy is fixed to 5, and the size of logistics information is 4kB. As shown in Figure 6, the processing time almost is between 1.5s and 2.6s. The computation overhead of encryption is efficient for administrator in practice.

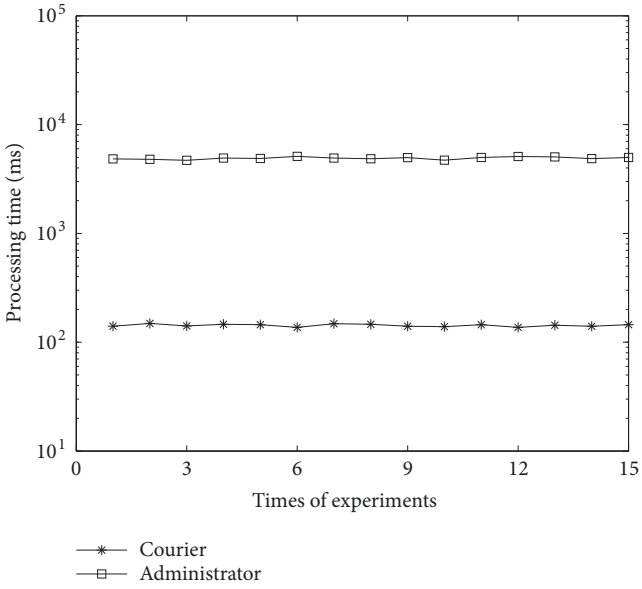

Figure 7: Computation overhead in retrieval phase.

Retrieval. In this phase, the courier and administrator collaborate to complete the retrieval. As shown in Figure 7, we evaluate the calculation costs of the administrator and the

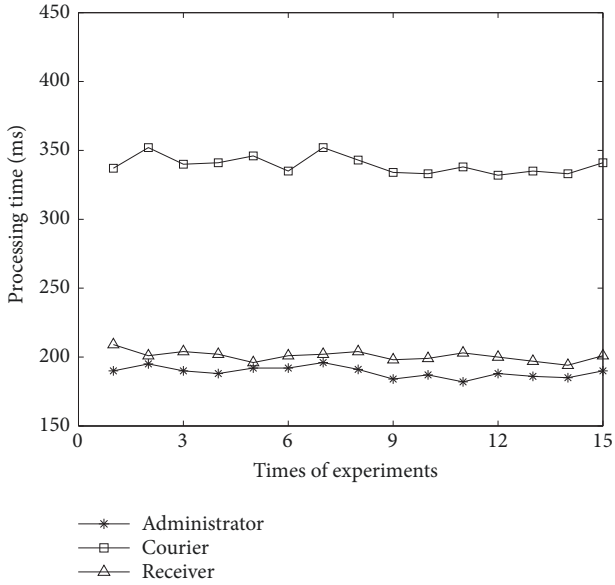

Figure 8: Computation overhead in reception phase.

courier, respectively. For courier, he (or she) needs to run I-PBKE to obtain K_6. Besides, the courier would decrypt the logistics information M_i. As a result, the computation overhead of courier consists of six $F(X_i, K_j)$ operations and one CP-ABE decryption operation. For administrator, he (or she) can employ landmarks to complete I-PBKE. At this protocol, landmarks need to generate five random large strings $\{X_i\}$. From Figure 7, we can see that the courier's computation overhead is far less than administrator's computation overhead.

Reception. In the reception phase, the courier delivers the parcel to receiver with the help of administrator. They use public key encryption and hash function specifically. We adopt SHA-256 and RSA-1024 to evaluate the computation overhead of administrator, courier, and receiver, respectively. As illustrated in Figure 8, the computation costs of administrator and receiver are all about 200ms. As for courier, he (or she) needs to complete extra decryption of logistics information. As a result, the courier's computation overhead is higher. In general, their computation overhead is all acceptable for real parcel delivery process.

In general, our scheme is efficient and feasible in practice. What is more, our scheme satisfies all the security requirements of LIoT. So the LIP-PA is available for mobile devices in real parcel delivery scenario.

7. Conclusions

In this paper, we propose LIP-PA, a logistics information privacy protection scheme with position and attribute-based access control on mobile devices. Different from existing schemes, our scheme provides privacy protection for both personal information and logistics information. In our scheme, customers could achieve verifiability and undeniability. The administrator could encrypt the logistics information based on the policy of position and attribute-based access control. In order to transmit the parcel to next station, couriers could only decrypt the required segment of logistics information but not all the logistics information. As a further contribution, we prove that our scheme can satisfy all the security requirements and show that it is available for mobile devices in practice based on the experiment results.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was funded by National Natural Science Foundation of China (61472310, U1536202, U1405255, 61672413, 61672415, 61671360, 61602360, and 61702404) and China 111 Project (Grant B16037).

References

[1] L. D. Xu, W. He, and S. Li, "Internet of things in industries: a survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[2] C. Sun, "Application of RFID technology for logistics on internet of things," *AASRI Procedia*, vol. 1, pp. 106–111, 2012.

[3] L. Tarjan, I. Šenk, S. Tegeltija, S. Stankovski, and G. Ostojic, "A readability analysis for QR code application in a traceability system," *Computers and Electronics in Agriculture*, vol. 109, pp. 1–11, 2014.

[4] L. Ye, Y. Wang, and J. Chen, "Research on the intelligent warehouse management system based on near field communication (NFC) technology," *International Journal of Advanced Pervasive and Ubiquitous Computing*, vol. 8, no. 2, pp. 38–55, 2016.

[5] A. Orsino, A. Ometov, G. Fodor et al., "Effects of heterogeneous mobility on D2D- and drone-assisted mission-critical MTC in 5G," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 79–87, 2017.

[6] D. Wang, H. Cheng, D. He, and P. Wang, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," *IEEE Systems Journal*, vol. 12, no. 1, pp. 916–925, 2018.

[7] Y. Zhang, M. Yang, G. Gu, and H. Chen, "Rethinking permission enforcement mechanism on mobile systems," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2227–2240, 2016.

[8] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "IPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1005–1016, 2017.

[9] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things," *IEEE Internet of Things Journal*, pp. 1-1, 2017.

[10] Q. Wei, C. Wang, and X. Li, "Express information privacy protection application based on RSA," *Application of Electronic Technique*, vol. 40, no. 7, pp. 58–60, 2014.

[11] W. Hu, Q. Wu, and C. Gu, "Scheme design of logistic personal information privacy protection based on QR code," *Communications Technology*, vol. 50, no. 9, pp. 2074–2079, 2017.

[12] D. He, M. Ma, S. Zeadall, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial internet of things," *IEEE Transactions on Industrial Informatics*, 2017.

[13] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2402–2415, 2017.

[14] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2052–2064, 2016.

[15] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipfs law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[16] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: an underestimated threat," in *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS '16)*, pp. 1242–1254, October 2016.

[17] D. He, N. Kumar, M. K. Khan, and J.-H. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks," *IEEE Transactions on Consumer Electronics*, vol. 59, no. 4, pp. 811–817, 2013.

[18] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2015.

[19] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 1-1, 2016.

[20] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, 2017.

[21] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912–925, 2018.

[22] Q. Wei and L. I. Xing-Yi, "Express information protection application based on K-anonymity," *Application Research of Computers*, vol. 31, no. 2, pp. 555–567, 2014.

[23] X. Zhang, H. Li, Y. Yang, G. Sun, and G. Chen, "LIPPS: logistics information privacy protection system based on encrypted QR code," in *Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 996–1000, Tianjin, China, August 2016.

[24] H. Qi, D. Chenjie, Y. Yingbiao, and L. Lei, "A new express management system based on encrypted QR code," in *Proceedings of the 2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, pp. 53–56, Nanchang, China, June 2015.

[25] T. Li, R. Zhang, and Y. Zhang, "PriExpress: privacy-preserving express delivery with fine-grained attribute-based access control," in *Proceedings of the 2016 IEEE Conference on Communications and Network Security, CNS 2016*, pp. 333–341, USA, October 2016.

[26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, May 2007.

[27] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Computers and Electrical Engineering*, vol. 63, pp. 182–195, 2017.

[28] J. Shen, D. Liu, M. Z. Bhuiyan, J. Shen, X. Sun, and A. Castiglione, "Secure verifiable database supporting efficient dynamic operations in cloud computing," *IEEE Transactions on Emerging Topics in Computing*, pp. 1-1, 2017.

[29] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2016.

[30] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[31] J. Zhang, J. Ma, C. Yang, and L. Yang, "Universally composable secure positioning in the bounded retrieval model," *Science China Information Sciences*, vol. 58, no. 11, pp. 1–15, 2015.

[32] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," in *Advances in cryptology—CRYPTO 2009*, vol. 5677 of *Lecture Notes in Comput. Sci.*, pp. 391–407, Springer, Berlin, 2009.

[33] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, and J. Ma, "Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems," *Journal of Ambient Intelligence and Humanized Computing*, no. 5, pp. 1–13, 2017.

[34] K. Jia, X. Chen, and G. Xu, "The improved public key encryption algorithm of kerberos protocol based on braid groups," in *Proceedings of the 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, pp. 1–4, Dalian, China, October 2008.

[35] J. Zhang, J. Ma, and S. Moon, "Universally composable one-time signature and broadcast authentication," *Science China Information Sciences*, vol. 53, no. 3, pp. 567–580, 2010.

[36] X. Dong, H. Qian, and Z. Cao, "Provably secure RSA-type signature based on conic curve," *Wireless Communications and Mobile Computing*, vol. 9, no. 2, pp. 217–225, 2009.

[37] W.-B. Hsieh and J.-S. Leu, "A dynamic identity user authentication scheme in wireless sensor networks," in *Proceedings of the 2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, pp. 1132–1137, Italy, July 2013.